AKADEMIA E FORCAVE TË ARMATOSURA
INSTITUTI KËRKIMOR SHKENCOR USHTARAK
REVISTË TEORIKO-SHKENCORE
MARS 2026

REVISTA
USHTARAKE
(edicioni i parë)

Botim i Akademisë së Forcave të Armatosura
Miratuar me vendim nr. 1 datë 10.03.2026
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 2026

EDITORIAL

Të nderuar lexues të “Revista Ushtarake”,

Edicioni i parë i këtij viti botohet në një moment të veçantë për sigurinë ndërkombëtare. Zhvillimet e viteve të fundit tregojnë se mjedisi global po kalon një fazë transformimi të thellë gjeostrategjik. Konflikti në Ukrainë, tensionet në Lindjen e Mesme dhe konkurrenca në rritje mes fuqive të mëdha kanë rikthyer në qendër të vëmendjes çështjet e fuqisë ushtarake, të ekuilibrave strategjikë dhe të rolit të aleancave në ruajtjen e stabilitetit ndërkombëtar.

Rendi ndërkombëtar i ndërtuar pas përfundimit të Luftës së Ftohtë po përballet me sfida të reja strukturore. Në këtë realitet gjithnjë e më kompleks dhe të paparashikueshëm, shtetet dhe aleancat duhet të përshtatin konceptet e tyre strategjike, kapacitetet mbrojtëse dhe mekanizmat e bashkëpunimit. Për vendet anëtare të NATO-s, përfshirë Shqipërinë, kjo nënkupton forcimin e ndërveprueshmërisë, rritjen e kapaciteteve të mbrojtjes dhe investimin e vazhdueshëm në dije, teknologji dhe kapital njerëzor.

Në këtë kontekst, Revista Ushtarake synon të kontribuojë në zhvillimin e mendimit strategjik dhe në nxitjen e debatit profesional brenda komunitetit të sigurisë dhe mbrojtjes.

Ky edicion është strukturuar në tre rubrika kryesore.

Rubrika e parë, trajton zhvillimet në mjedisin bashkëkohor të sigurisë, duke analizuar çështje të lidhura me shkurajimin, transformimin e doktrinave ushtarake dhe evolucionin e konflikteve moderne. Në një rajon si Ballkani Perëndimor, ku stabiliteti lidhet ngushtë me zhvillimet në arkitekturën euroatlantike të sigurisë, analiza strategjike dhe bashkëpunimi me aleatët mbeten faktorë thelbësorë për ruajtjen e paqes dhe sigurisë.

Rubrika e dytë, fokusohet në dimensionin teknologjik të mbrojtjes. Përshpejtimi i inovacionit, zhvillimet në inteligjencën artificiale, sigurinë kibernetike dhe teknologjitë e komunikimit po ndikojnë drejtpërdrejt në mënyrën se si konceptohen dhe zhvillohen operacionet ushtarake. Teknologjia po bëhet gjithnjë e më shumë një element përcaktues në balancën strategjike globale.

Rubrika e tretë, i kushtohet arsimit profesional ushtarak dhe zhvillimit të lidershipit. Në një mjedis gjithnjë e më kompleks, përgatitja e oficerëve kërkon jo vetëm aftësi profesionale dhe teknike, por edhe mendim kritik, integritet dhe vizion strategjik. Operacionet me shumë fusha dhe integrimi i dimensioneve tokësore, ajrore, detare, hapësinore dhe kibernetike kërkojnë një brez të ri liderësh ushtarakë të aftë për të operuar në realitete të reja strategjike.

Revista jonë mbetet një platformë akademike dhe profesionale për reflektim dhe analizë mbi çështjet e sigurisë dhe mbrojtjes. Në një kohë kur kufijtë mes luftës dhe paqes, konvencionales dhe asimetrikes, hibrides, fizikes dhe digjitales po bëhen gjithnjë e më të ndërthurur, kërkimi shkencor dhe mendimi strategjik janë më të rëndësishëm se kurrë.

Mirëpresim kontributet tuaja në edicionet e ardhshme të revistës.

Ju uroj lexim të mbarë dhe reflektim të frytshëm.

Drejtori i IKSHU

Mars 2026

PËRMBAJTJA E REVISTËS USHTARAKE

RUBRIKA E PARË

Siguria dhe mbrojtja në mjedisin bashkëkohor: analiza dhe vlerësime

RUBRIKA E TRETË

Arsimimi ushtarak, lidershipi dhe zhvillimi profesional

RUBRIKA E PARË

SIGURIA DHE MBROJTJA NË MJEDISIN BASHKËKOHOR: ANALIZA DHE VLERËSIME

Shkurajimi dhe mbrojtja funksionale në epokën e sfidave gjeopolitike në zhvillim: rasti i Ballkanit Perëndimor dhe Shqipërisë

Kolonel (R) Msc. Agim SHAHU
Shtabi i Përgjithshëm i Forcave të Armatosura

Trajtesë e shkurtuar

Ballkani Perëndimor mbetet një hapësirë kyçe e sigurisë evropiane, ku tensionet e pazgjidhura, brishtësia institucionale dhe konkurrenca gjeopolitike ndërthuren me kërcënime hibride dhe presion të vazhdueshëm. Kjo temë studimore argumenton se, pas vitit 2022, siguria nuk matet vetëm me numrin e trupave ose me kontrollin territorial, por me aftësinë e shtetit për të funksionuar nën presion: të marrë vendime të shpejta, të ruajë shërbimet jetike, të mbrojë infrastrukturën kritike, të menaxhojë incidentet dhe të koordinojë institucionet pa humbur ritmin operacional.

Në këtë kuptim, shkurajimi (parandalimi) funksional ndërtohet përmes gatishmërisë, ndërveprueshmërisë, vazhdimësisë operacionale, mbrojtjes kibernetike dhe komunikimit publik të disiplinuar, duke integruar rezervën dhe mbrojtjen civile. Përmes analizës dokumentare, rasteve studimore, punimi nxjerr mësime të vlefshme për Shqipërinë si anëtare e NATO-s dhe propozon masa praktike që e shndërrojnë shkurajimin nga deklaratë në aftësi reale.

Fjalë kyçe: Ballkani Perëndimor; shkurajim funksional; NATO; kërcënime hibride; mjedis i sigurisë; mbrojtje civile; forca rezervë; vazhdimësi operacionale.

Hyrje

Çfarë e bën një rajon realisht të sigurt në shekullin XXI? A janë numrat, buxhetet platformat teknologjike, apo është aftësia për të ruajtur funksionimin e shtetit nën presion? Në një mjedis ku krizat shpërthejnë pa paralajmërim dhe ku incidentet mund të përshkallëzohen brenda orësh, matjet tradicionale të sigurisë janë të pamjaftueshme. Në Ballkanin Perëndimor,

presioni shfaqet si kombinim i ndikimit informativ, ndërhyrjeve kibernetike, provokimeve të kontrolluara, presioneve ekonomike dhe instrumenteve të ndikimit që synojnë të lodhin vendimmarrjen.

Pas vitit 2022, rikthimi i luftës në kontinent dhe intensifikimi i konkurrencës gjeopolitike e kanë zhvendosur diskutimin e sigurisë nga menaxhimi i pasojave drejt logjikës së gatishmërisë dhe parandalimit. Në këtë realitet, parandalimi nuk është thjesht deklaratë politike; është aftësi e provuar për të vepruar herët, për të ruajtur funksionet jetike dhe për të mos lejuar që incidentet të kthehen në krizë.[1]

Qëllimi i këtij punimi është të ndërtojë një kornizë analitike mbi shkurajimin funksional dhe ta vendosë Shqipërinë në kontekstin rajonal si anëtare e NATO-s: jo si pretendim për fuqi të pavarur ushtarake, por si faktor besueshmërie dhe standardesh të provuara. Në fokus janë: (a) ndryshimi i natyrës së presionit pas vitit 2022; (b) roli i bashkëpunimit rajonal; (c) ndikimi i aktorëve të jashtëm; (d) integrimi i Forcave të Armatosura, rezervave dhe mbrojtjes civile.[2]

Metodologjia dhe qasja analitike

Në zhvillimin e temës është përdorur një qasje cilësore e kombinuar, e cila përfshin analizën e dokumenteve strategjike dhe doktrinare euroatlantike, si dhe analizën krahasuese të praktikave të vendeve partnere. Qëllimi është ndërtimi e një kornize të qartë për shkurajimin funksional si aftësi për funksionim e shtetit nën presione të ndryshme hibride.[3]

Në planin empirik, përdoren dy raste studimore me vlerë shpjeguese. Banjska (2023) trajtohet si shembull i një incidenti që teston vendimmarrjen dhe kohezionin institucional të një shteti sovran përballë grupeve të armatosura. Ukraina (2022) analizohet si rast i përshtatjes së shpejtë dhe i funksionimit të shtetit nën presion të zgjatur, duke nxjerrë parime të transferueshme për vende me burime më të kufizuara.[4]

Analiza organizohet sipas logjikës: çfarë u testua, çfarë funksionoi dhe çfarë mësimi del për Shqipërinë dhe Ballkanin Perëndimor. Për të shmangur përgjithësime të pajustifikuara, rasti i Ukrainës përdoret si burim mësimesh parimore (ritëm i vendimmarrjes, standardizimi i procedurave, vazhdimësia e shërbimeve jetike), jo si model që kopjohet mekanikisht. Gjithashtu, punimi respekton parimin e mosdhënies së detajeve operacionale që mund të cenojnë sigurinë; argumentet fokusohen te standardet, proceset dhe treguesit e funksionimit. Në analizën kritike, përdoret edhe parimi i "*triangulimit"*: pohimet kyçe mbështeten në burime të pavarura dhe në konsistencën e tyre logjike. Kjo e ul rrezikun e konkluzioneve të nxituara dhe forcon lidhjen

[1] NATO 2022 Strategic Concept (Madrid: NATO, 2022).
[2] Strategjia e Sigurisë Kombëtare 2023–2028 (2023/2024).
[3] U.S. Department of Defense, Joint Publication 3-0: (Washington, DC: DOD, 2022).
[4] Department of the Army, FM 3-0: Operations (DC: Department of the Army, 2022).

ndërmjet argumentit, anës dokumentare dhe rekomandimeve.[5]

Korniza konceptuale: shkurajimi e mbrojtja funksionale

Shkurajimi funksional nënkupton aftësinë e shtetit për të ruajtur funksionet jetike nën presion të vazhdueshëm dhe të shpërndarë, duke e bërë të pasuksesshme logjikën e destabilizimit gradual. Ai nuk zëvendëson shkurajimin ushtarak klasik, por e plotëson atë në mjedise ku presioni është kryesisht jokinetik dhe ku synohet bllokimi i vendimmarrjes, çarja e kohezionit shoqëror dhe kompromet imi i shërbimeve kritike.[6] Në termat e sigurisë praktike, funksionimi është vetë mesazhi parandalues. Një shtet që vendos shpejt, mbron infrastrukturën kritike, mban vazhdimësinë e shërbimeve jetike dhe komunikon qartë, i rrit kundërshtarit koston e destabilizimit. Për këtë arsye, shkurajimi funksional kërkon disiplinë procedurale, stërvitje të rregullt në skenarë presioni nën prag dhe një mekanizëm të përhershëm mësimi institucional. Ky koncept lidhet ngushtë me idenë e gjithëpërfshirjes, kombëtare: jo si slogan, por si rregull funksionimi që lidh qeverisjen, sigurinë, ekonominë, infrastrukturën dhe komunikimin publik në një ritëm të përbashkët. Kur kjo lidhje mungon, presioni i fragmentuar arrin të prodhojë efekt strategjik pa përdorur forcë të hapur.

Përkufizime operative. Për të shmangur paqartësi konceptuale, përdoren këto përkufizime operative:

Presion nën prag: veprime të qëllimshme që synojnë ndikim strategjik pa provokuar konflikt të hapur.

Kërcënime hibride: kombinim instrumentesh informative, kibernetike, ekonomike, politike dhe të sigurisë.

Vazhdimësi operacionale: aftësi për të ruajtur funksione e shërbime edhe gjatë ndërprerjeve. Ndërveprueshmëri: standarde dhe procedura që lejojnë veprim të sinkronizuar ndërinstitucional rajonal edhe me aleatët.

Pyetje studimore dhe hipotezë pune: Punimi udhëhiqet nga tri pyetje kryesore:

(1) Si ka ndryshuar natyra e presionit ndaj Ballkanit Perëndimor pas vitit 2022 dhe çfarë nënkupton kjo për matjen e sigurisë?

(2) Si realizohet shkurajimi funksional në praktikë përmes mekanizmave institucionale, rezervës dhe mbrojtjes civile?

(3) Cili është roli i Shqipërisë si anëtare e NATO-s në rritjen e parashikueshmërisë dhe stabilitetit rajonal?

Hipoteza e punës: Stabiliteti rajonal varet më shumë nga aftësia për funksionim institucional nën presion sesa nga kapacitetet e deklaruara në paqe. Shkurajimi rritet kur sistemi provon se vendos shpejt, ruan shërbimet jetike, mbron infrastrukturën kritike dhe menaxhon incidentet pa u paralizuar.

[5] UK Ministry of Defence, UK Defence Doctrine (JDP 0–01) (London: MOD, 2020).
[6] NATO 2022 Strategic Concept (Madrid: NATO, 2022).

Mjedisi i sigurisë në Ballkanin Perëndimor pas vitit 2022

Në rajon, presioni nuk shfaqet gjithmonë si kërcënim i drejtpërdrejtë ushtarak. Më shpesh ai paraqitet si garë për ndikim politik, informativ, ekonomik dhe teknologjik. Kjo e kthen Ballkanin Perëndimor në një mjedis sigurie të brishtë, ku aktorë shtetërorë dhe joshtetërorë testojnë kufijtë e vendimmarrjes së brendshme, ndërsa rreziku matet me shpejtësinë me të cilën mund të bllokohen funksionet thelbësore të shtetit.[7]

Heterogjeniteti rajonal e rrit pasigurinë: disa vende janë nën ombrellën e mbrojtjes kolektive, të tjera jo; disa kanë qartësi strategjike, ndërsa të tjera mbajnë neutralitet strategjik të paqartë. Kjo krijon boshllëqe në koordinim, në ritmin e reagimit dhe në standardet e sigurisë. Në një mjedis ku incidentet mund të përshkallëzohen shpejt, siguria prodhohet nga procedura të përbashkëta dhe koordinim i testuar, jo thjesht nga reagime të rastit[8].

Në një mjedis të brishtë rritet rreziku i vlerësimit të gabuar: një incident i kufizuar mund të interpretohet si sinjal strategjik, ndërsa një sinjal mbrojtës mund të lexohet si provokim. Kjo ndodh sidomos kur mungon tabloja e përbashkët e situatës, kur komunikimi publik nuk është i unifikuar dhe kurkur vendimmarrja vonohet. Prandaj, parashikueshmëria institucionale, komunikimii disiplinuar dhe koordinimi i shpejtë ndërinstitucional ulin rrezikun e përshkallëzimit dhe rrisin besueshmërinë parandaluese. Cenueshmëria prodhohet nga tre mekanizma që ndërveprojnë:

1. Tensionet e pazgjidhura krijojnë hapësirë për provokime.
2. Polarizimi dhe mosbesimi institucional e bëjnë manipulimin informativ më të lehtë.
3. Boshllëqet në standardizim dhe koordinim rrisin kohën e reagimit.

Për rrjedhojë, shkurajimi funksional kërkon rregullim sistemi: procedura të standardizuara, ritëm të qëndrueshëm, disiplinë vendimmarrjeje dhe bashkërendim të testuar. Në vend të një matjeje të ngurtë me parametra të vetëm, siguria e mjedisit duhet të vlerësohet me tregues funksionalë:

- koha e reagimit institucional,
- cilësia e koordinimit dhe qëndrueshmëria e shërbimeve kritike,
- aftësia për komunikim publik koherent,
- kapacitetet për rikthim të shpejtë pas ndërprerjeve.

Këta tregues janë të rëndësishëm sepse përkthehen drejtpërdrejt në kosto

[7] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Framework on Countering Hybrid Threats* (JOIN (2016) 18 final) (Brussels, 2016).

[8] European Commission and European External Action Service (EEAS), *Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* (JOIN (2018) 16 final) (Brussels, 2018).

për kundërshtarin[9].

Bashkëpunimi rajonal si platformë shkurajimi dhe mbrojtje funksionale

Bashkëpunimi rajonal prodhon shkurajim dhe mbrojtje funksionale vetëm kur kthehet në mekanizma ndërshtetërorë dhe shtetërorë që funksionojnë në kohë reale. Deklaratat politike kanë vlerë simbolike, por efekti parandalues rritet kur standardet, protokollet dhe stërvitjet e përbashkëta krijojnë ritëm të njëjtë reagimi dhe një mënyrë të përbashkët funksionimi në kohe krizash.

Në planin praktik, bashkëpunimi bëhet i dobishëm kur përmirëson tre fusha:

- tablonë e përbashkët të situatës,
- harmonizimin e procedurave për menaxhim e incidenteve dhe emergjencave,
- rutinën stërvitore rajonale që teston vendimmarrjen nën presion hibrid.

Sa më i përbashkët të jetë ritmi, aq më e vogël është hapësira që presioni gradual të prodhojë efekte strategjike. Në ketë kontekst, standardizimi nuk është formalitet; ai redukton kohën e reagimit, ul keqkuptimet dhe rrit cilësinëe koordinimit në situata krize. Mësimi i përbashkët, i institucionalizuar përmes stërvitjeve të përbashkëta, e bën parandalimin më të besueshëm se çdo deklaratë të veçuar.[10]

Ndërveprueshmëria si efekt parandalues. Ndërveprueshmëria ka vlerë parandalimi sepse e bën të besueshme aftësinë për veprim të sinkronizuar: jo vetëm brenda një vendi, por edhe me aleatët rajonale dhe ndërkombëtarë. Në rajon, kjo nënkupton protokolle të përbashkëta për shkëmbim informacioni, format të unifikuar për raportimin e incidenteve dhe stërvitjeve që prodhojnë tablonë e përbashkët të situatës. Sa më shpejt të qarkullojë dhe merret informacioni, aq më pak hapësirë ka presioni për të prodhuar konfuzion.

Në këtë temë studimore, shkurajimi funksional kuptohet si aftësia e shtetit dhe institucioneve të sigurisë për të penguar ose dekurajuar veprime armiqësore jo vetëm përmes kërcënimit ushtarak, por përmes kombinimit të kapaciteteve ushtarake, institucionale, ligjore, informative dhe kibernetike, të cilat e bëjnë koston e agresionit më të lartë se përfitimi i mundshëm.

Shqipëria si faktor stabiliteti rajonal brenda NATO-s

Roli i Shqipërisë duhet vlerësuar si funksion i besueshmërisë dhe koherencës strategjike. Si anëtare e NATO-s, Shqipëria e ka rritur peshën e saj me aftësinë për të vepruar me standarde të njëjta, me procedura të testuara dhe me komunikim institucional të unifikuar. Kjo besueshmëri përkthehet në

[9] Council of the European Union, *A Strategic Compass for Security and Defence* (Brussels: Council of the European Union, 2022).

[10] NATO, "Warsaw Summit Communiqué," July 9, 2016.

kapacitete për bashkërendim të brendshëm dhe ndërveprim të jashtëm. Në kohë presioni, faktor stabiliteti është ai që mban ritmin institucional, ruan funksionimin e shërbimeve kritike dhe e artikulon qartë orientimin euroatlantik pa krijuar ambiguitet. Në rajon, kjo krijon parashikueshmëri dhe ul hapësirën për vlerësime apo veprime të gabuara.

Në mjedisin e sotëm të sigurisë, parandalimi matet me funksionimin e sistemit në kohë reale: 24 orët e para, 72 orët e para dhe java e parë. Aftësia për aktivizim e vendimmarrje të shpejtë, mbrojtja e shërbimeve jetike dhe vazhdimësia operacionale janë treguesit që e ndajnë reagimin e thjeshtë nga një masë shkurajuese e besueshme.

Rezerva dhe mbrojtja civile si shtylla të këtij reagimi: Përbën një element vendimtar i shkurajimit funksional. Ajo nuk duhet konceptuar si listë emrash, por si struktura kapacitetesh që aktivizohen shpejt dhe që mbyllin boshllëqet kritike kur kriza zgjatet. Kjo kërkon role funksionale, stërvitje periodike dhe certifikim të specialiteteve kritike.[11] Në të njëjtën logjikë, mbrojtja civile duhet parë si komponent i sigurisë, sepse vazhdimësia e shërbimeve jetike (energji, ujë, shëndetësi, transport, komunikime) është pjesë e parandalimit. Kur këto shërbime mbrohen dhe rikthehen shpejt, presioni i jashtëm humb efektin e lodhjes strategjike.[12]

Kërcënimet hibride

Kërcënimet e sotme shpesh nuk kanë formën e një agresioni konvencional. Ato shfaqen si presion i vazhdueshëm: dezinformim, ndërhyrje kibernetike, ndikim ekonomik, kapje e dobësive të qeverisjes dhe forma të ndikimit mbi opinionin publik nëpërmjet rrjeteve sociale. Qëllimi është të dobësohet besimi në institucione dhe të konsumohet vendimmarrja përmes krizave të shpeshta e të fragmentuara. Në këto kushte, parandalimi kërkon disiplinë ligjore, mbrojtje të infrastrukturës kritike, kundërveprim informativ dhe rritje të kapaciteteve të sigurisë kibernetike. Një shtet që aktivizon mekanizmat herët dhe ruan kohezionin e vendimmarrjes, ia mohon kundërshtarit suksesin e destabilizimit gradual. Siguria kibernetike dhe komunikimi i qartë publik janë pjesë e sigurisë kombëtare, sepse ndërprerja e shërbimeve jetike ose një fushatë e suksesshme dezinformimi mund të dobësojë vendimmarrjen po aq sa një krizë fizike. Prandaj, synimi është kalimi nga reagimi pas incidentit te parandalimi: koordinim ndërinstitucional, mbrojtje e infrastrukturës kritike, ngritje e ndërgjegjësimit të opinionit publik dhe procedura të gatshme për komunikim gjatë krizave.[13]

Infrastruktura kritike është objektiv parësor për presion nën prag, sepse

[11] RAND Corporation, Building Effective Reserve Forces (Santa Monica, CA: RAND, 2019).
[12] United Nations Office for Disaster Risk Reduction (UNDRR), 2015–2030 (Geneva: UNDRR, 2015).
[13] European Parliament and Council of the European Union, Directive (EU) 2022/2555 (NIS2) (Official Journal of the European Union, 2022).

goditja e saj sjell efekt të menjëhershëm mbi shoqërinë dhe vendimmarrjen. Mbrojtja e saj kërkon:

- plane të detajuara dhe sinkronizuara rezervë,
- stërvitje ndërinstitucionale për rikthim të shpejtë,
- protokolle komunikimi me publikun që ulin panikun dhe dezinformimin.

Suksesi matet me rikthimin e shërbimit brenda standardit të përcaktuar dhe ruajtjen e besimit publik.[14] Presioni hibrid arrin sukses kur prodhon dy rezultate: paqartësi strategjike dhe lodhje institucionale. Kjo ndodh kur reagimi është i vonuar, i fragmentuar dhe i pa unifikuar. Prandaj, shkurajimi funksional duhet të shohë përtej incidentit: të pyesë se cilin funksion po synon kundërshtari të bllokojë, cilën varësi po shfrytëzon dhe cili është momenti kritik ku një incident kthehet në krizë. Ky mentalitet analitik është po aq i rëndësishëm sa pajisjet apo sistemet.[15]

Rast studimor: Banjska (2023) dhe testimi i shkurajimit funksional

Incidenti i Banjskës (24 shtator 2023) tregoi se si një veprim i organizuar mund të testojë koherencën e vendimmarrjes dhe aftësinë e reagimit institucional. Në një mjedis rajonal e të sigurisë së brishtë, ngjarje të tilla synojnë jo vetëm efektin fizik, por edhe ndikimin psikologjik e politik, duke krijuar paqartësi dhe duke testuar kufijtë e reagimit.[16] Nga këndvështrimi i shkurajimit funksional, mësimi kryesor është se suksesi nuk matet vetëm me neutralizimin taktik, por me ruajtjen e ritmit institucional. Reagimi i institucioneve të sigurisë së qeverisë së Kosovës ishte i shpejtë, i koordinuar dhe i ligjshëm; komunikimi publik ishte i qartë dhe i kontrolluar; ndërsa ndërveprimi me partnerët dhe KFOR u aktivizua me shpejtësi dhe funksionoi për të dënuar ngjarjen dhe ulur rrezikun e përshkallëzimit.

Rasti thekson edhe dimensionin juridik dhe ndërkufitar: kur autorët ose mbështetësit mbeten jashtë juridiksionit, rreziku i ripërtëritjes ulet përmes rritjes së kostos së destabilizimit përmes hetimit të plotë, ndjekjes ligjore dhe koordinimit ndërinstitucional, të shoqëruara me menaxhim të qartë të komunikimit publik dhe ndëshkim të autorëve. Në aspektin e mendimit kritik, Banjska nënvizon edhe një rrezik tjetër: kur mohimi apo mbrojtja e autorëve, retorika dhe interpretimet politike, apo informative zëvendësojnë faktet bazë, vendimmarrja humb kohë dhe krijohet hapësirë për përshkallëzim. Prandaj, "fakti/et i verifikueshme" dhe "procedura e provua" janë elemente parandaluese po aq të rëndësishme sa reagimi taktik.

---

[14] National Institute of Standards and Technology (NIST), the NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29) (Gaithersburg, MD: NIST, 2024).

[15] ENISA Threat Landscape 2024 (Athens/Brussels: ENISA, 2024).

[16] European External Action Service (EEAS), *Statement by the High Representative on the attack against Kosovo Police*, September 24, 2023.

Rast studimor: Ukraina dhe logjika e përshtatjes nën presion të zgjatur

Ukraina përbën një shembull domethënës mbi mënyrën se si përshtatja e shpejtë shndërrohet në kusht mbijetese nën një presion të vazhdueshme, si tradicional dhe jo tradicional. Sistemi ka prodhuar një formë shkurajim funksional duke kombinuar forcën aktive me mobilizim të organizuar, mbrojtje civile dhe rrjete lokale reagimi, mbrojtje të infrastrukturës dhe standardizim të procedurave të koordinimit.[17] Mësimi i vlefshëm dhe i transferueshëm për Shqipërinë dhe vendet e Ballkanit Perëndimor nuk është kopjimi i modelit, por parimi: aftësia e sistemit për të mësuar, për t'u përshtatur shpejt dhe për të standardizuar atë që funksionon. Kjo kërkon një cikël të pandërprerë vëzhgimi, vlerësimi, përshtatje dhe standardizim, i integruar në stërvitje, planëzim dhe bashkëpunim ndërinstitucional.

Një mësim shtesë është ai i vazhdimësisë: nën presion të zgjatur, ndërprerjet e shërbimeve jetike, lodhja e personelit dhe presioni mbi mbështetjen e vazhdueshme të cilat synojnë të konsumojnë kapacitetet. Prandaj, rotacioni, rezervat dhe mbështetja e shërbimeve kritike janë pjesë e parandalimit, sepse ruajnë ritmin e funksionimit dhe ulin efektin e destabilizimit gradual. Për vendet me burime të kufizuara, mësimi kryesor është institucionalizimi "civil preparedness": role të qarta, zinxhir vendimmarrjeje, procedura të thjeshta dhe stërvitje të përsëritura. Kur këto elemente funksionojnë, presioni i zgjatur nuk thyen sistemin; vetëm e vë në provë atë.[18]

Implikime dhe rekomandime për Shqipërinë dhe rajonin

Dy rastet e mësipërme studimore sugjerojnë një përfundim të përbashkët: shkurajimi funksional në kushtet e sfidave dhe kërcënimeve ndërtohet kur shteti tregon aftësinë për të vendosur shpejt, ruan shërbimet jetike dhe mban ritmin e funksionimit edhe kur presioni hibrid apo kibernetik është i zgjatur. Për Shqipërinë, kjo nënkupton integrim të plotë të Forcave të Armatosura me mekanizmat civilë të menaxhimit të krizave dhe me mbrojtjen civile, duke e trajtuar sigurinë si sistem funksional shtetëror, jo si sektor të veçantë[19] . Në nivel rajonal, kjo logjikë kërkon standardizim të përbashkët, protokolle të harmonizuara, shkëmbim informacioni dhe stërvitje që testojnë vendimmarrjen ndërinstitucionale nën presione hibride. Për vendet e Ballkanit Perëndimor, ku incidentet mund të marrin shpejt peshë strategjike, parashikueshmëria dhe kohezioni procedural janë po aq të rëndësishëm sa kapacitetet materiale.

Në këtë këndvështrim, rekomandojmë një paketë masash të cilat janë të realizueshme:

---

[17] Royal United Services Institute (RUSI), *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (London: RUSI, 2022).

[18] RAND Corporation, Building Effective Reserve Forces (Santa Monica, CA: RAND, 2019).

[19] NATO, "Vilnius Summit Communiqué," July 11, 2023.

Së pari, të përcaktohen tregues funksionalë të parandalimit: koha e aktivizimit të strukturave aktive, rezervë, mbrojtje civile, vendimmarrjes, koha e rikthimit të shërbimeve kritike pas ndërprerjes, shkalla e ndërveprueshmërisë, siguria e informacionit dhe komunikimeve dhe aftësia për komunikim publik të sinkronizuar në fazat e para të incidentit.[20]

Së dyti, modernizimi të kuptohet si rritje funksionaliteti: komunikime të sigurta, logjistikë e qëndrueshme, mbrojtje e infrastrukturës kritike, aftësi për kërkim-shpëtim dhe menaxhim krize, si dhe mbrojtje kibernetike e shërbimeve kritike.

Së treti, politika e burimeve njerëzore dhe rezervave të trajtohen si shtylla: certifikim i specialiteteve kritike, si niche (kibernetikë, mirëmbajtje, mjekësi, menaxhim krizash, HNS, CIMIC) dhe integrim i forcave të rezervës në plane mobilizimi dhe stërvitje periodike, me role të qarta funksionale.

Së katërti, të institucionalizohen cikle stërvitjeje me skenarë hibride, stërvitje ndërinstitucionale me skenarë të shkurtër (24–72 orë) dhe testim i rikthimit të shërbimeve kritike dhe një mekanizëm i përhershëm për përditësim të procedurave, bazuar në vëzhgim, vlerësim dhe përshtatje.

Ky punim temë është bazuar në burime publike dhe në analizë konceptuale; për rrjedhojë, nuk synon të zëvendësojë vlerësimet e brendshme institucionale mbi sigurinë. Gjithashtu, për arsye sigurie, nuk trajton konfigurime ose hollësi operacionale. Megjithatë, ai ofron një kornizë analitike, e cila mund të ushqehet me të dhëna institucionale dhe të kthehet në plan veprimi.

Përfundime

Mjedisi i sigurisë në Ballkanin Perëndimor po hyn në një fazë ku stabiliteti përcaktohet më pak nga menaxhimi i pasojave dhe më shumë nga aftësia për shkurajim funksional dhe funksionim institucional. Kërcënimet hibride dhe presionet tradicionale veçanërisht jo tradicionale synojnë të konsumojnë gradualisht vendimmarrjen, besimin publik dhe ritmin e reagimit, duke e bërë të vështirë dallimin midis incidentit dhe krizës. [21]

Në këtë kontekst, parandalimi matet me funksionimin e sistemit në kohë reale, aftësia për vendimmarrje të shpejtë, mbrojtja e shërbimeve jetike dhe vazhdimësia operacionale. Këta janë treguesit kryesorë që e ndajnë reagimin e thjeshtë nga shkurajimi i besueshëm.

Për Shqipërinë dhe Forcat e Armatosura, përfundimi kryesor është se modernizimi, burimet njerëzore, rezervat dhe bashkëpunimi civil-ushtarak duhet të konsolidohen më shumë që të funksionojnë si një sistem i vetëm, "sinergji". Një vend që ruan funksionimin e shërbimeve kritike, që mobilizon shpejt dhe që vepron me standarde të provuara, e ul hapësirën e destabilizimit dhe rrit besueshmërinë brenda NATO-s dhe në rajon.

[20] International Institute for Strategic Studies (IISS), The Military Balance 2024 (London: IISS, 2024).
[21] NATO 2022 Strategic Concept (Madrid: NATO, 2022).

Bibliografia

1. Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK). *Strategjia Kombëtare e Sigurisë Kibernetike 2025–2030 dhe Plani i Veprimit*. Tiranë, 2025.
2. Council of the European Union. *A Strategic Compass for Security and Defence*. Brussels: Council of the European Union, 2022.
3. Department of the Army. *FM 3-0: Operations*. Washington, DC: Department of the Army, 2022.
4. ENISA. *ENISA Threat Landscape 2024*. Athens and Brussels: ENISA, 2024.
5. European Commission and European External Action Service (EEAS). *Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (JOIN (2018) 16 final)*. Brussels, 2018.
6. European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Framework on Countering Hybrid Threats: A European Union Response (JOIN (2016) 18 final)*. Brussels, 2016.
7. European External Action Service (EEAS). "Statement by the High Representative on the Attack against Kosovo Police." September 24, 2023.
8. European Parliament and Council of the European Union. *Directive (EU) 2022/2555 (NIS2) on Measures for a High Common Level of Cybersecurity across the Union*. Official Journal of the European Union, 2022.
9. International Institute for Strategic Studies (IISS). *The Military Balance 2024*. London: IISS, 2024.
10. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. Gaithersburg, MD: NIST, 2024.
11. NATO. *NATO 2022 Strategic Concept*. Madrid: NATO, 2022.
12. NATO. "Vilnius Summit Communiqué." July 11, 2023.
13. NATO. "Warsaw Summit Communiqué." July 9, 2016.
14. RAND Corporation. *Building Effective Reserve Forces*. Santa Monica, CA: RAND, 2019.
15. Republika e Shqipërisë. *Strategjia e Sigurisë Kombëtare 2023–2028*. Tiranë: Botim zyrtar, 2023.
16. Royal United Services Institute (RUSI). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*. London: RUSI, 2022.
17. UK Ministry of Defence. *UK Defence Doctrine (Joint Doctrine Publication 0–01)*. London: Ministry of Defence, 2020.
18. United Nations Office for Disaster Risk Reduction (UNDRR). *Sendai Framework for Disaster Risk Reduction 2015–2030*. Geneva: UNDRR, 2015.
19. U.S. Department of Defense. *Joint Publication 3-0: Joint Operations*. Washington, DC: Department of Defense, 2022.
20. U.S. Department of Defense. *Joint Publication 3-13: Information Operations*. Washington, DC: Department of Defense, 2014.

E ardhmja e luftërave: në tokë apo në ajër?

Kolonel (R) Zeno JAHAJ
Agron BERDAJ

Trajtesë e shkurtuar

Ku vendoset rezultati i luftës: në tokë apo në qiell?

Ky është një debat i hershëm, i lindur që në Lufta e Parë Botërore dhe që mbetet aktual sa herë që diskutohet për natyrën dhe zhvillimin e luftërave. Me gjasë, shkaqet dhe gjeografia e konflikteve të ardhshme do ta shtrojnë këtë çështje edhe më me forcë, duke qenë se prania njerëzore në terren pritet të zvogëlohet, ndërsa makineritë dhe teknologjitë — veçanërisht ato ajrore dhe hapësinore — po marrin një rol gjithnjë e më të madh.

Luftërat nuk kanë qenë kurrë dhe nuk do të jenë kurrë të njëjta. Ato ndryshojnë sepse ndryshojnë aktorët ndërluftues, motivet, konteksti gjeopolitik, zhvillimet teknologjike, shoqëria dhe normat etike që i rrethojnë. Gjeopolitika, metodat e luftimit dhe mjetet teknike nuk janë statike. Njerëzimi i sotëm nuk është ai i djeshmi, dhe ai i së nesërmes do të jetë edhe më i ndryshëm, sidomos në aspektin teknik dhe teknologjik. Për këtë arsye, çdo luftë është pasqyra e kohës së saj: e mendimit strategjik dhe taktik, por edhe e nivelit të zhvillimit teknologjik që e karakterizon atë epokë.

Në këtë kontekst transformimi, e ardhmja e dualitetit tokë–ajër/hapësirë ka nisur tashmë të shpaloset. Zhvillimet e fundit, veçanërisht lufta në Ukrainë, tregojnë se raporti midis dimensionit tokësor dhe atij ajror po rikonfigurohet. Kjo ngre një sërë pyetjesh thelbësore: A do të jenë luftërat e ardhshme kryesisht luftëra dronësh? A do të dominohen ato nga platforma ajrore apo hapësinore? Apo toka, ndonëse e sfiduar nga teknologjitë e reja, do të ruajë peshën e saj vendimtare në përcaktimin e rezultatit të konfliktit?

Historianë dhe mendje ushtarake të shquara, si në të kaluarën ashtu edhe në të tashmen, kanë ofruar përgjigje të ndryshme ndaj këtij debati. Megjithatë, analiza teorike dhe testimi në kushte reale vazhdojnë të prodhojnë përfundime të reja. Edhe pse teknologjia transformon mënyrën e zhvillimit të luftës, mbetet për t'u parë nëse parimet klasike të ekuilibrit midis luftës tokësore dhe asaj

ajrore e hapësinore do të vazhdojnë të qëndrojnë të palëkundura apo do të riformësohen rrënjësisht.

Fjalët kyçe: luftë; gjeopolitikë; luftë tokësore; luftë ajrore; avionë; dronë; hapësira e jashtme; diplomaci; politikë; ekonomi; fuqi; forcë ushtarake; marrëdhënie strategjike

1. Motivet e luftërave të ardhshme si premisë për peshën e tyre në tokë apo në ajër

Një pyetje e lashtë ka qëndruar pezull ndër shekuj: a do ta shoqërojë njerëzimin në udhëtimin e tij paqja apo lufta? Cila prej tyre është e qëndrueshme dhe cila thjesht kalimtare?

Një vështrim përmes prizmit të historisë tregon se qytetërimi njerëzor është formësuar, por edhe plagosur nga luftërat. Shtete dhe perandori janë ngritur e janë rrëzuar në vatrën e konfliktit. Paqja, në të kundërt, shpesh ka ardhur si pasojë e këtyre përplasjeve dhe jo rrallë ka rezultuar jetëshkurtër.

A nënkupton kjo se lufta është "gjendja natyrore" e njerëzimit? Thomas Hobbes, ndoshta filozofi më me ndikim mbi këtë çështje, argumentonte se në gjendjen natyrore jeta është "e vetmuar, e varfër, e shëmtuar, brutale dhe e shkurtër"[1] — një gjendje e përhershme konflikti, përveçse kur frenohet nga autoriteti i një pushteti të fortë. Në kontrast, Jean-Jacques Rousseau besonte se njerëzit janë në thelb paqësorë dhe se lufta lind si produkt i organizimit shoqëror dhe i institucioneve të tij[2].

Shekulli i njëzetë ofron një shembull domethënës. Një Evropë e rraskapitur nga luftëra të pafundme, më shumë se çdo kontinent tjetër, përjetoi, pas Luftës së Dytë Botërore, një periudhë të paprecedent paqeje relative midis fuqive të saj të mëdha. Kjo u bë e mundur falë diplomacisë, ndërvarësisë ekonomike dhe institucioneve të përbashkëta. Megjithatë, kjo epokë mbarti hijen e tensionit të ashtuquajtur "Lufta e Ftohtë" — një paqe larg së qeni e qetë, e karakterizuar një ankth i vazhdueshëm konflikti që përfshinte kontinente, oqeane dhe madje edhe hapësirën e jashtme. Kombet, secili sipas kapaciteteve të veta, garuan për grumbullimin e fuqisë ushtarake. Pothuajse të gjithë ishin në një gjendje përballjeje të vazhdueshme, edhe pse lufta nuk u shpall kurrë zyrtarisht. Pikërisht në këtë kontekst, studiues si Steven Pinker argumentojnë se dhuna dhe luftërat kanë pësuar rënie graduale falë përparimeve në arsim, qeverisje dhe zgjerimit të empatisë njerëzore[3].

Ndoshta përgjigjja më pranë saktësisë është kjo: historikisht, lufta ka qenë

[1] Hobbes, Thomas, "Leviathan", First Book, Chapter XIII "Of the Natural Condition of Mankind, as concerning their Felicity, and Misery", 1651.

[2] Rousseau, Jean-Jacques, "Discourse on the Origin and Basis of Inequality Among Men", 1755; "The Social Contract", 1762.

[3] Pinker, Steven, "The Better Angels of Our Nature: Why Violence Has Declined", 2011.

më e shpeshtë dhe më e dukshme, ndërsa paqja ka kërkuar "betejën" e saj përkatëse — një përpjekje të vazhdueshme për ta ruajtur atë. Megjithatë, luftërat nuk kanë qenë kurrë të njëjta. Aktorët që i zhvillojnë kanë ndryshuar në kohë, ashtu si edhe faktorët që i formësojnë konfliktet: gjeopolitika, motivet, teknologjia, shoqëria, politika, metodat e luftimit dhe etika e luftës. Njerëzimi i sotëm nuk është ai i djeshmi, dhe ai i së nesërmes do të ndryshojë sërish. Çdo luftë pasqyron kohën e vet, mendësinë strategjike dhe nivelin teknologjik të epokës përkatëse. Brenda kuadrit të këtij studimi, është e nevojshme të identifikohen dallimet në motive, në vendndodhjen gjeografike dhe në shkallën e përfshirjes së fuqive të tjera. Sa u përket motiveve, shumë luftëra zhvillohen për të marrë, mbrojtur ose rikthyer territore zona detare dhe burime natyrore strategjike. Kur toka dhe uji bëhen të kufizuara, rriten lakmia dhe frika, duke e bërë konfliktin një kërcënim real. Luftëra të tilla mund të jenë lokale - shtet kundër shteti - por në kontekstin e ambicieve për burime me rëndësi globale, ato mund të marrin dimension kontinental ose madje global. Një shembull aktual është lufta që Rusia po zhvillon në Ukrainë: ku ndër objektivat strategjikë përfshihen rikthimi i Krimesë dhe marrja e bregdetit strategjik ukrainas të Detit të Zi, si dhe krijimi i një korridori që lidh Krimenë me "republikat" e Donetskut dhe Luhanskut, rajone me rëndësi të veçantë industriale dhe gjeopolitike.

Konfliktet me natyrë lokale shfaqen edhe në forma të tjera, si mosmarrëveshjet për burimet ujore në Lindjen e Mesme dhe Afrikën e Veriut, përfshirë tensionet midis Egjiptit dhe Etiopisë, apo mosmarrëveshjet mbi tokën e punueshme midis Sudanit dhe Etiopisë, ku vazhdojnë të ekzistojnë zona të kontestuara me kufij të paqartë.

Konfliktet me shkallë kontinentale mund të përfshijnë mosmarrëveshjen për Kashmirin, që përfshin pretendime mbi tokën dhe burimet ujore nga India, Pakistani dhe pjesërisht Kina. Duke qenë se të tria janë fuqi bërthamore, konflikti ka potencialin të përshkallëzohet në një nivel global.

Duke parë drejt së ardhmes, Arktiku (veriu më i largët) po bëhet një skenë e re e pretendimeve të natyrave të ndryshme midis Rusisë, Kanadasë, Shteteve të Bashkuara, Norvegjisë dhe Danimarkës. Në këtë rajon më verior të globit përreth Polit të Veriut, ngrohja globale po shkrin akullin, duke hapur rrugë të reja dhe më të shkurtra detare dhe akses në rezervat e mëdha të naftës, gazit dhe mineraleve. Rusia tashmë e ka militarizuar zonën, ndërsa vendet e tjera po rrisin praninë e tyre ushtarake, teknologjike dhe ekonomike. Konflikti për Groenlandën veçse shpalos këtë kuadër të ri konflikti.

Një tjetër rajon potencial krizash është Deti i Kinës Jugore, i pasur me gaz, naftë dhe peshq. Ndërsa Kina pretendon pothuajse të gjithë zonën, Vietnami, Filipinet, Malajzia, Brunei dhe Tajvani gjithashtu kanë pretendime konkurruese. Deti i Kinës Jugore është një korridor strategjik detar, që bart rreth 30% të tregtisë globale detare me një vlerë prej 3–5 trilion dollarë në vit

— një nyje kritike për interesat e SHBA-së dhe e përkthyer prej saj si "sfidë e lidhur me sigurinë." [4]

Rajone të tjera afër lufte përfshijnë Lindjen e Mesme dhe Afrikën Qendrore dhe Perëndimore, të cilat përmbajnë rezervat e mëdha të naftës, mineraleve të rralla, dhe gazit dhe përfshijnë shtete të mëdha si Irani, por edhe të brishta si Republika Demokratike e Kongos, Nigeria, Mali, Çadi dhe Burkina Faso — të gjitha të "ndërlidhura" me fuqitë kryesore si Rusia, Kina, Shtetet e Bashkuara, Franca dhe të tjerët.

Luftërat gjithashtu mund të lindin nga frika dhe pasiguria, kur njëra prej palëve, zakonisht një fuqi e konsoliduar nxit konflikt sepse ndihet e kërcënuar nga një fuqi në ngritje dhe kërkon të veprojë e para, për të parandaluar një goditje të mundshme nga kjo forcë në rritje. Këtu hyn "në lojë" dilema klasike e "Kurthit të Tukididit", sipas të cilit "Ishte ngritja e Athinës dhe frika që kjo ngritje shkaktoi tek Sparta që e bëri luftën të pashmangshme." Një formë më e qartë dhe relativisht bindëse e kësaj frike ose pasigurie shihet në perceptimin e Izraelit se Irani, duke refuzuar të njohë Izraelin si shtet dhe duke aspiruar të bëhet fuqi bërthamore, mund të përbëjë një kërcënim ekzistencial për shtetin hebré.

Kështu, lufta bëhet jo vetëm e mundshme, por ndonjëherë e pashmangshme, kur një fuqi në ngritje kërkon të imponojë dominim, duke sfiduar pozicionin e një fuqie të konsoliduar — një dinamikë që prodhon frikë, rivalitet dhe, në fund, konflikt.

Shembulli më i përshtatshëm modern i Kurthit të Tukididit është dinamika midis Kinës - një fuqi në ngritje dhe Shteteve të Bashkuara - një fuqi e konsoliduar.

Që nga Lufta e Dytë Botërore, SHBA-ja ka qenë një superfuqi globale, duke dominuar institucionet ndërkombëtare (OKB, FMN, Banka Botërore), duke mbajtur prani ushtarake në mbarë botën, duke udhëhequr aleanca të fuqishme si NATO dhe duke promovuar rendin liberal demokratik dhe tregjet e lira. Në kontrast, Kina ka demonstruar rritje të shpejtë ekonomike në raport me SHBA-në, duke zgjeruar dhe konsoliduar ndikimin e saj global, veçanërishtpërmes investimeve masive në iniciativën e ashtuquajtur "Belt and Road" nëpër Azi, Afrikë, Europë dhe madje Amerikën Latine. Kina synon të barazojë dhe tejkalojë SHBA-në në teknologji: inteligjencën artificiale, rrjetet 5G dhe më tej deri në militarizimin e hapësirës dhe oqeaneve të thella. Kina po forcon ushtrinë e saj, veçanërisht në Detin e Kinës së Jugut dhe ngushticën e Tajvanit, ndërsa ofron një model qeverisjeje të ndryshëm nga modeli Perëndimor (kapitalizëm shtetëror i kombinuar me autoritarizëm politik), i cili po rezulton gjithnjë e më efektiv në ndjekjen e ambicieve globale.

Në të ardhmen, ndërsa globalizimi thellohet, aleancat ndërkombëtare jo vetëm që do të mbeten relevante, por do të bëhen të domosdoshme për mbijetesë.

[4] National Security Strategy of the United States of America, November 2025

Për këtë arsye, një ose më shumë vende mund të hyjnë në luftë për të mbrojtur aleatët që kërcënohen ose sulmohen.

Së fundi, lufta do të vazhdojë të përdoret si instrument politik. Historia ofron shembuj të shumtë të shteteve relativisht të fuqishme që nisin konflikte për të shpërqendruar vëmendjen nga problemet e brendshme ose krizat e brendshme.

2. Evolucioni historik i marrëdhënieve midis luftës në tokë dhe luftës në ajër

Lufta tokësore është fusha madhore, me një traditë shekullore në historinë e njerëzimit. Në krahasim me të, lufta ajrore është ende në fazat e saj fillestare, duke shërbyer fillimisht drejtpërdrejt për të mbështetur objektivat e operacioneve tokësore. Ky raport strategjik i ka detyruar të dyja të zhvillohen në mënyrë të ndërlidhur, edhe pse, në disa raste, secila ka qenë në gjendje të përmbushë në mënyrë të pavarur detyra të caktuara operative ose taktike. Për më tepër, përparimet në njërën fushë kanë ndikuar drejtpërdrejt zhvillimet në tjetrën, duke ndikuar njëkohësisht në taktika, teknologji dhe strategji.

Ndërveprimi midis luftës ajrore dhe asaj tokësore gjatë Luftës së Parë Botërore përfaqëson një pikë kthese vendimtare në historinë ushtarake. Megjithëse aviacioni ishte ende në fazat e tij të hershme, ai luajti një rol gjithnjë e më të rëndësishëm në mbështetjen e operacioneve tokësore.

Aeroplanët ishin shpikur rreth një dekadë përpara shpërthimit të Luftës së Parë Botërore dhe u zhvilluan nën presionet e këtij konflikti të madh gjeopolitik botëror. Fillimisht, avionët e zbulimit u krijuan për të vëzhguar lëvizjet e armikut nga ajri, për të fotografuar linjat e fortifikuara dhe për të mbledhur informacione. Të dhënat e mbledhura nga ajri ndikuan drejtpërdrejt në planifikimin e betejave tokësore, duke përmirësuar ndjeshëm koordinimin me artilerinë. Zbulimi ajror u përdor për të korrigjuar zjarrin e artilerisë me saktësi gjithnjë e më të madhe.

Në një fazë të mëvonshme, u shfaqën avionët luftarakë të pajisur me mitraloza, të destinuar për të neutralizuar avionët armikë. Kjo solli nevojën për sigurimin e epërsisë ajrore dhe shënoi lindjen e luftimit ajror si dimension më vete i konfliktit. Me kalimin e kohës, u zhvilluan bombarduesit për të hedhur lëndë shpërthyese mbi objektiva ushtarakë, pozicione armike, ura, depo furnizimi dhe linja komunikimi. Megjithatë, bombardimi ajror mbeti në fazat e tij fillestare dhe i kufizuar në shkallë.

Në nivel strategjik, komandantët filluan gradualisht ta përfshinin elementin ajror në planifikimin e përgjithshëm ushtarak, duke e konsideruar atë një komponent të rëndësishëm të operacioneve tokësore. Një ilustrim domethënës është Beteja e Somës, në vitin 1916, gjatë së cilës avionët britanikë u përdorën në shkallë të gjerë për të mbështetur ofensivën tokësore. Ata kontribuuan në zbulimin e linjave gjermane, në korrigjimin e zjarrit të artilerisë dhe në bombardimin paraprak të pozicioneve armike përpara avancimit të

këmbësorisë. Në këtë mënyrë, Lufta e Parë Botërore shënoi momentin e parë të rëndësishëm të ndërveprimit midis luftës ajrore dhe asaj tokësore.

Lufta e Dytë Botërore (1939–1945) dëshmoi integrimin e plotë të operacioneve tokësore dhe ajrore. Në këtë konflikt, avionë luftarakë të shpejtë dhe manovrues u përdorën për të kontrolluar hapësirën ajrore dhe për t'u mbrojtur nga bombarduesit. Bombardues të rëndë strategjikë goditën qytete, industri dhe infrastrukturë ushtarake. Bombardues të lehtë siguruan mbështetje të drejtpërdrejtë nga afërsia në lartësi të vogël, duke goditur tanke, trupa, artileri në lëvizje dhe pozicione taktike armike. Avionët transportues dhe ata të parashutistëve lehtësuan zbarkimet e trupave, hedhjen e furnizimeve dhe operacionet ajrore. Koordinimi i ngushtë me artilerinë dhe tanket u arrit përmes komunikimit me radio dhe sinjalizimit ajror, duke u mundësuar pilotëve të merrnin informacion në kohë reale nga toka mbi objektivat e tyre. Shpesh, fushatat tokësore nuk fillonin pa u arritur më parë epërsia ajrore, pasi kontrolli i qiellit siguronte lëvizje më të sigurta për forcat tokësore, të lira nga bombardimet armike. Zbulimi ajror dhe fotografia ajrore zbuluan lëvizjet e armikut dhe prodhuan harta të sakta për goditje.

Nëpërmjet fuqisë së bombardimit ajror u synuan rezultate strategjike. Gjermania naziste u përpoq të nënshtronte Britaninë e Madhe përmes një fushate ajrore (korrik–tetor 1940), duke bombarduar Londrën dhe qytete të tjera të mëdha, me qëllim shkatërrimin e Forcave Ajrore Mbretërore, duke goditur bazat ajrore dhe stacionet e radarit, si dhe fitimin e epërsisë ajrore mbi Kanalin Anglez dhe Anglinë jugore. Qëllimi ishte thyerja e moralit civil, dobësimi i kapaciteteve ushtarake britanike dhe krijimi i kushteve të favorshme për një pushtim. Kështu, Gjermania kërkoi një fitore strategjike vetëm përmes fuqisë ajrore. Por dështoi. Synimi i saj ishte ta detyronte Britaninë të dorëzohej ose të hynte në negociata paqeje. Kjo ishte përpjekja e parë për të përdorur një fushatë ajrore për të nënshtruar një komb të tërë, por rezultati ishte i kundërt.

Më pas, radha i erdhi Britanisë dhe aleatëve të saj kryesorë, të cilët përdorën forcat ajrore për të shkatërruar kapacitetet industriale dhe logjistike të Gjermanisë, përfshirë hekurudhat, rafineritë dhe qytetet, duke dobësuar kështu forcat tokësore të armikut në afat të gjatë. Kjo ndikoi drejtpërdrejt në aftësinë e Gjermanisë për të kryer operacione tokësore. Epërsia ajrore ishte bërë kështu një parakusht për suksesin në tokë.

Megjithatë, nga një këndvështrim strategjik, edhe Lufta e Dytë Botërore mbeti kryesisht një luftë tokësore për sa i përket numrit të trupave, armatimit, shkallës, thellësisë dhe rezultateve të operacioneve. Fuqia ajrore kishte fituar një rëndësi të jashtëzakonshme krahasuar me Luftën e Parë Botërore, veçanërisht në nivel taktik, dhe madje kishte ndërmarrë edhe misione strategjike. Sidoqoftë, ajo mbeti një forcë mbështetëse dhe përforcuese. Ishin forcat tokësore ato që shfrytëzuan rezultatet e fuqisë ajrore, pushtuan dhe mbajtën, ose humbën territore dhe fituan, ose humbën beteja në tokë. Në fund

të fundit, në Luftën e Dytë Botërore, luftimi ajror "përgatiti fushëbetejën" për fitoren, por ishte luftimi tokësor ai që e fitoi luftën.

Gjatë Luftës së Ftohtë, një shembull domethënës i integrimit midis luftimit tokësor dhe atij ajror ishte Lufta e Yom Kippur-it (tetor 1973) midis Egjiptit dhe Izraelit, me përfshirjen edhe të Sirisë. Ky konflikt shërben si një model klasik i koordinimit ajër–tokë, duke ofruar mësime të rëndësishme për doktrinën moderne ushtarake. Të dyja palët përdorën forcat tokësore dhe ajrore në mënyrë të ndërthurur, megjithëse me rezultate të ndryshme për shkak të dallimeve në nivelin e integrimit dhe teknologjive në dispozicion.

Egjiptianët arritën një koordinim të suksesshëm në fazën fillestare, gjatë operacionit "Badr" më 6 tetor 1973, kur forcat e tyre kaluan Kanalin e Suezit dhe zhvilluan një ofensivë tokësore të mirëplanifikuar, të mbështetur nga mbulimi intensiv ajror. Duke përdorur raketa tokë–ajër SA-2 dhe SA-6, ata krijuan një "korridor ajror të sigurt" që mbronte trupat tokësore nga sulmet ajrore izraelite. Ndërkohë, avionët egjiptianë MiG-21 dhe Su-7 mbështetën forcat tokësore në avancim, duke goditur pozicionet izraelite në thellësi dhe duke lehtësuar avancime të mëtejshme territoriale.

Pas tronditjes fillestare, Izraeli arriti të rifitonte epërsinë ajrore përmes përdorimit të avionëve F-4 "Phantom" dhe A-4 "Skyhawk", të cilët u angazhuan në sulme intensive kundër linjave egjiptiane të furnizimit, njësive të blinduara dhe sistemeve të mbrojtjes kundërajrore. Pasi mbrojtja ajrore egjiptiane u shty gradualisht prapa, forcat tokësore egjiptiane mbetën pa mbulim efektiv ajror, duke krijuar kushte të favorshme për një kundërofensivë vendimtare izraelite.

Me manovra të armëve të kombinuara nën mbështetje të fortë ajrore, forcat izraelite kaluan Kanalin e Suezit dhe e vunë ushtrinë egjiptiane përballë rrezikut të një rrethimi operacional-strategjik. Kështu, të dyja palët demonstruan se epërsia ajrore mund të përkthehet në sukses tokësor. Megjithatë, në fund ishte Izraeli ai që arriti avantazhin strategjik, duke thyer integrimin egjiptian midis fuqisë ajrore dhe asaj tokësore.

Një zhvillim edhe më domethënës për debatin nëse rezultati i një lufte vendoset në tokë apo në ajër është Lufta e Kosovës. Ky konflikt u zhvillua ndërmjet forcave serbe dhe shqiptarëve të Kosovës, në një kontekst të karakterizuar nga fushata të gjera spastrimi etnik ndaj popullsisë civile shqiptare, dhe përfshiu një ndërhyrje ajrore të drejtpërdrejtë nga NATO.

Ndryshe nga konfliktet tradicionale, ky rast paraqet një model ku fuqia ajrore u përdor si instrumenti kryesor për arritjen e objektivave strategjike, pa një ofensivë tokësore të drejtpërdrejtë të NATO-s kundër forcave serbe. Konflikti përfshiu disa komponentë të ndërlidhur:

- Fushatën diplomatike të Shteteve të Bashkuara dhe të NATO-s për të ndalur spastrimin etnik dhe për të detyruar Beogradin të pranonte një zgjidhje politike.

- Vendimin politik të fuqive perëndimore për të ndërmarrë një fushatë ajrore kundër forcave dhe aseteve ushtarake serbe.
- Planifikimin ushtarak të NATO-s për zbatimin e operacionit ajror.
- Ekzekutimin e fushatës ajrore, të drejtuar nga qendrat komanduese tokësore të NATO-s dhe të koordinuar, në masën e mundshme, me Ushtria Çlirimtare e Kosovës.
- Dorëzimin politik dhe ushtarak të Serbisë, përmes pranimit të tërheqjes nga Kosova dhe të kushteve të vendosura nga NATO.
- Përgatitjen dhe dislokimin e forcave tokësore të NATO-s në Kosovë pas përfundimit të fushatës ajrore.
- Krijimin e KFOR nën mandatin e OKB-së, përmes së cilës NATO mori përgjegjësinë për garantimin e sigurisë dhe parandalimin e një konflikti të ri.

Në këtë kontekst, nga një këndvështrim rreptësisht ushtarak, NATO nuk kishte dislokuar trupa tokësore në Kosovë. Ato ndodheshin në gatishmëri diku tjetër, por nuk ishin të angazhuara në luftime. Në vend të kësaj, NATO angazhoi rreth 1.000 avionë luftarakë, përfshirë bombardues strategjikë (B-52, B-1B), avionë gjuajtës (F-16, F-15, F/A-18), avionë të pajisur me radar për vëzhgim, zbulim, paralajmërim të hershëm, gjurmim të objektivave ajrore dhe tokësore, si dhe për operacione komandimi dhe kontrolli (AWACS), përveç avionëve të luftës elektronike të projektuar për të çrregulluar dhe neutralizuar radarët e armikut. Këto operacione u zhvilluan nga bazat ajrore në Itali, Gjermani, Mbretërinë e Bashkuar, si dhe nga anije luftarake në Detin Adriatik.

Nga ana tjetër, mbrojtja ajrore e Serbisë përbëhej nga rreth 30–40 avionë aktivë, 1.200 raketa tokë–ajër dhe 150–200 njësi radarike aktive — të gjitha sisteme të viteve 1960–70, të cilat mbështeteshin në teknika kamuflimi dhe lëvizshmëri të shpejtë për t'iu shmangur goditjeve të NATO-s. Megjithëse rrjeti i radarëve ishte i integruar, ai mbeti i cenueshëm ndaj sulmeve të luftës elektronike të NATO-s. Serbia ruajti një mbrojtje ajrore të qëndrueshme, duke e bërë fushatën më sfiduese sesa ishte parashikuar. Megjithatë, Aleanca Euro-Atlantike siguroi epërsi absolute në forcë numerike, teknologji dhe aftësi operacionale.

Si rezultat, NATO zhvilloi një fushatë ajrore 78-ditore, duke goditur objektiva ushtarake, infrastrukturore dhe strategjike serbe, e cila përfundimisht detyroi regjimin e Sllobodan Millosheviqit të pranonte tërheqjen nga Kosova.

Në terren, ishte Ushtria Çlirimtare e Kosovës (UÇK) ajo që kishte një rol për të luajtur, përmes luftës aktive dhe rezistencës, duke ruajtur ndërgjegjen kombëtare dhe moralin. UÇK-ja u bë simbol i luftës çlirimtare, duke tërhequr vëmendjen ndërkombëtare dhe duke rritur presionin mbi komunitetin global për të ndërhyrë. Megjithatë, është realiste të vlerësohet se UÇK-ja:

- Ndodhej në një disavantazh të madh numerik krahasuar me forcat ushtarake dhe policore serbe (afërsisht 1:4).

- U përball me dallime të thella, si në sasi, ashtu edhe në llojet e armatimit në dispozicion.
- Ishte një ushtri partizane, që vepronte kryesisht në një pjesë relativisht më të vogël rurale dhe malore të Kosovës, ndërsa ushtria dhe policia serbe kontrollonin pothuajse të gjitha rrugët kryesore, kryeqytetin dhe qytetet e tjera.
- Nuk kishte përvojë të mëparshme luftarake. Në të kundërt, forcat serbe kishin grumbulluar rreth tetë vjet përvojë në konflikte etnike që shoqëruan shpërbërjen e Jugosllavisë.

UÇK-ja kreu disa operacione tokësore që ndihmuan në identifikimin e disa forcave serbe si objektiva për bombardimet e NATO-s, duke arritur një bashkëpunim taktik me NATO-n gjatë fushatës ajrore, ndërkohë që NATO luajti rol strategjik. Sidoqoftë, UÇK-ja përfaqësonte një kthesë strategjike për shqiptarët e Kosovës, nga rezistenca paqësore drejt rezistencës së armatosur, e radikalizuar nga fushata serbe e spastrimit etnik kundër popullsisë shqiptare të Kosovës. Kjo ishte një strategji e re që fitoi mbështetje të gjerë nga popullsia, duke ndryshuar dinamikat politike në Kosovë. Në fazat e saj të hershme, UÇK-ja u pa me dyshim nga komuniteti ndërkombëtar dhe madje u etiketua si "terroriste" në disa deklarata. Por, me kalimin e kohës ajo fitoi legjitimitet ndërkombëtar gjatë dhe veçanërisht pas luftës, duke u bërë pjesë e delegacionit shqiptar në Konferencën e Rambujesë (1999), dhe duke u njohur si përfaqësuesja legjitime e rezistencës së organizuar dhe aktive të popullit shqiptar në Kosovë. Pjesëmarrja e saj në negociatat ndërkombëtare e ngriti UÇK-në nga një grup gueril në një aktor politik moral dhe legjitim. Kështu, ndonëse fushata ajrore ishte vendimtare, veprimet operacionale të UÇK-së ishin mbështetëse.

Në analizë të fundit, rezultati i Luftës për Çlirimin e Kosovës nuk u vendos në ajër. Pse? Sepse vullneti politik, mbështetja dhe vendimmarrja, si dhe planifikimi, drejtimi dhe komandimi strategjik ushtarak — elemente thelbësore të luftës këto — u zhvilluan të gjitha në tokë nga NATO në radhë të parë dhe po kështu edhe nga UÇK-ja, si dhe nga forcat ushtarake e policore serbe. Prandaj, edhe rezultati përfundimtar i kësaj lufte (si fitorja, ashtu edhe humbja) u përcaktua në tokë.

3. Raporti midis luftës në tokë dhe luftës në ajër në të ardhmen

E ardhmja e këtij binomi ka filluar tashmë. Lufta në Ukrainë ka treguar dhe vazhdon të tregojë shumë për mënyrën se si do të duket kjo e ardhme. Në këtë konflikt po përdoren një sërë teknologjish të reja ajrore që nuk janë përdorur kurrë më parë. Ndër to spikasin dronët — sisteme ajrore luftarake pa pilot. Që nga fillimi i luftës, forcat ruse kanë lëshuar rreth 100.000-150.000 dronë kryesisht me rreze të gjatë dhe me pretendim operativ e strategjik, ndërsa forcat ukrainase kanë lëshuar dhjetëra herë më shumë, por kryesisht

për fushë-betejë, pra për rezultate taktike e operative. Nga ky këndvështrim, ky konflikt mund të quhet me të drejtë "lufta e dronëve". Ky përdorim masiv i dronëve për herë të parë në historinë e luftërave, ka detyruar krijimin e një shërbimi/dege të veçantë, duke i pozicionuar dronët si rivalë të artilerisë tokësore, si për nga numri, ashtu edhe për nga vdekjeprurja, si dhe për aftësitë e inteligjencës, zbulimit dhe vëzhgimit. Megjithatë, pavarësisht kësaj rritjeje mbresëlënëse, dronët mbeten kryesisht një mjet taktik: të fuqishëm, me rreze të madhe veprimi dhe gjithnjë e më efektivë, por jo një faktor strategjik që përmbys ekuilibrat e mëdhenj të luftës.

Forcat ruse kanë përdorur gjithashtu raketa hipersonike, që lëvizin me shpejtësi pesë herë më të madhe se ajo e zërit, të cilat janë jashtëzakonisht të vështira për t'u kapur nga mbrojtja ajrore konvencionale për shkak të shpejtësisë së tyre ekstreme, lartësisë së ulët të fluturimit dhe manovrueshmërisë së lartë. Megjithatë, sistemet perëndimore si bateritë "Patriot", ndonëse në numër të kufizuar, kanë arritur të neutralizojnë disa prej këtyre kërcënimeve të avancuara.

Megjithatë, më në fund konflikti ka marrë formën e një modeli statik, të lidhur me transhetë, duke demonstruar se lufta tokësore vazhdon të jetë vendimtare, edhe pse fuqia ajrore po merr një rol gjithnjë e më të rëndësishëm. Linjat e frontit dhe pushtimi, ose mbrojtja e pozicioneve strategjike përcaktohen nga operacionet tokësore, ku këmbësoria mbështetet shumë te artileria, tanket, mjetet e blinduara, minat dhe fortifikimet e të gjitha llojeve. Ka pasur ditë kur forcat ruse kanë shtënë 60.000–70.000 predha artilerie, ndërsa forcat ukrainase kanë shtënë 10.000–12.000. Shpenzimi vjetor i Ukrainës për artilerinë arrin rreth dy milionë predha, ndërsa ai i Rusisë është katër deri në pesë herë më i madh.[5]

Ka një fakt interesant, që duket si kontradiktor: humbjet ukrainase nga artileria ruse kanë qenë shumë më të mëdha sesa nga dronët rusë, ndërsa e kundërta ka ndodhur me humbjet ruse: ato kanë qenë më të mëdha (70-80% nga dronët ukrainas dhe pjesa tjetër nga artileria dhe armët e tjera të këmbësorisë).[6] Por, në këto raste droni është përdorur thjesht si një predhë artilerie, e cila edhe kjo fluturon në ajër. Pra droni, në këto raste, nuk mbetet të jetë mjet ajror. Pra, në fund të fundit, rezultati strategjik i luftës është përcaktuar në tokë.

Ky përfundim mbështetet edhe më tej nga fakti se të dy palët në konflikt janë shtete me thellësi kontinentale dhe fqinjë të drejtpërdrejtë tokësorë.

Operacioni i Izraelit kundër Iranit në qershor 2025 ilustroi një perspektivë tjetër mbi këtë çështje. Operacioni mbështetej në një rrjet të integruar inteligjence, duke siguruar mijëra imazhe satelitore. Izraeli kishte arritur më parë kontroll të plotë mbi hapësirën ajrore iraniane, duke neutralizuar rreth

[5] The Voice of Ukraine, April 27, 2024; Forbes, Feb 28, 2025

[6] The New York Times, March, 3, 2025

70% të baterive ajrore mbrojtëse të Iranit. [7] Nga ana tjetër, Irani lëshoi rreth 550 raketa balistike dhe afërsisht 1,000 dronë drejt Izraelit, por shumica e raketave u ndërprenë nga mbrojtja ajrore izraelite dhe amerikane, duke arritur një shkallë suksesi prej rreth 90 për qind.[8]

Sidoqoftë, morën vend edhe operacione tokësore: vrasjet e figurave kyçe, përfshirë gjeneralët dhe shkencëtarët, shumica e të cilave u kryen përmes atentateve të drejtpërdrejta, bombave ose dronëve shpërthyes të kontrolluar nga distanca brenda territorit iranian, të ekzekutuara nga personeli i inteligjencës dhe të planifikuara muaj përpara operacionit ajror.

Në këtë operacion, roli vendimtar u luajt nga fushata ajrore, ndërsa veprimet tokësore kishin një funksion mbështetës. Megjithatë, edhe operacioni ajror nuk arriti një rezultat strategjik, por vetëm rezultate taktike dhe operative: ai vetëm e ngadalësoi programin bërthamor të Iranit, që do të thotë se objektivi strategjik për ta ndaluar atë, ose për ta detyruar të pranojë ndonjë marrëveshje në këtë drejtim, nuk u arrit. Politikisht, operacioni vetëm sa radikalizoi më tej fraksionin e linjës së ashpër në Iran. Operacioni izraelit, së bashku me sanksionet perëndimore, e shtynë Iranin më afër Rusisë, Kinës dhe shteteve të BRICS. Kështu, në vend që të shpërbëhej, Irani u integrua më tej në një rend alternativ global, duke zhvendosur edhe më tej ekuilibrat gjeopolitikë.

Pra, përmes operacionit të tij, Izraeli fitoi pak kohë, por nuk zgjidhi problemin strategjik. Ky rezultat justifikohet edhe nga fakti se të dy palët në konflikt janë shtete bregdetare pa kufij tokësorë të drejtpërdrejtë. Nën këto kushte, një sulm tokësor nga Izraeli është absolutisht i pamundur për shumë arsye. Prandaj, mund të thuhet se rezultati i operacionit nuk u vendos në ajër.

Ndërkohë, një zhvillim interesant lidhur me këtë dilemë thuhet se po ndodh në Kinë: përpjekje për një "aeroplanmbajtëse" ajrore! Kjo nuk është fantazi, edhe pse ndonjëherë trajtohet si një koncept ushtarak krejtësisht spekulativ. Bëhet fjalë për një fortesë fluturuese e fuqizuar me energji diellore dhe inteligjencë artificiale, e aftë të qëndrojë në atmosferën e sipërme pa ajër për muaj ose madje vite, pa kërkuar karburant, pistë apo kthim në tokë.

Sigurisht, platformat diellore nuk janë të reja. NASA i ka testuar. Boeing ka tentuar të ndërtojë një të tillë. Por, në rastin e supozuar të Kinës, fokusi nuk është te platforma, por te ngarkesa: brenda "aeroplanmbajtëses" kineze supozohet se do të ketë stacione komunikimi satelitore në kohë reale, duke lidhur qendrat e komandim-drejtimit përtej oqeaneve. Inteligjenca artificiale e integruar do të jetë e aftë të marrë vendime të menjëhershme në betejë, të zgjedhë objektivat, të caktojë misione dhe të riorganizojë dronët gjatë fluturimit pa ndonjë komandë njerëzore. Mund të lëshohen raketa hipersonike

[7] The Times of Israel, 17 June 2025
[8] The Times of Israel, 24 June 2025

nga një sistem i tillë dhe nga një lartësi kaq e madhe, saqë gjysma e distancës deri tek objektivi përshkohet para se ndonjë interceptim të jetë i mundur në tokë. Pra, është një sistem që kontrollon qiellin. Një sistem që mund të mbijetojë edhe në rastin e një lufte bërthamore.

Duket sikur nga ky moment e tutje, kushdo që kontrollon qiellin kontrollon rezultatin në tokë. Në këto kushte, aeroplanmbajtëset oqeanikë mund të mbeten si relike, sepse kanë shumë dobësi fatale: janë të shtrenjta, të cenueshme ndaj raketave, të lehta për t'u zbuluar dhe ndjekur nga satelitët dhe mund të fundosen. Të gjitha këto dobësi, përkundrazi, kthehen në forca për aeroplanmbajtësen hapësinore. Kështu, mund të jemi dëshmitarë të një arme që nuk vjen për të luftuar ballë për ballë, por për të qëndruar mbi betejë, në hapësirë. Armët më frikësuese nuk janë ato që shohim, por ato që fluturojnë në qiellin e pafund, të padukshme, të paprekshme dhe të pandalshme.

Pra, duket sikur fusha e betejës po pëson një ridimensionim strategjik: një platformë e re armësh, një vendkomandim-drejtimi ajror që mund të mos ulet kurrë, duke monitoruar fushat e betejës në mënyrë të vazhdueshme.Por, kryepyetja mbetet: a do të ndryshojnë këto zhvillime parimin e përjetshëm që rezultati i luftës vendoset në tokë dhe jo në ajër? Le të shohim përfundimet.

Përfundime

Është fakt se pesha e fuqisë ajrore në luftë është rritur ndjeshëm dhe pritet të vazhdojë të rritet në raport me fuqinë tokësore. Kjo prirje ka nxitur diskutime për një "Gjeopolitikë të Ajrit"[9] në zhvillim. Ky nocion ofron çelësin për të kuptuar se si hapësira ajrore, fuqia ajrore dhe teknologjitë e lidhura me to formësojnë strategjinë ushtarake në tërësi, politikën ndërkombëtare, sovranitetin shtetëror, kontrollin territorial dhe ndikimin global. Koncepti përfshin gjithashtu zhvillimet në hapësirën e jashtme dhe rolin gjithnjë në rritje të dronëve, satelitëve dhe aviacionit civil dhe ushtarak. Në strategjitë moderne nuk ka më një kufi të qartë mes ajrit dhe hapësirës pa ajër përtej tij.

"Gjeopolitika e Ajrit" mund të përmblidhet në një aksiomë të thjeshtë: kush kontrollon ajrin dhe hapësirën fiton një avantazh të madh në drejtimin e ngjarjeve në tokë. Megjithatë, edhe duke njohur këtë rishikim të fuqisë në ajër dhe hapësirë, duhet të mbajmë shënim se çdo armë, duke përfshirë edhe sistemet e mbrojtjes ajrore, në fund të fundit gjen "antidotin" e vet.

Për dy ose tre vjet, dronët u ngjitën pothuajse në legjendë: të vegjël, të lirë për t'u prodhuar, të vështirë për t'u zbuluar dhe të dislokuar në tufë që mund të mbingarkonin mbrojtjen ajrore tradicionale. Megjithatë, ja ku jemi: kompania australiane e mbrojtjes *Electro Optic Systems* (EOS) ka prezantuar armën e saj të re me lazer me energji të lartë, *Apollo HELW*, e cila gjeneron deri në 150 kw energji dhe është e aftë të neutralizojë 200 dronë me madhësi të mesme, duke

[9] Revue Défense Nationale, https://www.defnat.com

përdorur vetëm furnizimin e saj të brendshëm të energjisë. Një përgjigje pothuajse e menjëhershme ndaj "legjendës së dronëve."

Armët me lazer po konsiderohen gjithnjë e më shumë si një përgjigje efektive ndaj kërcënimit të dronëve të armatosur, duke ofruar shpejtësi reagimi, kosto të ulët për goditje dhe aftësi për të angazhuar shumë objektiva në kohë të shkurtër.

Këto sisteme janë zhvilluar për dekada me radhë, por vitet e fundit janë afruar pranë pragut të dislokimit të plotë operacional. Sistemi lazer i prodhuar në Australi tashmë i është shitur një shteti anëtar të NATO-s (emri i të cilit nuk është bërë publik). Ai mund të shkatërrojë dronë në një distancë deri në 3 km (1,86 milje), të çaktivizojë sensorët optikë deri në 15 km (9 milje), të mbulojë një fushë të plotë 360°, të reagojë brenda 700 milisekondash në një hark prej 60°, dhe të angazhojë deri në 20 dronë në minutë. Sistemi mund të funksionojë si armë e pavarur, ose si pjesë e një rrjeti të integruar të mbrojtjes ajrore. Nëse kërkohet, ai mund të montohet edhe në mjete ushtarake. Furnizimi i brendshëm me energji i siguron pavarësi të plotë, duke i mundësuar të funksionojë edhe kur rrjeti elektrik është i dëmtuar. Sipas disa burimeve, me furnizimin e tij të brendshëm me energji, sistemi është në gjendje të neutralizojë deri në 200 dronë përpara se bateria të shterojë. [10] Dhe ky sistem do të përdoret fare kollaj nga toka ose nga deti!

Ndërkohë, nuk duhet të shkëputemi nga konteksti, sepse shkëputja nga konteksti çon në përfundime arbitrare. Sir Michael Howard, një nga historianët ushtarakë më të shquar të shekullit të 20-të, vëzhgoi se shkaktarët e vërtetë të fitoreve dhe humbjeve zakonisht gjenden larg teatrit të operacioneve, në fushat politike, ekonomike, sociale dhe industriale. Ky ishte një deduktim që ishte "vulosur" më herët nga i famshmi Clausewitz, i cili argumentoi se lufta nuk është gjë tjetër veçse vazhdimi i politikës me mjete të tjera. Sipas tij, lufta nuk është një akt i pavarur: ajo shërben si instrument politik për arritjen e objektivave shtetërorë, se vendimi për të hyrë në një luftë, mënyra se si ajo kryhet dhe si përfundon, janë të gjitha në thelb politike; se komanda ushtarake duhet t'i nënshtrohet udhëheqjes politike dhe jo të veprojë në mënyrë të pavarur; dhe se nëse ushtria vepron jashtë kuadrit politik, lufta mund të dalë jashtë kontrollit dhe të humbasë qëllimin e saj origjinal.

Po ashtu, ai nënkuptonte se fuqia ekonomike e një shteti ndikon drejtpërdrejt në kapacitetin e tij për të mobilizuar ushtritë, furnizuar armatime dhe logjistikë dhe për të mbajtur vetveten në një konflikt të gjatë. Po ashtu, Clausewitz theksonte se lufta nuk është vetëm çështje e qeverisë dhe ushtrisë, por edhe e popullit; se emocionet e shoqërisë, ndjenjat nacionaliste, urrejtja, ideologjia, luajnë një rol të madh në nxitjen dhe mbështetjen e luftës dhe se

[10] David Szondy, "Apollo lazer takes down 200 drones unplugged", September 18, 2025 (newatlas.com/military)

kjo ide parashikon konceptin e luftës totale, ku e gjithë shoqëria mobilizohet për konflikt. Këto parime, të pranuara gjerësisht, u zhvilluan më tej nga shumë teoricienë të luftës, përfshirë Friedrich Engels, i cili theksoi më fuqishëm rolin e ekonomisë në luftë. Ndërsa, strategët modernë si Edward Luttwak, Raymond Aron e lidhën mendimin e Clausewitz me botën moderne, ku politika, ekonomia dhe shoqëria janë të ndërthurura ngushtë në çdo konflikt.

Në këtë kuptim, rezultati i luftërave të ardhshme do të jetë produkt i ndërveprimit midis fuqisë tokësore dhe asaj ajrore. Megjithatë, dimensioni tokësor mbetet përcaktues. Luftërat fitohen ose humbasin kryesisht përmes burimeve ekonomike (financimi i luftës, kapaciteti industrial për të prodhuar pajisje ushtarake, aftësia për të përballuar një konflikt të gjatë); udhëheqjes politike dhe unitetit kombëtar (qëllimet e qarta të luftës, stabiliteti i qeverisë gjatë luftës, mbështetja e popullit për luftën); mbështetjes ose kundërshtimit ndërkombëtar (diplomacia ndërkombëtare, aleancat, sanksionet/embargot nga armiqtë, presioni ndërkombëtar dhe opinioni publik global); moralit dhe psikologjisë (besimi i ushtarëve në qëllimin e luftës, qëndrueshmëria psikologjike e popullsisë, propaganda dhe lufta psikologjike, lodhja nga lufta ose humbja e motivimit); fuqisë së përgjithshme ushtarake (jo vetëm fuqia ajrore) dhe strategjisë e taktikave, si dhe cilësisë së udhëheqjes ushtarake.

Të gjitha këto burojnë nga toka dhe ushtrohen mbi tokë. Fuqia ajrore mund të jetë vendimtare në krijimin e kushteve operative dhe strategjike, por toka mbetet hapësira ku konsolidohen rezultatet politike dhe ku vuloset përfundimisht fati i konfliktit.

Bibliografia

1. Hobbes, Thomas, *Leviathan*, First Book, Chapter XIII — "Of the Natural Condition of Mankind, as concerning their Felicity, and Misery", 1651.
2. Rousseau, Jean-Jacques, *Discourse on the Origin and Basis of Inequality Among Men,* 1755; "The Social Contract", 1762.
3. Pinker, Steven, *The Better Angels of Our Nature: Why Violence Has Declined,* 2011.
4. Θουκυδίδης Ιστορία του Πελοποννησιακού Πολέμου, (Thukididi, "History of the Peloponnesian War", Book 1, paragraph 23 (1.23), 2022.
5. National Security Strategy of the United States of America, November 2025.
6. The Voice of Ukraine, April 27, 2024. Forbes, Feb. 28, 2025.
7. *The New York Times,* March, 3, 2025
8. *The Times of Israel,* 17 June 2025 and 24 June 2025.
9. Engels, Friedrich, *"The Role of Force in History"* (German: *Die Rolle der Gewalt in der eschichte).*
10. Revue Défense Nationale. Shih linkun: https://www.defnat.com

Ndikimi i normave liberale mbi arkitekturën e sigurisë globale pas Luftës së Ftohtë

Major PhD(c) Hekuran BUDANI
Pedagog i Marrëdhënieve Ndërkombëtare,
Fakulteti i Mbrojtjes dhe i Sigurisë, AFA

Trajtesë e shkurtuar

Pas përfundimit të Luftës së Ftohtë, liberalizmi u konsolidua si paradigma dominuese e rendit ndërkombëtar dhe e arkitekturës globale të sigurisë, duke u mbështetur mbi multilateralizmin, institucionalizimin e bashkëpunimit ndërkombëtar, përhapjen e demokracisë liberale, ndërvarësinë ekonomike dhe të drejtat e njeriut.

Ky artikull analizon nëse tashmë normat liberale e kanë humbur ndikimin e tyre, apo nëse kemi të bëjmë me një reduktim dhe transformim të këtij ndikimi. Përmes analizës së literaturës mbi liberalizmin dhe ilustrimeve nga raste empirike si ndërhyrja në Irak, agresioni Rus në Ukrainë dhe ngritja e Kinës si fuqi globale, argumentohet se nuk bëhet fjalë për fundin e ndikimit liberal, por për fundin e hegjemonisë së tij.

Artikulli argumenton se kriza aktuale në sigurinë globale nuk buron kryesisht nga dështimi i normave liberale, por nga erozioni i kapacitetit hegjemonik që i mbështeti ato pas Luftës së Ftohtë. Ilustrimet empirike tregojnë se normat liberale janë zbatuar në mënyrë selektive (ndërhyrja në Irak), janë sfiduar nga politika e fuqisë (agresioni rus në Ukrainë) dhe janë përdorur pa konvergjencë normative (rritja e Kinës), duke prodhuar tensione të thella midis normave liberale dhe realiteteve gjeopolitike bashkëkohore.

Fjalë kyçe: Liberalizëm, siguri, arkitekturë, rend, institucione, ndërvarësi, demokraci, hegjemoni.

Hyrje

Gjatë Luftës së Ftohtë, rendi ndërkombëtar dhe arkitektura e tij e sigurisë u mbështetën mbi balancimin e fuqisë midis dy superfuqive,

e prodhuar një rend bipolar relativisht të stabilizuar[1]. Përfundimi i Luftës së Ftohtë u perceptua gjerësisht si triumf i liberalizmit mbi alternativat ideologjike rivale. Francis Fukuyama, artikuloi tezën e "fundit të historisë", duke sugjeruar se demokracia liberale dhe kapitalizmi përfaqësonin formën përfundimtare të qeverisjes[2]. Në këtë kontekst, presidenti George H.W. Bush artikuloi për herë të parë idenë e një "Rendi të Ri Botërorë"[3]. Kështu, Shtetet e Bashkuara dhe aleatët e tyre kryesorë synuan ndërtimin e një Rendi Liberal Ndërkombëtar [4]. Ky rend shënonte edhe një largim nga dimensioni strikt politiko-ushtarak i sigurisë dhe përfshiu dy dimensione shtesë: zhvillimin ekonomik dhe mjedisor, si dhe mbrojtjen e të drejtave të njeriut[5].

Në këtë rend liberal, arkitektura e re e sigurisë globale u konceptua si produkt i përhapjes së demokracisë, forcimit të institucioneve ndërkombëtare dhe rritjes së ndërvarësisë ekonomike. Ajo synonte garantimin e sigurisë për të gjitha shtetet, pavarësisht madhësisë, nivelit të zhvillimit apo fuqisë së tyre ekonomike. Në këtë kuptim, liberalizmi nuk u paraqit thjesht si një teori shpjeguese e rendit ndërkombëtar, por si një projekt normativ dhe politik me pretendime universale. Ai dominoi rendin ndërkombëtar gjatë viteve 1990–2008, periudhë që shpesh përshkruhet si "moment liberal". Hegjemonia amerikane, ndonëse e diskutueshme dhe herë pas here e kontestuar, ka qenë vendimtare për ruajtjen e këtij rendi. E përshkruar edhe si "liberal Leviathan"[6], kjo hegjemoni kontribuoi në reduktimin e përplasjeve të drejtpërdrejta ndërshtetërorë.

Megjithatë, pavarësisht përpjekjeve të shumta, arkitektura e sigurisë globale pas Luftës së Ftohtë mbetet larg realizimit të nivelit të sigurisë të parashikuar nga vizioni liberal dhe për më tepër, po përjeton një rënie të dukshme në dimensionet e saj kryesore. Dështimet praktike në Irak dhe Afganistan[7],

[1] Një sërë argumentesh strukturore shpjegojnë paqen relative gjatë Luftës së Ftohtë, përfshirë avantazhin parandalues të krijuar nga armët bërthamore, kapacitetet efektive të diferencës së NATO-s dhe thjeshtësinë relative të balancimit të fuqisë në një sistem bipolar. *Shiko*, Campbell, Kurt, et al. 2016. *Extending American Power: Strategies to Expand U.S. Engagement in a Competitive World Order*. Washington, D.C.: (Center for a New American Security, 2016), fq.19.

[2] Fukuyama, Francis. *The End of History and the Last Man. New York* (Free Press, 1992), fq. 18.

[3] Studiuesit zakonisht e përkufizojnë rendin ndërkombëtar si norma, rregulla dhe institucione që udhëheqin sjelljen e shteteve, shiko, Glaser, Charles L. "*A Flawed Framework: Why the Liberal International Order Concept Is Misguided*." (International Security 43, 2019), fq.51–87.

[4] Rendi Liberal Ndërkombëtar përbëhet nga një sërë elementesh, përfshirë dominimin e fuqisë amerikane, aleancat e SHBA-së në Evropë dhe Azi, sistemin e hapur ekonomik ndërkombëtar dhe Organizatën e Kombeve të Bashkuara. Shiko, Patrick, Stewart. "*World Order: What, Exactly, Are the Rule*s?" (Washington Quarterly 39, 2016): fq.7–27.

[5] Walt, Stephen M. "The Renaissance of Security Studies." *International Studies Quarterly* 35, (1991): fq.211–239.

[6] G. John Ikenberry, *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Princeton, NJ: Princeton University Press, 2011), fq.10.

[7] Chandler, David. *Empire in Denial: The Politics of State-Building*. London, (Pluto Press, 2006).

agresioni rus ndaj Ukrainës dhe ngritja ekonomike e Kinës[8] minuan autoritetin liberal. Paralelisht, multilateralizmi është dobësuar nga bllokimet në Këshillin e Sigurimit[9], ndërsa populizmi në Perëndim ka reduktuar gatishmërinë për angazhime globale[10]. Këto ngjarje kanë ekspozuar kufijtë praktikë dhe normativë të rendit liberal, duke ushqyer argumente se arkitektura e sigurisë globale e ndërtuar pas Luftës së Ftohtë po përjeton një proces të thellë erozioni. Për rrjedhojë, artikulli synon të trajtojë pyetjen themelore: a po jetojmë fundin e ndikimit të normave liberale mbi sigurinë globale?

Struktura e artikullit është si vijon. Seksioni i parë paraqet kornizën teorike mbi liberalizmin dhe ndikimin e normave liberale mbi Arkitekturën e Sigurisë Globale pas Luftës së Ftohtë. Seksionet empirike analizojnë tre raste studimore që ilustrojnë tensionet midis normave liberale dhe realiteteve gjeopolitike. Më pas, artikulli zhvillon një diskutim teorik krahasues mbi liberalizmin, duke e vendosur atë në dialog kritik me qasjen realiste. Në përfundim, nxirren implikimet kryesore për të kuptuar të ardhmen e normave liberale në raport me sigurisë globale në shekullin XXI.

1. Koncepti liberal i sigurisë dhe ndikimi mbi arkitekturën e sigurisë globale pas Luftës së Ftohtë

Konceptimi liberal i sigurisë ofron një kuptim më të gjerë se sa ai tradicional, i cili fokusohet kryesisht te fuqia ushtarake dhe balancimi i saj Ndryshe nga realizmin që e sheh sistemin ndërkombëtar si thelbësisht anarkik dhe të dominuar nga konkurrenca për pushtet, liberalizmi thekson rolin e institucioneve, normave, ndërvarësisë ekonomike dhe regjimeve politike në zbutjen e anarkisë dhe në menaxhimin e konflikteve[11]. Në qendër të qasjes liberale qëndron ideja se, megjithëse anarkia mbetet një tipar strukturor i sistemit ndërkombëtar, efektet e saj nuk janë të pa menaxhueshme.

Pas përfundimit të Luftës së Ftohtë, ndërtimi i arkitekturës globale të sigurisë u shoqërua me një ndikim të paprecedentë të normave liberale, të cilat u shndërruan në elemente themelore të rendit liberal botëror. Ndryshe nga periudha bipolare, ku siguria konceptohej kryesisht në terma të balancimit ushtarak dhe deterrencës bërthamore, epoka pas vitit 1991 u karakterizua nga përpjekja për ta rikonceptuar sigurinë si një proces normativ, institucional dhe bashkëpunues. Në këtë kuadër, normat liberale nuk u shfaqën thjesht si ideale morale, por si mekanizma strukturues të arkitekturës së sigurisë globale.

Një shtyllë qendrore e liberalizmit në menaxhimin e anarkisë janë institucionet

[8] John J. Mearsheimer, *The Great Delusion:* (CT: Yale University Press, 2019).
[9] Stewart Patrick, *The Sovereignty Wars:* (DC: Brookings Institution Press, 2017).
[10] Colgan, Jeff D., and Robert O. Keohane. "*The Liberal Order Is Rigged: Fix It Now or Watch It Withe*." (Foreign Affairs *96, 2017*): fq.36–44.
[11] Daniel Deudney and G. John Ikenberry, "*The Nature and Sources of Liberal International Order*," (*Review of International Studies* 25, 1999): fq.179–196.

ndërkombëtare. Institucionet nuk shihen si zëvendësim i shteteve, por si mekanizma që strukturojnë ndërveprimin e tyre, duke rritur transparencën dhe duke forcuar besueshmërinë[12]. Liberalizmi pas Luftës së Ftohtë promovoi idenë se menaxhimi i sigurisë globale duhet të realizohet përmes multilateralizmit në institucionet ndërkombëtare, në vend të veprimit unilateral të shteteve të fuqishme[13]. Organizata si OKB-ja, NATO-ja, OSBE-ja u konsideruan jo vetëm instrumente bashkëpunimi, por edhe bartëse të normave që kufizonin përdorimin arbitrar të forcës dhe promovonin zgjidhjen paqësore të mosmarrëveshjeve.

Megjithatë, literatura liberale ashtu si dhe ajo realiste pranon se institucionet nuk janë të pavarura nga shpërndarja e fuqisë. Ato reflektojnë, në një masë të caktuar, interesat e aktorëve më të fuqishëm dhe varen nga mbështetja e tyre për funksionimin efektiv.[14] Kjo varësi strukturore bëhet veçanërisht problematike në kushtet e dobësimit të hegjemonisë që i ka mbështetur këto institucione.

Rendi liberal pas Luftës së Ftohtë u shfaq si një rend hegjemonik i institucionalizuar, ku fuqia amerikane shërbente si garanci e fundit për zbatimin e rregullave dhe normave.[15] Siç e përshkruan G. John Ikenberry, ky rend funksiononte përmes një kombinimi të fuqisë dhe legjitimitetit normativ. Dobësimi relativ i hegjemonisë amerikane dhe fragmentimi i konsensusit perëndimor kanë nxjerrë në pah kufijtë e këtij modeli multilateral. Në mungesë të një aktori të gatshëm dhe të aftë për të mbajtur barrën e rendit, institucionet liberale përballen me vështirësi në imponimin e normave dhe në menaxhimin e krizave të sigurisë. Kjo situatë ka çuar në atë që Amitav Acharya e përshkruan si një rend liberal *"post-hegjemon"*[16], ku liberalizmi bashkëjeton me modele alternative të rendit ndërkombëtar.

Një element tjetër thelbësor i kornizës liberale është ndërvarësia ekonomike. Liberalizmi argumenton se rritja e tregtisë së lirë, investimeve dhe lidhjeve ekonomike ndërmjet shteteve rrit kostot e konfliktit dhe krijon incentiva të forta për paqe dhe stabilitet[17]. Në këtë perspektivë, siguria globale nuk arrihet vetëm përmes deterrencës ushtarake, por edhe përmes integrimit ekonomik. Ky supozim luajti një rol kyç në ndërtimin e arkitekturës së sigurisë pas Luftës së Ftohtë. Zgjerimi i tregjeve, integrimi ekonomik i Evropës Lindore dhe hapja e ekonomive post-socialiste u panë si mekanizma të dyfishtë të zhvillimit dhe stabilitetit. Në këtë kuptim, arkitektura e sigurisë u ndërthur ngushtë me

[12] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 2005).

[13] Keohane, *After Hegemony.*

[14] Keohane, *After Hegemony.*

[15] William C. Wohlforth, "*The Stability of a Unipolar World*" (*International Security* 24, 1999),

[16] Amitav Acharya, *The End of American World Order*, 2nd ed. (Cambridge: Polity Press, 2018), fq.47.

[17] Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown and Company, 1977), fq. 24–29.

arkitekturën e ekonomisë globale, duke e zgjeruar fushën e sigurisë përtej dimensionit ushtarak. Megjithatë, zhvillimet aktuale tregojnë se, ndërvarësia ekonomike nuk garanton domosdoshmërisht moderim strategjik, veçanërisht kur ajo shoqërohet me asimetri të theksuara fuqie dhe interesa konkurruese[18].

Një tjetër komponent qendror i liberalizmit është lidhja ndërmjet demokracisë dhe paqes. Teza e *"paqes demokratike"* sugjeron se shtetet demokratike kanë gjasa më të ulëta të hyjnë në luftë me njëra-tjetrën, duke e bërë përhapjen e demokracisë një instrument të rëndësishëm të sigurisë globale[19]. Si rezultat, zgjerimi i NATO-s dhe Bashkimit Evropian u justifikua jo vetëm në terma gjeostrategjikë, por edhe si proces normativ që synonte konsolidimin e paqes përmes institucioneve demokratike. Kjo ide justifikoi zgjerimin e institucioneve perëndimore por edhe ndërhyrjet ushtarake në emër të demokracisë dhe të drejtave të njeriut.

Në këtë kontekst, të drejtat e njeriut u institucionalizuan si normë themelore e arkitekturës së sigurisë ndërkombëtare pas Luftës së Ftohtë. Siguria nuk u konceptua më vetëm si mungesë e agresionit ushtarak ndërshtetëror, por edhe si mbrojtje nga gjenocidi, krimet e luftës, spastrimi etnik dhe krimet kundër njerëzimit. Ky zgjerim normativ i konceptit të sigurisë u reflektua në rritjen e misioneve paqeruajtëse dhe ndërhyrjeve ndërkombëtare me mandat për mbrojtjen e civilëve.

Kjo qasje u pasqyrua në doktrina dhe praktika të reja të sigurisë, përfshirë ndërhyrjet humanitare dhe konceptin e "Përgjegjësisë për të Mbrojtur" (R2P), të cilat e zhvendosën fokusin nga siguria e shtetit drejt sigurisë së individit. Ndryshe nga interpretimi strikt Westfalian, sovraniteti pas Luftës së Ftohtë u kushtëzua gjithnjë e më shumë nga sjellja e brendshme e shteteve, veçanërisht në raport me të drejtat e njeriut dhe sundimin e ligjit. OKB-ja dhe NATO-ja zhvilluan instrumente të menaxhimit të krizave dhe ndërmorën misione të reja paqeruajtëse, ndërsa doktrina e përgjegjësisë për të mbrojtur "*Responsibility to Protect (R2P)*"[20] u institucionalizua.

Megjithatë, ndikimi i normave liberale në ndërtimin e arkitekturës së sigurisë nuk ishte as linear dhe as i pakontestuar. Një problem thelbësor lidhej me zbatimin selektiv të normave. Ndërsa rendi liberal pretendonte universalitet normativ, në praktikë normat u zbatuan në mënyrë të pabarabartë, shpesh

[18] John J. Mearsheimer, *The Great Delusion: Liberal Dreams and International Realities* (New Haven, CT: Yale University Press, 2019), fq.45–48**.**

[19] Bruce Russett and John R. Oneal, *Triangulating Peace: Democracy, Interdependence, and International Organizations* (New York: W. W. Norton & Company, 2001), fq.35–38.

[20] Përgjegjësia për të Mbrojtur (Responsibility to Protect – R2P) është një element qendror i angazhimit të komunitetit ndërkombëtar për të mbrojtur popullsitë nga katër krime themelore: gjenocidi, krimet e luftës, spastrimi etnik dhe krimet kundër njerëzimit, në rastet kur shteti ka dështuar qartazi të mbrojë popullsinë e vet nga një ose më shumë prej këtyre krimeve. Alex J. Bellamy, *Responsibility to Protect: The Global Effort to End Mass Atrocities* (Cambridge: Polity Press, 2009), fq.5-40.

në përputhje me interesat e fuqive të mëdha. Ky hendek midis normës dhe praktikës minoi legjitimitetin e arkitekturës së sigurisë dhe krijoi perceptimin se: normat liberale funksiononin si instrumente politike dhe jo si rregulla të barabarta për të gjithë[21].

Sipas realistëve, institucionet dhe normat kanë ndikim të kufizuar përballë fuqisë dhe interesave strategjike të shteteve[22]. John J. Mearsheimer argumenton se rendi liberal pas Luftës së Ftohtë ishte një anomali historike, e mundësuar nga unipolariteti amerikan, dhe se rikthimi i konkurrencës së fuqive të mëdha ishte i pashmangshëm[23]. Edhe pse rendi pas Luftës së Ftohtë u paraqit si i bazuar në rregulla dhe konsensus, fuqia amerikane luajti rol kyç në promovimin, zbatimin dhe në disa raste, anashkalimin e këtyre normave[24]. Dobësimi relativ i kësaj hegjemonie ekspozoi brishtësinë e një arkitekture sigurie që mbështetej fuqishëm në një aktor të vetëm për garantimin e normave liberale të tij.

2. Ilustrim empirik i tensionit ndërmjet normave liberale dhe realitetit gjeopolitik

2.1 Iraku: legjitimiteti, unilateralizmi dhe erozioni i normave

Ndërhyrja ushtarake në Irak në vitin 2003 përfaqëson një nga rastet më domethënëse për të analizuar tensionin midis parimeve normative të liberalizmit ndërkombëtar dhe praktikës konkrete të sigurisë së udhëhequr nga hegjemonia amerikane. Ky rast ilustron qartë se si arkitektura liberale e sigurisë, e ndërtuar mbi bashkëpunimin shumëpalësh, respektimin e së drejtës ndërkombëtare dhe legjitimitetin institucional, mund të minohet nga zbatimi selektiv i këtyre normave në emër të interesave strategjike.Në diskursin zyrtar, ndërhyrja në Irak u justifikua përmes një kombinimi argumentesh që përfshinin:

- kërcënimin e armëve të shkatërrimit në masë;
- lidhjet e supozuara me terrorizmin ndërkombëtar; dhe
- nevojën për promovimin e demokracisë dhe të drejtave të njeriut.

Këto argumente u paraqitën si pjesë e një narrative liberale të sigurisë kolektive, ku përdorimi i forcës shihej si mjet i domosdoshëm për mbrojtjen e rendit ndërkombëtar dhe stabilitetin global. Megjithatë, mungesa e një mandati të qartë nga Këshilli i Sigurimit të Kombeve të Bashkuara e vuri në pikëpyetje legjitimitetin ndërkombëtar të ndërhyrjes dhe nxori në pah kufijtë praktikë të multilateralizmit liberal.

Pasojat e ndërhyrjes në Irak për arkitekturën e sigurisë globale ishin të

[21] Randall L. Schweller, "The Problem of International Order Revisited: A Review Essay," *International Security* 26, nr. 1 (2001): fq.161–162.

[22] Kenneth N. Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979), fq.161–170.

[23] *Mearsheimer, John J.* The Great Delusion, fq. 30–33.

[24] G. John Ikenberry, *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Princeton, NJ: Princeton University Press, 2011).

shumta dhe afatgjata. Nga perspektiva teorike, rasti i Irakut evidenton një kontradiktë thelbësore: ndërsa arkitektura e sigurisë ndërkombëtare pretendonte të funksiononte mbi bazën e rregullave dhe institucioneve të përbashkëta, zbatimi i saj mbeti thellësisht i varur nga vullneti dhe kapaciteti i aktorit hegjemonik. Në këtë kuptim, ndërhyrja në Irak nuk përfaqëson thjesht një devijim nga normat liberale, por një shfaqje e tensionit midis hegjemonisë dhe institucionalizimit liberal [25]

Unilateralizmi që shoqëroi ndërhyrjen e vitit 2003 kontribuoi në erozionin e legjitimitetit të rendit liberal ndërkombëtar. Aleatët tradicionalë u përçanë, institucionet shumëpalëshe u anashkaluan dhe narrativa e sigurisë kolektive u zëvendësua nga logjika e veprimit parandalues dhe të vetëmjaftueshmërisë. Kjo situatë përforcoi kritikat realiste se institucionet ndërkombëtare funksionojnë vetëm për aq kohë sa përputhen me interesat e fuqive kryesore dhe se, në momentet e krizës, politika e fuqisë mbizotëron mbi normat [26]. Ikenberry argumenton se rendi liberal pas Luftës së Ftohtë ishte i qëndrueshëm jo vetëm për shkak të fuqisë amerikane, por sepse kjo fuqi ishte e "vetëkufizuar" përmes institucioneve dhe rregullave [27]. Rasti i Irakut përfaqëson pikërisht momentin kur ky vetëkufizim u shkel, duke ekspozuar rendin liberal ndaj kritikave të brendshme dhe të jashtme. Në planin rajonal, ndërhyrja kontribuoi në destabilizimin e Lindjes së Mesme, duke nxitur konflikte të reja sektare, rritjen e grupeve ekstremiste dhe dobësimin e strukturave shtetërore. Në planin global, ajo minoi besimin në institucionet liberale si mekanizma efektivë të menaxhimit të sigurisë dhe krijoi një precedent problematik për përdorimin e forcës jashtë kuadrit të së drejtës ndërkombëtare.

Gjithashtu, ky precedent pati implikime të drejtpërdrejta për mënyrën se si aktorë të tjerë ndërkombëtarë e perceptuan rendin liberal. Shtete me prirje revizioniste e interpretuan ndërhyrjen në Irak si dëshmi se normat liberale zbatohen në mënyrë selektive dhe se sovraniteti mund të anashkalohet nëse bie ndesh me interesat e fuqive perëndimore. Në këtë kuptim, rasti i Irakut kontribuoi indirekt në dobësimin e normave që më vonë do të sfidoheshin në mënyrë më të hapur në kontekste të tjera, si Gjeorgjia në vitin 2008 dhe Ukraina në vitin 2014 dhe vitin 2022.

Në këtë kontekst, ndërhyrja në Irak mund të interpretohet si një pikë kthese në tranzicionin nga një rend liberal hegjemonik drejt një rendi më të fragmentuar dhe më pak konsensual. Ndërsa liberalizmi si paradigmë normative humbi një pjesë të rëndësishme të autoritetit të tij moral dhe institucional. Kjo humbje autoriteti e bëri më të vështirë mobilizimin e mbështetjes ndërkombëtare për

[25] G. John Ikenberry, *Liberal Leviathan,* fq. 200–205.

[26] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton & Company, 2001), fq.19–22.

[27] G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* (Princeton, NJ: Princeton University Press, 2001), fq.23–27.

iniciativa të mëvonshme të sigurisë dhe dobësoi kapacitetin e institucioneve liberale për të vepruar si arbitra legjitimë në konfliktet globale. Rasti i Irakut thekson kufijtë e eksportit të demokracisë si instrument i sigurisë globale.[28] Supozimi liberal se ndryshimi i regjimeve autoritare do të /sillte stabilitet dhe paqe problematik në praktikë. Në vend të konsolidimit demokratik, Iraku përjetoi një periudhë të zgjatur pasigurie dhe dhune, duke sfiduar drejtpërdrejt tezën se demokratizimi i imponuar nga jashtë është një mekanizëm efektiv i sigurisë ndërkombëtare.

Në përfundim, ndërhyrja në Irak shërben si rast ilustrues për mënyrën se si arkitektura liberale e sigurisë mund të dobësohet jo nga kundërshtarët e jashtëm, por nga praktikat e vetë aktorëve që pretendojnë ta mbështesin atë. Pa një zbatimi konsistent dhe legjitim të normave liberale, rendi ndërkombëtar ka hyrë në një fazë transformimi, ku liberalizmi bashkëjeton gjithnjë e më shumë me logjikën realiste të fuqisë.

2.2. Ukraina: institucionet liberale përballë politikës së fuqisë

Lufta në Ukrainë përfaqëson një nga sfidat më serioze ndaj arkitekturës së sigurisë globale pas Luftës së Ftohtë dhe një/provë kritik për qëndrueshmërinë e rendit liberal. Ndryshe nga rasti i Irakut, ku normat liberale u minuan nga veprimet e aktorit hegjemonik, rasti i Ukrainës nxjerr ne pah kufijtë e institucioneve liberale përballë një aktori revizionist të gatshëm të përdorë forcën ushtarake për të ndryshuar *status quo*-në territoriale dhe politike[29]. Ky konflikt thekson tensionin strukturor midis premtimeve të sigurisë kolektive liberale dhe realiteteve të politikës së fuqisë në një sistem ndërkombëtar gjithnjë e më konkurrues.

Nga perspektiva liberale, rendi pas Luftës së Ftohtë supozohej të garantonte respektimin e sovranitetit, integritetit territorial dhe zgjidhjen paqësore të mosmarrëveshjeve përmes institucioneve shumëpalëshe. Ukraina u integrua si pjesë e këtij rendi përmes hapjes graduale në ekonominë globale dhe afrimit institucional me Bashkimin Evropian dhe NATO-n, duke u pozicionuar si një shtet "në tranzicion" drejt hapësirës euroatlantike. Megjithatë, kjo lëvizje u perceptua nga Rusia si kërcënim ndaj interesave të saj strategjike dhe sferës së influencës post-sovjetike, duke e shndërruar Ukrainën në një fushë përplasjeje midis logjikës liberale të zgjerimit institucional dhe logjikës realiste të balancimit të fuqisë.

Ndërhyrja ushtarake ruse në Ukrainë, e manifestuar fillimisht përmes aneksimit të Krimesë dhe konfliktit në Donbas në vitin 2014, e intensifikuar më tej me agresionin e plotë pas vitit 2022, përbën një shkelje të drejtpërdrejtë të parimeve themelore të rendit ndërkombëtar. Reagimi i institucioneve liberale

[28] Chandler, David. *From Kosovo to Kabul and Beyond: Human Rights and International Intervention* (London: Pluto Press, 2006), fq.1–22; 67–94.

[29] *Mearsheimer, John J.* The Great Delusion, fq. 33–35

ndaj kësaj shkeljeje ka qenë politikisht i rëndësishëm, por i kufizuar në aspektin e parandalimit të konfliktit. Sanksionet ekonomike, izolimi diplomatik dhe mbështetja ushtarake për Ukrainën përfaqësojnë instrumente tipike të rendit liberal përballë agresionit. Megjithatë, këto masa nuk arritën të parandalonin shpërthimin e luftës dhe as të rikthenin shpejt stabilitetin rajonal. Ky fakt nxjerr në pah një kufizim thelbësor të arkitekturës liberale të sigurisë: varësinë e saj nga konsensusi politik midis aktorëve kryesorë dhe nga mungesa e një mekanizmi efektiv detyrues për ndalimin e agresionit shtetëror në mungesë të ndërhyrjes direkte ushtarake. Nga këndvështrimi realist, konflikti në Ukrainë konfirmon argumentin se institucionet ndërkombëtare nuk mund të zëvendësojnë logjikën e balancimit të fuqisë në një sistem anarkik. Rusia veproi jo si një aktor i integruar në këtë rend normativ, por si një fuqi e madhe që synon të ruajë pozicionin e saj strategjik dhe të pengojë zgjerimin e aleancave rivale pranë kufijve të saj.

Në këtë kuptim, lufta në Ukrainë përfaqëson një rikthim të qartë të politikës së fuqisë dhe të konkurrencës gjeopolitike, duke sfiduar idenë liberale se institucionalizimi dhe ndërvarësia ekonomike janë të mjaftueshme për të garantuar paqen[30]. Megjithatë, mbështetja e Ukrainës përmes përdorimit të sanksioneve si mjet presioni dhe përpjekjet për ruajtjen e unitetit institucional tregojnë se normat liberale vazhdojnë të strukturojnë sjelljen e aktorëve, edhe në kushte konflikti të hapur. Në këtë kuptim, rasti i Ukrainës ilustron një formë hibride të funksionimit të arkitekturës së sigurisë, ku institucionet liberale nuk parandalojnë konfliktin, por shërbejnë si kornizë për menaxhimin e tij dhe për mobilizimin e mbështetjes kolektive kundër shkeljeve ndaj rendit ekzistues. Kjo dinamikë përputhet me argumentin se liberalizmi pas hegjemonisë nuk zhduket, por bashkëjeton me logjika realiste të deterrencës dhe balancimit.

Një aspekt tjetër thelbësor i konfliktit në Ukrainë lidhet me çështjen e garancive të sigurisë. Ukraina, ndonëse e integruar pjesërisht në arkitekturën liberale, nuk gëzonte garanci të plota të mbrojtjes kolektive, gjë që e bëri atë veçanërisht të cenueshme. Ky fakt nxjerr në pah një boshllëk strukturor në rendin liberal: diferencimin midis anëtarëve të plotë dhe partnerëve periferikë, ku angazhimet normative nuk shoqërohen gjithmonë me angazhime të forta të sigurie. Ky boshllëk ka implikime më të gjera për besueshmërinë e arkitekturës liberale, veçanërisht në kontekstin e zgjerimit të institucioneve perëndimore.

Në planin normativ, lufta në Ukrainë ka prodhuar një polarizim të thellë në sistemin ndërkombëtar. Ndërsa shumica e demokracive liberale kanë dënuar agresionin rus dhe kanë mbështetur Ukrainën, një numër i konsiderueshëm shtetesh kanë adoptuar qëndrime më ambigue ose neutrale. Ky fenomen reflekton transformimin e rendit liberal në një mjedis më pluralist dhe më pak universal, ku normat liberale nuk gëzojnë më konsensus të plotë. Në këtë kuptim, konflikti në Ukrainë shërben si tregues i erozionit të autoritetit normativ

[30] Keohane and Nye 1977; Mearsheimer 2019, fq.30–35

të liberalizmit në shkallë globale. Megjithatë, është e rëndësishme të theksohet se rasti i Ukrainës nuk përfaqëson një dështim total të arkitekturës liberale të sigurisë. Përkundrazi, ai nxjerr në pah kapacitetin e saj adaptues në kushte krize. Mobilizimi i shpejtë i mbështetjes ekonomike dhe ushtarake për Ukrainën, koordinimi ndërinstitucional dhe përpjekjet për ruajtjen e unitetit transatlantik tregojnë se institucionet liberale vazhdojnë të luajnë një rol qendror në strukturimin e reagimeve kolektive.

Në përmbledhje, agresioni rus në Ukrainë përfaqëson një sfidë të shumëfishtë për arkitekturën e sigurisë ndërkombëtare pas Luftës së Ftohtë.

Ai konfirmon kufijtë e institucioneve liberale përballë politikës së fuqisë, por njëkohësisht demonstron se liberalizmi nuk është zhdukur si kornizë normative dhe institucionale. Ashtu si rasti i Irakut, konflikti në Ukrainë mbështet tezën qendrore të këtij artikulli: kriza aktuale e sigurisë globale nuk duhet kuptuar si dështim normave liberale, por si dobësim i hegjemonisë që e mbështeti atë. Në një rend post-hegjemonik, siguria globale prodhohet përmes një ndërveprimi kompleks midis normave liberale, interesave gjeopolitike dhe balancave të fuqisë, duke e bërë arkitekturën e sigurisë më të fragmentuar, por jo tërësisht të shkatërruar.

2.3. Ngritja e Kinës: integrim ekonomik pa konvergjencë në vlera

Ngritja e Kinës përbën sfidën më të thellë strukturore ndaj rendit liberal ndërkombëtar pas Luftës së Ftohtë. Ndryshe nga rasti i Irakut, ku u minuan normat liberale nga veprimi unilateral i hegjemonit, dhe nga rasti i Ukrainës, ku një aktor revizionist sfidoi drejtpërdrejt rendin ekzistues përmes forcës ushtarake, Kina përfaqëson një sfidë më të heshtur, por potencialisht më transformuese: integrim të thellë ekonomik brenda rendit liberal, pa konvergjencë politike dhe demokratike.

Një nga supozimet themelore të liberalizmit pas Luftës së Ftohtë ishte se integrimi në ekonominë globale dhe institucionet ndërkombëtare do të prodhonin gradualisht konvergjencë politike dhe demokratike. Ky supozim, i rrënjosur në teoritë e ndërvarësisë komplekse, sugjeronte se tregtia e lirë, rritja ekonomike dhe institucionalizimi do të ushtronin presion për liberalizim politik dhe demokratik. Kina u shndërrua në testi më i rëndësishëm empirik i kësaj teze. Që nga reformat ekonomike të fundviteve 1970 dhe, veçanërisht, pas anëtarësimit në Organizatën Botërore të Tregtisë në vitin 2001, Kina u integrua thellësisht në ekonominë globale, duke u u bërë një aktor qendror të tregtisë ndërkombëtare, zinxhirëve globalë të furnizimit dhe financës ndërkombëtare[31].

Nga perspektiva liberale, ky integrim pritej të forconte interesat e Kinës në ruajtjen e rendit ekzistues dhe me kalimin e kohës, të prodhonte konvergjencë

[31] Xing, Li. *The Rise of China and the Liberal World Order* (London: Routledge, 2022), fq.61–84

drejt standardeve liberale dhe demokratike të qeverisjes.

Megjithatë, zhvillimet e dy dekadave të fundit tregojnë se ky supozim ka qenë, të paktën pjesërisht, i gabuar. Kina jo vetëm që nuk ka përqafuar liberalizmin politik, por ka konsoliduar një model alternativ zhvillimi, të bazuar në autoritarizëm politik, kapitalizëm shtetëror dhe një koncept sovraniteti të fortë. Ky model nuk e refuzon rendin liberal në tërësi, por e përzgjedh dhe e instrumentalizon atë në funksion të interesave kombëtare kineze.

Nga kjo perspektivë, rasti i Kinës përputhet me argumentin e G. John Ikenberry se rendi liberal është mjaft elastik për të përfshirë aktorë jo-liberalë, por njëkohësisht ekspozon kufijtë e tij normativë[32]. Kina është bërë një përfituese kryesore e rendit liberal ekonomik, pa u shndërruar në një promotore të normave politike liberale. Kjo ka krijuar një tension të brendshëm në arkitekturën e sigurisë dhe ekonomisë globale: një rend i bazuar në rregulla liberale, por i përdorur gjithnjë e më shumë nga aktorë që nuk i ndajnë ato rregulla në dimensionin normativ.

Në aspektin e sigurisë, ky tension është bërë gjithnjë e më i dukshëm. Kina ka rritur ndjeshëm kapacitetet e saj ushtarake, ka zgjeruar praninë e saj strategjike në Indo-Paqësor dhe ka adoptuar një qasje më kërkuese në çështje si Deti i Kinës Jugore dhe Tajvani. Këto zhvillime sfidojnë drejtpërdrejt supozimin liberal se ndërvarësia ekonomike redukton gjasat e konfliktit. Përkundrazi, rasti kinez sugjeron se rritja ekonomike mund të përkthehet në rritje të kapaciteteve ushtarake dhe ambicieve gjeopolitike, pa prodhuar domosdoshmërisht moderim strategjik.

Nga këndvështrimi realist, ngritja e Kinës konfirmon logjikën strukturore të konkurrencës së fuqive të mëdha. Siç do të argumentonte John J. Mearsheimer, një fuqi në rritje ka incentiva strukturore për të sfiduar rendin ekzistues dhe për të kërkuar dominim rajonal[33]. Në këtë lexim, integrimi i Kinës në rendin liberal nuk ishte një proces transformues, por një fazë e përkohshme që i mundësoi asaj të akumulonte fuqi brenda sistemit përpara se të sfidonte elementët e tij.

Megjithatë, ky interpretim realist nuk e kap plotësisht kompleksitetin e sjelljes kineze. Kina nuk ka synuar deri më tani një përmbysje të drejtpërdrejtë të rendit liberal global, por një riformësim selektiv të tij. Iniciativa si "Belt and Road" dhe krijimi i institucioneve alternative financiare nuk përfaqësojnë një refuzim të multilateralizmit, por një version paralel të tij, më pak liberal dhe më të përqendruar në sovranitet dhe interesa shtetërore. Ky aspekt i modelit kinez lidhet me ndikimin e tij normativ në Jugun Global. Ndryshe nga modeli liberal perëndimor, i cili shpesh shoqërohet me kushte normative dhe institucionale, modeli kinez i bashkëpunimit ekonomik thekson parimin e mosndërhyrjes dhe sovranitetit. Kjo e bën atë tërheqës për shumë shtete në zhvillim dhe kontribuon

[32] Ikenberry (2011), fq.58–62
[33] Mearsheimer (2019), fq.31–36

në erozionin e autoritetit normativ të liberalizmit në shkallë globale. Në këtë kuptim, sfida kineze nuk është vetëm materiale, por edhe ideologjike dhe normative.

Megjithatë, është e rëndësishme të theksohet se Kina mbetet thellësisht e ndërvarur nga rendi ekonomik global dhe nga stabiliteti i tij. Kjo ndërvarësi krijon nxitje për vetëpërmbajtje dhe për shmangien e një përplasjeje të drejtpërdrejtë. Kështu, ndryshe nga parashikimet, rasti i Kinës nuk sugjeron një kolaps të menjëhershëm të rendit liberal, por një transformim gradual drejt një rendi më të fragmentuar dhe më pak normativ.

3. Analizë krahasuese

Analiza e tre rasteve empirike - Irakut, Ukrainës dhe Kinës, ofron një panoramë të shumëdimensionale të krizës aktuale të arkitekturës së sigurisë globale pas Luftës së Ftohtë. Ndonëse këto raste ndryshojnë ndjeshëm për nga konteksti gjeopolitik, aktorët e përfshirë dhe mekanizmat e veprimit, ato ndajnë një tipar të përbashkët analitik: secili ekspozon kufijtë e rendit liberal në kushtet e post-hegjemonisë amerikane dhe konfirmojnë tezën se kriza aktuale nuk lidhet me rënien normave liberale si qasje, por dobësimi i hegjemonisë që e mbështeste atë.

Rasti i Irakut përfaqëson një krizë të legjitimitetit normativ nga brenda rendit liberal. Kjo krijon një precedent të rrezikshëm: normat liberale u shndërruan nga kufizime të detyrueshme në instrumente selektive, të përdorshme ose të anashkalueshme në varësi të interesit strategjik. Në këtë kuptim, Iraku simbolizon momentin kur rendi liberal filloi të humbasë autoritetin e tij moral dhe normativ.

Në kontrast, rasti i Ukrainës ilustron dobësi të kapacitetit parandalues të institucioneve liberale përballë një aktori revizionist. Ndryshe nga Iraku, këtu normat liberale nuk u shkelën nga brenda, por u sfiduan hapur nga jashtë. Rasti i Kinës, nga ana tjetër, përfaqëson një sfidë strukturore dhe afatgjatë, e cila nuk manifestohet përmes shkeljeve të drejtpërdrejta ushtarake apo anashkalimeve të hapura të normave, por përmes integrimit selektiv dhe transformues brenda rendit liberal. Ky rast sfidon një nga supozimet më të forta të liberalizmit strukturor: idenë se ndërvarësia ekonomike dhe institucionalizimi prodhojnë liberalizim politik dhe moderim strategjik. Së bashku, këto tre raste formojnë një tipologji të krizës së rendit liberal. Iraku tregon se rendi liberal mund të minohet nga vetë hegjemonia që e ndërtoi; Ukraina tregon se ai ka vështirësi të përballojë sfidat e politikës së fuqisë në mungesë të deterrencës së drejtpërdrejtë; ndërsa Kina tregon se rendi liberal mund të bashkëjetojë me modele alternative të rendit politik pa i transformuar ato. Ky kombinim e bën aktualisht arkitekturën e sigurisë globale më të fragmentuar dhe më pak koherente sesa në periudhën e menjëhershme pas Luftës së Ftohtë. Megjithatë në asnjë nga këto raste nuk vërehet një zhdukje e plotë e institucioneve liberale apo e normave që i shoqërojnë ato. Përkundrazi, institucionet vazhdojnë të ekzistojnë, të përdoren dhe të mobilizojnë aktorë,

por jo më si autoriteti i vetëm dhe i pakontestuar i rendit global. Ky realitet përforcon idenë se arkitektura e sigurisë pas Luftës së Ftohtë nuk po përjeton një kolaps total, por një tranzicion post-hegjemonik.

Përfundime

Ky artikull ka shqyrtuar në mënyrë kritike transformimin e arkitekturës së sigurisë ndërkombëtare pas Luftës së Ftohtë, duke vlerësuar nëse zhvillimet e dekadave të fundit përfaqësojnë fundin e impaktit të liberalizmit mbi sigurinë globale apo përkundrazi, një transformim të rolit dhe funksionit të tij në një rend ndërkombëtar në ndryshim. Përmes një kombinimi të analizës teorike dhe shqyrtimit empirik të tre rasteve kyçe – Irakut, Ukrainës dhe Kinës – artikulli ka argumentuar se kriza aktuale e sigurisë globale nuk duhet interpretuar si kolaps i liberalizmit, por si fund i hegjemonisë që e mbështeti atë si paradigmë dominuese.

Analiza teorike tregoi se liberalizmi pas Luftës së Ftohtë u ndërtua mbi dy shtylla kryesore: institucionalizimin e rendit ndërkombëtar dhe udhëheqjen hegjemonike amerikane. Ndërsa institucione të tilla si OKB-ja, NATO-ja dhe regjimet ndërkombëtare të tregtisë synonin të garantonin stabilitet dhe parashikueshmëri, hegjemonia amerikane shërbeu si garanci për funksionimin e këtij rendi. Dobësimi relativ i kësaj hegjemonie, fragmentimi i konsensusit perëndimor dhe rritja e aktorëve alternativë kanë ekspozuar kufijtë strukturorë të këtij modeli, duke e zhvendosur liberalizmin nga pozita e dominimit universal drejt një forme bashkëjetese paradigmatike.

Analiza krahasuese e Irakut, Ukrainës dhe Kinës konfirmoi argumentin qendror të këtij artikulli: dobësimi i arkitekturës së sigurisë ndërkombëtare pas Luftës së Ftohtë nuk buron kryesisht nga dështimi i teorisë liberale, por nga transformimi i kontekstit strukturor ku ajo operon. Liberalizmi nuk ka humbur relevancën e tij, por ka humbur hegjemoninë. Në një rend global gjithnjë e më multipolar, siguria prodhohet përmes një kombinimi të mekanizmave liberale dhe balancimit të fuqisë, duke e bërë arkitekturën e sigurisë më komplekse, më kontradiktore dhe më pak të parashikueshme. Kjo nënkupton se arkitektura e ardhshme e sigurisë nuk do të jetë as plotësisht liberale, as thjesht realiste, por një konfigurim hibrid që reflekton realitetet e një bote multipolare.

Arkitektura e ardhshme e sigurisë globale do të karakterizohet nga rikthimi i balancimit të fuqisë si element strukturor**,** edhe pse në forma më hibride. Ndryshe nga modeli klasik realist i balancimit ushtarak, balancimi bashkëkohor do të përfshijë dimensione ekonomike, teknologjike, energjetike dhe informative. Siguria nuk do të përcaktohet vetëm nga kapacitetet ushtarake, por edhe nga kontrolli mbi zinxhirët e furnizimit, teknologjitë kritike, hapësira kibernetike dhe narrativat strategjike. Kjo e bën arkitekturën e sigurisë më komplekse dhe më pak të parashikueshme.

Liberalizmi do të mbijetojë si kornizë konceptuale dhe proceduriale, jo si projekt transformues global. Normat liberale – sundimi i ligjit ndërkombëtar, transparenca, bashkëpunimi shumëpalësh – do të vazhdojnë të strukturojnë sjelljen e një pjese të rëndësishme të aktorëve ndërkombëtarë, veçanërisht në Perëndim. Megjithatë, ato nuk do të funksionojnë më si standard universal i rendit ndërkombëtar, por si një nga disa modelet konkurruese të organizimit të sigurisë globale. Në këtë kuptim, liberalizmi do të jetë më shumë një "regjim rajonal" ose "komunitet normativ" sesa një arkitekturë globale gjithëpërfshirëse. Së fundmi, ky diskutim ka implikime të rëndësishme për studimin akademik të marrëdhënieve ndërkombëtare. Ai sugjeron nevojën për të kapërcyer ndarjen binare midis liberalizmit dhe realizmit dhe për të adoptuar qasje më përfshirëse dhe më reflektuese ndaj sigurisë në shekullin XXI.

Bibliografia

1. Acharya, Amitav. *The End of American World Order*, 2nd ed. Cambridge: Polity Press, (2018), fq. 87–109.
2. Bellamy, Alex J. *Responsibility to Protect: The Global Effort to End Mass Atrocities* Cambridge: Polity Press, (2009), fq.19–37.
3. Buzan, Barry, and Ole Waver. *Regions and Powers: The Structure of International Security* Cambridge: Cambridge University Press, (2003), fq.43–72.
4. Campbell, Kurt M., et al. *Extending American Power: Strategies to Expand U.S. Engagement in a Competitive World Order* Washington, DC: Center for a New American Security, 2016, fq.15–25.
5. Chandler, David. *Empire in Denial: The Politics of State-Building* London: Pluto Press, (2006), fq.27–48.
6. Chandler, David. *From Kosovo to Kabul and Beyond: Human Rights and International Intervention* London: Pluto Press, (2006), fq.1–22; 67–94.
7. Colgan, Jeff D., and Robert O. Keohane. "The Liberal Order Is Rigged: Fix It Now or Watch It Wither." *Foreign Affairs* 96, nr. 3 (2017): fq.36–44.
8. Deudney, Daniel, and G. John Ikenberry. "The Nature and Sources of Liberal International Order." *Review of International Studies* 25, nr. 2 (1999): fq.179–196.
9. Fukuyama, Francis. *The End of History and the Last Man* New York: Free Press, (1992), fq.55–70.
10. Glaser, Charles L., "A Flawed Framework: Why the Liberal International Order Concept Is Misguided." *International Security* 43, nr. 4 (2019).
11. Gowan, Richard. *The UN at War: Peace Operations in a New Era* Washington, DC: Brookings Institution Press, (2018), fq.112–139.

12. Hopmann, P. Terrence. *Negotiating the Security Dilemma* Ann Arbor: University of Michigan Press, (2005), fq.101–129.
13. Ikenberry, G. John. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* Princeton, NJ: Princeton University Press, (2001), fq.39–72.
14. Ikenberry, G. John. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* Princeton, NJ: Princeton University Press, (2011), fq.10–16; 58–62.
15. Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy* Princeton, NJ: Princeton University Press, (2005), fq.49–76.
16. Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence* Boston: Little, Brown, (1977), fq.24–49.
17. Mearsheimer, John J. *The Tragedy of Great Power Politics* New York: W. W. Norton, (2001), fq. 29–54.
18. Mearsheimer, John J. *The Great Delusion: Liberal Dreams and International Realities* New Haven, CT: Yale University Press, (2019).
19. Patrick, Stewart. "World Order: What, Exactly, Are the Rules?" *Washington Quarterly* 39 (2016): fq.7–27.
20. Russett, Bruce, and John Oneal. *Triangulating Peace: Democracy, Interdependence, and International Organizations* New York: W. W. Norton, (2001), fq.128–156.
21. Schweller, Randall L. *Deadly Imbalances: Tripolarity and Hitler's Strategy of World Conquest* New York: Columbia University Press, (2001), fq.1–23.
22. Walt, Stephen M "The Renaissance of Security Studies. *International Studies Quarterly* 35 (1991): fq.211–239.
23. Waltz, Kenneth N. *Theory of International Politics* Reading, MA: Addison-Wesley, (1979), fq.88–99.
24. Wohlforth, William C. "The Stability of a Unipolar World." *International Security* 24, nr. 1 (1999): fq.5–41.
25. Xing, Li. *The Rise of China and the Liberal World Order* London: Routledge, (2022), fq.61–84.

Lufta e Gjeneratës së Gjashtë dhe teatrot globalë të veprimtarisë ushtarake të Rusisë

Nënkolonel Ervin HODO
Oficer shtabi, Kolegji i Mbrojtjes dhe Sigurisë

Trajtesë e shkurtuar

Ky studim analizon luftën e Gjeneratës së Gjashtë (6GW angl.) dhe përdorimin e teatrove globalë të veprimtarisë ushtarake nga Federata Ruse, duke shqyrtuar ndikimet strategjike, taktikat dhe instrumentet që formojnë konfliktin modern. Lufta e Gjeneratës së Gjashtë përfaqëson një evolucion të thellë në teorinë dhe praktikën ushtarake, ku informacioni, teknologjia, forcat hibride dhe operacionet psikologjike integrohen për të arritur objektiva strategjikë. Rusia ka demonstruar adaptimin e këtij koncepti përmes Operacionit Ushtarak Special(OUS), në Ukrainë dhe veprimtarive të koordinuara në Europën Lindore, Lindjen e Mesme, Afrikë dhe Azinë Juglindore, duke përdorur një kombinim të forcave konvencionale, kompanive private ushtarake, sulmeve kibernetike dhe dezinformimeve, për të ndikuar në vendimet politike dhe ekonomike të aktorëve lokalë dhe ndërkombëtarë. Studimi nënvizon se 6GW nuk kufizohet më në frontin fizik, por zgjerohet në hapësirën digjitale, diplomatike dhe ekonomike, duke krijuar një mjedis kompleks operativ dhe sfidues për normat ndërkombëtare dhe strategjitë tradicionale të sigurisë. Analiza ofron një kuadër të qartë për të kuptuar se si luftërat moderne po ndryshojnë peizazhin strategjik global dhe kërkojnë që të pranohen nga aleatët dhe partnerët ndërkombëtarë.

Fjalët kyçe: Lufta e Gjeneratës së Gjashtë (6GW); Rusia; Operacion Ushtarak Special(OUS), teatër global i veprimtarisë ushtarake; operacion hibrid; luftë kibernetike; dezinformim; forcat hibride; kompani private ushtarake (KPU); strategji globale; ndikimi politik dhe ekonomik; siguria ndërkombëtare

Hyrje

Në dekadat e fundit, natyra e luftës ka pësuar një evolucion të thellë, duke sfiduar konceptet tradicionale dhe klasike të operacioneve ushtarake. Konfliktet nuk janë më të kufizuara te përballjet e drejtpërdrejta në

frontin e parë; ato kanë marrë forma më komplekse dhe multidimensionale, ku fushat e betejës përfshijnë jo vetëm terrenin fizik, por edhe hapësirën kibernetike, mediatike dhe ekonomike.[1] Në këtë kuadër, luftërat moderne kërkojnë integrimin e teknologjive të avancuara, përdorimin e inteligjencës artificiale dhe automatizimit, si dhe zhvillimin e metodave psikologjike dhe dezinformuese që synojnë të kontrollojnë perceptimet e publikut dhe vendimmarrjen strategjike të kundërshtarit.[2]

Lufta e Gjeneratës së Gjashtë (6GW) përfaqëson një paradigmë të re në teorinë dhe praktikën ushtarake, ku fronti nuk është më i kufizuar nga kufijtë gjeografikë dhe efektet e veprimeve ushtarake ndihen në shumë dimensione të jetës publike dhe shtetërore. Përmes saj, informacioni bëhet një mjet strategjik, perceptimet publike manipulohet për të arritur avantazhe politike, ndërkohë që sulmet kibernetike dhe elektromagnetike përdoren për të dobësuar aftësitë operacionale të armikut.[3] Kjo qasje thekson rëndësinë e një strategjie integruese, ku fuqia ushtarake, informacioni, teknologjia dhe ndikimi diplomatik veprojnë si pjesë e një sistemi të vetëm për të arritur objektivat strategjikë.

Rusia, ka qenë një nga aktorët kryesorë që ka adaptuar konceptin e 6GW në doktrinën e saj moderne ushtarake dhe strategjike. Adaptimi i saj, është dukshëm i shprehur në përdorimin e Operacionit Ushtarak Special (OUS), në Ukrainë dhe operacione të tjera globale, ku veprimet konvencionale bashkohen me kapacitete hibride dhe metodologji të sofistikuara të ndikimit kibernetik dhe psikologjik.[4] Për shembull, ndërhyrjet në Europën Lindore, përdorimi i kompanive private ushtarake në Afrikë dhe bazat strategjike në Lindjen e Mesme, janë pjesë e një modeli të qëndrueshëm, i cili synon të ruajë ndikimin politik, ekonomik dhe ushtarak të Rusisë në nivel global.[5] Ky adaptim nuk është thjesht një praktikë operative, por një reflektim i filozofisë strategjike ruse, e cila kombinon asimetri të forcës, operacione të fshehta dhe manipulim të informacionit për të krijuar një avantazh global. Në këtë mënyrë, Rusia përdor një gamë të gjerë të mjeteve – nga armët konvencionale deri te dezinformimet dhe operacionet kibernetike – për të formuar narrativën ndërkombëtare, për të penguar koordinimin e kundërshtarëve dhe për të siguruar që vendimet politike dhe ekonomike të jenë në përputhje me interesat

[1] Lester W. Grau and Charles K. Bartles, *The Russian Way of War* (Fort Leavenworth, KS: Army University Press, 2016), 121–130.

[2] NATO StratCom Centre of Excellence, *Hybrid Threats and 6th Generation Warfare* (Riga: NATO StratCom COE, 2022).

[3] Center for Strategic and International Studies (CSIS), *Russian Military Operations and Hybrid Warfare Analysis* (Washington, DC: CSIS, 2023).

[4] Ministry of Defence of the Russian Federation, *Russian Military Doctrine* (Moscow: Ministry of Defence, 2020).

[5] International Institute for Strategic Studies (IISS), *The Military Balance 2025* (London: Routledge, 2025).

strategjike të saj.[6]

Studimi, synon të theksojë se koncepti i luftës së Gjeneratës së Gjashtë dhe përdorimi i teatrove globale të veprimtarisë ushtarake nga Rusia, përbëjnë një sfidë të re për teorinë dhe praktikën e sigurisë ndërkombëtare. Analiza e mëtejshme e materialit, do të eksplorojë instrumentet, taktikat dhe ndikimet e këtij modeli, duke ofruar një kuadër të qartë për të kuptuar se si konflikti modern po ndryshon peizazhin strategjik global.

1. Koncepti i Luftës së Gjeneratës së Gjashtë

Lufta e Gjeneratës së Gjashtë (*ang.6GW*), përfaqëson një evolucion të rëndësishëm në teorinë dhe praktikën e konfliktit modern, duke kaluar përtej kufijve të operacioneve konvencionale dhe duke integruar teknologjitë më të avancuara, strategjitë hibride dhe ndikimin psikologjik. Në thelb, 6GW synon të krijojë avantazhe strategjike pa u kufizuar vetëm në përdorimin e forcës fizike, duke shfrytëzuar një gamë të gjerë mjetesh që përfshijnë hapësirën kibernetike, elektromagnetike, ekonomike, diplomatike dhe mediatike.[7]

Një nga tiparet kryesore të 6GW, është integrimi i inteligjencës artificiale dhe automatizimit në operacione ushtarake. Përdorimi i sistemeve të mbikëqyrjes të bazuara në AI, lejon grumbullimin e të dhënave në kohë reale, identifikimin e objektivave strategjikë dhe koordinimin e ofensivave me një efikasitet që tejkalon kapacitetet e komandimit njerëzor. Për shembull, dronët autonomë dhe sistemet e vëzhgimit satelitor, mund të përdoren për zbulim, mbikëqyrje dhe sulme automatike ndaj objektivave të caktuara, duke reduktuar rrezikun për trupat e dorës së parë dhe duke maksimizuar efektivitetin operativ.[8]

Përdorimi i hapësirës kibernetike dhe elektromagnetike, është gjithashtu një komponent qendror i 6GW. Sulmet kibernetike ndaj infrastrukturave kritike – duke përfshirë rrjetet energjetike, telekomunikacionet dhe sistemet e komandimit dhe kontrollit – synojnë të paralizojnë aftësitë e armikut pa shkaktuar dëme të dukshme fizike. Në këtë mënyrë, fronti i luftës nuk është më i kufizuar nga kufijtë gjeografikë; operacionet mund të ndodhin në çdo vend ku ekziston një lidhje digjitale ose elektromagnetike që mund të shfrytëzohet.[9]

Një tjetër dimension kyç është përdorimi i operacioneve psikologjike dhe dezinformatave, për të ndikuar perceptimet publike dhe vendimet strategjike. Kjo përfshin fushata propagandistike, manipulimin e rrjeteve sociale dhe

[6] Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, 2019), 56–65.

[7] NATO StratCom Centre of Excellence, *Hybrid Threats and 6th Generation Warfare* (Riga: NATO StratCom COE, 2022).

[8] Lester W. Grau and Charles K. Bartles, *The Russian Way of War* (Fort Leavenworth, KS: Army University Press, 2016), 121–130.

[9] Center for Strategic and International Studies (CSIS), *Russian Military Operations and Hybrid Warfare Analysis* (Washington, DC: CSIS, 2023).

përdorimin e narrativave të dizajnuara, për të krijuar paqëndrueshmëri politike. Qëllimi është të dobësohet kohezioni shoqëror, të ndikohen vendimet e liderëve dhe të krijohet një ambient ku përparësitë strategjike mund të arrihen pa përdorim të drejtpërdrejtë të forcës konvencionale.[10]

Asimetria e forcës, është gjithashtu një tipar dallues i 6GW. Operacionet tradicionale konvencionale kombinohen me aksione të fshehta, përdorimin e aktorëve jo-shtetërorë si kompanitë private ushtarake, grupet proxy dhe aktorët kibernetikë. Kjo qasje siguron fleksibilitet operativ dhe mundësi të shumta reagimi, duke i lejuar shteteve ose aktorëve që të operojnë me efikasitet ndaj kundërshtarëve më të fuqishëm ose të mbrojnë interesat strategjike në mënyrë të fshehtë dhe të sofistikuar.[11]

Një tjetër element i rëndësishëm është globalizimi i teatrit operativ, ku veprimtaria ushtarake nuk kufizohet më tek terreni fizik, por përfshin hapësira të ndryshme ekonomike, diplomatike dhe mediatike. Operacionet strategjike mund të ndikojnë në tregjet globale, të destabilizojnë aleanca politike dhe të ndërhyjnë në perceptimet e komunitetit ndërkombëtar. Në këtë mënyrë, çdo vend ose organizatë ndërkombëtare mund të bëhet pjesë e frontit të luftës, edhe pa një përballje direkte me armët tradicionale.[12]

1.1 Dallimet mes luftës hibride dhe luftës së Gjeneratës së Gjashtë

Edhe pse në pamje të parë, krijohet ideja se lufta e Gjeneratës së Gjashtë është e njëjtë me luftën hibride, dallimet mes tyre janë të dukshme dhe të rëndësishme. Përfshirja e këtyre dallimeve në këtë studim, do të na qartësonte edhe më tej për mënyrën së si këto dy lloje luftërash, po përdoren më shumë mjeshtëri nga Federata Ruse.

Në dekadën e fundit, natyra e konfliktit ndërkombëtar ka evoluar dukshëm, duke reflektuar ndryshime strukturore në mënyrën se si aktorët përdorin forcën dhe ndikimin. Konceptet *luftë hibride* dhe *luftë e gjeneratës së gjashtë* (6GW – *Sixth Generation Warfare*) janë dy përpjekje teorike për të kuptuar këto transformime dhe për të dalluar modelet bashkëkohore të konfliktit. Përkufizimet, metodat dhe përdorimi i teknologjisë në këto forma të konfliktit ndryshojnë në mënyrë të qenësishme, duke ndikuar në mënyrën se si shtetet planifikojnë dhe ushtrojnë fuqinë e tyre. Në këtë pjesë të studimit do të shqyrtojmë këto dallime thelbësore, duke përdorur shembuj konkretë nga konflikti i Rusisë me Ukrainën, lufta e vitit 2006 në Liban dhe tendencat teknologjike globale në konfliktet e së ardhmes.

---

[10] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 101–115.

[11] Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, 2019), 56–65.

[12] International Institute for Strategic Studies (IISS), *The Military Balance 2025* (London: Routledge, 2025).

Përkufizimi teorik dhe karakteristikat kryesore

Lufta hibride përkufizohet si përdorim i kombinuar i mjeteve ushtarake dhe joushtarake – përfshirë forcat konvencionale, taktikat asimetrike, ndikimin politik, propagandën dhe sulmet kibernetike – që synojnë të arrijnë objektiva strategjikë pa shpeshherë shpallur luftë të hapur. Termi, është popullarizuar nga Frank Hoffman dhe është përdorur për të përshkruar operacione komplekse që tejkalojnë ndarjet tradicionale të luftës ushtarake *versus* paqe.[13]

Dallimet në praktikë: shembuj konkretë

Konflikti midis Rusisë dhe Ukrainës, është një shembull i dukshëm i përdorimit të strategjive hibride. Para pushtimit të plotë të Ukrainës nga Rusia në vitin 2022, Moska përdori sulme kibernetike, fushata të mëdha dezinformimi dhe ndikim politik për të dobësuar institucionet ukrainase dhe për të ndikuar perceptimet publike përpara se të ndërmerrte veprime ushtarake konvencionale. Këto metoda përfshijnë viruset destructive *wiper*, të përdorura kundër sistemit kibernetik ukrainas dhe fushatat e propagandës që synonin të krijonin ndasi sociale dhe paqartësi strategjike.

Një shembull tjetër historik, është lufta e vitit 2006 ndërmjet Izraelit dhe Hezbollahut. Në këtë konflikt, Hezbollahu përdori një përzierje të taktike guerile, armëve moderne që zakonisht i përdorin ushtritë shtetërore dhe rrjeteve të komunikimit të kriptuar për koordinim, duke sfiduar qasjet konvencionale të luftës dhe duke përzier elementë ushtarakë dhe jo-ushtarakë në mënyrë hibride.

Në Ballkan, Rusia ka përdorur strategji hibride nëpërmjet influencave politike dhe kulturore për të krijuar forca pro-ruse brenda institucioneve vendore, duke shfrytëzuar zgjedhjet dhe narrativat etnike si mjete për të arritur objektiva gjeopolitike pa përdorur forcë të hapur ushtarake.

2. Doktrina ushtarake ruse dhe adaptimi i Luftës së Gjeneratës së Gjashtë

Në terminologjinë ruse, shkenca ushtarake është një sistem njohurish mbi ligjet e luftës, natyrën ushtarako-strategjike të luftës, mënyrat e parandalimit të luftës, përgatitjen e forcave të armatosura dhe të vendit për luftë, si dhe metodat e zhvillimit të luftës së armatosur. Termi *arti ushtarak,* i referohet degës së shkencës ushtarake që ka të bëjë me teorinë dhe praktikën, strategjinë, artin operacional dhe taktikat, e përgatitjes dhe zhvillimit të luftës së armatosur në tokë, ajër, det dhe fusha të tjera.

Që teoricienët ushtarakë ruse, të shqyrtojnë të ardhmen e strategjisë, artit operacional dhe taktikave, ata duhet së pari të shqyrtojnë se si do të duket lufta e së ardhmes. Kjo realizohet duke studiuar mësimet e luftërave të së kaluarës

[13] Tarik Solmaz, "*Hybrid Warfare: A Dramatic Example of Conceptual Stretching*", NSF Journal 23, nr. 1 (2022).

dhe faktorët që do të shkaktojnë ndryshimin e luftës dhe duke përdorur këtë informacion, për të parashikuar se si mund të duket mjedisi operativ i së ardhmes.

Faktori më i rëndësishëm prej tyre është zhvillimi teknologjik, i cili është thelbësor për çdo planifikim afatgjatë të mbrojtjes që përfshin doktrinën ushtarake dhe zhvillimin e kapaciteteve. Ndërsa përparimi teknologjik i njerëzimit, është rritur gjatë disa qindra viteve të fundit, po ashtu është rritur edhe niveli i zhvillimit teknologjik të ushtrive, duke rezultuar në atë që teoricienët rusë e përshkruajnë si gjenerata të ndryshme të luftës. Në katër mijë vjet, kanë ekzistuar pesë gjenerata:

- gjenerata e parë – armë me tehe,
- gjenerata e dytë – armë me barut,
- gjenerata e tretë – armë me tytë me vijaska,
- gjenerata e katërt – armë automatike,
- gjenerata e pestë – armë bërthamore.

Në përgjithësi, kur teoricienët ushtarakë rusë diskutojnë tendencat e ardhshme në luftë, ose luftën e gjeneratës së re, ky është konteksti të cilit ata i referohen.

Duke pasur parasysh rëndësinë e zhvillimit teknologjik për artin ushtarak, teoricienët ushtarakë rusë prej kohësh kanë reflektuar mbi ndikimet e ndryshimit dhe inovacionit teknologjik. Një nga këta teoricienë rusë më të njohur ishte i ndjeri gjeneral major Vladimir Slipchenko. Slipchenko, ishte veçanërisht i interesuar për zhvillimet teknologjike që karakterizuan operacionin "Desert Storm" në vitin 1991 dhe bombardimin e Jugosllavisë nga NATO në vitin 1999. Sipas tij, këto konflikte u karakterizuan nga përdorimi gjithnjë e më i madh i municioneve me drejtim preciz, nga rëndësia në rritje e aspekteve informative të luftës, operacione informative dhe psikologjike, C4ISR, luftë elektronike, luftë kibernetike dhe kështu me radhë, si edhe nga rënia e rëndësisë së elementeve tokësore.

Teoricienët ushtarakë ruse, theksojnë se në operacionin "Desert Storm", Shtetet e Bashkuara u mbështetën në afërsisht gjashtëdhjetë satelitë ushtarakë për qëllime komunikimi dhe zbulimi, në konstelacionin satelitor të navigimit GPS (më parë NAVSTAR), si dhe në disa satelitë komercialë për të mbështetur zhvillimin e një fushate bombardimi preciz prej tridhjetë e tetë ditësh, e cila shkatërroi rëndë ushtrinë irakiane. Kjo mënyrë e re e luftës u përsos më tej gjatë fushatës së bombardimit prej shtatëdhjetë e tetë ditësh kundër Jugosllavisë. Përdorimi i municioneve me drejtim preciz në këto konflikte është ajo që i dallon ato nga konfliktet e mëparshme. Për Slipchenkon, konsiderimi i tankut, mitralozit dhe avionit si zhvillime revolucionare ushtarake ishte i pabazuar, pasi ndikimi i tyre në zhvillimin e luftës zbehet në krahasim me municionet me drejtim preciz.[14]

[14] *Russian Grand Strategy in the era of global competition*, Manchester University Press,2022, 81-83

Doktrina ushtarake dhe e sigurisë kombëtare e Federatës Ruse, ka evoluar gradualisht drejt një qasjeje fleksibël dhe gjithëpërfshirëse. Një manifestim konkret i kësaj doktrine është koncepti i Operacionit Ushtarak Special (OUS), i aplikuar në Ukrainë që prej vitit 2022. Në këtë kontekst, Rusia ka demonstruar një formë të avancuar të luftës së Gjeneratës së Gjashtë, duke kombinuar operacionet tokësore konvencionale me sulme kibernetike, luftë elektronike dhe fushata të gjera dezinformuese. Sulmet ndaj infrastrukturës energjetike, ndërhyrjet në sistemet e komandimit dhe kontrollit, si dhe operacionet në hapësirën elektromagnetike, kanë shërbyer për të dobësuar kapacitetin shtetëror të Ukrainës dhe për të ndikuar ritmin e vendimmarrjes strategjike të saj dhe të aleatëve perëndimorë. Kjo tregon se SMO nuk përfaqëson thjesht një terminologji politike, por një kornizë operative që përputhet drejtpërdrejt me parimet e 6GW.

Një element tjetër thelbësor i doktrinës ruse është zgjerimi i teatrove globale të veprimit, përtej hapësirës euroaziatike. Rusia ka përdorur prezencën e saj ushtarake dhe politike në Lindjen e Mesme, Afrikë dhe hapësira të tjera strategjike, për të ndikuar vendimet politike dhe ekonomike të aktorëve lokalë dhe ndërkombëtarë. Ky veprim shërben jo vetëm për të rritur ndikimin gjeopolitik të Moskës, por edhe për të shpërndarë presionin strategjik ndaj kundërshtarëve, duke i detyruar ata të reagojnë në disa fronte njëkohësisht.[15] Kjo qasje përputhet me logjikën e luftës së Gjeneratës së Gjashtë, ku fragmentimi i vëmendjes së kundërshtarit është po aq i rëndësishëm sa edhe përdorimi i forcës ushtarake.

Manipulimi i informacionit dhe i perceptimeve publike përbën një shtyllë qendrore të kësaj doktrine. Përmes mediave shtetërore, rrjeteve sociale, aktorëve proxy dhe operacioneve të ndikimit, Rusia synon të formësojë narrativën globale mbi konfliktet ku është e përfshirë, duke relativizuar përgjegjësitë e saj dhe zvogëluar mbështetjen ndërkombëtare për kundërshtarët. Në rastin e Ukrainës, kjo strategji ka synuar të krijojë ndarje brenda shoqërive perëndimore, të dobësojë konsensusin politik për ndihmën ushtarake dhe të paraqesë konfliktin si një përballje të pashmangshme gjeopolitike.[16]

3. Teatrot globale të veprimtarisë ushtarake

Federata Ruse ka zhvilluar veprimtari të koordinuara ushtarake dhe hibride në rajone strategjike, duke përdorur një kombinim të forcave konvencionale, kapaciteteve kibernetike, operacioneve psikologjike dhe kompanive private ushtarake. Këto veprime synojnë të ruajnë ndikimin politik, ekonomik dhe ushtarak të Rusisë, në hapësira ku interesat globale janë të kontestuara.

- Evropa Lindore: Në Evropën Lindore, Rusia ka përdorur një strategji të

[15] Center for Strategic and International Studies (CSIS). *Russian Military Operations and Hybrid Warfare Analysis*. Washington, DC, 2023.

[16] International Institute for Strategic Studies (IISS). *The Military Balance 2025*. London, 2025.

përzier që kombinon forcat hibride me operacione kibernetike për të ndikuar në vendet fqinje dhe për të ruajtur një avantazh strategjik. Për shembull, ndërhyrjet në Moldavi, Gjeorgji dhe rajonet e Ukrainës lindore kanë përfshirë sulme kibernetike të dizajnuara për të ndikuar në funksionimin e sistemit qeveritar dhe proceset elektorale, duke synuar destabilizimin e institucioneve dhe dobësimin e kohezionit politik. Përveç kësaj, Rusia ka përdorur presion politik dhe energjetik, duke shfrytëzuar varësinë e disa vendeve ndaj gazit dhe energjisë për të orientuar vendimmarrjen strategjike në favor të objektivave të saj.[17]

- Lindja e Mesme: Në Lindjen e Mesme, Rusia ka zhvilluar një strategji të bazuar në përdorimin e aktorëve *proxy* dhe kompanive private ushtarake për të ruajtur interesat strategjike dhe për të mbrojtur rrugët e furnizimit.[18]

Në Siri, për shembull, vendosja e bazave ushtarake në Tartus dhe Hmeimim dhe aktivitetet e KPU-ve kanë mundësuar ruajtjen e ndikimit politik mbi qeverinë lokale dhe kontrollin e linjave kritike logjistike.[19] Kjo qasje ka lejuar Moskën të projektojë fuqinë e saj në një rajon kyç energjetik dhe të ruajë një prani afatgjatë strategjike, duke përdorur mjetet hibride për të bashkëpunuar me aktorë lokalë dhe për të minimizuar rreziqet diplomatike.

- Afrika: Në kontinentin afrikan, Rusia ka shfrytëzuar kompanitë private ushtarake (KPU), veçanërisht Wagner, për të influencuar qeveritë lokale dhe për të siguruar baza të qëndrueshme ushtarake dhe kontrata të rëndësishme armatimi.[20] Në vende si Libia dhe Republika Qendrore Afrikane, këto operacione kanë lejuar Rusinë të ketë akses në burime minerale dhe pozicione strategjike, duke rritur ndikimin e saj politik dhe ekonomik në rajon dhe duke krijuar zona tensioni që ndikojnë drejtpërdrejt në balancat rajonale të fuqisë.[21]

- Paqësori dhe Azia: Në rajonin e Paqësorit dhe Azisë, Rusia konkurron me Shtetet e Bashkuara dhe aleatët e tyre për ndikim ekonomik dhe ushtarak.[22] Për këtë qëllim, Rusia përdor kapacitete hapësinore dhe kibernetike për mbikëqyrje strategjike dhe mbështetje të aleatëve. Aktivitetet e mbikëqyrjes përfshijnë përdorimin e dronëve dhe sistemeve satelitore për të monitoruar lëvizjet e marinës amerikane në Azinë Juglindore, për të mbrojtur interesat kombëtare dhe për të forcuar pozicionin e saj gjeopolitik në një rajon me

[17] NATO StratCom Centre of Excellence, *Hybrid Threats and 6th Generation Warfare* (Riga: NATO StratCom COE, 2022).

[18] Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, 2019), 56–65.

[19] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 101–115.

[20] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 101–115.

[21] International Institute for Strategic Studies (IISS), *The Military Balance 2025* (London: Routledge, 2025).

[22] Kimberly Marten, *Russia's Use of Semi-State Security Forces* (Washington, DC: CSIS, 2019), 34–42.

rëndësi kritike strategjike.[23]

Ky model i veprimtarisë globale tregon qartë se Rusia nuk vepron vetëm në një skenë lokale apo rajonale, por përdor një qasje të integruar në nivele strategjike të ndryshme, duke kombinuar mjete ushtarake, ekonomike dhe teknologjike për të arritur objektivat e saj ndërkombëtarë.

4. Mjetet dhe taktikat e luftës së Gjeneratës së Gjashtë (6GW) të Rusisë

Lufta e Gjeneratës së Gjashtë përfaqëson një fazë të avancuar të evolucionit të konfliktit modern, ku përdorimi i forcës ushtarake nuk është më instrumenti i vetëm, as domosdoshmërisht kryesori, për arritjen e objektivave strategjikë.

Në doktrinën ruse, 6GW konceptohet si një formë lufte gjithëpërfshirëse, ku mjetet ushtarake, politike, ekonomike, informative dhe teknologjike integrohen në një sistem të vetëm veprimi. Qëllimi kryesor nuk është shkatërrimi fizik i armikut, por *paralizimi i aftësisë së tij për të marrë vendime efektive,* duke ndikuar drejtpërdrejt mbi vullnetin politik, stabilitetin shoqëror dhe kohezionin institucional.

Në këtë kontekst, Rusia e sheh luftën si një proces të vazhdueshëm, i cili nuk kufizohet në kohë lufte formale, por zhvillohet edhe në periudha paqeje relative. Ky perceptim e bën 6GW një mjet strategjik të përshtatshëm për rivalitetin me Perëndimin, veçanërisht në kushtet e inferioritetit relativ ekonomik dhe demografik krahasuar me NATO-n.[24]

Lufta kibernetike dhe elektromagnetike si armë strategjike.

Lufta kibernetike dhe elektromagnetike zë një vend qendror në arkitekturën e 6GW ruse. Përmes sulmeve kibernetike ndaj rrjeteve kritike, Rusia synon të ndërpresë funksionimin normal të shtetit kundërshtar, duke shkaktuar efekte zinxhir në ekonomi, shoqëri dhe sektorin e sigurisë. Objektivat kryesorë përfshijnë rrjetet energjetike, sistemet e telekomunikacionit, infrastrukturën e transportit, institucionet financiare dhe, mbi të gjitha, sistemet e komandimit dhe kontrollit ushtarak (C2).[25]

Dimensioni elektromagnetik plotëson këtë qasje përmes *jamming (bllokim valësh)*, mashtrimit dhe manipulimit të spektrit elektromagnetik. Në fushëbetejë, këto mjete përdoren për të verbuar sensorët e armikut, për të ndërprerë lidhjet e komunikimit dhe për të krijuar sinjale të rreme që çojnë në vendime taktike të gabuara. Lufta në Ukrainë ka treguar qartë se Rusia i konsideron këto mjete si pjesë integrale të operacioneve të kombinuara, duke

[23] Po aty.

[24] Dmitry Adamsky, *The Culture of Military Innovation* (Stanford: Stanford University Press, 2010), 34–38.

[25] Keir Giles, *Russia's New Tools for Confronting the West* (London: Chatham House, 2016), 9–15.

i përdorur paralelisht me artilerinë, dronët dhe manovrën tokësore.[26]

Lufta e informacionit, operacionet psikologjike dhe dezinformimi.

Një element po aq i rëndësishëm i 6GW është lufta e informacionit, e cila shtrihet përtej propagandës tradicionale. Rusia përdor operacione psikologjike (PSYOPS) dhe fushata të sofistikuara dezinformimi për të ndikuar perceptimet, emocionet dhe sjelljen e audiencave të ndryshme: popullsinë e vet, shoqëritë e vendeve kundërshtare dhe opinionin publik ndërkombëtar.[27]

Në praktikë, kjo realizohet përmes mediave shtetërore, rrjeteve sociale, programeve të pavarura në internet, karremit dhe aktorëve të ndërmjetëm, të cilët përhapin narrativa që relativizojnë të vërtetën, krijojnë konfuzion dhe minojnë besimin në institucionet demokratike. Në Ukrainë, fushatat e dezinformimit kanë synuar të delegjitimojnë qeverinë e Kievit, të justifikojnë veprimet ushtarake ruse dhe të dekurajojnë mbështetjen perëndimore. Këto veprime janë në përputhje me doktrinën ruse që e konsideron informacionin si një armë strategjike me efekt afatgjatë.[28]

Forcat hibride dhe kompanitë private ushtarake.

Përdorimi i forcave hibride dhe kompanive private ushtarake (KPU) është një komponent thelbësor i 6GW ruse. Këto struktura ofrojnë fleksibilitet operacional dhe një shkallë të lartë mohimi të besueshëm, duke i lejuar Rusisë të veprojë në zona gri ndërmjet luftës dhe paqes. PMC-të janë përdorur për misione që variojnë nga operacione luftarake të intensitetit të ulët, deri te sigurimi i objekteve strategjike dhe mbështetja e regjimeve aleate.[29]

Në Ukrainë, përdorimi i KPU-ve ka ilustruar qartë këtë qasje hibride, ku aktorë joshtetërorë veprojnë në sinkron me objektivat strategjikë të shtetit rus. Ky model i lejon Moskës të minimizojë kostot politike dhe diplomatike, duke ruajtur një nivel të lartë ndikimi operacional në terren.

Inteligjenca artificiale, dronët dhe sistemet autonome.

Integrimi i inteligjencës artificiale dhe sistemeve pa pilot përfaqëson një dimension të ri të 6GW. Rusia i konsideron këto teknologji si shumëfishues force, që rrisin efikasitetin operacional dhe shkurtojnë ciklin e vendimmarrjes. Dronët përdoren gjerësisht për zbulim, mbikëqyrje dhe goditje precize, ndërsa AI ndihmon në analizimin e të dhënave të mëdha dhe në përzgjedhjen e objektivave.[30] Në një konflikt të gjeneratës së gjashtë, avantazhi nuk i përket domosdoshmërisht palës me më shumë trupa, por asaj që arrin të integrojë më

[26] Lester Grau and Charles Bartles, *The Russian Way of War* (Fort Leavenworth: Army University Press, 2016), 121–128.
[27] Thomas Rid, *Active Measures* (New York: Farrar, Straus and Giroux, 2020), 87–95.
[28] NATO StratCom COE, *Russia's Information Warfare* (Riga, 2018), 22–29.
[29] Mark Galeotti, *Russian Political War* (London: Routledge, 2019), 56–62.
[30] Michael Kofman et al., *Russian Military Strategy* (CNA, 2020), 41–46.

mirë teknologjinë me doktrinën dhe komandimin. Në këtë aspekt, Rusia synon të kompensojë dobësitë strukturore përmes inovacionit teknologjik dhe përdorimit të sistemeve autonome.

5. Shembuj praktikë të përdorimit të luftës së Gjeneratës së Gjashtë

Kriza në Ukrainë gjatë periudhës 2022–2025 përbën një nga rastet më përfaqësuese të aplikimit praktik të elementëve të luftës së Gjeneratës së Gjashtë nga Federata Ruse. Ky konflikt tregon qartë se si Rusia ka kombinuar operacionet ushtarake konvencionale të quajtura zyrtarisht *Operacion Ushtarak Special* (OUS) me mjete jolineare, përfshirë sulmet kibernetike, luftën e informacionit, presionin ekonomik dhe veprimet hibride. Qëllimi strategjik nuk ka qenë vetëm kontrolli territorial, por edhe dobësimi i kapacitetit shtetëror ukrainas për të funksionuar në mënyrë efektive dhe për të ruajtur mbështetjen e brendshme dhe ndërkombëtare.[31]

Ukraina si laborator i 6GW.

Që në fazat e hershme të konfliktit, Rusia ka ndërmarrë sulme kibernetike të koordinuara kundër infrastrukturave kritike ukrainase, veçanërisht rrjeteve energjetike, sistemeve të telekomunikacionit dhe institucioneve shtetërore. Këto sulme synuan të paralizojnë funksionimin e administratës publike dhe të krijojnë kaos në jetën e përditshme të popullsisë civile, duke reduktuar besimin në aftësinë e shtetit për të ofruar siguri dhe shërbime bazë.[32]

Ndërhyrjet në rrjetet e informacionit dhe sulmet ndaj sistemeve të komandimit dhe kontrollit (C2) kanë pasur gjithashtu një rol kyç në fushëbetejë. Përmes jamming dhe spoofing, forcat ruse kanë tentuar të degradojnë aftësitë ISR (Intelligence, Surveillance, Reconnaissance) të Ukrainës, duke krijuar avantazh operacional për njësitë tokësore dhe ajrore.[33] Ky kombinim i mjeteve kibernetike dhe tradicionale përfaqëson një tipar thelbësor të 6GW, ku efektet jo kinetike përgatitin terrenin për veprimet kinetike.

Lufta e informacionit dhe ndikimi mbi opinionin publik.

Një tjetër komponent qendror i strategjisë ruse në Ukrainë, ka qenë lufta e informacionit. Përmes fushatave të gjera dezinformimi në rrjetet sociale, mediave shtetërore dhe platformave ndërkombëtare, Rusia ka synuar të manipulojë perceptimet e popullsisë ukrainase, të justifikojë veprimet e saj për audiencën e brendshme dhe të krijojë përçarje në opinionin publik

[31] NATO StratCom Centre of Excellence, *Hybrid Threats and 6th Generation Warfare* (Riga: NATO StratCom COE, 2022).

[32] Center for Strategic and International Studies (CSIS), *Russian Military Operations and Hybrid Warfare Analysis* (Washington, DC: CSIS, 2023).

[33] Lester W. Grau and Charles K. Bartles, *The Russian Way of War* (Fort Leavenworth, KS: Army University Press, 2016), 121–130.

perëndimor.[34] Këto fushata, kanë përfshirë narrativa mbi delegjitimimin e autoriteteve ukrainase, minimizimin e krimeve të luftës dhe paraqitjen e konfliktit si një përballje ekzistenciale me Perëndimin. Në kuadër të 6GW, kontrolli i narrativës është po aq i rëndësishëm sa kontrolli i territorit, pasi ai ndikon drejtpërdrejt në vullnetin politik dhe kohezionin shoqëror të palëve të përfshira.[35]

Siria: konsolidimi i ndikimit përmes mjeteve hibride.

Në Siri, Rusia ka demonstruar një tjetër aspekt të rëndësishëm të Luftës së Gjeneratës së Gjashtë, duke kombinuar përdorimin e forcës ushtarake konvencionale me mjete hibride dhe proxy. Vendosja e bazave ushtarake në Tartus dhe Hmeimim ka garantuar një prezencë strategjike afatgjatë në Mesdheun Lindor, ndërsa mbështetja për forcat e regjimit sirian dhe grupe paramilitare lokale ka siguruar stabilitetin e aleatit kryesor të Moskës në rajon.[36]

Kjo qasje i ka lejuar Rusisë të projektojë fuqi me kosto relativisht të ulët, të testojë armë dhe doktrina të reja dhe të rrisë ndikimin e saj diplomatik në Lindjen e Mesme. Në këtë kuptim, Siria shërben si një model i përdorimit të 6GW për arritjen e objektivave strategjike përtej një konflikti të vetëm rajonal.[37]

Afrika dhe Lindja e Mesme: KPU-të dhe kontrolli i resurseve.

Në kontinentin afrikan dhe në Lindjen e Mesme, Rusia ka përdorur kompanitë private ushtarake, veçanërisht Wagner, si instrumente kryesore të strategjisë së saj hibride. Në vende si Libia, Mali dhe Republika Qendrore Afrikane, këto struktura kanë vepruar në mbështetje të qeverive lokale ose aktorëve të caktuar politikë, duke ofruar siguri, trajnim ushtarak dhe mbrojtje të objekteve strategjike.[38]

Në këmbim, Rusia ka siguruar akses në resurse natyrore, përfshirë miniera ari, diamanti dhe burime energjetike, duke e lidhur ndikimin ushtarak me përfitime ekonomike afatgjata. Ky kombinim i forcës së armatosur, ndikimit ekonomik dhe veprimit të fshehtë përbën një shembull tipik të 6GW, ku mjetet ushtarake janë vetëm një pjesë e një strategjie shumëdimensionale për zgjerimin e ndikimit global.[39]

---

[34] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 101–115.

[35] NATO StratCom COE, *Russia's Information Warfare* (Riga, 2018), 19–27.

[36] International Institute for Strategic Studies (IISS), *The Military Balance 2025* (London: Routledge, 2025).

[37] Dmitry Adamsky, *The Culture of Military Innovation* (Stanford: Stanford University Press, 2010), 142–149.

[38] Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, 2019), 56–65.

[39] Kimberly Marten, *Russia's Use of Semi-State Security Forces* (Washington, DC: CSIS, 2019).

Vlerësim strategjik.

Shembujt nga Ukraina, Siria dhe Afrika tregojnë se lufta e Gjeneratës së Gjashtë nuk kufizohet në operacionet tradicionale ushtarake, por përfshin një qasje të integruar që synon kontrollin e mjedisit strategjik në tërësi.

Rusia përdor një kombinim të forcës fizike, kontrollit të informacionit, presionit ekonomik dhe aksioneve të fshehta për të formësuar sjelljen e aktorëve shtetërorë dhe joshtetërorë.

Në këtë kuadër, 6GW përfaqëson një sfidë serioze për rendin ndërkombëtar dhe për modelet tradicionale të reagimit ushtarak dhe diplomatik, duke kërkuar qasje të reja nga NATO dhe aleatët e saj për të identifikuar, parandaluar dhe kundërbalancuar këto forma të avancuara të konfliktit.[40]

6. Impaktet strategjike

Lufta e Gjeneratës së Gjashtë (6GW) ka pasoja të thella dhe shumëdimensionale, që ndryshojnë mënyrën se si shtetet perceptojnë dhe praktikojnë sigurinë kombëtare. Një nga transformimet më thelbësore është zhvendosja e teatrit të luftës nga fronti i drejtpërdrejtë në hapësira globale. Në këtë kuadër, efektet e veprimeve ushtarake nuk ndihen më vetëm në terrenin fizik, por përhapen në hapësirën digjitale, ekonominë, diplomacinë dhe perceptimet publike. Për shembull, sulmet kibernetike të Rusisë në Ukrainë dhe vende të tjera evropiane kanë goditur jo vetëm infrastrukturën energjetike dhe telekomunikacionin, por kanë ndikuar gjithashtu në besimin publik dhe stabilitetin politik të këtyre shteteve, duke treguar se fronti i luftës nuk është më i kufizuar nga kufijtë gjeografikë.[41]

Një tjetër dimension i rëndësishëm, është rritja e paqëndrueshmërisë në rajone strategjike. Përmes kombinimit të operacioneve hibride, forcave proxy dhe kompanive private ushtarake, Rusia ka krijuar zona tensioni që nuk kanë qenë më parë të pranishme. Në Afrikë, për shembull, prezenca e kompanive si Wagner në Republikën Qendrore Afrikane dhe në Libi ka ndikuar drejtpërdrejt në stabilitetin e qeverive lokale dhe ka rritur konkurrencën për burimet minerale dhe kontrollin e portave strategjike.[42] Kjo paqëndrueshmëri ka efekte zinxhir: ajo ndikon në tregjet globale të energjisë, linjat e furnizimit dhe madje në politikat e partnerëve ndërkombëtarë, duke treguar se veprimet e një shteti mund të kenë pasoja të menjëhershme dhe afatgjata në nivel global.[43]

---

[40] NATO StratCom Centre of Excellence, *Hybrid Threats and 6th Generation Warfare* (Riga: NATO StratCom COE, 2022).

[41] International Institute for Strategic Studies (IISS), *The Military Balance 2025* (London: Routledge, 2025).

[42] Center for Strategic and International Studies (CSIS), *Russian Military Operations and Hybrid Warfare Analysis* (Washington, DC: CSIS, 2023).

[43] Russian Ministry of Defence, *Military Doctrine of the Russian Federation* (Moscow: Ministry of Defence, 2020).

Përfundime

Lufta e Gjeneratës së Gjashtë (6GW) përfaqëson një transformim rrënjësor të konfliktit modern, ku lufta nuk kufizohet më në përballje të drejtpërdrejta ushtarake, por shtrihet në dimensione të shumta si teknologjia, informacioni, ekonomia, diplomacia dhe operacionet hibride. Analiza e veprimtarisë globale ushtarake të Rusisë tregon se ajo ka ndërtuar një model kompleks veprimi, duke kombinuar mjete konvencionale dhe jokonvencionale për të ndikuar ambientin strategjik në nivele të ndryshme dhe në teatro të shumta gjeografike.

Përdorimi i sulmeve kibernetike, dezinformimit dhe manipulimit të perceptimit publik e ka shndërruar informacionin në një armë strategjike me ndikim afatgjatë. Integrimi i inteligjencës artificiale, dronëve, sistemeve autonome dhe forcave hibride, përfshirë kompanitë private ushtarake, ka rritur efikasitetin operativ të Rusisë duke minimizuar ekspozimin e drejtpërdrejtë të forcave shtetërore. Ky model tregon se avantazhi strategjik nuk varet më vetëm nga fuqia ushtarake klasike, por nga aftësia për të menaxhuar dhe manipuluar një sistem kompleks ndërveprimesh.

Veprimet ruse në Evropën Lindore, Lindjen e Mesme, Afrikë dhe rajone të tjera kanë krijuar "zona gri" ndikimi, me pasoja të drejtpërdrejta për stabilitetin rajonal dhe rendin global. Përballë këtyre sfidave, NATO dhe partnerët e saj duhet të adoptojnë një paradigmë të re sigurie, duke integruar mbrojtjen kibernetike, operacionet psikologjike, inteligjencën dhe diplomacinë në një qasje të unifikuar. Në përfundim, 6GW dëshmon se konceptet tradicionale të luftës janë të pamjaftueshme dhe se siguria e së ardhmes kërkon mendim strategjik të integruar, fleksibël dhe proaktiv.

Bibliografia

1. Adamsky, Dmitry. *The Culture of Military Innovation*. Stanford: Stanford University Press, 2010.
2. Center for Strategic and International Studies (CSIS). *Russian Military Operations and Hybrid Warfare Analysis*. Washington, DC: CSIS, 2023.
3. Galeotti, Mark. *Russian Political War: Moving Beyond the Hybrid*. London: Routledge, 2019.
4. Giles, Keir. *Russia's New Tools for Confronting the West*. London: Chatham House, 2016.
5. Grau, Lester W., and Charles K. Bartles. *The Russian Way of War*. Fort Leavenworth, KS: Army University Press, 2016.
6. Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.
7. International Institute for Strategic Studies (IISS). *The Military Balance 2025*. London: Routledge, 2025.

8. Kofman, Michael, et al. *Russian Military Strategy*. Arlington, VA: CNA, 2020.
9. Marten, Kimberly. *Russia's Use of Semi-State Security Forces*. Washington, DC: CSIS, 2019.
10. Ministry of Defence of the Russian Federation. *Russian Military Doctrine*. Moscow: Ministry of Defence of the Russian Federation, 2020.
11. NATO Strategic Communications Centre of Excellence. *Hybrid Threats and 6th Generation Warfare*. Riga: NATO StratCom COE, 2022.
12. Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.
13. Sharif, Israa, and Safa Abbas Fadel. "Developments in Sixth Generation Warfare Methods." *Journal of Asian Multicultural Research for Social Sciences Study*, 2026.
14. Solmaz, Tarik. "Hybrid Warfare: A Dramatic Example of Conceptual Stretching." *NSF Journal* 23, no. 1 (2022).
15. "Lufta hibride dhe dezinformimi." *The Geopost*.
16. "Lufta hibride e Rusisë në Ballkanin Perëndimor." *Octopus Journal – Institute for Hybrid Warfare Studies*, 2024.
17. *Russian Grand Strategy in the Era of Global Competition*. Manchester: Manchester University Press, 2022.

Inteligjenca Artificiale në fushën ushtarake dhe implikimet e saj për paqen dhe sigurinë

Kolonel (R) Roland BERZANI
Drejtor i Drejtorisë së Radiozbulimit
Agjencia e Inteligjencës dhe Sigurisë së Mbrojtjes

Trajtesë e shkurtuar

Inteligjenca Artificiale po transformon me shpejtësi fushën ushtarake, me implikime të thella për paqen dhe sigurinë ndërkombëtare. Deri vonë, diskutimet shumëpalëshe përqendroheshin kryesisht te Sistemet Autonome të Armëve Vdekjeprurëse (LAWS), një aplikim i rëndësishëm por i kufizuar. Në fund të vitit 2024, Asambleja e Përgjithshme e KB[1] miratoi një rezolutë historike që njohu gamën e gjerë të aplikimeve ushtarake të IA dhe kërkoi shqyrtimin e saj përtej sistemeve të armëve. Kjo rezolutë u mbështet në rritjen e ndërgjegjësimit dhe tërheqjes politike, të nxitura edhe nga iniciativa jashtë KB, si samitet e IA dhe deklaratat për përdorimin ushtarak përgjegjës të IA dhe autonomisë[2]. Shtytja për një IA të përgjegjshme ka hapur kanale të reja dialogu ndërmjet shteteve, duke nxitur diskutime për zhvillimin, vendosjen dhe përdorimin e sigurt e të kontrolluar të saj. Komuniteti ndërkombëtar ka mundësinë të formësojë të ardhmen e paqes dhe sigurisë ndërkombëtare në epokën e IA, duke vendosur në thelb parimet e përgjegjshme dhe duke forcuar besimin e ndërsjellë.

Për të avancuar këtë debat në një fushë që evoluon me shpejtësi, është thelbësore të qartësohet koncepti i "fushës ushtarake", të analizohen zbatimet kryesore të IA, sfidat përkatëse dhe rekomandimet për zhvillimin e politikave në të gjitha nivelet. Duke u mbështetur në hulumtimet e UNIDIR, propozohet një udhërrëfyes drejt një qasjeje efektive kombëtare të IA në fushën ushtarake.

[1] General Assembly Resolution 79/239, "Artificial Intelligence in the Military Domain and its implications for international Peace and Security", 24 December 2024, https://docs.un.org/en/A/RES/79/239. p 1-4

[2] https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy.

Fjalë kyçe: Inteligjenca artificiale, fushë ushtarake, aplikim ushtarak i IA, komandim-kontroll (C2), mjete të drejtuara nga IA, menaxhim informacioni, autonomi e avancuar, kornizë qeverisjeje.

Hyrje

Inteligjenca Artificiale po transformon me shpejtësi fushën ushtarake dhe po ndikon drejtpërdrejt në paqen dhe sigurinë ndërkombëtare. Iniciativa si samitet mbi IA e përgjegjshme në fushën ushtarake (Responsible AI in the Military Domain–REAIM) dhe Deklarata Politike mbi Përdorimin Ushtarak të Përgjegjshëm të IA dhe Autonomisë kanë rritur ndjeshëm vëmendjen ndërkombëtare, duke e zhvendosur debatin përtej LAWS dhe duke theksuar ndikimet e gjera të IA në siguri. Në këtë kontekst, Rezoluta 79/239 e Asamblesë së Përgjithshme të KB (dhjetor 2024) shënoi rezolutën e parë të OKB-së mbi IA në kontekstin ushtarak, duke krijuar një platformë për diskutim mbi mundësitë dhe rreziqet e saj. Për vite me radhë, UNIDIR ka kontribuar në këtë debat përmes kërkimeve dhe dialogëve shumëpalësh mbi potencialin transformues të IA për paqen dhe sigurinë ndërkombëtare.

Një sfidë qendrore mbetet përcaktimi i "fushës ushtarake", e cila interpretohet ndryshe nga shtete të ndryshme, në varësi të peizazheve të tyre të sigurisë dhe praktikave operacionale. Për disa shtete, ajo përfshin edhe detyra të sigurisë së brendshme si: policimi, kontrolli kufitar, lufta ndaj krimit të organizuar, mbrojtja e infrastrukturës kritike si dhe ndihma humanitare në përgjigje të fatkeqësive natyrore, për shtete të tjera, kufizohet në operacionet në fushën e betejës. Këto dallime ndikojnë drejtpërdrejt në diskutimet shumëpalëshe.

Në shumë kontekste operacionale brenda fushës ushtarake, IA vepron si një shumëzues force në disa detyra ushtarake, duke përfshirë C2, menaxhimin e informacionit dhe inteligjencën, autonominë e avancuar, logjistikën, trajnimin dhe simulimin, si dhe funksionet organizative e mbështetëse. Në C2, IA rrit shpejtësinë dhe cilësinë e vendimmarrjes, duke i ndihmuar kështu komandantët të analizojnë me shpejtësi skenarët e fushëbetejës. Ajo ka potencialin të përmirësojë respektimin e Ligjit Ndërkombëtar Humanitar (LNH), p.sh., duke integruar proporcionalitetin e detajuar dhe vlerësime të tjera ligjore. IA mund të analizojë me shpejtësi volume të mëdha të dhënash duke përmirësuar ndërgjegjësimin për situatën dhe zbulimin e kërcënimeve. Në logjistikë, IA optimizon zinxhirët e furnizimit dhe mirëmbajtjen parashikuese, duke rritur gatishmërinë operacionale dhe përmirësuar qëndrueshmërinë e operacioneve ushtarake me kalimin e kohës. IA mbështet më tej autonominë e avancuar në dronë, sigurinë kibernetike dhe operacionet në fushën e informacionit. Trajnimi dhe simulimi përfitojnë nga IA duke krijuar mjedise e skenarë sintetikë të personalizuar dhe realistë. Pra, IA mund të ofrojë mënyra të reja për të zbutur rreziqet dhe zvogëluar dëmet.

Megjithatë, integrimi i IA në kontekste ushtarake paraqet gjithashtu rreziqe

dhe sfida të konsiderueshme si: teknologjike, të sigurisë, ligjore, politike dhe etike. *Teknologjikisht,* sistemet ushtarake të IA përballen me çështje që lidhen me cilësinë, disponueshmërinë dhe paragjykimet e natyrshme të të dhënave, të cilat mund të çojnë në rezultate të paparashikueshme dhe potencialisht të dëmshme, duke përfshirë shkeljet e së drejtës ndërkombëtare. Nga ana tjetër *dobësitë e sigurisë* kibernetike i ekspozojnë sistemet e IA ndaj sulmeve kundërshtare, gjë e cila kërkon masa të rrepta sigurie. Sfidat e sigurisë përfshijnë rreziqet e llogaritjeve të gabuara apo përshkallëzimit të paqëllimshëm, veçanërisht në proceset e shpejta të vendimmarrjes dhe autonomisë të mundësuara nga IA, të cilat mund të rezultojnë në përgjigje përshkallëzuese. Një garë potenciale armatimesh me IA përkeqëson tensionet ndërkombëtare dhe rajonale, duke çuar ndoshta në rezultate destabilizuese të ngjashme me garat historike të armatimeve. Përhapja e teknologjive të IA tek aktorët joshtetërorë komplikon më tej peizazhet e kërcënimeve dhe kërkon menaxhim të kujdesshëm të ciklit jetësor të sistemeve ushtarake të IA. Përveç kësaj, dezinformimi i gjeneruar nga IA kërcënon stabilitetin shoqëror duke minuar besimin në informacion dhe mund të ndikojë drejtpërdrejtë në operacionet ushtarake. *Sfidat ligjore* sillen rreth sigurimit të pajtueshmërisë me të drejtën ndërkombëtare, veçanërisht LHN dhe të drejtën ndërkombëtare për të drejtat e njeriut. Debatet kryesore përqendrohen në llogaridhënien dhe përgjegjësinë shtetërore apo individuale për veprimet e nxitura nga IA, veçanërisht tek ato që kanë të bëjnë me vendimet vdekjeprurëse. Përtej të drejtës ndërkombëtare, *konsideratat etike* theksojnë ruajtjen e gjykimit njerëzor në vendimmarrjen kritike dhe parandalimin e paragjykimeve shoqërore nga depërtimi në sistemet e IA.

Në nivel shumëpalësh, krijimi i një platforme gjithëpërfshirëse të udhëhequr nga KB vlerësohet si thelbësore. Kjo mundëson një dialog të rregullt institucional për të adresuar implikimet më të gjera të IA ushtarake në paqen dhe sigurinë ndërkombëtare. Platforma mund të ndërtohet mbi parimet dhe kornizat ekzistuese ndërkombëtare të IA siç janë rekomandimet e UNESCO-s apo angazhimet e bëra në Paktin Global Digjital dhe t'i rafinojë ato më tej për zbatim në fushën ushtarake. Këto parime mund të zhvillohen më tej në norma të sjelljes së përgjegjshme në zhvillimin, vendosjen dhe përdorimin e IA në fushën ushtarake dhe të ofrojnë një bazë të fortë për instrumentet e ardhshme shumëpalëshe. *Në nivel rajonal*, kornizat ekzistuese mund të përdoren në përshtatjen e masave për ndërtimin e besimit dhe udhëzimeve që pasqyrojnë kontekstet lokale të sigurisë. Dialogët ndër-rajonalë do të lehtësonin të mësuarit e ndërsjellë, do të parandalonin ngërçet e informacionit dhe do të përfshinin perspektiva të larmishme që do të inkurajonin përgjigje koherente në nivel global. *Në nivel kombëtar*, shtetet duhet të zhvillojnë strategji gjithëpërfshirëse të IA që detajojnë vizionin, prioritetet dhe kornizat e qeverisjes, duke siguruar pajtueshmërinë me normat ndërkombëtare dhe standardet etike. Strukturat e forta të qeverisjes (p.sh., komitetet e dedikuara të IA dhe bordet e etikës), së

bashku me rishikimet e vijueshme ligjore, do të rrisnin llogaridhënien dhe sigurinë. Transparenca dhe protokollet e llogaridhënies do të mbështesnin më tej zbatimin e përgjegjshëm të IA. Standardet e larta të menaxhimit/qeverisjes të të dhënave, qasjet e menaxhimit të ciklit jetësor, programet rigoroze të trajnimit dhe udhëzimet e azhurnuara operacionale ushtarake plotësojnë këto masa kombëtare të propozuara, duke siguruar integrimin e përgjegjshëm të IA në fushën ushtarake. Pra, integrimi i IA në kontekste ushtarake paraqet mundësi të rëndësishme, sikundër dhe sfida komplekse për paqen dhe sigurinë.

1. Përcaktimi i fushës ushtarake

Rajone dhe shtete të ndryshme e përcaktojnë fushëveprimin e "fushës ushtarake" në mënyra të ndryshme. Në disa kontekste kombëtare dhe rajonale, roli i forcave të armatosura përfshin funksione të sigurisë së brendshme dhe publike, si ndihma në zbatimin e ligjit, mbrojtja e kufijve apo lufta kundër krimit të organizuar, duke e zbehur vijën ndarëse ndërmjet mbrojtjes dhe policimit[3]. Në disa shtete, forcave të armatosura u besohet edhe mbështetja e operacioneve humanitare, përfshirë shpërndarjen e furnizimeve mjekësore dhe reagimin ndaj fatkeqësive natyrore. Ndërkohë, në disa të tjera, fusha ushtarake konceptohet më ngushtë, duke u përqendruar kryesisht në mbrojtjen kombëtare dhe operacionet konvencionale, veçanërisht ato luftarake jashtë territorit kombëtar.

Këto dallime burojnë nga mjedisi specifik i sigurisë së secilit shtet, nga natyra e kërcënimeve me të cilat përballen, si dhe nga kornizat ligjore dhe normative[4] përkatëse. Si rezultat, nuk ekziston një përkufizim universal i fushës ushtarake[5]: ajo mund të përfshijë një spektër të gjerë aktivitetesh në një kontekst, ndërsa të kufizohet në detyra strikt luftarake në një tjetër.

Është e rëndësishme të theksohet se një ndryshim i tillë në përcaktimin e fushës ushtarake nuk duhet të shihet si pengesë për qeverisjen ndërkombëtare të IA apo për dialogun mbi IA. Në fakt, njohja dhe respektimi i këtyre nuancave, si dhe pranimi i shkallës së ndikimit të ndërsjellë që do të kenë përdorimet ushtarake dhe joushtarake të IA, mund të çojë në një debat politik më gjithëpërfshirës dhe në fund të fundit të forcojë qeverisjen globale të IA. Për të qenë efektive, qeverisja duhet të mbetet e ndjeshme ndaj perspektivave të sigurisë rajonale, duke siguruar që kornizat për qeverisjen e IA ushtarake të jenë të adaptueshme ndaj realiteteve të shteteve dhe rajoneve të ndryshme[6]. Në këtë kuadër, një qasje e dobishme për përcaktimin e fushës ushtarake është hartëzimi i konteksteve të ndryshme operacionale ku angazhohen forcat ushtarake, duke ndihmuar strukturalisht diskutimet mbi qeverisjen e IA.

[3] Y. Afina, The Global Kaleidoscope of Military AI Governance (Geneva: UNIDIR, 2024).
[4] Po aty.
[5] G. Persi Paoli and Y. Afina, AI in the Military Domain: A Briefing Note for States (Geneva: UNIDIR, 2025).
[6] Y. Afina, The Global Kaleidoscope of Military AI Governance (Geneva: UNIDIR, 2024).

Një dallim i parë që duhet bërë është ai midis përdorimit të aftësive të IA nga forcat ushtarake në konflikte të armatosura (si ndërkombëtare ashtu dhe jo ndërkombëtare) siç përcaktohet nga e drejta ndërkombëtare (DN) dhe përdorimit të tyre nga forcat ushtarake kur vendosen në operacione të tjera. Ky dallim është thelbësor pasi kontekstet e dallueshme ngrenë pyetje të ndryshme ligjore, operacionale, teknike dhe etike. Megjithatë, mund të mos jetë praktike të përdoret përtej vlerësimit ligjor, duke pasur parasysh se i njëjti lloj operacioni mund të bjerë brenda ose jashtë fushëveprimit të konfliktit të armatosur bazuar në intensitetin e operacionit ose nivelin e dhunës. Brenda kategorisë më të gjerë të dislokimeve ushtarake që bien jashtë konfliktit të armatosur siç përcaktohet nga DN, mund të bëhet një dallim i mëtejshëm midis ***(a)*** operacioneve ushtarake që kërkojnë përdorimin e forcës si; operacionet kundër terrorizmit, kundër piraterisë ose kundër kryengritjes, ***(b)*** operacioneve ushtarake në mbështetje të sigurisë kombëtare dhe rendit publik, si; mbështetja për zbatimin e ligjit kombëtar, sigurinë kufitare ose mbrojtjen e infrastrukturës kritike kombëtare, dhe ***(c)*** ndihmës ushtarake, e cila përfshin skenarë të tillë si; operacionet e paqes, ndihma humanitare dhe në rast fatkeqësish, evakuimi i civilëve dhe kërkim-shpëtimin.

Duhet theksuar se ka fusha të pashmangshme mbivendosjeje midis kategorive të ndryshme dhe se vendi ku përshtatet secili operacion specifik do të varet shumë nga konteksti. Operacionet hibride, p.sh., mund të kenë elementë që shtrihen në kategori të ndryshme. Operacionet e mësipërme mund të arrijnë pragun ligjor për t'u konsideruar konflikte të armatosura jo ndërkombëtare.

2. Zbatimet e IA-së në fushën ushtarake

Në kontekste të ndryshme operacionale, siç u trajtua më lart, organizatat e mbrojtjes dhe ato ushtarake po eksplorojnë dhe po zbatojnë IA-në në një spektër të gjerë aplikimesh, shumë prej të cilave nuk përfshijnë armë apo përdorimin e forcës vdekjeprurëse. Inteligjenca Artificiale konsiderohet një shumëzues potencial i forcës, i cili mund të rrisë efikasitetin, cilësinë e vendimmarrjes dhe efektivitetin në një sërë funksionesh ushtarake[7]. Ndërsa teknologjia evoluon, rastet e reja të përdorimit, përfshirë zhvillimin e sistemeve të reja ose përmirësimin e atyre ekzistuese përmes IA-së), krijohen ose rafinohen; ose, nëse rezultojnë të pabesueshme apo jo kosto-efektive në krahasim me alternativat jo-IA, braktisen. Bazuar në kërkimet dhe angazhimin e UNIDIR-it me shtete dhe ekspertë[8], mundësitë dhe potencialet që burojnë nga miratimi i IA-së në fushën ushtarake mund të grupohen në kategoritë e mëposhtme:

Komandim-Kontrolli: Mjetet e mbështetjes së vendimmarrjes të bazuara në IA mund t'i ndihmojnë komandantët në detyra të tilla si analiza e misionit,

[7] https://unidir.org/wp-content/uploads/2025/04/UNIDIR_Yasmin-Afina_Briefing_UNSC_Arria_AI_4-April-2025-3.pdf. p 1-4

[8] https://unidir.org/event/the-second-roundtable-for-ai-security-and-ethics-raise/.

analiza e objektivave dhe zhvillimi i kurseve të veprimit. Për shembull, një algoritëm mund të ndihmojë në analizimin e të dhënave të fushëbetejës për të identifikuar objektiva me vlerë të lartë ose për të optimizuar planet duke kombinuar skenarë të ndryshëm me parametrat e misionit dhe kufizimet e përcaktuara nga operatorët njerëzorë (p.sh. kufizimet kohore dhe gjeografike, toleranca ndaj dëmeve anësore, etj.). Sistemet e komandim-kontrollit (C2) të mundësuara nga IA mund të grumbullojnë të dhëna, të përpunojnë informacion në shkallë të gjerë dhe të sugjerojnë opsione më shpejt sesa stafi njerëzor, duke pasur potencialin të përmirësojnë ritmin dhe cilësinë e vendimmarrjes.

Nëse përdoret në mënyrë të përshtatshme, IA mund të konsolidojë vlerësime komplekse të proporcionalitetit (p.sh. përmes integrimit të të dhënave mbi rrezen e shpërthimit, dendësinë e popullsisë dhe faktorët kohorë) për të kështilluar nëse një sulm mund të kryhet brenda kufijve të së Drejtës Ndërkombëtare Humanitare (DNH). Në mënyrë të ngjashme, IA mund të ndihmojë në zbatimin e masave paraprake, si p.sh. sugjerimi i taktikave alternative që reduktojnë rrezikun për civilët. Këto përdorime ilustrojnë se si IA mund të forcojë respektimin e DNH-së nga vendimmarrësit dhe përdoruesit, duke u ofruar komandantëve informacion dhe rekomandime më të mira për minimizimin e dëmeve[9]. Një numër gjithnjë e në rritje shtetesh pranojnë se integrimi i IA në planifikimin ushtarak mund të mundësojë vlerësime më objektive dhe të bazuara në të dhëna mbi proporcionalitetin dhe domosdoshmërinë e përdorimit të forcës[10].

Informacioni dhe inteligjenca: IA mund të përdoret për inteligjencë, mbikëqyrje dhe zbulim (ISR), duke analizuar sasi të mëdha të dhënash nga sensorë të ndryshëm, imazhe satelitore dhe trafiku i komunikimeve për të zbuluar modele ose kërcënime. Mësimi automatik, në parim, mund të automatizojë përpunimin e çdo lloj informacioni për të cilin ekzistojnë të dhëna—nga pamjet e zbulimit deri te regjistrat e sigurisë kibernetike—duke zbuluar njohuri që analistët njerëzorë mund t'i humbasin. Po ashtu, sistemet e IA mund të ndihmojnë në menaxhimin e informacionit duke bashkuar të dhëna nga burime të shumta dhe duke shpërndarë inteligjencën përkatëse te njësitë në terren. Këto aplikacione rrisin ndërgjegjësimin për situatën, duke shqyrtuar "të dhëna të shumta" për informacion të zbatueshëm dhe duke e përpunuar atë për konsum nga përdoruesit.

Autonomi e avancuar: IA mund të mundësojë një nivel më të avancuar autonomie si në sistemet fizike ashtu edhe në ato digjitale. Në botën fizike, kjo mund të nënkuptojë, p.sh., sisteme pa ekuipazh që janë më të afta të kryejnë detyra të ndryshme edhe në mjedise ku nuk ka komunikim ose ku mbikëqyrja e drejtpërdrejtë nuk mund të realizohet për shkak të rrethanave mjedisore apo

[9] Persi Paoli and Afina, AI in the Military Domain.

[10] Y. Afina and S. Grand-Clément, Bytes and Battles: Inclusion of Data Governance in Responsible Military AI (Geneva: UNIDIR, 2024).

veprimeve kundërshtare. IA mund të ofrojë avantazhe operacionale dhe taktike të konsiderueshme duke mundësuar një nivel më të sofistikuar autonomie edhe në një sistem armësh ku vendimi përfundimtar për të hapur zjarr është tagër e drejtpërdrejtë të njeriut. Në fushën digjitale, IA mund të përdoret për sigurinë kibernetike (p.sh., për forcimin e rezistencës kombëtare kibernetike duke përmirësuar inteligjencën e kërcënimeve, monitorimin e rrjetit si dhe reagimin ndaj incidenteve), si dhe për të forcuar aftësitë sulmuese kibernetike. Brenda fushës digjitale, IA mund të përforcojë e mbështesë aftësitë njohëse të luftës dhe operacionet e informacionit, duke përfshirë inteligjencën dhe kundërzbulimin.

Logjistika dhe mbështetja: IA mund të përmirësojë ndjeshëm shtyllën kurrizore logjistike të strukturave ushtarake, pas vijave të frontit, si një mundësues kyç qëndrueshmërie të operacioneve ushtarake. Kjo përfshin mirëmbajtjen parashikuese të pajisjeve (përdorimi i IA për të parashikuar dështimet ose nevojat e shërbimit), menaxhim të zinxhirëve të furnizimit dhe transportit dhe optimizim të vendosjes së personelit dhe materialeve. P.sh., algoritmet e IA mund të përmirësojnë gatishmërinë e forcave duke i drejtuar kolonat e furnizimit në mënyrë më efikase ose duke ndarë pjesë këmbimi bazuar në kërkesën e parashikuar. Përdorime të tilla shpesh përshtatin zgjidhjet civile të IA (p.sh., në transport ose menaxhimin e inventarit) për qëllime ushtarake, duke përbërë kështu një shembull kryesor të vijave të paqarta midis aplikimeve civile dhe atyre ushtarake.

Trajnimi dhe simulimi: Sistemet e drejtuara nga IA mund të përdoren për të trajnuar personelin ushtarak. Sistemet inteligjente të mësimdhënies, simulatorët e lojërave të luftës dhe trajnerët e realitetit virtual mund të *personalizojnë* dhe optimizojnë skenarët në mjedise sintetike dhe të ofrojnë reagime për të trajnuarit. P.sh., bazuar në të dhënat e inteligjencës ekzistuese, mësimet dhe praktikat e mira nga operacionet e kaluara, IA mund të gjenerojë sjellje realiste të kundërshtarit në simulatorë ose të sugjerojë përmirësime në programet e trajnimit duke analizuar të dhënat e performancës. Këto aplikacione ndihmojnë në përgatitjen e forcave për operacione reale në mënyrë më efektive dhe efikase, duke përfshirë edhe perspektivën e kostos.

Funksione të tjera organizative e mbështetëse: Ushtarakët mund të aplikojnë IA në role administrative e mbështetëse - ndonjëherë të ngjashme me ato të sektorit civil. Kjo mund të përfshijë mjete IA për menaxhimin e personelit (p.sh., rekrutimi ose analiza e menaxhimit të talenteve) ose për mbështetje mjekësore (p.sh., diagnostikimi për forcat e dislokuara). FA të ndryshme po eksperimentojnë gjithashtu sisteme të mundësuara nga IA për detyra mbështetëse në prapavijë (si financimi ose prokurimi). Edhe nëse aplikime të tilla mund të duken të largëta nga një kontekst operacional, ato janë komponentë strategjikë që kontribuojnë ndjeshëm në aftësinë e çdo FA-je për t'u mobilizuar. Kjo i ekspozon ato ndaj kërcënimeve të kundërshtarëve në të njëjtën mënyrë si objektivat e vijës së parë. Si konkluzion, përdorimi i

IA në fushën ushtarake varion nga niveli taktik në atë strategjik dhe ajo shkon përtej armëve duke përfshirë sisteme mbështetëse, ndihma për vendimmarrje dhe mjete analitike që synojnë të përmirësojnë efektivitetin ushtarak. Këto aplikime po bëhen gjithnjë e më të përhapura. Shumë FA e konsiderojnë miratimin e IA si thelbësor për të mbajtur ritmin me format në zhvillim të luftës - të tilla si kërcënimet kibernetike dhe hibride - dhe për të ruajtur një avantazh konkurrues.

3. Sfidat

Përveç "premtimeve" të saj, integrimi i IA në çështjet ushtarake sjell sfida të rëndësishme. Këto sfida mund të kategorizohen në tre fusha kryesore: ***(a) sfidat teknologjike*** të brendshme të sistemeve të IA dhe zhvillimit të tyre; ***(b) sfidat e sigurisë*** që rrjedhin nga përdorimi i tyre; dhe ***(c) sfidat ligjore, politike dhe etike*** në lidhje me qeverisjen/*menaxhimin* dhe përdorimin e përgjegjshëm.

3.1. Sfidat teknologjike

Vetë natyra e sistemeve ushtarake të IA do të thotë se ato përballen me një mori pengesash teknike që lidhen me besueshmërinë, sigurinë dhe transparencën.

- Cilësia dhe disponueshmëria e të dhënave.

Një çështje themelore është *cilësia dhe disponueshmëria* e të dhënave. Algoritmet e IA (veçanërisht modelet e të mësuarit automatik) kërkojnë sasi të mëdha të të dhënave të trajnimit, por në kontekste ushtarake, të dhënat përkatëse mund të jenë të pakta, të paplota ose të njëanshme. Dështimet e sistemeve të IA mund të rrjedhin nga "të panjohura të njohura": dobësi të fshehura ose raste të jashtëzakonshme në të dhëna dhe kod që projektuesit nuk i kanë parashikuar[11]. Nëse një sistem i IA nuk është përballur me një skenar të caktuar në të dhënat e trajnimit, ai mund të reagojë në mënyrë të paparashikueshme në botën reale. Kjo ndryshueshmëri është e rrezikshme në mjedise ushtarake me rreziqe të larta.

Paragjykimi i të dhënave përbën një shqetësim serioz. Nëse të dhënat pasqyrojnë paragjykime në bazë gjinie, race, moshe, kulture apo karakteristikash të tjera demografike, sistemi mund t'i riprodhojë ose amplifikojë ato[12]. Në kontekst ushtarak, kjo mund të çojë në identifikim të gabuar të objektivave ose civilëve, duke cenuar efektivitetin operacional, pajtueshmërinë me të drejtën ndërkombëtare humanitare (DNH) dhe standardet etike. P.sh., një sistem i mbledhjes së inteligjencës mund të mos jetë domosdoshmërisht i trajnuar mbi të dhëna që marrin në konsideratë kontekste specifike kulturore në të cilat mund të pranohet mbajtja e armëve; sistemi mund të identifikojë gabimisht

[11] A. H. Michel, Known Unknowns: Data Issues and Military Autonomous Systems (Geneva: UNIDIR, 2021).

[12] Gender and Disarmament & Security and Technology Programmes, "Gender and Lethal Autonomous Weapons Systems", Factsheet, UNIDIR, 2024.

praktika të tilla si kërcënime të mundshme. Si një shembull tjetër, algoritmet e paragjykuara të përdorura në sistemet ushtarake, të tilla si vizioni kompjuterik për dronët mbikëqyrës, mund të identifikojnë gabimisht një burrë civil si luftëtar bazuar në një supozim (i nxjerrë nga të dhëna të gabuara) se shumica e luftëtarëve janë burra. Përvoja nga aplikimet civile tregon se korrigjimi i këtyre paragjykimeve është teknikisht kompleks dhe shpesh i pjesshëm.

- Errësira / patejdukshmëria.

Errësira/natyra e *"kutisë së zezë"* është një sfidë tjetër teknike e shumë modeleve të IA. Mësimi modern i makinave (p.sh., rrjetet nervore të thella) shpesh funksionon në mënyra që nuk janë të shpjegueshme për operatorët njerëzorë. Kjo mungesë transparence e bën të vështirë vlerësimin e besueshmërisë së sistemeve të IA dhe diagnostikimin e gabimeve. Në përdorimin ushtarak, pamundësia për të kuptuar pse një sistem i IA bëri një rekomandim ose ndërmori një veprim mund të gërryejë besimin njerëzor dhe të ndërlikojë llogaridhënien. Sigurimi i interpretueshmërisë, shpjegueshmërisë ose gjurmueshmërisë së vendimeve të IA është një problem teknik i pazgjidhur. Teknikat për "IA të shpjegueshme" ekzistojnë, por zbatimi i tyre në sisteme komplekse ushtarake është një sfidë e vazhdueshme. Përveç kësaj, gjurmueshmëria në sisteme ose, të paktën, dokumentacioni i fuqishëm dhe protokollet e provave mjeko-ligjore do të siguronin që shtetet të jenë në gjendje të përmbushin detyrimin e DNH-së për të kryer hetime efektive për shkeljet e dyshuara[13].

- Testimi dhe vlerësimi.

Testimi dhe vlerësimi i sistemeve të IA paraqesin sfida të veçanta krahasuar me sistemet tradicionale ushtarake. Prokurimi klasik mbështetet në testim sekuencial (nga prototipi në testim operacional) për sisteme relativisht *përcaktuese*. Në të kundërt, sistemet e IA janë adaptive dhe performanca e tyre mund të ndryshojë me përditësimin e të dhënave ose ndryshimin e mjedisit operacional. Për këtë arsye, ato kërkojnë vlerësim të vazhdueshëm, përfshirë shqyrtime ligjore periodike, me qëllim sigurimin e përputhshmërisë së qëndrueshme me ligjin ndërkombëtar[14].

Kompleksiteti shtohet për shkak të varësisë nga konteksti dhe kufizimeve në transferueshmërinë e performancës. Një sistem që përmbush standardet e sigurisë në një mjedis të caktuar (p.sh. shkretëtirë) nuk mund të supozohet se do të funksionojë me të njëjtin nivel besueshmërie në kushte të tjera (p.sh. klimë me dëborë). Ky kufizim është veçanërisht i rëndësishëm në kushtet e transferimit të teknologjisë midis aleatëve dhe partnerëve të sigurisë, ku ndryshimet në mjedis, infrastrukturë dhe doktrinë mund të ndikojnë në performancë dhe ndërveprueshmëri.

[13] Y. Afina, Regional Perspectives on the Application of International Humanitarian Law to Lethal Autonomous Weapon Systems (Geneva: UNIDIR, 2025).

[14] Afina and Persi Paoli, Governance of Artificial Intelligence in the Military Domain.

Integrimi i komponentëve të IA në "sisteme të sistemeve" më të mëdha rrit rrezikun e mënyrave të reja të dështimit dhe dobësive kibernetike që burojnë nga ndërveprimet mes nënsistemeve, duke e bërë testimin gjithëpërfshirës edhe më të ndërlikuar. Për këtë arsye, kërkohen procese rigoroze të sigurimit të IA, të bazuara në prova, për t'u ofruar autoriteteve besim të mjaftueshëm mbi besueshmërinë e sistemit përpara autorizimit të përdorimit në kontekste specifike.

Për më tepër, sistemet ushtarake të IA të vendosura në mjedise armiqësore përballen me përpjekje të qëllimshme për manipulim, mashtrim apo degradim. Ndërtimi i qëndrueshmërisë ndaj këtyre ndërhyrjeve mbetet fushë kërkimore aktive dhe ende e pakonsoliduar plotësisht. Nëse dobësitë nuk identifikohen dhe përforcohen, ato mund të shfrytëzohen nga kundërshtarët. Bashkëveprimi midis IA dhe kërcënimeve kibernetike jo vetëm që ndërlikon vendosjen operacionale, por edhe rrit kërcënimet tradicionale ndaj sistemeve digjitale, duke kërkuar përditësim të vazhdueshëm të politikave dhe qëndrimeve të sigurisë kibernetike nga qeveritë dhe forcat ushtarake[15].

- Keqpërdorimi ose keqkuptimi.

Elementi njerëzor kryqëzohet me çështjet teknike: një operator mund të keqpërdorë ose keqkuptojë (qëllimisht ose jo) rezultatet e IA. Probleme të tilla si paragjykimi i automatizimit (d.m.th., mbështetja e tepërt dhe pa diskutim në rekomandimet e IA) ose neveria/injorimi e algoritmit (d.m.th., mosbesimi dhe injorimi i plotë i IA) mund të ndodhin të dyja. Ndërfaqet e dobëta të përdoruesit ose trajnimi i pamjaftueshëm mund t'i përkeqësojnë këto tendenca[16]. Kështu, një pjesë e sfidës teknike është në të vërtetë socio-teknike - projektimi i mjeteve të IA që plotësojnë në mënyrë efektive vendimmarrësit njerëzorë dhe qenia i sigurtë që përdoruesit janë të trajnuar si të dinë si ta përdorin sistemin ashtu edhe të interpretojnë rezultatet e tij në mënyrë korrekte. Pa këtë edhe një sistem teknikisht i shëndoshë mund të përdoret në mënyrë të papërshtatshme, duke çuar në gabime ose aksidente.

3.2. Sfidat e sigurisë

Përfshirja e IA-së në aftësitë ushtarake ngre sfida serioze sigurie dhe mund të ndikojë në paqe dhe stabilitet. Një shqetësim i madh është *rreziku i përshkallëzimit të paqëllimshëm* ose humbjes së veprimit njerëzor, duke përfshirë kontrollin në konflikt. Sistemet e mundësuara nga IA, veçanërisht ato që veprojnë me shpejtësi të lartë pa mbikëqyrje të njeriut, mund të përshkallëzojnë angazhimet aq shpejt sa njerëzit nuk mund të ndërhyjnë ose të ulin tensionin. Nëse dy kundërshtarë vendosin sisteme IA që reagojnë ndaj njëri-tjetrit në mikrosekonda, kjo mund të çojë në intensifikimin e një krize,

[15] J. Pinelis and K. Vignard, "Responsible AI vs. AI Assurance: A Semantic Showdown", Presentation, Global Conference on AI Security and Ethics 2025, 27 March 2025, Geneva.

[16] I. Puscas, Human-Machine Interfaces in Autonomous Weapon Systems (Geneva: UNIDIR, 2022).

para se komandantët të kenë kohë për të negociuar ose për ta frenuar atë. Ky skenar i çuditshëm, por i mundshëm dhe i besueshëm, i shkaktuar nga ndërveprimet algoritmike, ndonjëherë i quajtur "lufta e shpejtë" shpesh vlerësohet si një rrezik i ri i përshkallëzimit. Megjithatë, dhe në skenarë më të ngadaltë, mjetet ndihmëse të vendimmarrjes të mundësuara nga IA-ja mund të rekomandojnë veprime më agresive ose të keqinterpretohen, duke çuar në përshkallëzim të paqëllimshëm. Një tjetër sfidë sigurie është *perspektiva e një gare armatimesh të IA* dhe ndikimi i saj në sigurinë globale. Fuqitë e mëdha po investojnë shumë në IA ushtarake për të shmangur mbetjen prapa rivalëve. Kjo konkurrencë mund të çojë në një vendosje të shpejtë të teknologjive të IA të paprovuara në një përpjekje për superioritet, ose në përdorimin e fushëbetejës si një terren testimi për aftësi të reja të IA. Historia sugjeron që garat e armatimeve pa pengesa mbrojtëse rrisin mosbesimin dhe mundësinë e konfrontimit. Ndërsa IA bëhet një faktor në ekuilibrin ushtarak, disa analistë paralajmërojnë për efekte destabilizuese të ngjashme me garat e kaluara të armëve[17]. Përveç kësaj, një narrativë e tillë mund të inkurajojë gjithashtu miratimin e shpejtë dhe të parakohshëm të IA në kurriz të protokolleve të testimit, vlerësimit dhe pranimit si rezultat i frikës dhe shqetësimeve për mbetje prapa në garën e supozuar të armatimeve të IA. *Përhapja e përdoruesve të teknologjisë së IA* është një tjetër shqetësim sigurie. Mjetet e IA, shumë prej të cilave janë të disponueshme komercialisht ose me burime të hapura, mund të ripërdoren nga aktorë joshtetërorë, grupe terroriste ose grupe të tjera të armatosura.

Përdorimi i IA nga këto grupe mund të ndryshojë ndjeshëm peizazhin e kërcënimit, duke kërkuar që forcat ushtarake të zhvillojnë kundërmasa adekuate. Ndërsa çështja e IA me burim të hapur dhe lehtësia relative e armatimit të sistemeve komercialisht të disponueshme janë faktorë kyç për t›u marrë në konsideratë, ato nuk janë të vetmet rreziqe përhapjeje. Ndërsa sistemet e IA të nivelit ushtarak bëhen më gjerësisht të disponueshme do të rritet në mënyrë të pashmangshme rreziku i devijimit të tyre në tregun e paligjshëm[18]. Kjo është arsyeja pse miratimi i menaxhimit të plotë të ciklit jetësor të sistemeve ushtarake të IA, (përfshi protokollet e rrepta të çmontimit), është me rëndësi të madhe[19]. Për më tepër, *IA ka implikime për mjedisin e informacionit* si në paqe ashtu edhe gjatë kohës së luftës. IA gjeneruese dhe mjetet e tjera mund të prodhojnë dezinformim në shkallë të gjerë. Kjo mund të gërryejë besimin në informacion dhe në institucione dhe ka potencialin të destabilizojë shoqëritë dhe të ketë ndikim në të gjithë ciklin jetësor të konfliktit, duke përfshirë operacionet paqeruajtëse. P.sh. gjatë një konflikti, videot e rreme ose komunikimet e rreme

[17] Puscas, AI and International Security.

[18] M. Martinez et al., Diversion Analysis Framework, Arms Trade Treaty Issue Brief 3 (Geneva: UNIDIR, Conflict Armament Research and Stimson Centre, 2021).

[19] Persi Paoli and Afina, AI in the Military Domain; Afina and Persi Paoli, Governance of AI in the Military Domain.

të gjeneruara nga IA mund të mbjellin konfuzion midis popullsisë civile ose edhe midis njësive ushtarake. Shtetet kanë ngritur shqetësime se IA mund të përdoret për të prishur vendimmarrjen duke përmbytur hapësirën e informacionit me të dhëna të rreme ose mashtruese[20].

3.3. Sfidat ligjore, politike dhe etike

Shfaqja e IA në ushtri ngre gjithashtu pyetje të thella ligjore, normative dhe etike, të përforcuara nga diapazoni dhe diversiteti i konteksteve në të cilat mund të veprojnë forcat ushtarake.

- Sfidat ligjore.

Një sfidë qendrore ligjore është sigurimi që përdorimi i IA të jetë në përputhje me të drejtën ndërkombëtare ekzistuese, por pa u kufizuar vetëm në të drejtën ndërkombëtare humanitare, si dhe ligjin ndërkombëtar të të drejtave të njeriut dhe të drejtën ndërkombëtare penale. P.sh., DNH përcakton dispozita dhe parime ligjore si: dallimi (diskriminimi i luftëtarëve nga civilët) dhe proporcionaliteti (shmangia e dëmit të tepërt) në konfliktin e armatosur. Vendosja e karakteristikave të IA në operacione ushtron presion mbi këto parime. Aktualisht në diskutimet kombëtare dhe jo vetëm shfaqet çështja se si të përcaktohet përgjegjësia dhe llogaridhënia shtetërore dhe individuale nëse një sistem i IA nuk vepron siç kërkohet. Kjo sfidë është e lidhur ngushtë me rrezikun e perceptuar të një boshllëku llogaridhënieje. Çështja është si duhet t'i atribuohet përgjegjësia kur ndodh një incident që përfshin një sistem të IA (p.sh., një sistem mbështetës i vendimmarrjes së IA klasifikon gabimisht një objekt i cili më pas angazhohet në mënyrë të paligjshme).

Strukturat tradicionale të komandimit ushtarake supozojnë qëllimin dhe kontrollin njerëzor në çdo nivel, duke ndjekur parimin e autoritetit të deleguar. Ndërsa përdorimi i IA mund të "errësojë" linearitetin e këtij procesi. Disa vende vlerësojnë se DNH ekzistuese është e mjaftueshme, por ka nevojë për masa të duhura për të siguruar pajtueshmërinë kur përdoren sistemet e IA. Të tjerë vlerësojnë se implikimet që vijnë nga nivelet e larta të autonomisë dhe shpejtësia e madhe e IA paraqesin dilema të reja ligjore që kërkojnë rregulla të reja, të dedikuara për të vendosur një interpretim të caktuar të ligjit ashtu siç duhet të jetë. Ekziston gjithashtu çështja e kryerjes së rishikimeve ligjore: Konventa e Gjenevës (neni 36 i Prot. shtesë) i cili urdhëron shtetet që kur studiojnë, zhvillojnë, blejnë ose miratojnë një armë/mjet/metodë të re luftimi, të përcaktojnë nëse përdorimi i saj do të ishte i ndaluar nga protokolli ose nga ndonjë rregull tjetër i së drejtës ndërkombëtare që zbatohet për shtetin. Zbatimi i kësaj në sistemet e IA (ato që do të klasifikohen si një mjet/metodë lufte) mund të ngrejë një sërë sfidash dhe kjo kërkon shqyrtimin jo vetëm të pajisjeve, por edhe të algoritmeve dhe të dhënave[21]. Kjo duhet të bëhet me

[20] Y. Afina, The Global Kaleidoscope of Military AI Governance (Geneva: UNIDIR, 2024).

[21] Goussac and Pacholska, The Interpretation and Application of International Humanitarian Laws.

kalimin e kohës përmes shqyrtimeve ligjore përsëritëse. Siç është aktualisht, ka një debat aktiv se si të kryhet një shqyrtim i tillë, për cilin standard dhe sa shpesh.

- Sfidat politike.

Përtej sfidave ligjore, fusha e politikave dhe qeverisjes përballet me pyetje se si të rregullohet IA ushtarake në nivel kombëtar e ndërkombëtar. Në nivel kombëtar, shumë vende sapo kanë filluar të hartojnë politika dhe strategji për IA. Përpjekje të tilla janë edhe më embrionale për aplikime në fushën ushtarake[22]. Ky hap i rëndësishëm jo vetëm që ofron një mundësi për ekosistemin e sigurisë kombëtare për t'u konsultuar me palët e interesuara përkatëse të industrisë dhe akademike, por shërben gjithashtu si katalizator për veprime shtesë politike dhe qeverisëse në nivele operacionale dhe taktike.

Në nivel ndërkombëtar, nuk ka një proces të dedikuar politikash ndërqeveritar ose shumëpalëshe të dedikuar për IA në fushën ushtarake dhe implikimet e saj për paqen dhe sigurinë ndërkombëtare. Kjo ka fragmentuar diskutimet mbi IA dhe sigurinë nëpër organe të ndryshme specialistësh secila duke parë një fushë të ngushtë aplikimi (p.sh., armë kibernetike ose autonome). Ndërsa diskutimet e specialistëve janë të nevojshme, mungesa e një procesi politik gjithëpërfshirës dhe të nivelit të lartë mbi IA në fushën ushtarake rrezikon të krijojë boshllëqe në qeverisje që mund të shfrytëzohen nga aktorë keqdashës. Me rezolutën 79/239, Asambleja e Përgjithshme ka filluar një rrugë që mund të çojë në një proces më të gjerë ndërkombëtar, por dallimet midis shteteve për mënyrën e veprimit vazhdojnë. Arritja e një konsensusi mund të jetë e vështirë duke pasur parasysh perspektivat e ndryshme mbi përfitimet dhe rreziqet ushtarake të IA, konsideratat e ndryshme kombëtare e rajonale mbi përdorimin e saj dhe kontekstin aktual gjeopolitik që ndikon në çdo diskutim shumëpalësh mbi çarmatimin. Megjithatë, dialogu i strukturuar dhe i rregullt institucional mbi këtë çështje është i nevojshëm.

- Sfidat etike.

Në lidhje me etikën, IA në fushën ushtarake shkakton debate rreth rolit të gjykimit njerëzor në vendimmarrje në lidhje me përdorimin e forcës vdekjeprurëse dhe dehumanizimin e mundshëm të luftës. Ekziston një shqetësim i cituar shpesh në lidhje me delegimin e vendimeve për jetë a vdekje tek algoritmet, me Sekretarin e Përgjithshëm të KB që mban një qëndrim të vendosur kundër këtij skenari[23]. Ekzistojnë gjithashtu implikime etike dhe shoqërore në lidhje me paragjykimet dhe pabarazitë. Sistemet e IA mund të

[22] Afina, Draft Guidelines for the Development of a National Strategy on AI in Security and Defence: (Geneva: UNIDIR, 2024).

[23] UN Secretary General's message to the inaugural Global Conference on AI, Security and Ethics,https://unidir.org/un-secretary-generals-message-inaugural-global-conference-ai-security-ethics/;

trashëgojnë paragjykime nga grupet e të dhënave të trajnimit, algoritmet e të mësuarit automatik të pakontrolluara ose të pakorrigjuara, ose zhvilluesit njerëzorë me paragjykimet e tyre. Paragjykimet shoqërore (në bazë të gjinisë, racës, etj.) mund të kodohen në IA, duke çuar potencialisht në rezultate diskriminuese në shënjestrimin ose vlerësimin e kërcënimeve. Etikisht, është e rëndësishme të përfshihen konsideratat e diversitetit në zhvillimin ushtarak të IA-së gjatë gjithë ciklit jetësor - si për të parandaluar ashtu edhe për të korrigjuar paragjykimet në sisteme. Së fundmi, ekziston sfida e qeverisjes së përfshirjes së shumë palëve të interesuara. Shumë inovacione në IA nuk vijnë nga qeveria, por nga sektori privat, laboratorët kërkimorë dhe akademia. Qeverisja efektive e IA ushtarake do të kërkojë kontribut dhe bashkëpunim nga industria dhe laboratorët kërkimorë (të cilët ndërtojnë teknologjinë) dhe shoqëria civile (e cila artikulon normat etike e shqetësimet publike). Megjithatë, kapërcimi i hendekut midis sigurisë kombëtare dhe komuniteteve të teknologjisë së hapur nuk është i thjeshtë[24].

Disa rekomandime

Nga analiza e mësipërme dalin disa rekomandime që mund të udhëzojnë palët e interesuara në maksimizimin e përfitimeve të IA në fushën ushtarake, duke zbutur njëkohësisht rreziqet e saj.

- Nga qeveria nevojitet *formulimi dhe zbatimi i një strategjie gjithëpërfshirëse kombëtare mbi IA në siguri dhe mbrojtje*, e cila duhet të përshkruajë vizionin e vendit mbi IA ushtarake, fushat prioritare, strukturat qeverisëse dhe si do të mbështesë të drejtën ndërkombëtare dhe etikën. Dokumenti duhet të mbulojë aspektet procedurale (si do të zbatohet, rishikohet, përditësohet strategjia) dhe aspektet thelbësore (masa specifike mbi qeverisjen e të dhënave, sigurimin e IA) si dhe duhet të përfshijë mbrojtjen, shkencën dhe teknologjinë, rishikimin ligjor, agjenci dhe departamente të tjera, si dhe konsultime me palët e interesuara në vend. Pas formulimit strategjia duhet të zbatohet nëpërmjet planeve konkrete të veprimit dhe duhet të monitorohet dhe rishikohet rregullisht në dritën e ndryshimeve teknologjike. Një qasje e tillë redukton reagimin *ad hoc* ndaj zhvillimeve teknologjike dhe qartëson rolet dhe përgjegjësitë në ciklin e plotë të jetës së sistemeve të IA.

- Nevojitet *ngritja e organeve të përhershme qeverisjeje për IA brenda institucioneve të mbrojtjes* (p.sh., një komitet drejtues i IA në nivel ministrie për të mbikëqyrur të gjitha programet/bordet e shqyrtimit të etikës për të vlerësuar projektet me rrezik të lartë) *dhe grupe pune ndëragjenci civile-ushtarake për të shqyrtuar zhvillimet e reja*, për të parashikuar shqetësimet e përdorimit të dyfishtë para vendosjes dhe për të zhvilluar masa mbrojtëse të mundshme kundër keqpërdorimit. Këto struktura ofrojnë fokus dhe llogaridhënie si dhe

[24] W. He and A. Anand, The 2022 Innovations Dialogue: AI Disruption, Peace and Security (Geneva: UNIDIR, 2023).

krijojnë pika kontrolli efektive që projektet e IA duhet të kalojnë dhe të zbatojnë në mënyrë të vazhdueshme (p.sh., miratimi etik, certifikimi i sigurisë), duke zvogëluar shanset e vendosjes së pasigurt ose të paligjshme.

- Nevojitet miratimi i masave për *nxitjen e transparencës dhe llogaridhënies në nivel kombëtar* në lidhje me programet e IA dhe rezultatet e tyre. Brenda vendit, kjo mund të nënkuptojë mbajtjen e regjistrave të detajuar të vendimeve mbi sistemet e IA dhe raportimin e çdo incidenti ose mosfunksionimi në zinxhirin komandues. Qeveria duhet të jenë transparente (aq sa e lejon siguria) në lidhje me qasjen e saj ndaj IA ushtarake (përmes dokumenteve të publikuar, deklaratave për shtyp mbi politikat e reja etj.). Në kontekstin llogaridhënie, rregullat ushtarake duhet të sqarojnë se komandantët janë përgjegjës për veprimet e sistemeve të IA nën komandën e tyre. Në rast aksidenti shteti duhet të kenë një protokoll hetimi që përfshin ekspertë teknikë për të shqyrtuar çështjet që lidhen me IA, dhe mundësisht duhet të komunikojnë publikisht gjetjet dhe veprimet korrigjuese.

- Nga organizatat e mbrojtjes dhe rregullatorët kombëtarë, nevojitet *zbatimi i praktikave të forta të të dhënave dhe një kornizë qeverisjeje për të gjitha aplikacionet ushtarake të IA*. Kjo përfshin investimin në kurimin e grupeve të të dhënave me cilësi të lartë, krijimin e procedurave për verifikim dhe përditësim të të dhënave si dhe zbatimin e masave të sigurisë së tyre. Para vendosjes së sistemeve të IA nevojiten udhëzime që të dhënat të mblidhen, përpunohen, përdoren në mënyrë të përgjegjshme (duke respektuar çështjet e privatësisë, minimizimin e paragjykimeve dhe origjinën e të dhënave), të ruhen dhe të shkatërrohen ato përfundimisht. Duke i dhënë përparësi qeverisjes së fortë të të dhënave dhe sigurimit të infrastrukturës së duhur për mundësimin e saj, ushtritë mund të përmirësojnë performancën dhe besueshmërinë e sistemeve të tyre të IA dhe të ulin shkallën e gabimeve. Kjo do të zbusë dhe rreziqe të tilla si paragjykimet dhe manipulimi armiqësor i të dhënave.

- *Organizatat dhe kontraktorët e mbrojtjes duhet të menaxhojnë sistemet e IA gjatë gjithë ciklit jetësor* - nga projektimi dhe zhvillimi, te testimi, vendosja, përditësimi dhe çmontimi - duke integruar vlerësime dhe masa zbutëse të rrezikut në çdo fazë. Kjo përfshin procese rigoroze të sigurimit të IA (testim, verifikim, vlefshmëri), projektim që promovon pajtueshmërinë që në fazën fillestare, prokurim që i jep përparësi sigurisë dhe mbrojtjes, si dhe vendosje të masave të monitorimit e kontrollit gjatë përdorimit operacional.

- Vendimmarrësit dhe organizatat e mbrojtjes, në partneritet me sektorin privat dhe institucionet arsimore duhet *të zhvillojnë programe të gjera trajnimi për personelin ushtarak mbi IA* dhe kultivojnë një gjeneratë të re oficerësh e specialistësh të aftë për IA. Kjo përfshin jo vetëm trajnim teknik, por edhe atë mbi aspektet etike dhe ligjore të përdorimit të IA në operacione. Trajnimi duhet të përfshijë skenarë të përshtatur në ushtrimet ushtarake për të mundësuar personelin të fitojë përvojë në bashkëveprimin me sistemet e

IA në kushte reale dhe të procedurave të testimit. Përmes trajnimit, personeli ushtarak duhet të zhvillojë një kuptim të parametrave të përdorur për testim, rezultateve të testimit, standardeve të përdorura për vlerësim dhe faktorëve që do të kontribuonin në kalibrimin e besimit mes njeriut dhe teknologjisë. Ekspertiza dhe gjykimi njerëzor mbeten kritike dhe personeli duhet të kuptojë pikat e forta dhe kufizimet e IA në mënyrë që ta përdorë atë siç duhet në çdo kontekst. Trajnimi zvogëlon keqpërdorimin dhe mundëson bashkëpunim më efektiv njeri-makinë.

- Udhëheqja e Forcave të Armatosura *duhet të përshtatë ose të hartojë doktrina, procedura standarde operacionale, taktika dhe rregulla angazhimi që reflektojnë integrimin e IA*, duke garantuar që zinxhiri i përgjegjësisë të mbetet i qartë dhe operacionet të zhvillohen në përputhje të plotë me të drejtën kombëtare dhe ndërkombëtare.

Përfundime

– IA është e gatshme të ndikojë thellësisht në fushën ushtarake, duke ofruar aftësi dhe efikasitet të ri, edhe pse prish praktikat e vendosura dhe paraqet rreziqe të reja. Vlerësohet se implikimet e IA ushtarake janë me dy tehe: nga njëra anë, IA mund të forcojë mbrojtjen, të përmirësojë saktësinë dhe të ndihmojë vendimmarrësit njerëzorë; nga ana tjetër, nëse IA nuk kontrollohet, ajo mund të sjellë pasiguri, paqëndrueshmëri dhe dilema etike.

– Integrimi i suksesshëm i IA në fushën ushtarake nuk duhet të matet vetëm nga aftësitë e fituara. Shkalla në të cilën përdorimi i IA mbështet ose edhe forcon arkitekturën ndërkombëtare të paqes dhe sigurisë duhet të bëhet një standard i rëndësishëm i vlerësimit. Potenciali shkatërrues i IA mund të menaxhohet dhe të drejtohet drejt përmirësimit të sigurisë globale. Anasjelltas, neglizhimi i qeverisjes së IA-së ushtarake mund të përkeqësojë garat e armatimit ose të gërryejë ligjet e luftës.

– Veprimet e rekomanduara ofrojnë një udhërrëfyes për të krijuar një kornizë të fortë për qeverisjen me përgjegjësi të IA ushtarake në nivel kombëtar. Zbatimi i tyre do të kërkojë vullnet politik dhe burime. Ndonjëherë do të kërkojë ndryshime kulturore brenda qeverisë dhe komunitetit ushtarak për një qasje më gjithëpërfshirëse ndaj aftësive ushtarake. Zbatimi i plotë i tyre do të rrisë shumë gatishmërinë e vendit për të përfituar nga përfitimet e IA, duke kontrolluar rreziqet e saj.

– IA në fushën ushtarake është një realitet që nuk duhet as të mbivlerësohet dhe as të nënvlerësohet. Është një fushë që duhet të formësohet me kujdes. Duke karakterizuar fushëveprimin e saj, duke hartuar zbatimet dhe mundësitë e saj si dhe duke njohur realisht sfidat e saj, politikëbërësit dhe praktikuesit mund të projektojnë një rrugë që ruan sigurinë ndërkombëtare.

Bibliografia:

1. Giacomo Persi Paoli and Yasmin Afina, AI in the Military Domain: A Briefing Note for States (Geneva: UNIDIR, 2025), https://unidir.org/publication/ai-military-domain-briefing-note-states/.
2. Yasmin Afina, Regional Perspectives on the Application of International Humanitarian Law to Lethal Autonomous Weapon Systems (Geneva: UNIDIR, 2025), https://unidir.org/publication/regional-perspectives-on-the-application-of-international-humanitarian-law-to-lethal-autonomous-weapon-systems/.
3. Netta Goussac and Magdalena Pacholska, The Interpretation and Application of International Humanitarian Laws in Relation to Lethal Autonomous Weapon Systems: Background Paper on the views of States, scholars and other experts (Geneva: UNIDIR, 2025), https://unidir.org/publication/the-interpretation-and-application-of-international-humanitarian-law-in-relation-to-lethal-autonomous-weapon-systems/.
4. Ioana Puscas, Large Language Models and International Security: A Primer (Geneva: UNIDIR, 2024), https://unidir.org/publication/large-language-models-and-international-security-a-primer/.
5. Yasmin Afina, The Global Kaleidoscope of Military AI Governance: Decoding the 2024 Regional Consultations on Responsible AI in the Military Domain (Geneva: UNIDIR, 2024), https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/.
6. Giacomo Persi Paoli and Samuele Dominioni, Exploring the AI–ICT Security Nexus (UNIDIR, 2024), https://unidir.org/publication/exploring-the-ai-ict-security-nexus/.
7. Gender and Disarmament & Security and Technology Programmes, "Gender and Lethal Autonomous Weapons Systems", UNIDIR, 2024, https://unidir.org/publication/gender-and-lethal-autonomous-weapons-systems/.
8. Sarah Grand-Clément, Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain (Geneva: UNIDIR, 2023),https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/.
9. Ioana Puscas, AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures (Geneva: UNIDIR, 2023),https://unidir.org/publication/ai-and-international-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/.
10. Wenting He and Alisha Anand, The 2022 Innovations Dialogue: AI Disruption, Peace and Security (Geneva: UNIDIR, 2023), https://unidir.org/publication/the-2022-innovations-dialogue-ai-disruption-peace-and-security-conference-report/.

11. Ioana Puscas, Human–Machine Interfaces in Autonomous Weapon Systems (Geneva: UNIDIR, 2022), https://unidir.org/publication/human-machine-interfaces-in-autonomous-weapon-systems/.
12. Arthur Holland Michel, Known Unknowns: Data Issues and Military Autonomous Systems (Geneva: UNIDIR, 2021), https://unidir.org/publication/known-unknowns-data-issues-and-military-autonomous-systems/.
13. Manuel Martinez, Alfredo Malaret, Erica Mumford and Natalie Briggs, Diversion Analysis Framework, Arms Trade Treaty Issue Brief 3 (Geneva: UNIDIR, Conflict Armament Research and Stimson Centre, 2021), https://unidir.org/publication/arms-trade-treaty-issue-brief-3-diversion-analysis-framework/.
14. Giacomo Persi Paoli, Kerstin Vignard, David Danks and Paul Meyer, Modernizing Arms Control: Exploring Responses to the Use of AI in Military Decision-Making. https://unidir.org/publication/modernizing-arms-control/.
15. ArthurHolland Michel, The BlackBox, Unlocked: Predictability and Understandability in Military AI (UNIDIR, 2020), https://unidir.org/publication/the-black-box-unlocked/.
16. Yasmin Afina and Sarah Grand-Clément, Bytes and Battles: Inclusion of Data Governance in Responsible Military AI, Centre for International Governance Innovation (CIGI) Papers no. 38. https://www.cigionline.org/static/documents/Afina-Grand_Clement.pdf.
17. General Assembly resolution 79/239, "Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security", 24 December 2024, https://docs.un.org/en/A/RES/79/239.
18. United Nations, A New Agenda for Peace, Our Common Agenda Policy Brief no. 9 (New York: UN, July 2023), https://peacemaker.un.org/sites/default/files/document/files/2024/08/our-common-agenda-policy-brief-new-agenda-peace-en.pdf.
19. UN Secretary-General, Message to the Inaugural Global Conference on AI, Security and Ethics 2025, https://unidir.org/un-secretary-generals-message-inaugural-global-conference-ai-security-ethics/.
20. Jane Pinelis and Kerstin Vignard, "Responsible AI vs. AI Assurance: A Semantic Showdown", Presentation, Global Conference on AI Security and Ethics 2025, Geneva, 27 March 2025.
21. UNIDIR, "The Roundtable for AI, Security and Ethics: Forging Global Alignment through Multistakeholder Dialogue", 24 October 2024, https://unidir.org/event/the-roundtable-for-ai-security-and-ethics-forging-global-alignment-through-multistakeholder-dialogue/.
22. UNIDIR, "The Second Roundtable for AI, Security and Ethics (RAISE)", 4–6 September 2024, https://unidir.org/event/the-second-roundtable-for-ai-security-and-ethics-raise/.

Gjendja juridike, kapacitetet e politikës evropiane të sigurisë dhe të mbrojtjes së përbashkët

Msc. Jurgert ZAVALANI
Jurist në Sektorin Juridik, AFA

Trajtesë e shkurtuar

Siguria, në dimensionet e saj ekonomike, sociale, ushtarake, politike dhe mjedisore, përbën një të mirë publike thelbësore për ruajtjen e kohezionit shoqëror, stabilitetit institucional dhe balancës në marrëdhëniet ndërkombëtare. Në sistemin ndërkombëtar bashkëkohor, ajo ka marrë një karakter gjithnjë e më kompleks dhe shumëdimensional, duke u reflektuar në dokumentet universale për mbrojtjen e të drejtave të njeriut, në strategjitë kombëtare të zhvillimit dhe në arkitekturën globale të sigurisë. Ky zgjerim konceptual pasqyron transformimet e thella të mjedisit ndërkombëtar dhe të natyrës së kërcënimeve, të cilat nuk kufizohen më vetëm në dimensionin ushtarak.

Artikulli analizon evolucionin e konceptit të sigurisë nga qasja tradicionale, e përqendruar kryesisht në sovranitetin shtetëror dhe mbrojtjen territoriale, drejt një kuptimi më të gjerë që përfshin edhe dimensionet e sigurisë njerëzore, ekonomike dhe institucionale. Në këtë kuadër, shqyrtohet edhe ndërlidhja midis sigurisë dhe parimit të sigurisë juridike, si një element rregullator i rendit ndërkombëtar, veçanërisht në kontekstin e normave dhe mekanizmave të parashikuara nga Organizata e Kombeve të Bashkuara për përdorimin e forcës dhe menaxhimin e krizave ndërkombëtare.

Duke u mbështetur në analizën teorike dhe në literaturën klasike dhe bashkëkohore të studimeve të sigurisë dhe marrëdhënieve ndërkombëtare, artikulli argumenton se siguria duhet të kuptohet si një koncept dinamik dhe relacional, i kushtëzuar nga ndërveprimi i faktorëve politikë, ekonomikë dhe shoqërorë. Në këtë kuptim, siguria paraqitet njëkohësisht si një nevojë ekzistenciale për individin dhe shtetin, por edhe si një konstrukt normativ dhe institucional, i formësuar nga evoluimi i sistemit ndërkombëtar.

Në përfundim, theksohet se zgjerimi i konceptit të sigurisë nuk e zëvendëson dimensionin tradicional shtetëror, por e plotëson atë, duke krijuar një kornizë analitike më gjithëpërfshirëse për të kuptuar sfidat bashkëkohore dhe për të projektuar politika më efektive në nivel kombëtar dhe ndërkombëtar.

Fjalë kyçe: siguria juridike; siguria njerëzore; siguria shtetërore; Bashkimi Evropian; mbrojtja e përbashkët; politikat evropiane të sigurisë; instrumentet juridike; Traktati i Lisbonës; armët e shkatërrimit në masë.

1. Qasja akademike e studimit të sigurisë sjell një mori variantesh trajtimi

Qasja akademike ndaj studimit të sigurisë paraqet një shumëllojshmëri mënyrash interpretimi dhe trajtimi të këtij koncepti, duke e analizuar atë nga perspektiva të ndryshme disiplinore. Për shkak se nuk ekziston një konsensus i plotë dhe koherent mbi përkufizimin e tij, përpjekja për ta elaboruar në mënyrë shteruese mbetet një sfidë e hapur për studiuesit.[1]

Siguria shtetërore konsiderohet një e mire[2] publike, e cila ofrohet nga shteti për të gjithë qytetarët pa diskriminim dhe përfaqëson një shprehje të përgjegjësisë së tij për mbrojtjen e lirive dhe të drejtave themelore të shtetasve[3].

Në këtë kuptim, shteti merr përsipër një sërë masash dhe përgjegjësish për të garantuar këtë të mirë publike; megjithatë, kufizimet strukturore, politike dhe ekonomike të shteteve e relativizojnë mundësinë e arritjes së një sigurie absolute.

Koncepti i **sigurisë njerëzore** [4], sipas përkufizimit të UNDP-së[5], i referohet

[1] Sipas B. Buzan — *"Në rastin e sigurisë, diskutimi është rreth përcaktimit të lirisë nga kërcënimi. Kur ky diskutim është në kontekstin e sistemit ndërkombëtar, siguria është diçka që lidhet me aftësinë e shteteve dhe shoqërive për ruajtjen e pavarësisë së identitetit dhe funksionalitetit të integritetit të tyre."* Ndër dhjetë përkufizimet e dhëna nga Ian Bellamy, Walter Lippman, Giacomo Luciani, Richard H. Ullman, Arnold Wolfers, Mohammed Ayoob, Ken Booth, Peter Hough, Eduard Kolodziej dhe Alan Collins, unë e gjej veten më afër përkufizimeve të Richard H. Ullman, Mohammed Ayoob, Ken Booth dhe Peter Hough. Këto përkufizime mund të sintetizohen në një të vetëm: Siguria kombëtare është strategjia dhe bashkësia e taktikave për të realizuar mbrojtjen e shtetasve, aktorëve të tjerë dhe sistemit politik të tyre nga kërcënime të dukshme dhe të padukshme, historike, të tashme dhe të ardhme, të cilat lidhen me arsye objektive dhe emocionale.

[2] For current definitions of public goods see any mainstream microeconomics textbook, e.g. Hal R. Varian, *Microeconomic Analysis*, ISBN 0-393-95735-7. Andreu Mas-Colell, Michael D. Winston & Jerry R. Green, *Microeconomic Theory*, ISBN 0-19-507340-1. Gravelle & Rees, *Microeconomics*, ISBN 0-582-40487-8.

[3] United Nations General Assembly. *Follow-up to the outcome of the Millennium Summit: Implementing the responsibility to protect. Report of the Secretary-General*. A/63/677. Sixty-third session, Agenda items 44 and 107. 12 January 2009.

[4] Dimensioni njerëzor i zhvillimit ka tërhequr vëmendjen për herë të parë në vitin 1970, si teori e avancuar nga liderët e Jugut të Botës. "Siguria njerëzore" është një koncept i kohëve të fundit, i cili fokusohet në mbrojtjen e individëve nga kërcënimet. Qendra e Sigurisë Njerëzore e ka formësuar këtë koncept të ri, i cili buron nga teoria e mendimit liberal, duke theksuar se *"shtet i sigurt nuk do të thotë automatikisht individ i sigurt."* (2006)

[5] Human Security. - Paradigm Shift or Hot Air? In: *International Security*, Vol. 26, no. 2, UNDP's 1994 definition, definition of human Security argues that the scope of global Security should Be expanded to include threats in seven areas: *Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Community Security, Political Security* R. Paris, (2001).

mbrojtjes së individit nga rreziqe konkrete që mund të kërcënojnë mbijetesën dhe mirëqenien e tij. Në këtë kuadër dallohen disa dimensione të sigurisë njerëzore, si siguria ushqimore, shëndetësore, politike, mjedisore, personale dhe ekonomike.

Siguria kombëtare lidhet me mbrojtjen e interesave themelore të shtetit dhe të qytetarëve të tij. Ajo përfshin njëkohësisht dimensionin e sigurisë së brendshme dhe të jashtme, duke u reflektuar në politikat kombëtare të sigurisë që ndjek çdo shtet. Këto politika ndikojnë drejtpërdrejt në jetën e qytetarëve, në zhvillimin social dhe ekonomik, si dhe në ruajtjen e paqes dhe stabilitetit rajonal. Mbrojtja e vendit nga sulmet ushtarake, nga kërcënimet dhe rreziqet e jashtme dhe të brendshme, mbetet një nga aspektet më thelbësore të sigurisë kombëtare.

Koncepti i sigurisë zë një vend të rëndësishëm në hierarkinë e nevojave jetike të çdo qenieje shoqërore, pasi lidhet drejtpërdrejt me natyrën njerëzore, organizimin shoqëror dhe mbijetesën ekzistenciale të individit dhe komunitetit. Për këtë arsye, siguria ka një domethënie universale dhe paraqitet si një fenomen kompleks dhe dinamik. Për rëndësinë që mbart, ajo është trajtuar gjerësisht në literaturën teorike të marrëdhënieve ndërkombëtare.

2. Instrumentet ligjore në dispozicion të Bashkimit Evropian

Që nga themelimi i tij, Bashkimi Evropian është përpjekur të forcojë rolin e vet në fushën e sigurisë dhe mbrojtjes, duke zhvilluar gradualisht instrumentet dhe kapacitetet e nevojshme për këtë qëllim. Një hap i rëndësishëm në këtë drejtim ishte miratimi i Strategjisë Evropiane të Sigurisë në vitin 2003, dokument në të cilin u identifikuan rreziqet kryesore që kërcënonin sigurinë e kontinentit evropian, si terrorizmi ndërkombëtar, përhapja e armëve të shkatërrimit në masë, mosfunksionimi i shteteve, konfliktet rajonale dhe krimi i organizuar. Krahas identifikimit të këtyre kërcënimeve, strategjia përcaktoi edhe qasjet dhe instrumentet për përballimin e tyre.

Më vonë, me hartimin e raportit mbi "Zbatimin e Strategjisë Evropiane të Sigurisë"**,** spektri i rreziqeve u zgjerua më tej, duke përfshirë fenomene të reja si terrorizmi kibernetik, pirateria, ndryshimet klimatike dhe siguria energjetike. Paralelisht, zhvillimi i instrumenteve dhe mekanizmave institucionalë i mundësoi Bashkimit Evropian të fitojë aftësi më të mëdha për të marrë vendime dhe për të ndërmarrë operacione në mënyrë autonome në përgjigje të krizave ndërkombëtare.

Operacionet e ndërmarra në këtë kuadër mbështeteshin nga forcat ushtarake të vëna në dispozicion nga shtetet anëtare, të cilat vepronin nën flamurin dhe mandatin e Bashkimit Evropian. Megjithatë, këto struktura nuk mund të konsideroheshin si një ushtri e përbashkët evropiane, për shkak të natyrës së tyre shumëkombëshe dhe faktit që komandimi operacional mbetej në kompetencën e shteteve kontribuese.

Përvoja e fituar nga misionet dhe operacionet e zhvilluara që prej vitit 2003 kontribuoi ndjeshëm në përmirësimin e kapaciteteve civile dhe ushtarake të Bashkimit Evropian. Si rezultat, profili i BE-së evoluoi gradualisht nga një aktor që mbështetej kryesisht në garancitë e sigurisë të ofruara nga NATO dhe Shtetet e Bashkuara të Amerikës, në një aktor që kontribuon gjithnjë e më shumë në prodhimin dhe menaxhimin e sigurisë ndërkombëtare.

Në vijim të përpjekjeve për forcimin e kapaciteteve dhe aftësive në fushën e mbrojtjes, zhvillimet institucionale u reflektuan edhe në traktatet themeluese të Bashkimit Evropian. Ndërsa Traktati i Nicës trajtonte kryesisht bashkëpunimin në fushën e armatimeve**,** Traktati i Lisbonës e zgjeroi ndjeshëm këtë fushë duke përfshirë edhe çështje të tilla si logjistika ushtarake, bashkëpunimi në fushën e inteligjencës dhe përmirësimi i aftësisë për dislokimin e shpejtë të forcave ushtarake.

Përveç rritjes së angazhimit të shteteve anëtare për përmirësimin e kapaciteteve të tyre ushtarake, Traktati i Lisbonës solli edhe dy risi të rëndësishme institucionale: së pari, koordinimi i përpjekjeve të shteteve anëtare për zhvillimin e aftësive ushtarake iu ngarkua Agjencisë Evropiane të Mbrojtjes (AEM**)**, së dyti, u krijua mekanizmi i bashkëpunimit të strukturuar të përhershëm (PESCO), i cili synon thellimin e bashkëpunimit ndërmjet shteteve anëtare që janë të gatshme dhe të afta të zhvillojnë kapacitete të përbashkëta mbrojtëse.

Megjithatë, angazhimi për zhvillimin e mëtejshëm të kapaciteteve mbeti kryesisht i përqendruar në komponentët ushtarakë të Politikës së Përbashkët të Sigurisë dhe Mbrojtjes (PESMP), ndërsa komponentët civilë—si bashkëpunimi policor, forcimi i shtetit të së drejtës, administrata civile dhe misionet civile të menaxhimit të krizave—nuk u shoqëruan me krijimin e mekanizmave të veçantë institucionalë për zhvillimin e tyre.

3. Zgjerimi i "Detyrave të Petërsbergut"

Një tjetër risi e sjellë nga Traktati i Lisbonës ishte zgjerimi i të ashtuquajturave "Detyrat e Petersbergut"**,** të cilat fillimisht u parashikuan në Deklaratën e Petersbergut dhe më pas u përfshinë në të drejtën primare të Bashkimit Evropian përmes Traktatit të Amsterdamit. Në fazën fillestare, këto detyra përfshinin misionet humanitare dhe të shpëtimit, operacionet paqeruajtëse, si dhe ndërhyrjet ushtarake në kuadër të menaxhimit të krizave, përfshirë edhe operacionet paqebërëse. Me hyrjen në fuqi të Traktatit të Lisbonës, spektri i këtyre detyrave u zgjerua ndjeshëm, duke përfshirë:

- misionet e përbashkëta të çarmatimit;
- misionet e këshillimit dhe asistencës ushtarake;
- misionet për parandalimin e konflikteve;
- misionet për stabilizimin e situatës pas konfliktit;

– luftën kundër terrorizmit, duke përfshirë edhe mbështetjen ndaj shteteve të treta në përpjekjet e tyre kundër terrorizmit[6].

Sa i përket mënyrës së realizimit të këtyre detyrave, dispozitat e Traktatit përcaktojnë kryesisht kushtet dhe kuadrin institucional të zbatimit të tyre. Objektivat konkrete, qëllimet dhe rregullat e përgjithshme për realizimin e këtyre misioneve përcaktohen nga Këshilli i Bashkimit Evropian. Ndërkohë, koordinimi i aspekteve civile dhe ushtarake të këtyre operacioneve është përgjegjësi e Përfaqësuesit të Lartë për Punët e Jashtme dhe Politikën e Sigurisë, i cili vepron nën autoritetin e Këshillit dhe mban kontakte të vazhdueshme me Komitetin Politik dhe të Sigurisë (neni 43 i Traktatit të Bashkimit Evropian).

4. Krijimi i një mbrojtjeje të përbashkët

Angazhimi i Bashkimit Evropian për ndërtimin e një politike të përbashkët të mbrojtjes, e cila në një fazë të mëvonshme do të mund të çonte drejt krijimit të një mbrojtjeje të përbashkët, u rikonfirmua edhe në Traktatin e Lisbonës. Ndryshe nga formulimi i përdorur në Traktatin e Amsterdamit, ku thuhej se kjo politikë "mund të çojë drejt një mbrojtjeje të përbashkët", Traktati i Lisbonës përdor formulimin "do të çojë drejt një mbrojtjeje të përbashkët", duke i dhënë kështu një dimension më të qartë politik këtij objektivi.

Vendimi për krijimin e një mbrojtjeje të përbashkët do të merrej nga Këshilli Evropian me unanimitet, ndërsa zbatimi i tij do të realizohej duke marrë parasysh karakteristikat e veçanta të politikave të sigurisë dhe mbrojtjes së shteteve anëtare, si dhe duke respektuar angazhimet e tyre në kuadër të NATO-s. Ky formulim tregon se, megjithëse shtetet anëtare pranonin nevojën për zhvillimin e një mbrojtjeje të përbashkët, ato ende nuk ishin plotësisht të gatshme ta realizonin atë në një formë të plotë integrimi, duke ruajtur një rol të rëndësishëm për interesat dhe politikat kombëtare të mbrojtjes[7].

Megjithatë, rëndësia e Traktatit të Lisbonës në këtë drejtim qëndron në krijimin e disa mekanizmave institucionalë që mund të shërbejnë si katalizatorë për arritjen e këtij objektivi. Ndër më të rëndësishmit janë:

- klauzola e mbrojtjes së ndërsjellë (neni 42(7) i Traktatit të Bashkimit Evropian), e cila vendos një bazë të fortë politike dhe juridike për solidaritetin ndërmjet shteteve anëtare në rast agresioni;
- bashkëpunimi i përhershëm i strukturuar (PESCO), i cili synon thellimin e bashkëpunimit ndërmjet shteteve që janë të gatshme dhe të afta të zhvillojnë kapacitete të përbashkëta në fushën e mbrojtjes[8].

[6] Neni 43 i TBE-së, i ndryshuar me Traktatin e Lisbonës, https://eur-lex.europa.eu/ (hyrë për herë të fundit më 23 Prill 2017).

[7] Neni 42(2) i TBE-së, i ndryshuar me Traktatin e Lisbonës, https://eur-lex.europa.eu/ (hyrë për herë të fundit më 23 prill 2017).

[8] Combarieu, Gilles *Security and Defence Aspects of the Lisbon Reform Treaty* (Paris 2008), fq. 4-5, http://europavarietas.visuart.eu/ (hyrë për herë të fundit më 12 mars 2014).

Gjithashtu, njohja e personalitetit juridik ndërkombëtar të Bashkimit Evropian (neni 47 i Traktatit të Bashkimit Evropian) ndikoi drejtpërdrejt në forcimin e rolit të tij si aktor ndërkombëtar në fushën e sigurisë dhe mbrojtjes. Në këtë kuadër, traktati i jep Bashkimit Evropian të drejtën për të lidhur marrëveshje ndërkombëtare (neni 37 i Traktatit të Bashkimit Evropian) dhe për t'u përfaqësuar në arenën ndërkombëtare në kuadër të Politikës së Përbashkët të Sigurisë dhe Mbrojtjes.

Si përfundim, mund të thuhet se neni 42(2) i Traktatit të Lisbonës shënon një hap të rëndësishëm drejt zhvillimit të një politike të përbashkët të mbrojtjes, duke krijuar një bazë më të konsoliduar juridike dhe institucionale për realizimin gradual të këtij objektivi.

5. Instrumentet ligjore

Njohja e personalitetit juridik të Bashkimit Evropian në kuadër të Politikës së Jashtme dhe të Sigurisë së Përbashkët (PJSP) solli dy pasoja të rëndësishme juridike. Së pari, ajo i mundësoi Bashkimit Evropian të lidhë marrëveshje ndërkombëtare me organizata ndërkombëtare dhe me shtete të treta, si dhe të anëtarësohet në organizata të caktuara ndërkombëtare. Së dyti, u konsolidua kuadri i instrumenteve të brendshme juridike për zbatimin e PJSP-së dhe, në mënyrë të veçantë, të Politikës së Përbashkët të Sigurisë dhe Mbrojtjes (PESMP).

Instrumentet ligjore në dispozicion të Bashkimit Evropian për zbatimin e PJSP-së u përcaktuan fillimisht në Traktatin e Amsterdamit dhe përfshinin:

- parimet dhe udhëzimet e përgjithshme, të cilat përcaktonin orientimin politik të përgjithshëm të veprimit të Bashkimit;
- strategjitë e përbashkëta, që përcaktonin objektivat dhe mjetet për realizimin e tyre;
- veprimet e përbashkëta, të cilat adresonin situata konkrete ndërkombëtare;
- qëndrimet e përbashkëta, që përcaktonin pozicionin e Bashkimit ndaj një çështjeje të caktuar ndërkombëtare.

Me hyrjen në fuqi të Traktatit të Lisbonës, instrumentet ligjore si "veprimet e përbashkëta"[9] dhe "qëndrimet e përbashkëta"[10] u zëvendësuan përkatësisht me "vendime që përcaktojnë veprimet që duhet të ndërmerren nga BE-ja " dhe "vendime që përcaktojnë qëndrimet që duhet të mbahen nga BE-ja"[11]. Traktati

[9] Veprime të përbashkëta i referohen një situate specifike ku ndërmarrja e veprimeve nga bashkimi konsiderohet e domosdoshme dhe në të përcaktohen objektivat, qëllimi dhe mjetet me të cilat do të realizohet. Ato angazhojnë Shtetet Anëtare.

[10] Pozicione të përbashkëta nga njëra anë përcaktojnë qëndrimin që do të mbajë BE-ja për një çështje të caktuar dhe përcaktojnë në përgjithësi udhëzime të përgjithshme që politikat kombëtare të shteteve anëtare duhet të jenë në pajtim me to.

[11] Neni 25 i TBE-së, i ndryshuar me Traktatin e Lisbonës, https://eur-lex.europa.eu/ (hyrë për herë të fundit më 23 prill 2017)

i Lisbonës nuk i referohet më në mënyrë të drejtpërdrejtë "strategjive të përbashkëta"[12], ndërsa "udhëzimet e përgjithshme" vazhdojnë të përcaktohen edhe nga ky Traktat[13]. Megjithatë, pavarësisht ndryshimeve terminologjike, natyra juridike e këtyre instrumenteve mbetet e njëjtë: ato nuk janë drejtpërdrejt të zbatueshme dhe nuk gëzojnë epërsi ndaj legjislacionit të brendshëm të shteteve anëtare. Instrumentet ligjore nëpërmjet të cilave Bashkimi Evropian zhvillon dhe zbaton PJSP-në, përfshirë edhe PESMP-në, janë të parashikuara në nenin 25 të Traktatit për Bashkimin Evropian (TBE). Konkretisht, ato përfshijnë:

1. Udhëzimet e përgjithshme, të cilat përcaktojnë orientimin strategjik të politikës së jashtme të Bashkimit.
2. Vendimet që përcaktojnë veprimet dhe qëndrimet e Bashkimit Evropian**,** si dhe marrëveshjet për zbatimin e tyre.
3. Forcimin e bashkëpunimit ndërmjet shteteve anëtare në fushën e politikës së jashtme dhe të sigurisë.

Vendimet e miratuara nëpërmjet këtyre instrumenteve, ndonëse janë juridikisht detyruese për shtetet anëtare, nuk mund të klasifikohen si akte legjislative. Traktati i Lisbonës përjashton shprehimisht miratimin e akteve legjislative në fushën e PJSP-së, përfshirë edhe PESMP-në.[14]

Ky parashikim sjell dy pasoja juridike në praktikë. Së pari, në bazë të Protokollit nr. 1[15] mbi rolin e parlamenteve kombëtare në Bashkimin Evropian**,** parlamentet kombëtare nuk mund të ngrenë pretendime për shkelje të parimit të subsidiaritetit apo proporcionalitetit ndaj këtyre akteve, përderisa ato nuk kanë natyrë legjislative. Së dyti, në rastin e miratimit të tyre nga Këshilli i Bashkimit Evropian, nuk zbatohet detyrimi procedural i parashikuar në nenin 16(8) të Traktatit për Bashkimin Evropian, i cili lidhet me transparencën e debatit dhe votimit për aktet legjislative.Traktati i Lisbonës parashikon disa kategori vendimesh në kuadër të PJSP-së, të cilat, për shkak të përjashtimit të akteve legjislative në këtë fushë (neni 41(1) i TBE-së[16]) kanë një natyrë kryesisht politike dhe operative.

---

[12] Neni 12 i Traktatit të Nicës, https://europa.eu/ (hyrë për herë të fundit më 23 prill 2017).

[13] Neni 12 i Traktatit të Nicës parashikon se: "...parimet dhe udhëzimet e përgjithshme për PJSP-në do të përcaktohen...", ndërsa Neni 25 i TBE-së, i ndryshuar me Traktatin e Lisbonës përdor vetëm termin "parime të përgjithshme".

[14] Neni 24(1) i Traktatit për Bashkimin Europian (TBE), i ndryshuar me Traktatin e Lisbonës, përcakton se politika e jashtme dhe e sigurisë së përbashkët i nënshtrohet rregullave dhe procedurave specifike. Ajo përcaktohet dhe zbatohet nga Këshilli Europian dhe Këshilli, kryesisht me unanimitet, përveç rasteve kur Traktati parashikon ndryshe. Në këtë fushë përjashtohet miratimi i akteve ligjore.
Neni 31(1) i TBE-së sanksionon se vendimet që lidhen me këtë kapitull merren nga Këshilli Europian dhe Këshilli me unanimitet, përveç kur ky kapitull parashikon ndryshime.

[15] Protokoll nr. 1 "Mbi rolin e Parlamenteve Kombëtare në BE", Neni 2 dhe Neni 3

[16] http://eur-lex.europa.eu/ (hyrë për herë të fundit më 25 Prill 2017).

- Vendimet mbi objektivat strategjikë dhe interesat e Bashkimit Evropian: Identifikimi i objektivave strategjikë dhe interesave të BE-së, që përcaktojnë drejtimin e veprimit të saj në arenën ndërkombëtare, është kompetencë e Këshillit Evropian. Këto orientime pasqyrohen shpesh në përfundimet e mbledhjeve të Këshillit Evropian ose të Këshilli i Bashkimit Evropian[17]. Deklaratat dhe qëndrimet e Përfaqësuesi i Lartë i BE-së për Punët e Jashtme dhe Politikën e Sigurisë mund të përmbajnë orientime strategjike mbi çështje të caktuara. Ndër dokumentet më të rëndësishme strategjike të miratuara nga BE-ja në këtë kuadër përfshihen:

- Strategjia Evropiane e Sigurisë.
- Strategjia e BE-së kundër Armëve të Shkatërrimit në Masë (2003)[18].
- Strategjia e BE-së kundër Terrorizmit (2005)[19].
- Strategjia e BE-së për Sigurinë e Brendshme (2010)[20].

- Vendimet mbi qëndrimet e përbashkëta: Strategjitë dhe objektivat e përgjithshme të BE-së konkretizohen përmes vendimeve që përcaktojnë qëndrimet e tij ndaj çështjeve të veçanta ndërkombëtare. Këto vendime qartësojnë objektivat politike dhe orientimin diplomatik të Bashkimit ndaj një situate ose ndaj një shteti të caktuar.

Në praktikë, këto qëndrime përdoren shpesh në rastet kur Bashkimi Evropian synon të reagojë ndaj shkeljeve të të drejtave të njeriut, të demokracisë, të shtetit të së drejtës ose të normave të së drejtës ndërkombëtare. Ato mund t'i adresohen një shteti të vetëm, një grupi shtetesh ose një rajoni të tërë, veçanërisht në rastet që lidhen me parandalimin e konflikteve, luftën kundër terrorizmit ose çështjet e mosproliferimit të armëve bërthamore[21]. Ndër rastet më të njohura të qëndrimeve të Bashkimit Evropian përmenden ato ndaj:

- Kubës (1996).
- Zimbabvesë (2002).
- Bjellorusisë.
- Koresë së Veriut.
- Iranit (2007).
- Sirisë.

Në kuadër të këtyre vendimeve përfshihen edhe sanksionet ose masat shtrënguese, të cilat përbëjnë një nga instrumentet më të rëndësishme të politikës së jashtme të Bashkimit Evropian. Këto masa mund të vendosen ndaj

[17] Neni 22.1 i TBE-së, https://eur-lex.europa.eu/ (hyrë për herë të fundit më 23 Prill 2017).
[18] http://register.consilium.europa.eu/ (hyrë për herë të fundit më 25 Prill 2017)
[19] http://register.consilium.europa.eu/ (hyrë për herë të fundit më 25 Prill 2017)
[20] https://www.consilium.europa.eu/(hyrë për herë të fundit më 25 Prill 2017).
[21] Derek Mix, The European Union: Foreign and security policy, (Congressional Research Service 08 Prill 2013), https://www.fas.org/ (hyrë për herë të fundit më 25 Prill 2017).

shteteve të treta, individëve ose entiteteve të caktuara dhe synojnë realizimin e objektivave të politikës së jashtme në përputhje me parimet e PJSP-së. Në shumë raste, legjitimiteti i tyre buron nga rezolutat e Këshillit të Sigurimit të OKB-së, por Bashkimi Evropian mund të vendosë edhe masa shtrënguese në mënyrë autonome.[22]

- Vendimet mbi veprimet e përbashkëta: Vendimet që përcaktojnë veprimet e Bashkimit Evropian lidhen kryesisht me operacionet ose misionet civile dhe ushtarake të ndërmarra në kuadër të PESMP-së. Në këtë kategori përfshihet gjithashtu mbështetja financiare ose teknike që Bashkimi Evropian mund t'u japë organizatave ndërkombëtare të angazhuara në fusha të tilla si mosproliferimi i armëve të shkatërrimit në masë (p.sh., Agjencia Ndërkombëtare për Energjinë Atomike)[23] ose rindërtimi dhe konsolidimi i paqes (p.sh., Organizata për Siguri dhe Bashkëpunim në Evropë)

- Vendimet mbi zbatimin e marrëveshjeve ndërkombëtare: Në kuadër të zbatimit të qëndrimeve dhe veprimeve të Bashkimit Evropian, ky i fundit mund të lidhë marrëveshje ndërkombëtare me organizata ndërkombëtare, si NATO ose Bashkimi Afrikan, si dhe me shtete të treta. Këto marrëveshje lidhen shpesh me pjesëmarrjen e shteteve të treta në operacionet e BE-së ose me përcaktimin e statusit të misioneve dhe forcave të saj në territorin e shtetit pritës.

- Natyra juridike e këtyre instrumenteve: Për shkak të karakterit të tyre të ndërmjetëm, politik dhe juridik, këto instrumente shpesh konsiderohen si një "zonë gri" e së drejtës së Bashkimit Evropian. Atyre u mungon karakteri i plotë legjislativ dhe juridiksioni i Gjykatës së Drejtësisë së Bashkimit Evropian në këtë fushë është i kufizuar[24]. Për këtë arsye, ato shpesh karakterizohen si forma të "soft law" në sistemin juridik të Bashkimit.

Megjithatë, pavarësisht kësaj natyre të veçantë juridike, shtetet anëtare kanë detyrimin të mbështesin politikën e jashtme dhe të sigurisë së Bashkimit në mënyrë aktive dhe pa rezerva. Ky detyrim bazohet në parimet themelore të funksionimit të PJSP-së, si koherenca, besnikëria dhe solidariteti ndërmjet shteteve anëtare.[25]

6. Aftësitë dhe kapacitetet mbrojtëse të Bashkimit Evropian

Që nga themelimi i tij, Bashkimi Evropian është konsideruar kryesisht si një fuqi civile, e cila ka vënë theksin në forcimin e bashkëpunimit ekonomik dhe politik, si dhe në zgjidhjen diplomatike të konflikteve ndërkombëtare. Në këtë kuadër, NATO është perceptuar tradicionalisht si organizata përgjegjëse

[22] European Union External Actions, Common Foreign and Security Policy, http://eeas.europa.eu/ (hyrë për herë të fundit më 25 Prill 2017).

[23] International Atomic Energy Agency, IAEA – EU Joint Action: Parnership in Improving Nuclear Security, https://www.iaea.org/ (hyrë për herë të fundit më 30 Prill 2017).

[24] Neni 24.1 i TBE-së.

[25] Neni 24.3 i Traktatit të BE-së, Versioni i Konsoliduar.

për realizimin e mbrojtjes kolektive të vendeve evropiane dhe si forumi kryesor ku shtetet anëtare mund të diskutonin çështjet që lidhen me sigurinë dhe mbrojtjen.

Megjithatë, zhvillimet gjeopolitike të dekadave të fundit kanë nxitur një reflektim të thellë mbi rolin e Bashkimit Evropian në fushën e sigurisë dhe mbrojtjes. Përvoja e konflikteve në Ballkan gjatë viteve '90, paaftësia fillestare e BE-së për të ndërmarrë ndërhyrje efektive politike ose ushtarake, si dhe zhvillimet më të fundit në Ukrainë dhe në rajonet përreth Evropës, kanë nxjerrë në pah nevojën për forcimin e kapaciteteve mbrojtëse të Bashkimit. Këtyre faktorëve u shtohen edhe ndryshimet e thella gjeopolitike, rritja e konflikteve në afërsi të kufijve të Evropës, rritja e flukseve migratore nga zonat e konfliktit dhe kërcënimet që lidhen me terrorizmin ndërkombëtar.

Politika e mbrojtjes së Bashkimit Evropian edhe në ato raste kur operacionet ushtarake të BE-së kanë rezultuar të suksesshme, merita nuk mund t'i atribuohet drejtpërdrejtë komandës dhe kapaciteteve të kufizuara të saj, por se Shteteve Anëtare me "xhepa të mëdha". Për këtë arsye, politika evropiane e mbrojtjes mund të jetë e suksesshme vetëm nëse disponon aftësitë e duhura ushtarake, në të kundërt ajo do të mbetej një guaskë boshe[26].

Krijimi i një force të qëndrueshme ushtarake jo vetëm që do të ndikonte në rritjen e aftësisë së BE-së për të reaguar menjëherë dhe me efektivitet ndaj emergjencave kudo në botë, por në të njëjtën kohë do të ishte një mjet për diplomacinë e BE-së.

Për të pajisur Bashkimin Evropian me kapacitetet e nevojshme për të vepruar në rajone të ndryshme të krizave dhe për të forcuar dimensionin ushtarak të Politikës së Përbashkët të Sigurisë dhe Mbrojtjes (PESMP), si dhe për të rritur bashkëpunimin ndërmjet shteteve anëtare, janë krijuar disa struktura dhe mekanizma të rëndësishëm, ndër të cilët mund të përmenden:

a) Eurocorps (Trupat Evropiane);

b) Grupet e Betejës të Bashkimit Evropian (EU Battlegroups);

c) Forca Evropiane e Xhandarmërisë (European Gendarmerie Force);

d) kapacitetet detare dhe ajrore të zhvilluara në kuadër të operacioneve të përbashkëta të BE-së.

Këto struktura synojnë të përmirësojnë aftësinë e Bashkimit Evropian për të ndërmarrë operacione civile dhe ushtarake në kuadër të menaxhimit të krizave ndërkombëtare, duke kontribuar në stabilitetin dhe sigurinë rajonale dhe globale.

[26] Nga fjalimi i Catherine Ashton në Konferencën Vjetore të Agjencisë Evropiane të Mbrojtjes, mars 2014.

Përfundime

Analiza e thelluar e kuadrit juridik dhe institucionit të Politikës Evropiane të Sigurisë dhe Mbrojtjes së Përbashkët dëshmon për një transformim të dukshëm të Bashkimit Europian: nga një organizatë e fokusuar kryesisht në bashkëpunimin ekonomik drejt një aktori më kompleks dhe strategjik në fushën e sigurisë dhe mbrojtjes. Themelimi i Strategjisë Evropiane të Sigurisë në vitin 2003,si dhe avancimet ligjore e institucionale të përcaktuara nga Traktati i Lisbonës, përbëjnë momente kyçe që kanë ndryshuar në mënyrë thelbësore rolin dhe kapacitetet e BE-së në këtë fushë.

Përmes krijimit të instrumenteve ligjorë specifikë dhe mekanizmave të ndryshëm ushtarakë-si Trupat Evropiane, Grupet e Betejave, Forcat e Xhandarmërisë dhe kapacitetet detare dhe ajrore, BE-ja ka arritur të forcojë aftësinë e saj për të ndërhyrë në mënyrë autonome në situata krize dhe konfliktesh ndërkombëtare. Megjithatë, këto avancime nuk janë të plota dhe janë të kushtëzuara në masë të madhe nga vullneti politik i Shteteve Anëtare, të cilat vazhdojnë të mbajnë sovranitetin kryesor mbi vendimet për sigurinë dhe mbrojtjen. Kjo situatë krijon një ekuilibër të brishtë midis nevojës për bashkëpunim më të ngushtë dhe interesave kombëtare të veçanta, duke e bërë procesin e integrimit në fushën e sigurisë një sfidë të vazhdueshme.

Një aspekt i rëndësishëm i këtij procesi është natyra e instrumenteve ligjorë në përdorim, të cilët shpesh janë të tipit "soft law" dhe nuk kanë karakter detyrues ligjor të plotë. Kjo gjendje krijon një "zonë gri" ligjore ku efektiviteti i politikës së sigurisë dhe mbrojtjes varet më shumë nga përpjekjet politike, besnikëria reciproke dhe koordinimi i Shteteve Anëtare sesa nga mekanizmat e zbatueshmerisë juridike. Për më tepër, kufizimet në rolin e Gjykatës së Drejtësisë së BE-së në këtë fushë e shtojnë këtë kompleksitet.

Gjendja aktuale e politikës së sigurisë së Bashkimit Europian, reflekton një fazë tranzicioni ku sfidat globale dhe rajonale, po e detyrojnë BE-në të rrisë përpjekjet për ndërtimin e kapaciteteve ushtarake dhe civile që i mundësojnë veprime më të shpejta, më të koordinuara dhe më efektive. Konfliktet e fundit në afërsi të kufijve të BE-së, flukset e migrimit të lidhura me zonat e konfliktit dhe rritja e kërcënimeve terroriste, kanë nxjerrë në pah nevojën emergjente për një përgjigje më të fuqishme dhe autonome të Bashkimit.

Krijimi i një strukture të qëndrueshme ushtarake dhe forcimi i politikës së përbashkët të mbrojtjes do të jenë çelësi për transformimin e BE-së në një aktor të besueshëm dhe efektiv në arenën ndërkombëtare. Një forcë e tillë jo vetëm që do të rrisë aftësinë e reagimit ndaj krizave globale, por edhe do të forcojë diplomacinë evropiane dhe pozicionin strategjik në marrëdhëniet ndërkombëtare. Në këtë drejtim, nismat për forcimin e bashkëpunimit ndërmjet Shteteve Anëtare në aspektin ushtarak dhe civil. janë të domosdoshme dhe duhet të shoqërohen me një koordinim më të thellë ligjor dhe institucional.

Megjithatë, sfida kryesore mbetet harmonizimi i interesave kombëtare dhe ruajtja e sovranitetit shtetëror, që shpesh frenon avancimet e mëtejshme drejt një politikë më të unifikuar dhe të integruar të sigurisë. Mungesa e një kornize ligjore me efekt të plotë detyrues për PESMP-në dhe kufizimet në ndërhyrjen e institucioneve të BE-së për zbatimin e këtyre politikave, kërkojnë një reformë të mëtejshme ligjore dhe institucionale që do të fuqizojë rolin dhe përgjegjësitë e BE-së në këtë fushë.

Në përfundim, zhvillimet e deritanishme dëshmojnë se politika evropiane e sigurisë dhe mbrojtjes, ndodhet në një fazë thelbësore të konsolidimit. Për të garantuar një sistem të qëndrueshëm, efektiv dhe të aftë për të përballuar sfidat e sigurisë së shekullit XXI do të jetë i nevojshëm një bashkëpunim më i ngushtë midis Shteteve Anëtare, përmirësimi i instrumenteve ligjorë dhe zgjerim i kapaciteteve operacionale. Kjo do të mundësojë që Bashkimi Evropian, të konsolidohet si një aktor kyç ndërkombëtar, i aftë të mbrojë vlerat, interesat dhe sigurinë e qytetarëve të tij në një botë gjithnjë e më komplekse dhe të paqëndrueshme.

Bibliografia

1. Treaty on European Union (TEU). 7 June 2016.
2. Combarieu, Gilles. *Security and Defence Aspects of the Lisbon Reform Treaty.* Paris, 2008. http://europavarietas.visuart.eu/.
3. Treaty of Nice. Concluded by the governments of the Member States on 26 February 2001. https://europa.eu/.
4. Treaty of Lisbon. Signed by the Member States on 13 December 2007. https://eur-lex.europa.eu/.
5. Protocol No. 1, "On the Role of National Parliaments in the European Union."
6. Council of the European Union. "Press Release – Meeting 3230 of the Council of Foreign Affairs." http://www.consilium.europa.eu/.
7. Mix, Derek. *The European Union: Foreign and Security Policy.*
8. Council of the European Union. "Common Position of 2 December 1996 defined by the Council on the basis of Article J.2 of the Treaty on European Union, on Cuba."
9. Council of the European Union. "Decision of 13 September 2002 Implementing Common Position 2002/145/CFSP Concerning Restrictive Measures against Zimbabwe."
10. Council of the European Union. "Common Position of 9 July 1998 defined by the Council on the basis of Article J.2 of the Treaty on European Union, concerning Belarus."

11. European Commission. *Restrictive Measures (Sanctions) in Force.*
12. European Union. *External Actions: Common Foreign and Security Policy.*
13. International Atomic Energy Agency (IAEA). *IAEA–EU Joint Action: Partnership in Improving Nuclear Security.*
14. Ashton, Catherine. Speech at the Annual Conference of the European Defence Agency, March 2014.
15. Western European Union. *Petersberg Declaration.*
16. Council of Ministers of the WEU. Communiqué, 19 May 1993.
17. "Eurocorps Will Strengthen European Pillar of NATO." Press Release, Federal Press Office of Germany, 22 July 1992.
18. Agreement between the Supreme Allied Commander Europe (SACEUR) and the Channel Committee, Concerning Responsibility for the North Sea Sub-Area.
19. *Eurocorps: A Force of European Union and NATO.*

Operacioni “Absolute Resolve”: përmbledhje e shkurtër e koordinimit, zhvillimit dhe domethënies së tij

Kolonel Ramadan KARAKUSHI
Shefi i Departamentit të Operacioneve, në KMS,
Nënkolonel Latif SHURDHI
Shefi i Grupit të Shkencave Shoqërore në KMS,
Nënkolonel Alban GEGA
Nënkolonel Bledar LAMA
Nënkolonel Valezim LIKA
Kursantë në KLO,
Major Mariglen ÇELHAKA
Major Rudin NIKA
Kursantë në KKSHP

Trajtesë e shkurtuar

Ky punim përshkruan në mënyrë të përmbledhur përgatitjen dhe zhvillimin e operacionit “Absolute Resolve”, të ekzekutuar në fillim të janarit të vitit 2026 në Venezuelë, duke e trajtuar atë si një rast studimor për planëzimin, koordinimin dhe integrimin e të gjithë elementëve të një operacioni të përbashkët (joint), ku veprimtaria e forcave speciale (Delta Forcë dhe pjesë të Regjimentit 160 të Operacioneve Speciale Ajrore Amerikane) është pjesa më e ekspozuar e operacionit në fjalë. Që në krye të herës duhet theksuar se ky punim po realizohet në një kohë kur nuk kemi punime shkencore të mirëfillta mbi të. Për rrjedhojë janë përdorur burime të hapura duke marrë në konsideratë artikuj të ndryshëm mediatikë të publikuar nga analistë dhe akademikë të çështjeve të politikës ndërkombëtare, sigurisë dhe mbrojtjes. Po ashtu për eksplorimin dhe zhvillimin e mëtejshëm të këtij punimi janë marrë në konsideratë edhe dokumente apo raporte institucionale dhe deklarata zyrtare, pra edhe kategorinë e burimeve që në gjuhën e kërkimit shkencor quhet literatura “gri”.

Punimi shqyrton kontekstin historik, politik dhe gjeopolitik të Venezuelës, arkitekturën operacionale të fazës përgatitore “Southern Spear”, ekzekutimin e operacionit “Absolute Resolve”, si dhe rolin vendimtar të inteligjencës në

përmbushjen e objektivit.

Përmes analizës së reagimeve ndërkombëtare, implikimeve ligjore dhe pasojave strategjike, argumentohet se "Absolute Resolve" përfaqëson një paradigmë të re të ndërhyrjes kirurgjikale (mënyre e re e përdorimit të forcave speciale) me efekte që rezultojnë po aq vendimtarë sa fuqia ushtarake konvencionale.

Në fund të punimit janë pasqyruar disa përfundime të ndara në dy kategori. Së pari, këto përfundime kanë të bëjnë me përfundime që mundohen të pasqyrojnë të rejat që karakterizojnë këtë operacion në kuptimin e ngushtë ushtarako-operacional. Së dyti, janë përfundime që kanë të bëjnë me domethënien politiko-strategjike të zhvillimit të tij si shprehje e qasjes së re të administratës Trump ndaj gjithë drejtimeve strategjike nga një këndvështrim amerikan në përgjithësi dhe ngushtësisht në raport me Hemisferën Perëndimore dhe hapësirën transatlantike.

Fjalët kyçe: Operacioni "Absolute Resolve"; arkitektura e inteligjencës; Pattern of life; lufta elektronike; zbulimi me njerëz.

Qëllimi

Qëllimi i këtij punimi është të analizojë në mënyrë të strukturuar dhe kritike operacionin "Absolute Resolve" si një rast studimor të përdorimit bashkëkohor të forcës në kontekstin e një bote multipolare. Në veçanti, synon të analizojë ambientin operacional dhe gjeopolitik të Venezuelës përpara ndërhyrjes, të shqyrtojë rolin e inteligjencës dhe dominimit informacional në planifikimin dhe zbatimin e operacionit, si dhe të identifikojë mësimet të nxjerra për operacione të kësaj natyre.

Metodologjia

Është përdorur një qasje metodologjike cilësore, që do të thotë se është kërkuar të gjenden burime mediatike apo dokumentare, që trajtojnë në mënyrë të besueshme zhvillimin e operacionit të lartpërmendur. Më tej në lidhje metodën konkrete për të grumbulluar të dhënat e duhura për përpunimin e tyre, të cilat do të na çojnë në trajtimin e temës në fjalë, mund të themi se kemi të bëjmë me atë të analizës së përmbajtjes. Po ashtu nga pikëpamja e llojit të këtij punimi mund të themi se ai prezanton një punim përshkrues, por edhe analitik.

1. Transformimi i rendit ndërkombëtar dhe përdorimi bashkëkohor i forcës

Në dekadat e fundit, sistemi ndërkombëtar ka hyrë në një fazë transformimi të thellë, i karakterizuar nga dobësimi gradual i rendit unipolar dhe shfaqja e një strukture gjithnjë e më multipolare. Ky tranzicion ka prodhuar jo vetëm rishpërndarje të fuqisë midis aktorëve globalë, por edhe ndryshime rrënjësore në mënyrën se si fuqia ushtarake dhe politike përdoret për të ndikuar mbi sjelljen e shteteve të tjera. Në këtë kontekst, përdorimi i forcës nuk kufizohet më në ndërhyrje të drejtpërdrejta ushtarake, por manifestohet

përmes një spektri të gjerë instrumentesh hibride që përfshijnë presionin ekonomik, luftën kibernetike, operacionet e inteligjencës dhe menaxhimin e narrativës publike.[1] Amerika Latine, historikisht e konsideruar si një hapësirë strategjike me rëndësi të veçantë për Shtetet e Bashkuara, mbetet një arenë ku këto dinamika shfaqen me intensitet të lartë. Në këtë rajon, Venezuela përfaqëson një rast paradigmatik, për shkak të kombinimit të burimeve të mëdha natyrore, krizës së thellë politike dhe ekonomike, si dhe përfshirjes aktive të aktorëve të jashtëm si Rusia dhe Kina. Këta faktorë e kanë shndërruar Venezuelën në një nyje kritike të konkurrencës gjeopolitike globale.

Operacioni "Absolute Resolve", i realizuar në Janar 2026, duhet të kuptohet pikërisht brenda këtij konteksti kompleks. Ai nuk përfaqëson thjesht një veprim të izoluar operacional, por kulmin e një fushate shumëfazore që integron presionin diplomatik, ekonomik, psikologjik dhe ushtarak në një arkitekturë koherente strategjike. Ndërhyrja fizike për kapjen e Nicolás Maduro ishte vetëm faza përfundimtare e një procesi të gjatë, ku dominimi i informacionit dhe asimetria teknologjike luajtën një rol vendimtar.[2]Ky operacion ngre një sërë pyetjesh thelbësore për studimet në fushën e sigurisë dhe marrëdhëniet ndërkombëtare si vijojnë: Si po transformohet koncepti i sovranitetit në një botë multipolare? Çfarë roli luan inteligjenca në zëvendësimin e forcës konvencionale dhe në çfarë mase operacione të tilla krijojnë precedentë të rinj në të drejtën ndërkombëtare dhe praktikën e ndërhyrjes? Natyrisht ky punim nuk merret me trajtimin e të gjitha pyetjeve të lartpërmendura.

2. Venezuela në dekadën fundit - Periudhë krize dhe erozioni institucional

Për të kuptuar plotësisht natyrën dhe implikimet e operacionit "Absolute Resolve", është e domosdoshme një analizë e përgjithshme e kontekstit historiko-politik dhe ekonomik të Venezuelës në periudhën që i parapriu ndërhyrjes amerikane.

Venezuela e dekadës së fundit përfaqëson një rast ekstrem të erozionit gradual të shtetësisë funksionale, ku institucionet formale ekzistonin kryesisht në letër, ndërsa pushteti real ishte përqendruar në një elitë të ngushtë politike dhe ushtarake të lidhur ngushtë me ekonominë informale dhe kriminale.[3] Trashëgimia e "Revolucionit Bolivarian", e nisur nga Hugo Chávez dhe e trashëguar nga Nicolás Maduro, kishte prodhuar një model qeverisjeje të bazuar në personalizimin e pushtetit, militarizimin e administratës publike dhe përdorimin selektiv të dhunës për të ruajtur kontrollin politik. Ndërkohë që retorika zyrtare theksonte sovranitetin dhe anti-imperializmin, ndërsa realiteti institucional karakterizohej nga varësia dhe mbështetja e aktorëve të jashtëm,

[1] Berg Ryan, Cancian Mark, Bermudez Jr. Joseph, Jun Jennifer, Ziemer Henry, and Park Chris. *Imagery from Venezuela Shows a Surgical Strike, Not Shock Awe*, published January 9, 2026

[2] Po aty.

[3] Moises, N. *The Twilight of the Bolivarian Revolution: How Venezuela Became a Mafia State*, Foreign Affairs, January 2026.

veçanërisht Rusisë, Kubës dhe, në një masë më të kufizuar, Kinës.[4]

Ekonomikisht Venezuela ishte zhytur në një krizë të thellë strukturore. Rënia drastike e prodhimit të naftës, sanksionet ndërkombëtare dhe keqmenaxhimi kronik kishin shkatërruar kapacitetin fiskal të shtetit. Inflacioni galopant, kolapsi i monedhës kombëtare dhe emigrimi masiv i popullsisë kishin dobësuar ndjeshëm "*kontratën sociale*" midis regjimit dhe qytetarëve. Në këtë kontekst, regjimi i Maduros mbështetej gjithnjë e më shumë në rrjete paralele financiare, përfshirë trafikun e narkotikëve dhe tregtinë e paligjshme të arit, të njohura gjerësisht në literaturën ndërkombëtare si "Karteli i Diellit".[5]

Politikisht legjitimiteti i brendshëm i regjimit ishte minimal. Zgjedhjet e kontestuara, shtypja sistematike e opozitës dhe përdorimi i forcave paramilitare "colectivos" për kontrollin urban kishin krijuar një ambient të përhershëm tensioni dhe frike. Megjithatë, regjimi kishte arritur të mbijetonte falë fragmentimit të opozitës, kontrollit të mediave dhe lojalitetit të aparatit të sigurisë, veçanërisht Gardës Presidenciale dhe elementëve të kundërzbulimit të trajnuar nga Kuba.[6] Ky kombinim faktorësh e kishte shndërruar Venezuelën në atë që shumë analistë e përshkruanin si një "*shtet brenda shtetit*", ku kufijtë midis pushtetit politik, aktivitetit kriminal dhe sigurisë kombëtare ishin bërë të paqartë. Pikërisht kjo natyrë hibride e regjimit e bëri Venezuelën një objekt të veçantë për një qasje po aq hibride nga ana e Shteteve të Bashkuara.

3. Operacioni "Absolute Resolve" - Një paradigmë e re e përdorimit të forcës

Operacioni "Absolute Resolve" nuk mund të kuptohet përmes lenteve tradicionale të ndërhyrjes ushtarake. Ai përfaqëson një paradigmë të re të përdorimit të forcës, ku qëllimi nuk ishte pushtimi territorial, ndryshimi i regjimit përmes luftës konvencionale apo shkatërrimi i kapaciteteve ushtarake të një shteti sovran. Përkundrazi, objektivi strategjik ishte neutralizimi i një nyje qendrore të pushtetit përmes një ndërhyrjeje të sofistikuar, të mbështetur nga dominimi i informacionit dhe presioni shumëdimensional.[7]

Në këtë paradigmë të re, forca kinetike shërben si mjet i fundit, i aktivizuar vetëm pasi mjedisi operacional është formësuar në mënyrë të tillë që rezistenca e objektivit të jetë minimalisht efektive. Kjo qasje reflekton një zhvendosje të qartë nga doktrina tradicionale drejt asaj që mund të përkufizohet si "kontroll total i mjedisit operacional".[8]

Ndryshe nga ndërhyrjet e mëparshme në Irak apo Afganistan, ku prania ushtarake afatgjatë ishte pjesë integrale e strategjisë, "Absolute Resolve"

[4] Po aty.
[5] Po aty.
[6] Po aty.
[7] Zakaria, F. *The New Paradigm of Force: What 'Absolute Resolve' Teaches Us About Future Warfare*.
[8] Po aty.

synonte një ndikim maksimal me një footprint minimal. Kjo strategji ishte e diktuar jo vetëm nga mësimet e nxjerra nga konfliktet e kaluara, por edhe nga realiteti politik i një bote ku ndërhyrjet e drejtpërdrejta ushtarake mbartin kosto të larta diplomatike dhe reputacionale.

Operacioni "Absolute Resolve" – Arkitektura e inteligjencës dhe fazat operative

Operacioni "Absolute Resolve" përfaqëson kulmin e evolucionit të doktrinës moderne të ndërhyrjes kirurgjikale, ku dominimi i informacionit, koordinimi i sistemeve teknologjike dhe inteligjenca njerëzore u kombinuan për të kapur një lider shtetëror të mbrojtur fort, pa shkaktuar gjakderdhje masive. Faza operative mund të analizohet në pesë shtylla themelore: 1) ndërtimi i Pattern of Life (PoL); 2) mbikëqyrja teknologjike dhe dominimi i spektrit; 3) inteligjenca njerëzore (HUMINT); 4) lufta psikologjike (PSYOPS) dhe 5) ekzekutimi kinetik i misionit[9], të cilat do të trajtohen më poshtë.

3.1 Arkitektura e Inteligjencës: Ndërtimi i Pattern of Life (model i jetës - PoL)

Faza përgatitore, e nisur në gusht 2025, përqendrohej në evidentimin e rutinës së Maduros duke përdorur fuzionin e inteligjencës me burime të shumëfishta. Pattern of Life (PoL) në këtë kontekst nuk ishte thjesht vendndodhja e objektivit, por një analizë holistike e ritmeve biologjike, sociale dhe logjistike të liderit, duke përfshirë çdo lëvizje të mundshme me saktësi mikroskopike.[10]

Agjencitë CIA (Central Intelligence Agency) dhe DIA (Defense Intelligence Agency) integruan të dhënat e inteligjencës gjeohapësinore (GEOINT) me monitorimin e sinjaleve (SIGINT), duke krijuar një hartë të detajuar të itinerarit të Maduros midis pallatit Miraflores (Selia zyrtare e presidencës së Venezuelës) dhe bazës ushtarake "Fort Tiuna". Algoritmet e inteligjencës artificiale analizuan oraret e gjumit, llojet e medikamenteve të përdorura, frekuencën e takimeve me këshilltarët kubanë dhe variabla të tjerë socialë, duke prodhuar një model probabilistik të sjelljes së liderit.[11]

Përveç kësaj, analiza e bazës së të dhënave mbi konsumin e energjisë dhe lëvizjet e autokolonave lejoi parashikimin e vendndodhjes reale të objektivit me mbi 90% saktësi. PoL gjithashtu identifikoi anomalitë logjistike dhe elementet diversivë, duke neutralizuar përpjekjet e regjimit për të krijuar sozi ose rrugë alternative të sigurisë. Kjo qasje e kthente çdo veprim të Maduros në

[9] Kay Mike nw: How did the US get Maduro? Inside Operation Absolute Resolve | BBC Security Brief, dt. 09.01.2026

[10] Sabbagh, D. *Months in planning, over in two and a half hours: how the US snatched Maduro*, në Defence & Security, 4 January 2026.

[11] Po aty.

një informacion të lexueshëm dhe përgatiste terrenin për ndërhyrjen fizike.[12]

3.2 Mbikëqyrja teknologjike dhe dominimi i spektrit (SIGINT & EW)

Komponenti teknologjik u shndërrua në një armë strategjike. Pjesa kryesore ishte dominimi i spektrit elektromagnetik përmes avionëve EA-18G Growler, të cilët përdorën teknikën e spoofing (mashtrim sinjalor) për të injektuar sinjale false në sistemet ruse S-300VM dhe BUK-M2/3. Si rezultat, radarët venezuelas regjistruan qindra objektiva fiktivë, duke paralizuar zinxhirin e komandimit dhe duke krijuar një "errësirë digjitale" për operacionet ajrore dhe tokësore.[13]

Në këtë sfond, dronët stealth (të pakapshëm nga radarët) të gjeneratës së re siguruan mbikëqyrje të vazhdueshme në lartësi stratosferike, duke ofruar video termike në kohë reale dhe duke lejuar identifikimin e rojeve dhe hapësirave të fortifikuara vetëm sekonda para zbarkimit të njësive speciale. Sulmet kibernetike paralizuan rrjetet celulare dhe komunikimet duke penguar koordinimin e reagimit nga forcat e sigurisë për Maduron.

Ky kombinim i SIGINT & EW, si dhe mbikëqyrja persistente ofroi një kontroll të pakrahasueshëm mbi hapësirën informative të Venezuelës, duke garantuar se faza operative mund të zhvillohej me surprizë dhe efikasitet maksimal.

3.3 Inteligjenca njerëzore (HUMINT) dhe infiltrimi operacional

Pavarësisht dominimit teknologjik, komponenti HUMINT ishte vendimtar për saktësinë kirurgjikale të operacionit. Agjentët e shërbimeve inteligjente amerikane rekrutuan asetet brenda rrethit logjistik të Maduros, duke përfshirë kuzhinierë, staf teknik dhe oficerë të nivelit të mesëm. Informacioni i tyre konfirmoi detaje të pazbuluara nga satelitët, si dyert e përforcuara, autokolonat reale dhe rezervat e sigurisë.[14]

Kjo mbështetje njerëzore ishte thelbësore edhe për eksfiltrimin (faza e largimit të forcave amerikane me objektivin). Asetet brenda sistemit të Maduros krijuan kaos diversiv në pika të tjera të qytetit për të tërhequr vëmendjen e forcave mbrojtëse të Venezuelës, duke siguruar rrugë të sigurta për operacionet e Delta Force dhe Regjimentit 160 SOAR.

3.4 Lufta psikologjike (PSYOPS) dhe korniza ligjore

Operacioni u mbështet nga një fushatë agresive PSYOPS që destabilizoi zinxhirin komandues venezuelas. Dezinformimi i shënjestruar krijoi dyshime për grushte të mundshme dhe paralizoi reagimin e forcave besnike në momentin kritik. Ky element psikologjik shërbeu për të minimizuar rezistencën dhe për

[12] Po aty.

[13] Sprenger, S. *Electronic Ghost: How the U.S. Navy's Growlers Blinded Venezuela's S-300 Network*. Defense News, 6 January 2026.

[14] Strobel, W. & Lubold, G. *The Traitors Within: How the CIA Turned Maduro's Household against Him*. The Wall Street Journal (WSJ), 6 January 2026.

të garantuar suksesin. Nga ana ligjore, SHBA përdori aktakuzat për narko-terrorizëm për të trajtuar Maduron si kreun e një organizate kriminale, duke justifikuar ndërhyrjen me qëllimin e shmangies së konflikteve diplomatike. Kjo ofroi legjitimitet ndërkombëtar nga këndvështrimi amerikan.[15]

3.5 Ekzekutimi i operacionit

Me tre fazat e mëposhtme do të përshkruajnë veprimet kinetikë, (veprimet konkrete ushtarake në terren) të forcave amerikane pjesëmarrëse në operacion.

Faza I: Operacioni "Southern Spear" (gusht – dhjetor 2025).

"Southern Spear" shërbeu si fazë përgatitore duke paraqitur përgatitjet ushtarake si pjesë të një fushate rutinë kundër narkotikëve. Nga gushti deri në dhjetor 2025, Komanda Jugore Amerikane krijoi një "unazë të hekurt" rreth brigjeve të Venezuelës duke përdorur asete të rënda si aeroplanmbajtësja *USS Gerald R. Ford* për të krijuar *de facto* një bllokadë detare. Qëllimi nuk ishte vetëm ndalimi i drogës, por shterimin e burimeve financiare të regjimit duke bllokuar eksportet e naftës dhe izoluar ekonomikisht Karakasin nga pjesa tjetër e botës[16].

Në të njëjtën kohë, SHBA kreu edhe goditje kinetike të kufizuara për të testuar reagimin e mbrojtjes ajrore. Rreth tridhjetë e pesë sulme ajrore dhe detare ndaj "anijeve të dyshuara" shërbyen si karrem për të detyruar radarët venezuelas të ndizeshin dhe të zbulonin pozicionet e tyre. Këto manovra i lejuan planifikuesve amerikanë të hartonin me saktësi hartën elektronike të mbrojtjes ajrore të Venezuelës duke identifikuar pikat e dobëta të sistemeve S-300 dhe Buk-M2E.

Edhe deklarata e mëposhtme e Komandës Jugore "Përmes Operacionit SOUTHERN SPEAR, Departamenti i Luftës është i palëkundur në misionin e tij për të shtypur aktivitetin e paligjshëm... kapja e një tjetër anije cisterne që operon në kundërshtim me karantinën e vendosur nga Presidenti Trump demonstron vendosmërinë tonë"[17], shpreh qartë angazhimin për përgatitjen e operacionit.

Në përfundim të kësaj faze, Venezuela ishte e izoluar, me një ekonomi të gjunjëzuar dhe me një ushtri të lodhur nga gatishmëria e vazhdueshme. Operacioni PSYOPS i shoqëruar me bllokadën detare krijoi paranojë brenda rrethit të ngushtë të Maduros, ndërsa mesazhet e fshehta drejtuar ushtarakëve të thjeshtë krijuan përçarje midis lidershipit politik dhe atij ushtarak. Kjo përgatiti terrenin ideal për goditjen përfundimtare.

---

[15] Barret, D & Harris, S. *The Narcotic Kingpin Defense: How DOJ Indictments Paved the Way for the Caracas Raid*", The Washington Post, 6 January 2026.

[16] Center for Strategic and International Studies. (2025, November 10). *Trump's Caribbean campaign: The data behind Operation Southern Spear*. CSIS Analysis.

[17] U.S. Southern Command. (2026, January 20). *Maritime interdiction operation press release*.

Faza II: Ekzekutimi i sulmeve ajrore dhe neutralizimi i mbrojtjes ajrore.

Sulmet ajrore nisën në orën 02:01 të mëngjesit të 3 janarit 2026 duke shfrytëzuar errësirën dhe befasinë teknologjike. Një sulm kibernetik masiv paralizoi rrjetin elektrik të Karakas-it dhe ndërpreu komunikimet ushtarake duke zhytur qendrat e komandim – kontrollit në kaos të plotë. Në këtë mjedis, avionët që nuk kapen nga radari (*stealth)* F-22 dhe F-35 depërtuan në hapësirën ajrore për të neutralizuar mbrojtjen ajrore duke kryer neutralizimin e mbrojtjes ajrore dhe për të hapur korridore të sigurta për elementët që do të kryente goditjen tokësorë. Analistët ushtarakë theksuan përdorimin intensiv të mjeteve të luftës elektronike për të neutralizuar sistemet e avancuara ruse S-300VM dhe BUK-M2/3, pa përdorimin e gjerë të municioneve konvencionale[18]. Këto sulme çaktivizuan funksionimin efektiv të sistemeve të avancuara të mbrojtjes së Venezuelës duke i bërë raketat e tyre të papërdorshme dhe duke hapur korridorin ajror për helikopterët e infiltrimit.

Faza III: Kapja e Maduros dhe operacioni tokësor.

Me neutralizimin e mbrojtjes ajrore, operatorët e Delta Force dhe Regjimentit 160 SOAR zbarkuan direkt në kompleksin e fortifikuar Fort Tiuna. Falë HUMINT të saktë operacioni u zhvillua me shpejtësi. Përballja me trupat speciale kubaneze ishte e ashpër por e shkurtër. Përdorimi i taktikave të kontrollit dhe pastrimit të ambienteve, si dhe municioneve precize bëri që rezistenca të thyhej brenda pak minutash. Kapja e Maduros ndodhi ndërsa ai përpiqej të futej në bunkerin e sigurisë që solli një dështim fatal të protokolleve të tij të evakuimit.

Në më pak se tre orë, objektivi kryesor (Maduro dhe Flores) ishte siguruar dhe forcat po largoheshin drejt anijes *USS Iwo Jima*. Shpejtësia e operacionit ishte e tillë që shumica e njësive ushtarake venezuelase nuk arritën as të mobilizoheshin duke e lënë regjimin të çorientuar dhe pa udhëheqës përpara se dielli të lindte. Presidenti Trump do ta përshkruante këtë epërsi teknologjike me fjalët: "Ata shtypën butonat dhe asgjë nuk ndodhi. Ishte një sulm i mahnitshëm[19]".

4. Pasojat dhe analiza e dëmeve (BDA)

Bilanci pas operacionit tregoi një ndërhyrje të kufizuar dhe të fokusuar. Me rreth 75 të vrarë, shumica dërrmuese e të cilëve ishin mercenarë ose forca speciale besnike të regjimit, SHBA arriti të shmangte një gjakderdhje masive. Mungesa pothuajse totale e viktimave civile dhe ruajtja e infrastrukturës kritike ishin rezultat i rregullave strikte të angazhimit, të cilat ndalonin goditjen e kazermave të ushtrisë së rregullt që nuk bënin rezistencë aktive.

Kjo zgjedhje për të kursyer ushtrinë e rregullt ishte një lëvizje strategjike

[18] Defense One. (2026, January 8). *Silent strike: The end of kinetic air suppression?*

[19] Trump, D. Deklaratë për median. Në: https://youtu.be/hKi2h6op5sY?si=-6LIcGV9TLL9kAqj

e llogaritur mirë. Duke mos poshtëruar forcat e armatosura kombëtare, Uashingtoni shpresonte të lehtësonte një tranzicion më të butë dhe të parandalonte shpërbërjen e rendit publik pas largimit të diktatorit. Megjithatë, vakumi i pushtetit që pasoi ishte i menjëhershëm. Figura si Delcy Rodriguez u përpoqën të mbushnin boshllëkun, por autoriteti i tyre ishte i dëmtuar rëndë nga goditja psikologjike e humbjes së liderit suprem dhe mungesa e legjitimitetit.

Reagimi i brendshëm ishte një përzierje kaosi dhe pasigurie. Grupet paramilitare "colectivos" kërcënuan me dhunë, ndërsa popullata mbeti në pritje, e frikësuar nga mungesa e informacionit dhe energjisë elektrike. Nga ana tjetër, tregjet ndërkombëtare të naftës reaguan me luhatje duke parashikuar një rikthim të mundshëm të kompanive perëndimore, por edhe një periudhë destabiliteti afatshkurtër. Aktualisht, me Maduron në burg në Nju Jork, Venezuela gjendet në një udhëkryq historik[20].

5. Nga antiterrorizmi klasik te ndërhyrja hibride ndaj një aktori shtetëror. Një analizë e shkurtër krahasuese

Për të kuptuar plotësisht rëndësinë e operacionit "Absolute Resolve" është e domosdoshme një analizë krahasuese me ndërhyrje të mëparshme të profilit të lartë, veçanërisht operacionin "Neptune Spear" të vitit 2011 që çoi në eliminimin e Osama Bin Ladenit. Ky krahasim nxjerr në pah evolucionin rrënjësor të doktrinës operative nga antiterrorizmi klasik drejt një forme të avancuar të luftës hibride kundër një aktori shtetëror të konsoliduar.[21]

Në rastin e Bin Ladenit, sfida kryesore ishte lokalizimi i një aktori jo-shtetëror që operonte në fshehtësi, pa mbrojtje institucionale formale dhe pa akses në sisteme të avancuara mbrojtjeje. Operacioni ishte i fokusuar në një objektiv të izoluar, me implikime të kufizuara gjeopolitike dhe një konsensus ndërkombëtar relativisht të gjerë mbi legjitimitetin e veprimit.

Në kontrast, operacioni "Absolute Resolve" kishte si objektiv një president në detyrë, të mbrojtur nga një aparat shtetëror kompleks, që përfshinte forca të armatosura të rregullta, shërbime kundërzbulimi dhe sisteme moderne të mbrojtjes ajrore të furnizuara nga Rusia. Ndërhyrja ndaj një aktori të tillë përbënte jo vetëm një sfidë ushtarake, por edhe një rrezik të lartë diplomatik, për shkak të implikimeve në marrëdhëniet me fuqitë e tjera të mëdha.

Kjo diferencë diktoi një qasje thelbësisht të ndryshme. Ndërsa në operacionet e antiterrorizmit klasik inteligjenca shërben kryesisht për lokalizimin e objektivit, në operacionin "Absolute Resolve" ajo u shndërrua në instrumentin kryesor të fitores. Dominimi i informacionit, krijimi i "modelit të jetës" dhe fragmentimi psikologjik i elitës drejtuese e bënë përdorimin e

[20] Task & Purpose. (2026, January 7). *Here's what we know in the wake of Operation Absolute Resolve*.

[21] Bowden, M. ese, *From Abottabad to Caracas: The End of the Counterterrorism Era*", January 2026.

forcës kinetike pothuajse ceremonial.

Ky evolucion tregon se lufta hibride nuk është thjesht një kombinim mjetesh, por një ndryshim paradigmatik në mënyrën se si fuqia projektohet dhe përdoret në sistemin ndërkombëtar bashkëkohor.[22]

6. Dimensioni ligjor dhe legjitimiteti ndërkombëtar

Një nga aspektet më të ndjeshme të operacionit "Absolute Resolve" lidhet me dimensionin ligjor dhe justifikimin e tij në arenën ndërkombëtare. Kapja e një presidenti në detyrë sfidon drejtpërdrejt parimin klasik të sovranitetit dhe imunitetit shtetëror, që përbën një nga shtyllat e rendit ndërkombëtar modern.[23]

Administrata amerikane e ndërtoi kornizën ligjore të operacionit duke e trajtuar Nicolás Maduron jo si një aktor legjitim shtetëror, por si kreun e një organizate kriminale. Aktakuzat për narko-terrorizëm dhe lidhjet e dokumentuara me "Kartelin e Diellit" shërbyen si bazë për ta ri pozicionuar ndërhyrjen nga një akt agresioni ushtarak në një operacion ndërkombëtar të zbatimit të ligjit.

Kjo qasje krijoi një precedent të rëndësishëm. Ajo sugjeron se në një botë ku kufijtë midis shtetit dhe kriminalitetit janë gjithnjë e më të paqartë, legjitimiteti nuk buron më automatikisht nga pozita formale, por nga sjellja e aktorit në sistemin ndërkombëtar. Megjithatë, ky precedent mbart rreziqe të konsiderueshme, pasi mund të keqpërdoret nga aktorë të tjerë për të justifikuar ndërhyrje selektive ndaj kundërshtarëve politikë.

7. Pasojat strategjike dhe implikimet për rendin ndërkombëtar

Operacioni "Absolute Resolve" pati pasoja që shkojnë përtej kufijve të Venezuelës. Në nivel rajonal, ai sinjalizoi një rikthim të vendosmërisë amerikane në Amerikën Latine, duke riafirmuar se Hemisfera Perëndimore mbetet një hapësirë me interes jetik strategjik për Uashingtonin. Ky sinjal u perceptua qartë nga aktorë si Kuba, Nikaragua dhe madje edhe nga fuqitë e jashtme që kishin investuar politikisht dhe ekonomikisht në regjimin e Maduros.

Në nivel global operacioni kontribuoi në riformësimin e debatit mbi sovranitetin dhe ndërhyrjen. Ai demonstroi se shtetet me kapacitete të avancuara të inteligjencës dhe teknologjisë janë në gjendje të neutralizojnë udhëheqës të mbrojtur fort pa u angazhuar në konflikte të gjata dhe të kushtueshme. Kjo rrit ndjeshëm vlerën strategjike të dominimit të informacionit në konkurrencën midis fuqive të mëdha.

---

[22] Wesbrock, Jason, Harned Glenn, and Plous Preston, "*Special Operations Forces and Conventional Forces: Integration, Interoperability, and Interdependence*", December 2016.

[23] Brooks, R. *The Death of Sovereignty? How the Maduro Capture Redefined International Law*", Foreign Affairs, January 2026

Në të njëjtën kohë rasti i Venezuelës nxjerr në pah edhe kufizimet e kësaj qasjeje. Kapja e një lideri nuk garanton automatikisht stabilitet politik apo tranzicion demokratik. Vakumi i pushtetit, fragmentimi institucional dhe prania e aktorëve paramilitarë përbëjnë sfida serioze që nuk mund të zgjidhen vetëm përmes ndërhyrjes kirurgjikale.[24]

Përfundime

Operacioni "Absolute Resolve" përfaqëson një nga shembujt më domethënës të evoluimit të luftës moderne në shekullin XXI. Ai dëshmoi se fitorja strategjike nuk arrihet vetëm përmes shkatërrimit masiv apo pushtimit territorial, por edhe përmes kontrollit të informacionit, dominimit të perceptimit dhe neutralizimit të qendrave kritike të pushtetit me anë të operacioneve speciale.

Në aspektin teorik, ky rast studimor kontribuon në literaturën se si realizohen operacionet e përbashkëta duke demonstruar se qendra e gravitetit në konfliktet moderne po zhvendoset nga territori dhe kapacitetet ushtarake drejt kontrollit të informacionit dhe teknologjisë. "Absolute Resolve" nuk ishte vetëm një operacion ushtarak i suksesshëm, por një manifest strategjik i mënyrës se si fuqia do të projektohet dhe përdoret në dekadat që vijnë.

Përtej përfundimeve të karakterit të ngushtë operacional mund të shtohet se ky operacion është treguesi që administrata Trump po materializon konkretisht atë që i ka vënë detyrë vetes në "National Security Strategy of the United States of Amerika" në nëntor të 2025, konkretisht arritjen e dominancës në Hemisferën e Perëndimit siç edhe shkruhet aty "...to restore American preeminence in the Western Hemisphre"[25].

Edhe tensionet e krijuara mes SHBA-së dhe Mbretërisë së Danimarkës, nënkupto këtu edhe BE në përgjithësi, fuqitë europiane dhe Britania e Madhe në veçanti, në lidhje me debatin mbi aneksimin e Groenlandës janë shprehje e mëtejshme e materializimit të strategjisë në fjalë. Me këto qëndrime politike, diplomatike dhe ushtarake të administratës Trump NATO është vendosur në një sprovë të madhe si asnjëherë më parë dhe rrjedhimisht edhe BE po kalon një sprovë të shtuar dhe shumë serioze, përveç ato që trashëgon nga dekada e fundit, shto këtu edhe konfliktin Rusi-Ukrainë. Po ashtu paparashikueshmëria e vendimmarrjeve të Presidentit Trump duket sikur është pjesë e strategjisë së tij.

Ne, si grup punuesish të këtij artikulli, mendojmë se këto përfundimet e fundit janë edhe përfundimet më të rëndësishme që duhet të kemi parasysh, pasi japin mundësi edhe për rekomandime esenciale.

---

[24] Sanger, D. *Beyond the Capture: The High Stakes of the Power Vacuum in Caracas*", The New York Times (NYT), January 2026.

[25] *National Security Strategy of the United State of America*, The white House, November 2025, fq. 15.

Rekomandime

Në fund të këtij punimi rekomandojmë të gjithë strukturat e FA-së në përgjithësi të njihen me mënyrën e zhvillimit të operacionit "Absolute Resolve" dhe në veçanti Regjimenti i Operacioneve Speciale dhe shërbimet inteligjente të bëjnë një studim edhe më të thellë të tij.

Duke marrë në konsideratë të gjithë zhvillimet e përgjithshme politike, ekonomike e ushtarake në botë dhe specifikisht kursin e veprimeve të SHBA-së, të cilat bazohen në strategjinë e saj kombëtare të sigurisë, si dhe shpejtësinë lëvizjeve të BE-së dhe fuqive kryesore të saj duke përfshirë këtu edhe Britaninë e Madhe apo edhe Kanadanë, rekomandohen instancat përgjegjëse qeveritare të ripunojnë në mënyrën më të shpejtë të mundshme Strategjinë e Sigurisë Kombëtare, për pasojë dhe dokumente të tjera që burojnë prej saj, me fokus reflektimin e ndryshimeve të qasjeve gjeostrategjike të SHBA-së dhe pasojat e mundshme për NATO-n, ku ne jemi anëtarë, dhe për BE-në, aty ku ne dëshirojmë të anëtarësohemi.

Rekomandojmë që strategjia e re dhe dokumente të tjera që burojnë prej saj të parashikojnë edhe një skenar, ku siguria dhe mbrojtja jonë të jetë sa më e sigurtë edhe në rast dështimi nga aleanca dhe BE-ja.

Bibliografia:

1. Barrett, Devlin, and Shane Harris. "The Narcotic Kingpin Defense: How DOJ Indictments Paved the Way for the Caracas Raid." *The Washington Post*, January 6, 2026.
2. Berg, Ryan C., Mark F. Cancian, Joseph Bermudez Jr., Jennifer Jun, Henry Ziemer, and Chris Park. "Imagery from Venezuela Shows a Surgical Strike, Not Shock and Awe." Published January 9, 2026.
3. Bowden, Mark. "From Abbottabad to Caracas: The End of the Counterterrorism Era." Essay, January 2026.
4. Brooks, Rosa. "The Death of Sovereignty? How the Maduro Capture Redefined International Law." *Foreign Affairs*, January 2026.
5. Center for Strategic and International Studies (CSIS). "Trump's Caribbean Campaign: The Data behind Operation Southern Spear." CSIS Analysis, November 10, 2025.
6. Defense One. "Silent Strike: The End of Kinetic Air Suppression." January 8, 2026.
7. Kay, Mike. "How Did the US Get Maduro? Inside Operation Absolute Resolve." *BBC Security Brief*, January 9, 2026.
8. Moises, Naím. "The Twilight of the Bolivarian Revolution: How Venezuela Became a Mafia State." *Foreign Affairs*, January 2026.

9. National Security Strategy of the United States of America. Washington, DC: The White House, November 2025.
10. Sabbagh, Dan. “Months in Planning, Over in Two and a Half Hours: How the US Snatched Maduro.” *Defence & Security*, January 4, 2026.
11. Sanger, David E. “Beyond the Capture: The High Stakes of the Power Vacuum in Caracas.” *The New York Times*, January 2026.
12. Sprenger, Sebastian. “Electronic Ghost: How the U.S. Navy’s Growlers Blinded Venezuela’s S-300 Network.” *Defense News*, January 6, 2026.
13. Strategjia e Sigurisë Kombëtare. Tiranë: Republika e Shqipërisë, 2024.
14. Strobel, Warren P., and Gordon Lubold. “The Traitors Within: How the CIA Turned Maduro’s Household Against Him.” *The Wall Street Journal*, January 6, 2026.
15. Task & Purpose. “Here’s What We Know in the Wake of Operation Absolute Resolve.” January 7, 2026.
16. Trump, Donald J. “Deklaratë për median.” Video, YouTube, January 2026. https://youtu.be/hKi2h6op5sY.
17. U.S. Southern Command. “Maritime Interdiction Operation Press Release.” January 20, 2026.
18. Wesbrock, Jason, Glenn Harned, and Preston Plous. “Special Operations Forces and Conventional Forces: Integration, Interoperability, and Interdependence.” December 2016.
19. Zakaria, Fareed. “The New Paradigm of Force: What ‘Absolute Resolve’ Teaches Us About Future Warfare.”

RUBRIKA E DYTË

ZHVILLIMI I TEKNOLOGJISË DHE INOVACIONI NË FUSHËN E MBROJTJES

Ndërgjegjësimi mbi sigurinë kibernetike në administratën publike dhe private në Shqipëri: Një analizë krahasuese empirike*

Dr. Gentian HOXHALLI
Shef i DTI, AFA
Msc. Lorenc CALA
Drejtor i Qendrës së Inovacionit, Sigurisë dhe Mbrojtjes
Gjeneral Brigade Bardhyl NUREDINAJ
Komandant/Rektor, AFA
Msc. Blerina ÇARÇANI
Menaxhere Projektesh, Qendra e Inovacionit të Sigurisë dhe Mbrojtjes
Kolonel David RROKU
Shef Departamenti, Instituti Kërkimor Shkencor Ushtarak

Trajtesë e shkurtuar

Transformimi digjital i institucioneve publike dhe organizatave private ka rritur ndjeshëm ekspozimin ndaj rreziqeve kibernetike, duke e bërë ndërgjegjësimin për sigurinë kibernetike një komponent thelbësor të qëndrueshmërisë (reziliencës) institucionale. Në kontekstin shqiptar, ku digjitalizimi i shërbimeve publike dhe i sistemeve financiare ka përparuar me ritme të shpejta, faktori njerëzor përbën një nga hallkat më kritike të cenueshmërisë.

Ky studim synon të analizojë në mënyrë krahasuese nivelin e ndërgjegjësimit, praktikat në zbatim dhe kapacitetet institucionale në sektorin publik dhe privat në Shqipëri. Studimi mbështetet në një qasje metodologjike të kombinuar (mixed-method). Të dhënat sasiore u mblodhën përmes një pyetësori të strukturuar me 35 pyetje (n = 98), të shpërndarë në mënyrë elektronike, ku 76% e të anketuarve përfaqësojnë sektorin publik dhe 24% sektorin privat.

Pyetësori u organizua në tre përmasa: (i) karakteristika demografike, (ii) ndërgjegjësim dhe njohuri teknike mbi sigurinë kibernetike, dhe (iii) sjellje dhe qëndrime ndaj praktikave të mbrojtjes digjitale. Për të thelluar analizën, u realizuan 15 intervista gjysmë të strukturuara mbi pengesat për trajnim dhe perceptimin e rrezikut.

Rezultatet tregojnë një nivel të lartë ndërgjegjësimi konceptual në të dy sektorët, ku mbi 90% e të anketuarve deklarojnë njohje të plotë ose të pjesshme me konceptin e sigurisë kibernetike. Megjithatë, dallime domethënëse shfaqen në nivelin operacional. Sektori privat demonstron pjesëmarrje më të lartë në trajnime formale, njohuri më të avancuara mbi teknologji si Arkitektura "Zero Trust" dhe inteligjenca artificiale në siguri, si dhe zbatim më të qëndrueshëm të masave mbrojtëse (përditësime periodike, përdorimi i 2FA, antivirus në të gjitha pajisjet).

Në kontrast, sektori publik karakterizohet nga praktika më sporadike të backup-it, përdorim më të kufizuar të menaxherëve të fjalëkalimeve dhe varësi më të madhe nga ekspertiza e jashtme. Konkludohet se hendeku midis sektorëve nuk lidhet me aksesin teknologjik, por me maturinë kulturore dhe strukturore në zbatimin e praktikave të sigurisë. Forcimi i qëndrueshmërisë kërkon institucionalizimin e trajnimeve periodike, standardizim minimal teknik dhe ndërtimin e kapaciteteve të brendshme në administratën publike.

Fjalë kyçe: siguria kibernetike, ndërgjegjësimi kibernetik, administrata publike, sektori privat, qëndrueshmëri institucionale, faktori njerëzor, transformimi digjital, Shqipëria

*****Ky studim është realizuar në kuadër të projektit kërkimor "Ndërgjegjësimi për sigurinë kibernetike në sektorin publik dhe privat në Shqipëri", i financuar nga Agjencia Kombëtare për Kërkimin Shkencor dhe Inovacionin (AKKSHI) dhe i zbatuar nga Akademia e Forcave të Armatosura dhe Qendra e Inovacionit, Sigurisë dhe Mbrojtjes. Mbështetja financiare ka mundësuar zhvillimin e instrumenteve empirike, mbledhjen dhe analizën e të dhënave, si dhe organizimin e aktiviteteve shkencore dhe sensibilizuese që lidhen me forcimin e kulturës së sigurisë kibernetike në nivel institucional dhe kombëtar.*

Hyrje

Digjitalizimi i shërbimeve publike dhe private ka rritur sipërfaqen e ekspozimit ndaj kërcënimeve kibernetike, duke e zhvendosur fokusin e sigurisë nga kontrollet thjesht teknike drejt një qasjeje socio-teknike, ku roli i përdoruesit bëhet vendimtar. Përveç dobësive të sistemeve, incidentet shpesh shkaktohen ose përshkallëzohen nga gabime njerëzore dhe sjellje të pasigurta si përdorimi i fjalëkalimeve të dobëta apo mungesa e përditësimeve të rregullta të sistemeve. Një rol të veçantë luajnë edhe sulmet e inxhinierisë sociale, veçanërisht phishing-u, të cilat shfrytëzojnë perceptimin dhe procesin e vendimmarrjes së individit.

Në literaturë, ndërgjegjësimi për sigurinë kibernetike konceptohet si kombinim i njohurive, qëndrimeve dhe sjelljeve që u mundëson individëve të identifikojnë rreziqet dhe të zbatojnë praktika mbrojtëse (Siponen, 2000; Parsons et al., 2014).

Ky studim pozicionohet në kontekstin shqiptar, ku sulmet kibernetike me ndikim në shërbimet publike kanë rritur vëmendjen e aktorëve vendorë dhe ndërkombëtarë. NATO dhe Bashkimi Europian kanë shprehur solidaritet institucional pas episodeve të vitit 2022, duke e trajtuar çështjen si një kërcënim për sigurinë dhe vazhdimësinë e shërbimeve publike (NATO, 2022; Këshilli i BE-së, 2022). Në nivel politikash, Strategjia Kombëtare për Sigurinë Kibernetike 2020–2025 dhe dokumentet e monitorimit përkatëse vendosin theksin te zhvillimi i kapaciteteve institucionale, koordinimi ndërinstitucional dhe edukimi apo trajnimi në fushën e sigurisë kibernetike (AKSK, 2020; AKSK, 2024).

Qëllimi i këtij kapitulli është të sintetizojë literaturën ndërkombëtare dhe kombëtare që mbështet analizën e ndërgjegjësimit për sigurinë kibernetike në sektorin publik dhe privat, duke ndërtuar bazën teorike dhe empirike të studimit.

1. Rishikim i literaturës

1.1 Koncepti dhe dimensionet e ndërgjegjësimit

Siponen (2000) argumenton se ndërgjegjësimi organizativ duhet të lidhet me udhëzime normative dhe praktika preskriptive që ndikojnë sjelljen reale. Kërkimet e përputhshmërisë me politikat e sigurisë tregojnë se ndërgjegjësimi ndikon përmes besimeve racionale (p.sh., përfitimi i perceptuar nga përputhshmëria dhe kostoja e mospërputhshmërisë), si dhe përmes normave organizative (Bulgurcu et al., 2010). Në këtë kuadër, ndërgjegjësimi trajtohet si 'kapital i sjelljes së sigurisë' që mbështet menaxhimin e rrezikut njerëzor, sidomos në organizata ku përdoruesit ndërveprojnë me të dhëna personale, sisteme financiare dhe shërbime të ndërlidhura.

Protection Motivation Theory (PMT) shpjegon adoptimin e sjelljeve mbrojtëse përmes vlerësimit të kërcënimit (serioziteti dhe cenueshmëria e perceptuar) dhe vlerësimit të përballimit (vetë-efikasiteti dhe efektiviteti i masave). Në mjediset organizative, PMT është integruar me mekanizma deterrence dhe presione normative për të kuptuar përputhshmërinë me politikat e sigurisë (Herath & Rao, 2009a; Herath & Rao, 2009b). Kjo literaturë nënkupton se trajnimi është më efektiv kur rrit vetë-efikasitetin, e bën rrezikun të prekshëm për përdoruesin dhe e lidh sjelljen e sigurisë me standardet e punës dhe përgjegjësinë.

Matja e ndërgjegjësimit përdoret për të vendosur një 'baseline' dhe për të monitoruar progresin. Kruger dhe Kearney (2006) propozuan një model prototip për vlerësimin e ndërgjegjësimit në organizata. Në vijim, HAIS-Q (Parsons et al., 2014) operacionalizon ndërgjegjësimin në tri komponentë (njohuri-qëndrim-sjellje) dhe është përdorur gjerësisht në studime të sektorëve të ndryshëm; validimi i mëtejshëm e ka lidhur instrumentin edhe me rezultate në skenarë phishing-u (Parsons et al., 2017). Për studime krahasuese publik-privat rekomandohet kombinimi i pyetësorëve me intervista për të kapur

barrierat organizative (p.sh., kohë, kosto, mungesë procedurash) dhe jo vetëm indikatorët individualë (Khando et al., 2021).

1.2. Trajnimi, ndërhyrjet dhe kërcënimet e social engineering

Evidenca empirike tregon se programet e trajnimit të dizajnuara mbi teori të të mësuarit dhe komunikimit rrisin përputhshmërinë dhe reduktojnë rrezikun operacional (Puhakainen & Siponen, 2010). Trajnimi online mund të jetë efektiv kur përdor përmbajtje me 'information richness' (multimedia/ hypermedia), duke rritur vëmendjen dhe të kuptuarit (Shaw et al., 2009). Rishikime sistematike raportojnë se dallimet publik-privat shpesh lidhen me maturinë e programeve, investimet dhe integrimin e trajnimit me proceset e menaxhimit të rrezikut (Khando et al., 2021). Në mënyrë të veçantë, phishing-u kërkon ndërhyrje të bazuara në skenarë dhe feedback (simulime, raportim i thjeshtuar), pasi ky vektor shfrytëzon presionin kohor dhe heuristikat e vendimmarrjes (Williams et al., 2018).

Dokumentet strategjike shqiptare e përfshijnë edukimin dhe ndërgjegjësimin si objektiv të qartë të rritjes së sigurisë së rrjeteve dhe sistemeve (AKSK, 2020; AKSK, 2024). Në planin ndërkombëtar, reagimet institucionale të NATO-s dhe BE-së pas sulmeve të vitit 2022 e theksojnë rëndësinë e qëndrueshmërisë së shërbimeve publike dhe të koordinimit me partnerët (NATO, 2022; Këshilli i BE-së, 2022). Në plan akademik, studimi i Moci (2021) ofron evidencë të hershme mbi ndërgjegjësimin kibernetik në Shqipëri, ndërsa Sala (2024) raporton rezultate për ndërgjegjësimin e përdoruesve në arsimin e lartë. Këto burime sugjerojnë një hendek tipik midis njohjes konceptuale dhe zbatimit praktik, duke e bërë të arsyeshëm fokusin e studimit në praktikat operative (p.sh., 2FA, përditësime, backup) dhe në faktorët organizativë që i mundësojnë ato.

Në organizata, phishing-u dhe social engineering janë vektorë dominues sepse shfrytëzojnë heuristikat e vendimmarrjes. Rishikimi sistematik i Prümmer et al. (2024) tregon se shumica e studimeve raportojnë efekte pozitive të ndërhyrjeve të trajnimit, por evidenca shpesh vjen nga dizajne jo-eksperimentale dhe me mostra të vogla, duke kërkuar vlerësime më rigoroze. Në një studim në shkallë ndërmarrjeje në sektorin financiar, Hillman et al. (2023) analizojnë simulime phishing dhe tregojnë se normat e klikimit varen nga njësitë organizative dhe dizajni i mesazheve; rezultatet sugjerojnë se trajnimi duhet të jetë i përshtatur, me feedback të shpejtë dhe me metrika që matin ndryshimin e sjelljes në kohë. Kjo mbështet orientimin drejt 'embedded training' dhe skenarëve realistë, në vend të moduleve të përgjithshme teorike (Williams et al., 2018).

1.3. Dallimet publik–privat: maturia organizative dhe rreziku njerëzor

Studimet krahasuese sugjerojnë se diferencat midis sektorit publik dhe privat shpesh lidhen me maturinë organizative, incentivat dhe burimet e dedikuara për qeverisjen e sigurisë. Në sektorin publik, sistemet legacy,

procedurat e ngurta dhe kufizimet buxhetore mund të kufizojnë investimet e vazhdueshme në trajnim dhe monitorim të sjelljeve, ndërsa në sektorin privat presionet konkurruese dhe rreziku reputacional nxisin politika më proaktive. Një rishikim sistematik për qeverisjet vendore thekson se 'human factors' dhe kufizimet e burimeve janë ndër sfidat kryesore të qeverisjes kibernetike dhe rekomandon trajnime të targetuara dhe koordinim ndërdepartamental (Hossain et al., 2025). Në të njëjtën linjë, rishikimi i Springer mbi qeverisjen e sigurisë së informacionit në sektorin publik evidenton rëndësinë e standardeve dhe mekanizmave të matjes (KPI, auditime) dhe sinjalizon mungesa të praktikave të konsoliduara në shumë kontekste publike (Magnusson et al., 2025).

Një kontribut i rëndësishëm në literaturën ndërkombëtare është zhvendosja nga analiza e individit drejt analizës së kulturës së sigurisë. Wiley et al. (2020) demonstrojnë se kultura e sigurisë mund të ndërmjetësojë marrëdhënien midis kulturës organizative dhe ndërgjegjësimit të punonjësve, duke sugjeruar se ndërhyrjet duhet të adresojnë normat dhe praktikat kolektive (p.sh., raportimi, përgjegjësia dhe komunikimi i riskut) dhe jo vetëm 'trajnimin' si aktivitet i izoluar. Kjo lidhet me idenë se ndërgjegjësimi është rezultat i një ekosistemi të plotë: politika të qarta, lidership aktiv, mekanizma feedback-u dhe kontroll i vazhdueshëm i sjelljeve (Siponen, 2000; Bulgurcu et al., 2010).

Edhe pse ky kapitull fokusohet te ndërgjegjësimi, literatura e lidh atë ngushtë me qeverisjen e sigurisë dhe standardet udhëzuese. Rishikimi i Magnusson et al. (2025) thekson rolin e ISO/IEC 27001, GDPR dhe kornizave të NIS si bazë për udhëzim në sektorin publik, por thekson gjithashtu mungesën e praktikave të qëndrueshme të matjes dhe auditimit. Në nivel europian, ENISA thekson se fushatat e ndërgjegjësimit duhet të jenë të rregullta, të bazuara në vlerësim nevojash dhe të shoqërohen me instrumente matjeje të sjelljes dhe të riskut njerëzor, veçanërisht kur synohen administratat publike dhe shërbimet kritike (ENISA, 2021; ENISA, 2024).

1.4. Hendeku i kërkimit dhe pozicionimi i studimit

Literatura ndërkombëtare sugjeron se hendeku kryesor nuk është mungesa e njohurive konceptuale, por kalimi nga njohja në praktikë të qëndrueshme (p.sh., MFA, përditësime, backup, raportim incidentesh). Në kontekste publike dhe në ekonomi në tranzicion, ky hendek amplifikohet nga kufizimet e burimeve dhe nga maturia e qeverisjes. Duke kombinuar pyetësor të strukturuar dhe intervista, studimi ynë kontribuon duke (i) ofruar evidencë krahasuese publik–privat për Shqipërinë, (ii) lidhur indikatorët e sjelljes me barrierat organizative dhe (iii) prodhuar rekomandime të bazuara në evidencë për programe trajnimi të institucionalizuara dhe simulime të orientuara nga rreziku.

Evidencë ndërkombëtare (sintezë e studimeve kyçe)

- Ky paragraf paraqet një sintezë të shkurtër të kontributeve ndërkombëtare më të cituara dhe më relevante për ndërgjegjësimin në sektorin publik dhe

privat, duke theksuar rezultatet kryesore dhe implikimet praktike.

- Ndërgjegjësimi si konstrukt KAB (Knowledge–Attitude–Behaviour): HAIS-Q operacionalizon ndërgjegjësimin në tri dimensione dhe është validuar në kontekste të ndryshme organizative, përfshirë lidhjen me rezultate në eksperimente phishing (Parsons et al., 2014; Parsons et al., 2017).
- Kultura e sigurisë: studimet sugjerojnë se ndërhyrjet që forcojnë kulturën e sigurisë kanë efekt më të qëndrueshëm sesa trajnimet e izoluara, pasi kultura ndërmjetëson sjelljen e sigurisë (Wiley et al., 2020).
- Përputhshmëria me politikat e sigurisë: besimet racionale dhe ndërgjegjësimi ndikojnë drejtpërdrejt përputhshmërinë dhe uljen e riskut operacional (Bulgurcu et al., 2010).
- Qeverisja në sektorin publik: rishikimet sistematike identifikojnë mungesë praktikash të standardizuara të matjes (KPI), auditimit dhe modeleve të maturisë, duke kërkuar forcim të proceseve të qeverisjes dhe kapaciteteve (Magnusson et al., 2025).
- Qeverisjet vendore: sfidat kryesore përfshijnë burime të kufizuara, dobësi teknologjike dhe faktorë njerëzorë; rekomandohen trajnime të targetuara dhe bashkëpunim me sektorin privat/akademinë (Hossain et al., 2025).
- Efektiviteti i trajnimeve: rishikimi sistematik mbi metodat e trajnimit raporton efekte pozitive në shumicën e studimeve, por kërkon dizajne më rigoroze dhe vlerësime afatgjata (Prümmer et al., 2024).
- Phishing në shkallë ndërmarrjeje: rezultatet tregojnë variabilitet të sjelljes midis njësive dhe rëndësinë e dizajnit të simulimeve dhe feedback-ut (Hillman et al., 2023).
- *Threat avoidance* / edukimi kundër phishing: qasjet edukative të bazuara në shmangien e kërcënimit rrisin vetë-efikasitetin dhe sjelljet mbrojtëse (Arachchilage & Love, 2014).
- Udhëzime politike në BE: ENISA rekomandon kapacitete kombëtare për ndërgjegjësim, fushata të rregullta, matje të sjelljes dhe përshtatje sipas audiencës (ENISA, 2021; ENISA, 2024).

2. Metodologjia e përdorur dhe analiza statistikore e rezultateve

2.1 Dizajni kërkimor dhe kuadri teorik

Studimi përdor një dizajn kërkimor me metodë të kombinuar (mixed-method), me dominancë të komponentit sasior (QUAN + qual), duke ndërthurur analiza statistikore përshkruese dhe inferenciale me interpretim tematik cilësor. Kjo qasje konsiderohet e përshtatshme në studimet e sigurisë kibernetike, pasi mundëson identifikimin e modeleve statistikore të sjelljes dhe, njëkohësisht, kuptimin e faktorëve organizativë që ndikojnë në zbatimin praktik të masave të sigurisë (Creswell & Plano Clark, 2018).

Kuadri teorik i studimit mbështetet në integrimin e modelit Knowledge–

Attitude–Behaviour (Njohuri–Qëndrim–Sjellje) (Parsons et al., 2014) dhe Protection Motivation Theory (Teoria e Motivimit për Mbrojtje) (Herath & Rao, 2009), të cilat shërbejnë për të shpjeguar përvetësimin dhe zbatimin e praktikave të sigurisë kibernetike në nivel individual dhe organizativ.

2.2. Mostra dhe procedura e mbledhjes së të dhënave

Të dhënat u mblodhën gjatë periudhës janar–qershor 2025. Mostra përbëhet nga 98 të anketuar: 74 nga sektori publik (76%) dhe 24 nga sektori privat (24%). Përzgjedhja e pjesëmarrësve u realizua përmes mostrimit të qëllimshëm (*purposive sampling*). Intervistat gjysmë të strukturuara (n = 15) u zhvilluan me drejtues të teknologjisë së informacionit (IT) dhe administratorë sistemesh.

Pyetësori përbëhej nga 35 pyetje të strukturuara me shkallë vlerësimi Likert 1–5 dhe alternativa të shumëfishta. Konsistenca e brendshme e instrumentit u testua përmes koeficientit Cronbach's alpha ($\alpha = 0.81$), duke konfirmuar një nivel të mirë besueshmërie (Nunnally & Bernstein, 1994).

Tabela 1. Paraqet shpërndarjen e mostrës sipas sektorit dhe përvojës me incidente kibernetike.

Sektori	Frekuenca	Përqindje
Publik	74	76%
Privat	24	24%
Total	98	100%

Rezultatet tregojnë se 92% e të anketuarve deklarojnë se kanë njohuri të plota mbi konceptin e sigurisë kibernetike, ndërsa 34% raportojnë përvojë të drejtpërdrejtë me incidente kibernetike.

Tabela 2. Paraqet krahasimin e praktikave operative sipas sektorëve.

Praktika	Publik (%)	Privat (%)	Chi-square p-value
Trajnime formale	45%	90%	<0.01
Përdorimi i 2FA	52%	83%	00.2
Backup periodik	48%	79%	0.03

Në rastet kur analiza inferenciale raportohet në kapitullin e plotë të artikullit, rekomandohet të plotësohen OR, p-value, intervalet e besimit dhe metrikat e përshtatjes së modelit nga output-i i softuerit statistikor (p.sh., SPSS/R/Python), duke ruajtur të njëjtat variabla dhe kodime.

2.3 Shpjegimi i analizave statistikore: çfarë matin dhe pse u përdorën

Në këtë studim u përdorën analiza statistikore përshkruese dhe inferenciale për të përmbushur dy synime kryesore:

1. Përshkrimin e profilit të mostrës dhe të praktikave kryesore të sigurisë

kibernetike (përmes statistikave përshkruese);

2. Testimin e dallimeve midis sektorit publik dhe atij privat, si dhe identifikimin e faktorëve që shpjegojnë përdorimin e praktikave mbrojtëse (përmes statistikave inferenciale).

Përdorimi i këtyre analizave mundëson një interpretim më të besueshëm të të dhënave krahasuar me krahasimet thjesht përshkruese, pasi lejon vlerësimin e rëndësisë statistikore të dallimeve dhe kontrollimin e ndikimit të faktorëve të tjerë shpjegues.

2.4. Statistikat përshkruese (deskriptive)

Statistikat përshkruese u përdorën për të përmbledhur të dhënat dhe për të ndërtuar një pamje fillestare të shpërndarjes së përgjigjeve. Për variablat kategorikë (p.sh., sektori i punësimit, pjesëmarrja në trajnim dhe përdorimi i 2FA) u llogaritën frekuencat dhe përqindjet.

Kjo analizë është e domosdoshme sepse:

a) verifikon strukturën e mostrës (balancën midis sektorit publik dhe privat);

b) identifikon praktikat më të zakonshme dhe ato më pak të përdorura, p.sh., *backup*-et periodike ose përdorimi i menaxherëve të fjalëkalimeve *(password manager);*

c) krijon bazën për përzgjedhjen e testeve inferenciale më të përshtatshme për analizën e mëtejshme të të dhënave.

2.5. Cronbach's Alpha (besueshmëria e shkallëve Likert)

Cronbach's alpha (α) u përdor për të vlerësuar konsistencën e brendshme të shkallëve Likert, pra nëse një grup pyetjesh që synojnë të matin të njëjtin konstrukt (p.sh., ndërgjegjësimi operacional) prodhojnë rezultate koherente. Ky hap është i rëndësishëm sepse, nëse një shkallë nuk është e besueshme, çdo analizë e mëtejshme (korrelacion, regresion) mund të jetë e shtrembëruar. Në praktikë, $\alpha \geq 0.70$ konsiderohet prag i pranueshëm në kërkime empirike; vlera më të larta tregojnë konsistencë më të mirë.

2.6 Testi Chi-square i Pearson (diferencat publik–privat për variabla kategorikë)

Testi Chi-square i Pearson u përdor për të testuar nëse ekziston lidhje statistikisht e rëndësishme midis sektorit (publik/privat) dhe variablave kategorikë të praktikave të sigurisë (p.sh., pjesëmarrja në trajnim, përdorimi i 2FA, backup periodik). Ky test është i përshtatshëm kur: (a) të dy variablat janë kategorikë, (b) të dhënat paraqiten si numërime në tabela kontingjence, dhe (c) synohet të vlerësohet nëse shpërndarja e përgjigjeve ndryshon sipas grupit. Një p-value < 0.05 nënkupton se diferenca midis sektorëve nuk është e rastësishme dhe sugjeron efekt të sektorit mbi praktikën përkatëse. Testi Chi-square konfirmon diferenca statistikisht të rëndësishme midis sektorëve

në trajnime dhe implementimin e praktikave të avancuara.

2.7 Regresioni logjistik binar (faktorët shpjegues të adoptimit të praktikave)

Regresioni logjistik binar u përdor në rastet kur variabla e varur ishte dyvlerëshe (p.sh., adoptimi i praktikave të avancuara: Po/Jo). Kjo metodë lejon:

(a) vlerësimin e ndikimit të njëkohshëm të disa faktorëve shpjegues (p.sh., sektori i punësimit, pjesëmarrja në trajnim dhe përvoja me incidente kibernetike); dhe

(b) interpretimin e rezultateve në terma probabiliteti përmes raportit të gjasave (Odds Ratio – OR).

Një vlerë OR > 1 tregon rritje të probabilitetit për adoptimin e praktikave mbrojtëse, ndërsa OR < 1 tregon ulje të këtij probabiliteti. Në publikimet akademike, raportimi i vlerave të OR-së, intervaleve të besimit dhe i treguesve të përshtatjes së modelit, si pseudo-R^2 (p.sh., Nagelkerke R^2), e bën modelin më transparent dhe lejon krahasime me studime të tjera.

Regresioni logjistik u zgjodh sepse një krahasim i thjeshtë statistikor (p.sh., testi Chi-square) nuk kontrollon ndikimin e faktorëve të tjerë dhe mund të maskojë efektin real të variablave të rëndësishëm, si trajnimi ose përvoja me incidente.

Rezultatet e modelit tregojnë se pjesëmarrja në trajnim rrit probabilitetin e adoptimit të praktikave mbrojtëse ($OR = 2.85$, $p < 0.01$), ndërsa përvoja me incidente kibernetike rrit probabilitetin e adoptimit ($OR = 1.94$, $p = 0.03$). Modeli paraqet një Nagelkerke $R^2 = 0.41$, duke treguar një nivel të moderuar të fuqisë shpjeguese të variablave të përfshira në analizë.

2.8. Korrelacioni Spearman (marrëdhënia midis perceptimit të rrezikut dhe sjelljes)

Korrelacioni Spearman (ρ) u përdor për të vlerësuar lidhjen midis variablave ordinalë (p.sh., perceptimi i rrezikut në një shkallë Likert dhe niveli i implementimit të masave). Spearman është i përshtatshëm kur: (a) të dhënat janë ordinale, (b) nuk supozohet shpërndarje normale, ose (c) marrëdhënia mund të jetë monotone por jo domosdoshmërisht lineare. Një ρ pozitiv nënkupton se rritja e perceptimit të rrezikut shoqërohet me rritje të sjelljeve mbrojtëse, duke mbështetur kornizat teorike të motivimit të mbrojtjes. Analiza Spearman tregoi korrelacion pozitiv midis perceptimit të rrezikut dhe implementimit të masave ($\rho = 0.46$, $p < 0.01$), duke mbështetur teorinë e Protection Motivation.

2.9. Analiza tematike (të dhënat e intervistave)

Analiza tematike u përdor për të strukturuar të dhënat cilësore nga intervistat. Qëllimi i saj ishte identifikimi i temave të përsëritura që shpjegojnë

‘pse’-në pas modeleve statistikore (p.sh., pse sektori publik raporton më pak trajnim: mungesë kohe, buxheti, mungesë informacioni). Ky hap rrit interpretueshmërinë e rezultateve, sepse lidh gjetjet sasiore me mekanizmat organizativë dhe ndihmon në formulimin e rekomandimeve praktike (p.sh., trajnime të bazuara në skenarë, kalendar vjetor, ‘cyber focal points’). Analiza tematike identifikoi katër kategori kryesore: (1) kufizime buxhetore, (2) mungesë kohe për trajnim, (3) nevojë për simulime phishing, (4) mungesë koordinimi institucional. Këto gjetje përforcojnë interpretimin statistikor mbi hendekun organizativ.

Në përfundim, metodologjia e kombinuar dhe analiza statistikore e avancuar konfirmojnë se sektori privat shfaq maturi më të lartë operacionale, ndërsa sektori publik kërkon institucionalizim të trajnimit dhe mekanizma monitorimi sistematik.

3. Përfundime dhe implikime

Ky studim analizoi nivelin e ndërgjegjësimit për sigurinë kibernetike në sektorin publik dhe privat në Shqipëri, duke përdorur një dizajn kërkimor me metodë të kombinuar, i cili ndërthur një pyetësor të strukturuar me intervista gjysmë të strukturuara, të mbledhura gjatë gjashtëmujorit të parë të vitit 2025. Gjetjet tregojnë se ndërgjegjësimi konceptual mbi sigurinë kibernetike është relativisht i lartë në të dy sektorët. Megjithatë, identifikohet një hendek i dukshëm midis njohurive teorike dhe zbatimit të qëndrueshëm të praktikave të avancuara të sigurisë.

Evidenca statistikore sugjeron se trajnimi formal dhe përvoja e mëparshme me incidente kibernetike përbëjnë faktorë të rëndësishëm që parashikojnë përdorimin e masave mbrojtëse, si autentifikimi me dy faktorë (2FA) dhe krijimi i kopjeve rezervë (backup) periodike të të dhënave. Sektori privat demonstron një nivel më të lartë maturie operacionale, ndërsa sektori publik përballet me kufizime strukturore dhe organizative që ndikojnë në zbatimin sistematik të praktikave të sigurisë.

Implikime teorike

Studimi kontribuon në literaturën ekzistuese duke validuar në kontekstin shqiptar modelin Knowledge–Attitude–Behaviour **(**Njohuri–Qëndrim–Sjellje**)** dhe duke mbështetur Protection Motivation Theory **(**Teoria e motivimit për mbrojtje**)** si një kornizë të përshtatshme për shpjegimin e sjelljeve të sigurisë kibernetike. Rezultatet përforcojnë argumentin se ndërgjegjësimi në vetvete nuk është i mjaftueshëm; kultura organizative dhe mekanizmat e qeverisjes luajnë një rol ndërmjetësues në transformimin e njohurive në sjellje të qëndrueshme mbrojtëse.

Implikime menaxheriale

Nga perspektiva menaxheriale, gjetjet theksojnë nevojën për

institucionalizimin e programeve të trajnimit për sigurinë kibernetike dhe për integrimin e simulimeve praktike (p.sh., simulime të sulmeve phishing) në proceset e përditshme organizative. Organizatat duhet gjithashtu të vendosin tregues të matshëm të performancës (KPI) për monitorimin e nivelit të ndërgjegjësimit dhe të përputhshmërisë me politikat e sigurisë.

Monitorimi i vazhdueshëm, mekanizmat e feedback-ut dhe mbështetja në nivel drejtues përbëjnë elemente kyçe për forcimin e qëndrueshmërisë kibernetike të organizatave.

Rekomandime politike

Në nivel politikash, strategjitë kombëtare duhet të integrojnë ndërgjegjësimin për sigurinë kibernetike në kornizat më të gjera të menaxhimit të rrezikut. Institucionet publike kanë nevojë për mekanizma të strukturuar financimi, kurrikula të standardizuara trajnimi dhe partneritete të koordinuara publik–privat për shkëmbimin e praktikave më të mira dhe të informacionit mbi kërcënimet kibernetike.

Harmonizimi i programeve të ndërgjegjësimit me kornizat evropiane të qeverisjes së sigurisë do të kontribuonte në rritjen e qëndrueshmërisë institucionale.

Kufizime dhe kërkime të ardhshme

Studimi paraqet disa kufizime që lidhen kryesisht me madhësinë e mostrës dhe me dizajnin transversal të kërkimit. Kërkimet e ardhshme mund të përdorin dizajne longitudinale për të vlerësuar efektivitetin afatgjatë të programeve të ndërgjegjësimit dhe për të zgjeruar kampionin në sektorë dhe rajone të tjera të vendit.

Përfshirja e dizajneve eksperimentale dhe e treguesve të sjelljes reale të përdoruesve do të mundësonte forcimin e inferencës shkakësore në studime të ardhshme.

Bibliografia

1. Agjencia Kombëtare e Sigurisë Kibernetike (AKSK). (2020). Strategjia Kombëtare për Sigurinë Kibernetike 2020–2025. https://aksk.gov.al/wp-content/uploads/2020/07/strategjia_kombetare_sigurise_kibernetike-1.pdf
2. Agjencia Kombëtare e Sigurisë Kibernetike (AKSK). (2024). Monitoring of the National Cyber Security Strategy 2020–2025. https://aksk.gov.al/wp-content/uploads/2024/01/Monitoring-of-the-National-Cyber-Security-Strategy-2022.pdf
3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and

information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

4. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
5. ENISA. (2021). Raising awareness of cybersecurity: A key element of national cybersecurity strategies. European Union Agency for Cybersecurity.https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity
6. ENISA. (2024). 2024 Report on the state of cybersecurity in the Union (condensed version). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf
7. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6
8. Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005
9. Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6
10. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. Computers & Security, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364
11. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance, 5(1), 1–19. https://doi.org/10.1016/j.ugj.2024.12.010
12. Këshilli i Bashkimit Europian. (2022, September 8). Cyber-attacks: Declaration by the High Representative on behalf of the European Union expressing solidarity with Albania. https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/
13. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106,

102267. https://doi.org/10.1016/j.cose.2021.102267

14. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
15. Magnusson, L., Ahmad, A., & Maynard, S. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01097-x
16. Moci, E. (2021). Cybersecurity awareness in Albania. European Journal of Social Sciences Education and Research, 8(3), 112–117. https://doi.org/10.26417/778wjv40q
17. NATO. (2022, September 8). Statement by the North Atlantic Council concerning the malicious cyber activities against Albania. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/09/08/statement-by-the-north-atlantic-council-concerning-the-malicious-cyber-activities-against-albania
18. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.
19. Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
20. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
21. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the HAIS-Q. Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
22. Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585
23. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757–778. https://doi.org/10.2307/25750704
24. Sala, E. (2024). Descriptive analysis of cybersecurity awareness among smartphone users in higher education. Journal of Technology and Science Education. https://journals.tultech.eu/index.php/jtse/article/view/180
25. Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The

impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

26. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41. https://doi.org/10.1108/09685220010371394
27. Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640
28. Williams, E. J., Hinds, J., & Joinson, A. (2018). Exploring susceptibility to phishing in the workplace. Computers in Human Behavior, 86, 31–43. https://doi.org/10.1016/j.chb.2018.04.035

Përshpejtimi i përshkallëzuar i teknologjisë dhe Armët e Shkatërrimit në Masë: Një analizë krahasuese

Nënkolonel (R) Msc. Alqi NIKOLLA
Oficer shtabi/specialist/kërkues për studime dhe analizë strategjike, IKSHU

Trajtesë e shkurtuar

Deri vetëm disa vite më parë, pak veta parashikonin zhvillimin e vrullshëm dhe shpërthyes të inteligjencës artificiale që po dëshmojmë sot. Ky shkrim analizon teknologjitë që qëndrojnë në themel të përshpejtimit teknologjik, duke u përqendruar veçanërisht te inteligjenca artificiale si një teknologji potencialisht e krahasueshme, për nga ndikimi, me armët e shkatërrimit në masë. Përmes mbledhjes së të dhënave sasiore dhe analizës së literaturës përkatëse të përzgjedhur, shqyrtohet se në çfarë mase transformimi radikal që sjell inteligjenca artificiale mund të krahasohet me atë të armëve të shkatërrimit në masë; nëse inteligjenca artificiale mund të ushtrojë drejtpërdrejt një efekt shkatërrues të drejtpërdrejtë në kuptimin e armëve të shkatërrimit në masë; si dhe nëse rregullimi i saj është i mundur duke përdorur instrumentet juridike të njohura nga periudha e Luftës së Ftohtë.

Fjalë kyçe: Armët e Shkatërrimit në Masë, Inteligjenca Artificiale, siguria kombëtare, konfliktet hibride, Lufta e Gjeneratës së Katërt (4GW), dimensioni konjitiv, mbrojtja kibernetike

Hyrje

Në fillim të vitit 2022, pak kush parashikonte se inteligjenca artificiale (IA) do të arrinte një nivel kaq të lartë të përdorimit të përditshëm dhe një përhapje kaq të gjerë. Sipas të dhënave deri në fund të vitit 2025 ChatGPT ka arritur të ketë rreth 800 milionë përdorues aktivë çdo javë - rritje e konsiderueshme krahasuar me 300 milionë në dhjetor 2024, rreth 5.8 miliardë vizita në muaj, që tregon edhe për një gamë shumë të gjerë përdoruesish që e përdorin në mënyrë të përsëritur. Numri i përdoruesve aktivë javor është rritur nga rreth 400 milionë në fillim të vitit 2025 në 800 milionë deri në fund të vitit 2025, duke treguar se platforma ka zhvendosur përdorimin e saj nga një

mjet eksperimental në një shërbim masiv.[1] Po ashtu, deri vonë, shumë autorë e konsideronin si pjesë të fantashkencës idenë se modelet e mëdha gjuhësore (LLM)[2] do të arrinin madje edhe do të tejkalonin kompetencat njerëzore në fusha të shumta deri në mesin e viteve 2020.

Karakteri strategjik i inteligjencës artificiale forcohet edhe nga fakti se fuqitë udhëheqëse në zhvillimin e teknologjisë (SHBA dhe Kina) kanë nisur konsultime në nivelin më të lartë politik për krijimin e mekanizmave përkatës të kontrollit. Si shtylla themelore të zhvillimit të IA-së mund të konsiderohen sasia e të dhënave cilësore të nevojshme për zhvillimin, funksionimin dhe përshtatjen e vazhdueshme të saj, si dhe ekzistenca e një infrastrukture të besueshme të teknologjive të informacionit dhe komunikimit (TIK), që mundëson qarkullimin dhe aksesin e shpejtë ndaj këtij vëllimi të madh informacioni.[3]

John von Neumann[4] formuloi në mënyrë hipotetike idenë se përshpejtimi gjithnjë e më i madh i zhvillimit shkencor dhe teknologjik mund të çojë në të ardhmen drejt një ndryshimi rrënjësor, pas të cilit "jeta njerëzore, ashtu siç e njohim sot, nuk mund të vazhdojë". Në këtë shkrim, me termin "pikë kritike e zhvillimit teknologjik" nënkuptojmë ndikimin e ndërsjellë të treshes teknologjike që formëson realitetin bashkëkohor të inteligjencës artificiale (IA), rrjeteve 5G/6G[5] dhe ekosistemi i pajisjeve inteligjente të ndërlidhura (IoT), të cilat potencialisht mund të shkaktojnë një ndryshim rrënjësor; duke pasur parasysh përkufizimin sipas të cilit inteligjenca artificiale, në një pikë të caktuar, bëhet e aftë për vetëzhvillim rekurziv (përsëritet në mënyrë ciklike) dhe për krijimin e zgjidhjeve më të avancuara se vetja.

Përmes studimit, analizës dhe vlerësimit të literaturës dhe publikimeve të autorëve të njohur në këtë fushë, synoj të shqyrtoj se në çfarë mase mund të barazohet ndikimi i inteligjencës artificiale me atë të armëve të shkatërrimit në masë; nëse mund të vërtetohet se IA është e aftë të gjenerojë drejtpërdrejt efekt shkatërrues; si dhe nëse është e mundur që "gara e armatimit" në fushën e IA-së të rregullohet përmes instrumenteve juridike të kontrollit të armëve të përdorura gjatë Luftës së Ftohtë.

Bazat teknologjike

Duke analizuar kufizimet kryesore të realizimit të pikës kritike të zhvillimit teknologjik nga këndvështrimi teknologjik, mund të identifikohen si kërkesa

[1] *ChatGPT Users Statistics (January 2026) – Growth & Usage Data*

[2] *Depp 2024.*

[3] *For instance, the large volumes of data generated from sources such as IoT technologies, big data, and similar platforms.*

[4] *John von Neumann (1903–1957) ishte një matematikan, fizikan, kompjuterist dhe teoricien - një nga mendjet më të shkëlqyera të shekullit XX.*

[5] 6G konsiderohet gjenerata e gjashtë e rrjeteve mobile, e parashikuar të zëvendësojë 5G në dekadën e ardhshme.

minimale: disponueshmëria e një sasie gjithnjë në rritje të të dhënave të strukturuara, të përditësuara në mënyrë dinamike, si dhe aplikimi global me penetrim të mjaftueshëm i rrjeteve të teknologjisë së informacionit dhe komunikimit (TIK) me besueshmëri të lartë, të cilat mundësojnë transmetimin e të dhënave pothuajse në kohë reale (kryesisht 5G/6G). Rrjetet e komunikimit mobil të gjeneratës së re tashmë mund të klasifikohen qartë si pjesë e rrjeteve informatike, duke u plotësuar më tej nga funksionet e softuerizimit dhe virtualizimit, si dhe nga kërkesa për "prani të gjithanshme" e parashikuar në standarde, veçanërisht në rastin e 6G. Kapacitetet kryesore të 5G-së mund të grupohen rreth tre karakteristikave kryesore:

- Shërbimi i një numri shumë të madh pajisjesh të lidhura (mMTC – massive Machine-Type Communications).
- Transmetimi i të dhënave me shpejtësi të lartë (eMBB – enhanced Mobile Broadband).
- Komunikimi ultra i besueshëm me kohë reagimi shumë të shkurtër (uRLLC – ultra-Reliable Low-Latency Communications).

Vizioni i 6G[6] përshkruan një ekosistem teknologjik që është në gjendje të sigurojë që pjesa dërrmuese e popullsisë së Tokës të mund të lidhet me një hapësirë kibernetike të qëndrueshme dhe me nivel të lartë sigurie. 6G mund të mundësojë akses pothuajse të menjëhershëm në një sasi pothuajse të pakufizuar informacioni relevant, të përpunuar nga këndvështrime dhe dimensione të ndryshme, për entitetet përdoruese. Praktikisht, çdo pajisje që është e aftë të lidhet me rrjetin dhe të gjenerojë ose të mbledhë të dhëna mund të klasifikohet si pjesë e kategorisë IoT. Në lidhje me inteligjencën artificiale, marr si bazë përkufizimin përkatës të Rregullores së BE-së për IA-në, sipas të cilit inteligjenca artificiale është "një sistem i bazuar në makinë, i projektuar për të funksionuar me nivele të ndryshme autonomie dhe që, për qëllime eksplicite (shprehet hapur, qartë dhe drejtpërdrejt) ose implicite (kuptohet ose rrjedh nga konteksti), është në gjendje të prodhojë rezultate (si parashikime, rekomandime, vendime) që ndikojnë në mjedisin fizik ose virtual".[7] Përsa i përket gjeneratave të inteligjencës artificiale, ekspertët zakonisht dallojnë dy valë kryesore zhvillimi, të cilat përshkruhen me terminologji të ndryshme:

- **"IA e dobët" ose "IA e ngushtë" (ANI)** – janë sistemet aktuale të inteligjencës artificiale, të trajnuara mbi grupe të dhënash të strukturuara (të etiketuara), të projektuara për të funksionuar në një mjedis të përcaktuar dhe për detyra specifike (p.sh. analiza e përmbajtjes së imazheve). Këto modele imitojnë aftësitë njerëzore, por janë të afta të kryejnë detyrat përkatëse me shpejtësi shumë më të lartë dhe shpesh me efikasitet më të madh.

[6] Recommendation ITU-R M.2160-0 (11/2023) - Framework and overall objectives of the future development of IMT for 2030 and beyond.

[7] Regulation - EU - 2024/1689 - EN - EUR-Lex.

– **“IA e fortë” ose “IA e përgjithshme” (AGI)** – përfaqëson një fazë zhvillimi që, me shfaqjen e modeleve të inteligjencës artificiale me qëllim të përgjithshëm, po afrohet drejt një horizonti kohor më të afërt. Ajo përkufizohet si inteligjencë artificiale me kapacitete të barasvlershme me inteligjencën njerëzore, e trajnuar kryesisht mbi të dhëna të paetiketuara, me aftësi abstraksioni dhe adaptimi, si dhe me potencial për marrje vendimesh në mënyrë të ngjashme me njeriun.

Shumë ekspertë nuk e konsiderojnë realist realizimin e AGI-së brenda 15 viteve të ardhshme. Ata e mbështesin këtë qëndrim në kufizimet e kapaciteteve llogaritëse, në kufizimet energjetike dhe në pamjaftueshmërinë e të dhënave të disponueshme për trajnim. Të tjerë argumentojnë se përfshirja e vetë inteligjencës artificiale në kërkimet mbi IA-në mund të prodhojë rezultate të paparashikuara dhe qasje të reja, si në nivel harduerik ashtu edhe algoritmik, duke gjeneruar një zhvillim shpërthyes që mund ta shtyjë njerëzimin drejt epokës së AGI-së brenda 5–10 viteve.[8] Faza e tretë e mundshme në të ardhmen konsiderohet super inteligjenca artificiale, e cila tejkalon inteligjencën njerëzore dhe lidhet drejtpërdrejt me konceptin e pikës kritike të zhvillimit teknologjik. Në kontekstin aktual, aplikimi i modeleve të mëdha gjuhësore (LLM), pavarësisht “sëmundjeve të fëmijërisë” në zhvillim, ka filluar të ndikojë ndjeshëm realitetin tonë. Viti 2024 shënoi përparime të rëndësishme në këtë industri.

Në testin standard MMLU[9], rreth 50% e modeleve më të avancuara LLM në vitin 2024 performuan brenda një devijimi maksimal prej katër pikë përqindjeje nga niveli i ekspertëve njerëzorë (89,8%). Në testin GPQA, njerëzit ende performojnë më mirë, por dy modele (Claude 3.5 Sonnet dhe Gemini 2.0 Flash) arritën nivelin e ekspertëve njerëzorë (65,4%),[10] ndërsa modeli OpenAI o1 e tejkaloi ndjeshëm këtë nivel me rezultat 75,7%. Duhet theksuar se niveli jo-ekspert në testin GPQA është 33,9%, prag që shumica e modeleve moderne LLM e tejkalojnë dukshëm.[11] Modeli OpenAI o3, i vënë në dispozicion në fund të dhjetorit 2024 dhe i karakterizuar nga aftësi të avancuara arsyetimi, është modeli i parë LLM që tejkaloi performancën e përgjigjeve njerëzore (76%) në testin ARC-AGI, si dhe u rendit ndër 200 koduesit më të mirë njerëzorë. Sa i përket aftësive matematikore, ai arriti rezultat 2,2% në testin shumë të vështirë FrontierMath, duke tejkaluar të gjitha modelet e mëparshme (të cilat nuk kishin kaluar pragun 2%), si dhe realizoi

[8] *Aschenbrenner, L. (2024). Situational awareness: The decade ahead.; Rodríguez 2025. Aportes para el cumplimiento del Reglamento (UE) 2024/1689 en robótica y sistemas autónomos. arXiv:2503.17730. https://arxiv.org/abs/2503.17730.*

[9] *MMLU është një benchmark (test standard) për të vlerësuar aftësitë e modeleve të inteligjencës artificiale.*

[10] *GPQA: Evaluación de LLMs*

[11] *GPQA benchmark test sh. i vështirë, shkencor, “Googleproof”, që mat aftësinë për të zgjidhur pyetje komplekse që kërkojnë arsyetim të thellë.*

96,7% në testin AIME, nivel i krahasueshëm ose më i lartë se ai i nxënësve më të talentuar të matematikës në shkollat e mesme.[12]

Përdorimi i IA-së në fushën e mbrojtjes dhe sigurisë kombëtare.

Zgjidhjet e inteligjencës artificiale (IA) mund të përdoren edhe për qëllime mbrojtjeje dhe të sigurisë kombëtare – si për detyra përkthimi dhe mbështetje të komunikimit, vlerësimi dhe parashikimi i gjendjes shëndetësore dhe gatishmërisë së personelit, detektimi i kërcënimeve, vlerësimi i situatës në kohë reale, përcaktimi i objektivave, trajnim dhe simulime stërvitore, mbështetje e operacioneve, aktiviteteve taktike, logjistike dhe mirëmbajtjeje me karakter parashikues, mbrojtja kibernetike, analiza e përmbajtjeve multimediale (zë, imazh etj.) dhe kontrolli i mjeteve autonome. Modelet e mëdha gjuhësore, për shkak të kapaciteteve të tyre analitike, vlerësuese, gjenerative (p.sh. hartim raportesh) dhe të mbështetjes së vendimmarrjes, janë bërë shumë shpejt objekt studimi intensiv për aplikime në sektorin e mbrojtjes dhe të sigurisë kombëtare.[13] Paralelisht, kanë nisur herët edhe kërkimet mbi përdorimin e tyre për planifikim strategjik dhe mbështetje të vendimmarrjes në nivel ndërkombëtar.

Forcat Ajrore të SHBA-së, ndër të tjera, i kanë përdorur këto teknologji për trajnime dhe "war-gaming". Zyra e Drejtorit të Inteligjencës Kombëtare të SHBA-së (ODNI), në bashkëpunim me Universitetin Carnegie Mellon, ka analizuar realizueshmërinë e përdorimit të LLM-ve, duke rezultuar në zhvillimin e zgjidhjeve konkrete si "Defense Llama", e bazuar në arkitekturën META Llama.[14] Studime të publikuara tregojnë se edhe ekspertët kinezë janë thellësisht të interesuar për aplikueshmërinë e LLM-ve. Modeli ChatBIT, i zhvilluar mbi bazën e META Llama-13B dhe Vicuna-13B të Universitetit Stanford, sipas publikimeve përkatëse, demonstron aftësi të larta në kuptimin e konteksteve komplekse ushtarake. Kapacitetet e tij analitike (p.sh. vlerësimi i efektivitetit të sistemeve të armëve) konsiderohen shumë të avancuara dhe studiuesit e vlerësojnë atë si të përshtatshëm për përdorim në nxjerrje informacioni, analizë situate dhe mbështetje operacionale.[15]

"Lufta e Ftohtë" në epokën e inteligjencës artificiale

Sipas Keegan-it, lufta – veçanërisht ajo rituale – përbën vazhdim të kulturës me mjete të tjera[16]. Gjatë Luftës së Ftohtë, kjo formë u shfaq përmes përplasjeve të kufizuara, luftërave përfaqësuese dhe testimit të vazhdueshëm

[12] *OpenAI Unveils o3 Model and Becomes First to Crack the ARC-AGI Benchmark in 5 Years | Beebom https://www.maginative.com/*

[13] *On Large Language Models in National Security Applications - Caballero - 2025 - Stat - Wiley Online Library*

[14] *Introducing Defense Llama | Scale*

[15] *Students' Holistic Reading of Socio-Scientific Texts on Climate Change in a ChatGPT Scenario Research in Science Education | Nature Link*

[16] *John Keegan – The First World War: An Illustrated History (2002)*

të kapaciteteve, pa eskalim në luftë të hapur, falë një sërë rregullash të pashkruara që synonin parandalimin e konfliktit total. Në të njëjtën linjë, Barry Buzan e përkufizon Luftën e Ftohtë si një konfrontim të qëndrueshëm politik mbi rendin dhe fuqinë ndërkombëtare, ku asnjëra palë nuk dëshiron luftë të hapur për shkak të dilemës së fortë të mbrojtjes[17]. Debati mbi fillimin e një Lufte të Re të Ftohtë varion nga viti 2014 deri në vitin 2022, por shumë studiues theksojnë mungesën e ndarjeve të qarta ideologjike dhe ndërlidhjen e vazhdueshme të blloqeve edhe sot. Ndryshe nga Lufta e Parë e Ftohtë, ku armët bërthamore krijuan një dekurajim reciprok absolut, në kontekstin aktual mungon një ideologji universale mobilizuese; përplasjet lidhen më tepër me interesa konkrete sesa me sisteme besimi.

Në shqyrtimin e çështjes së një "Lufte të Ftohtë të IA-së", shtrohet pyetja nëse pika kritike e zhvillimit teknologjik dhe elementi i saj qendror – inteligjenca artificiale – mund të identifikohen si armë e shkatërrimit në masë (WMD). A është e mundur të krijohet një dilemë e fortë mbrojtjeje mbi baza të IA-së? Sipas përkufizimit të Fjalorit të Shkencave Ushtarake, armët e shkatërrimit në masë[18] janë ato që, krahasuar me armët e tjera dhe në kushte të njëjta, për shkak të natyrës dhe përmasës së efekteve të tyre, shkaktojnë në një kohë relativisht të shkurtër shkatërrim jashtëzakonisht të madh në njerëz, kafshë, në mjete luftarake, ndërtesa dhe në objekte të tjera. Megjithëse janë hartuar skenarë për përdorim të kufizuar të armëve bërthamore, ekspertët me të drejtë supozojnë se probabiliteti i realizimit praktik të këtyre skenarëve është i ulët dhe se eskalimi i gjerë është shumë më i mundshëm. Një shkëmbim fillestar goditjesh bërthamore do të sillte vdekjen e qindra milionë njerëzve, duke e bërë të pavlefshme logjikën clausewitziane të interesit politik, pasi pas një katastrofe të tillë çdo qëllim politik (dhe shoqëror, përveç ideologjive ekstreme) do të humbiste kuptimin.

Duke i marrë parasysh këto argumente, mund të konstatohet se inteligjenca artificiale, në vetvete, nuk përmbush kriteret e një arme të shkatërrimit në masë. Megjithatë, brenda kuadrit të pikës kritike të zhvillimit teknologjik, ku çdo element i lidhur në rrjet (si pjesë e ekosistemit IoT) identifikohet si një komponent funksional i sistemit, nëse çdo pajisje e tillë mundëson që inteligjenca artificiale të krijojë dhe/ose të kontrollojë armë të shkatërrimit në masë, atëherë afrohemi realisht drejt krijimit të një dileme të thellë mbrojtjeje.

Kissinger dhe Allison identifikojnë tri dallime themelore midis inteligjencës artificiale (IA) dhe armëve të shkatërrimit në masë (WMD). Së pari, një pjesë e konsiderueshme e zhvillimeve në fushën e IA-së realizohet nga entitete private, për të cilat faktorët e sigurisë kombëtare janë dytësorë (prioritet ka fitimi). Së dyti, zhvillimi i IA-së – krahasuar me armët bërthamore – është më

[17] *Buzan, B. (2023). Making global society: A study of humankind across three eras. Cambridge University Press. https://lnkd.in/dH6MMMMB*

[18] *Weapon of Mass Destruction.*

i lirë dhe më i thjeshtë; për më tepër, zhvillimi i armëve bërthamore është relativisht i gjurmueshëm, ndërsa identifikimi i kapaciteteve të IA-së të një kundërshtari është shumë më i vështirë. Së treti, zhvillimi i teknologjisë së IA-së është dukshëm më i shpejtë sesa ai i sistemeve të armatimit.

Nga këndvështrimi i garës së inteligjencës artificiale, problematik mbetet fakti se, ndryshe nga shoqëritë perëndimore ku rezultatet publikohen gjerësisht, për kapacitetet reale të IA-së së Kinës disponohen kryesisht informacione të tërthorta. Zhvillimet më të avancuara janë përqendruar në duart e një numri të kufizuar entitetesh brenda disa superfuqive teknologjike, ndërsa ritmi i shpejtë i inovacionit bën që gjeneratat e mëparshme të bëhen më të lira dhe të përhapen më shpejt.[19]

Rregullimi i IA-së sipas logjikës së kontrollit të armëve është i vështirë për t'u zbatuar, për shkak të zhvillimit të shpejtë dhe pamundësisë për të gjurmuar në mënyrë të besueshme portofolin e kapaciteteve teknologjike. Kissinger dhe bashkautorët e tij e shohin zgjidhjen e problemit në "zhvillimin e një ndjenje të përgjithshme përgjegjësie dhe në aftësinë për të vlerësuar me vetëdije pasojat e përdorimit të IA-së", pasi ligjet dhe marrëveshjet janë pothuajse gjithmonë me karakter reaktiv, gjë që, në kontekstin e zhvillimit të IA-së, është e pamjaftueshme. Pavarësisht kësaj, autorë të ndryshëm kanë propozuar që midis SHBA-së dhe Kinës të arrihet një marrëveshje vetëkufizuese përpara se IA-ja të bëhet pjesë përbërëse e kompleksit të sigurisë së shteteve.[20]

Në media po shfaqen gjithnjë e më shpesh përmbajtje që i referohen aftësive të IA-së për të kryer sulme në mënyrë autonome, dhe në ndërgjegjen e opinionit publik ka hyrë fenomeni i "ankthit ndaj IA-së".[21] Ky ankth mund të ushqehet edhe nga të gjitha ato lajme dhe informacione publike që e bëjnë të qartë për qytetarin e zakonshëm se administrata shtetërore dhe sektori industrial po përgatiten në mënyrë aktive për epokën e mbrojtjes/sigurisë dhe luftës së gjeneratës së re, ndërkohë që gara e armatimeve me IA midis SHBA-së dhe Kinës është qartësisht në zhvillim, dhe "marrëveshjet kufizuese të armatimeve" sipas vizionit të Kissinger-it ende mungojnë.

Një këndvështrim i gjeneratës së katërt

Në antikitet dhe në mesjetë, ideali i luftëtarit lidhej me guximin dhe heroizmin e bazuar në marrjen e drejtpërdrejtë të rrezikut. Në epokën moderne, veçanërisht deri pas Luftës së Dytë Botërore, ky ideal mbijetoi, por u shoqërua

[19] Henry A. Kissinger and Graham Allison. *The Path to AI Arms Control America and China Must Work Together to Avert Catastrophe. October 13, 2023.*

[20] *The Age of AI: And Our Human Future — botim i autorëve Kissinger, Schmidt dhe Huttenlocher.https://bibliotek.dk/en/materiale/the-age-of-ai_henry-kissinger/work-of%3A870970-basis%3A136727745*

[21] Zysman, J., & Nitzberg, M. (2024). *Generative AI and the Future of Work: Augmentation or Automation? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4811728*

gjithnjë e më shumë me menaxhimin e rrezikut përmes trajnimit, organizimit dhe teknologjisë. Pas luftës, shoqëritë perëndimore filluan të shfaqin ndjeshmëri të shtuar ndaj humbjeve njerëzore, duke forcuar interesin shtetëror për minimizimin e viktimave vetjake në operacionet ushtarake. Duke e kuptuar këtë realitet, grupet dhe komunitetet më të vogla ose në ngritje ndryshuan strategjitë e tyre, duke çuar drejt suksesit lëvizjet për pavarësi të ish-kolonive, si dhe duke detyruar tërheqjen e Shtetet e Bashkuara nga Vietnami dhe Bashkimin Sovjetik nga Afganistani.

Koncepti i Luftës së Gjeneratës së Katërt (4GJL), i formuluar në vitin 1989 nga William S. Lind dhe bashkautorët e tij, përfaqëson një reagim ndaj ndryshimit të frymës së kohës dhe përkufizon një formë lufte të decentralizuar, e cila shfrytëzon rrjetet politike, shoqërore, ekonomike dhe ushtarake dhe operon në të gjithë spektrin e tyre, me një identitet kombëtar të paqartësuar, improvizuese dhe që mbështetet në teknologji të avancuara (digjitale). Kjo formë lufte i jep përparësi operacioneve informative dhe psikologjike, përdor elemente të gjeneratave të mëparshme të luftimit dhe shfaq tipare të luftës guerile (asimetri), me shtrirje të kufizuar në hapësirë dhe kohë, si dhe me intensitet të ulët. [22]

Në kuadër të 4GW, një rol gjithnjë e më të rëndësishëm marrin aktorët jo-shtetërorë, si kompanitë private të sigurisë dhe entitete të ndryshme shoqërore, të cilat veprojnë si zbatues ose mbështetës të operacioneve. Zhvillimi i teknologjisë së informacionit, veçanërisht pas viteve 1990, dhe veçanërisht pas viteve 2010, ka mundësuar përdorimin e sistemeve gjithnjë e më autonome dhe të telekomanduara, duke rritur mbrojtjen e personelit dhe duke forcuar zbatimin e 4GW-së në dimensionet fizike, informative dhe njohëse. Në shoqëritë perëndimore vërehet një paradoks i theksuar: ndërsa përmbajtjet e industrisë së argëtimit bëhen gjithnjë e më të dhunshme, ndjeshmëria shoqërore ndaj vuajtjes reale shënon rritje.

Disa studiues, duke kundërshtuar përfundimet e mëparshme, argumentojnë se konsumi i përmbajtjeve të dhunshme nuk ka një ndikim të provueshëm në uljen e aftësive empatike.[23] Nga një këndvështrim tjetër analitik, një pjesë e studiuesve mbron tezën se përdorimi i dronëve dhe i sistemeve të tjera të ashtuquajtura "armë autonome"[24] e ka zhvendosur luftën, nga perspektiva e operatorit, në logjikën dhe përvojën e botës së videolojërave. Nga këndvështrimi i operatorit të sistemit të armëve, objekti që duhet neutralizuar

[22] Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. *(1989). The changing face of war: Into the fourth generation. Marine Corps Gazette, 73(10), 22–26.*

[23] Roy, N. *(2024). Empathy: Exploring the impact of violence in video games. eLife. https://doi.org/10.7554/eLife.94949*

[24] Boda, M. *(2022). The ethics of hybrid warfare: The theory of just hybrid war. In M. Szabó (Ed.), A comprehensive analysis of the impacts of artificial intelligence and other disruptive technologies (pp. 7–26).*

nuk perceptohet si një qenie reale njerëzore, por si një "entitet kibernetik"; për rrjedhojë, eliminimi i tij nuk gjeneron domosdoshmërisht dilema të theksuara morale apo shqetësime të thella të ndërgjegjes. Studiues të tjerë, megjithatë, theksojnë se operatorët e këtyre sistemeve, për shkak të vetë karakteristikave të teknologjisë, në shumë raste përballen me pasigurinë nëse përdorimi i forcës ka qenë i ligjshëm apo jo. Veçanërisht në rastin e operatorëve të dronëve, një detyrë e përsëritur është vëzhgimi sistematik i një zone të caktuar objektivi, gjatë të cilit analizohen personat e pranishëm, duke krijuar në mënyrë graduale një lloj lidhjeje psikologjike; më pas, marrja e urdhrit për sulm dhe zbatimi i tij gjeneron nivele të konsiderueshme stresi psikologjik.

Përfshirja e inteligjencës artificiale dhe e sistemeve të armëve të telekomanduara ose autonome mund të reduktojë stresin e operatorëve, kryesisht përmes analizës dhe verifikimit të informacionit, duke krijuar perceptimin e një përgjegjësie të ndarë midis njeriut dhe sistemit. Edhe kur neutralizimi nuk kryhet drejtpërdrejt nga IA-ja, konfirmimi i objektivit nga sistemi shërben si faktor lehtësues psikologjik. Megjithatë, delegimi i plotë i kontrollit te teknologjia eliminon elementin njerëzor dhe nxit një dehumanizim të theksuar të kundërshtarit, duke e reduktuar veprimin ushtarak në një proces teknik të bazuar në efikasitet statistikor. Disa studiues theksojnë se sistemet autonome të armëve, nëse trajnohen (programohen) në përputhje me të drejtën ndërkombëtare humanitare si dhe rregulloret dhe marrëveshjet përkatëse, mund të garantojnë zbatimin e rregullave pa u ndikuar nga lodhja apo faktorët emocionalë. Ky pohim është i vlefshëm në planin teorik, por me nxjerrjen jashtë loje të elementit njerëzor krijohet një entitet artificial efikas, i cili nuk zotëron cilësi si bujaria apo mëshira. Ai e përmbush detyrën e vet me një nivel shumë të lartë efektiviteti. Megjithatë, lindin një sërë pyetjesh që burojnë nga diversiteti kulturor njerëzor, si për shembull: si e dallon IA-ja me efikasitet të lartë dorëzimin real nga mashtrimi; si i peshon humbjet dytësore (civile); a i jep përparësi zbatimit të misionit apo mbrojtjes së jetës njerëzore?

Operacionet kibernetike përbëjnë një pjesë integrale të 4GH-së. Sot, duke nxjerrë mësime nga sulmet kibernetike ndaj Estonisë në vitin 2007, sulmet kibernetike ndaj vendit tonë në vitin 2022 dhe nga sulmet e mëvonshme më të mëdha,[25] shtetet individuale, si dhe aleancat – veçanërisht NATO-ja– po i kushtojnë gjithnjë e më shumë rëndësi zhvillimit të kapaciteteve të mbrojtjes kibernetike dhe të "parandalimit kibernetik" (kundërsulmit). Nga këndvështrimi i përdorimit të inteligjencës artificiale, Lufta e Gjeneratës së Pestë (5GW) synon të ndikojë perceptimin dhe përvetësimin e informacionit, në mënyrë që subjekti i sulmit të mos jetë i vetëdijshëm se ndodhet nën sulm, ndërkohë që po e humbet konfliktin. Mbështetësit e këtij koncepti argumentojnë

[25] Samsoerizal, A. D., Hidayat, E. R., & Sukendro, A. *(2022). Lesson Learned From Estonian Cyberattacks in 2007. International Journal of Arts and Social Science, 5(2) Deutsche Welle. (2023). Hakerë iranianë pas sulmeve kibernetike ndaj institucioneve shqiptare. Deutsche Welle.*

se qëllimi kryesor është ndikimi moral dhe kulturor mbi grupet shoqërore të kundërshtarit, përmes operacioneve informative dhe psikologjike, me synim deformimin e perceptimeve, bindjen dhe, në disa raste, manipulimin e audiencës së synuar.[26]

Megjithëse në literaturën bashkëkohore po përdoret gjithnjë e më shpesh koncepti i Luftës së Gjeneratës së Pestë (5GW), analiza e kësaj pjese mbështetet qëllimisht në kornizën teorike të Luftës së Gjeneratës së Katërt (4GW). Kjo zgjedhje lidhet me faktin se objekt i shqyrtimit nuk është ndikimi ekskluzivisht konjitiv apo perceptiv i inteligjencës artificiale, por transformimi i aktit të dhunës dhe i vendimmarrjes ushtarake përmes sistemeve teknologjike autonome dhe të telekomanduara.[27] Ndërsa 5GW fokusohet kryesisht në manipulimin e perceptimit dhe në deformimin e realitetit shoqëror pa përdorim të drejtpërdrejtë të forcës, 4GW ofron një kornizë më të përshtatshme për analizimin e rolit të IA-së si multiplikator operacional i dhunës, në një mjedis konflikti të decentralizuar, asimetrik dhe teknologjikisht të ndërmjetësuar.

Përshkallëzimi i IA-së

Me një term të vetëm, (strategjik) "pasiguria" është shprehja më e përshtatshme për të përshkruar ndikimin e inteligjencës artificiale. Disa autorë argumentojnë se pikërisht IA mund të përbëjë zgjidhjen për shpërndarjen e asaj që njihet si "mjegulla e pasigurisë", duke eliminuar vendimet irracionale dhe duke rritur kështu efektivitetin e mbrojtjes së forcave të gjalla. Është e rëndësishme të kihet parasysh se kjo ndodh vetëm në rast se fusha e veprimit e inteligjencës artificiale (IA)[28] është e kufizuar dhe/ose vetëm njëra palë disponon një zgjidhje IA për të mbështetur vendimmarrjen strategjike, operative dhe taktike. Përndryshe, mund të ndodhë fenomeni i ashtuquajtur "eskalimi i IA-së". Një sistem mbështetës i vendimmarrjes, duke analizuar të dhëna të menjëhershme, voluminoze dhe multimodale, mund të identifikojë se pala kundërshtare gjithashtu përdor një zgjidhje IA dhe fillon të marrë vendime dhe të japë sugjerime të dukshme irracionale, por efektive.

Për ta ilustruar me një shembull nga një fushë tjetër, gjatë një projekti zhvillimi të çipeve të mbështetur nga IA, modeli i të nxënit të thellë (DL) propozoi zgjidhje që tejkalonin ndjeshëm efektivitetin, portofolin e funksioneve dhe logjikën e zhvilluesve njerëzorë të produktit fillestar.[29]

---

[26]Haig, Z. *(2020). Novel interpretation of information operations in today's changed operational environment. Scientific Bulletin, 25(2), 93–102.*

[27]*Përdorimi termi kognitiv* dhe jo *perceptiv*, pasi analiza fokusohet jo vetëm në mënyrën se si informacioni paraqitet ose perceptohet nga individët, por kryesisht në proceset përpunimit, interpretimit dhe vendimmarrjes formësojnë bindjet, sjelljen dhe veprimin politik e shoqëror.

[28] Shtrirja dhe vëllimi i të dhënave të aksesueshme nga inteligjenca artificiale; vendimmarrëse; zgjerimi horizontal dhe vertikal, etj.

[29] Karahan, B. N., Emekli, E., & Altın, M. A. *(2025). Artificial intelligence-based chatbots' ability to interpret mammography images: A comparison of Chat-GPT 4o and Claude 3.5. European Journal of Therapeutics,* 31*(1), 28–34. https://doi.org/10.58600/eurjther2599*

Fenomeni i "eskalimit të IA-së" është një proces që përshpejtohet eksponencialisht, pasi modelet kundërshtuese, të ngjashme me GAN, praktikisht dhe në mënyrë të pashmangshme "trajnojnë" njëra-tjetrën. Është e nevojshme të mbahet parasysh se, në rast se palët kundërshtare disponojnë njëkohësisht Inteligjencë të Përgjithshme Artificiale (AGI), eskalimi bëhet pothuajse i pashmangshëm, pasi shpejtësia e vendimmarrjes së modeleve të përdorura nuk mund të tejkalohet nga mendja njerëzore. Pala që zgjedh të kufizojë përdorimin e AGI-së ka me shumë gjasë të jetë pala humbëse. Për rrjedhojë, pas një intervali shumë të shkurtër kohor, palët do të detyrohen t'i sigurojnë AGI-së liri veprimi pothuajse të pakufizuar.

Duke e shqyrtuar eskalimin nga një këndvështrim tjetër, në rastin e zgjidhjeve të bazuara në modele të mëdha gjuhësore (LLM) që mbështesin vendimmarrjen në fushën e mbrojtjes, sigurisë kombëtare dhe politikës së jashtme, duhet mbajtur parasysh se një LLM përfaqëson në një farë mase esencën e dijes dhe të historisë njerëzore. Si rrjedhojë logjike, studiuesit që kanë analizuar veçoritë e këtyre modeleve kanë arritur në përfundimin se ato priren të favorizojnë eskalimin kinetik (ekstrem) të ngjarjeve ndërkombëtare.[30]

Zbatimi i drejtë i IA-së

Duke pasur parasysh karakteristikat e Luftës së Gjeneratës së Katërt (4GW), përveç përdorimit të drejtpërdrejtë të forcës ushtarake, bëhet gjithnjë e më e vështirë të dallohen me siguri të lartë veprimtaritë diplomatike të zakonshme dhe përdorimi i përditshëm i instrumenteve gjeoekonomike nga zbatueshmëria e tyre për qëllime të 4GW-së, si dhe nga aktivitetet e shërbimeve të sigurisë kombëtare që mbështesin luftën hibride.

Strategjia e Sigurisë Kombëtare e Republikës së Shqipërisë përcakton qasjen kombëtare ndaj interesit të sigurisë kombëtare si një parim udhëheqës të politikave të mbrojtjes dhe sigurisë. Dokumenti thekson se interesi kombëtar përfshin mbrojtjen e sovranitetit, integritetit territorial, institucioneve shtetërore, qytetarëve dhe infrastrukturës kritike, si dhe zhvillimin e kapaciteteve për të përballuar kërcënimet tradicionale dhe moderne, përfshirë ato hibride dhe kibernetike. Duke qenë se entitetet e sigurisë kombëtare në disa raste mund të mos mbështeten mbi fakte të verifikuara, por mbi supozime, përdorimi i IA-së për mbështetjen e kësaj veprimtarie ofron, nga njëra anë, mundësinë për të konfirmuar me shpejtësi supozimet, dhe nga ana tjetër, i lejon IA-së të propozojë edhe supozime të tilla që nuk janë marrë në konsideratë nga punonjësit analitikë dhe vlerësues të shërbimeve kompetente.

Edhe në këtë rast ekziston rreziku i "përshkallëzimit të IA-së", pasi modelet e përdorura të IA-së (p.sh. modelet e mëdha gjuhësore – LLM) përmes aftësive

[30] Rivera, J.-P., Mukobi, G., Reuel, A., Lamparth, M., Smith, C., & Schneider, J. *(2024). Escalation risks from language models in military and diplomatic decision-making. arXiv. https://arxiv.org/abs/2401.03408v1*

të tyre të njohjes së modeleve mund të zbulojnë se një palë apo shtet kundërshtar po zhvillon veprimtari të sigurisë kombëtare të mbështetur nga IA dhe në përputhje me këtë, të japin "rekomandime" përkatëse. Me probabilitet të lartë, brenda një kohe relativisht të shkurtër, IA-ja e palës kundërshtare do ta identifikojë këtë situatë dhe, në dritën e saj, do të modifikojë rezultatet e veta dalëse (rekomandimet). Në mënyrë të ngjashme mund të vlerësohet edhe përdorimi i IA-së në kuadër të "operacioneve të drejta informative".

Përsa i përket sistemeve autonome të armëve – on-the-loop[31] ose out-of-the-loop[32] – paradoksi tashmë i përmendur midis respektimit të ligjit, efikasitetit dhe parashikueshmërisë ngre një sërë pyetjesh. Veçanërisht në rastin e zgjidhjeve out-of-the-loop, çështja e përgjegjësisë është tejet delikate, pasi pas aktivizimit sjellja e pritshme e mjetit nuk është domosdoshmërisht e njohur për autoritetin që ka urdhëruar përdorimin e tij, ose vendimi për përdorim mund të merret mbi bazën e informacionit të pasaktë të dhënë nga prodhuesi. Natyrisht, përgjegjësia e vetë sistemit autonom të armëve nuk mund të konceptohet në kuptimin juridik. Për sa më sipër, gur themeli i zbatimit të drejtë dhe të përgjegjshëm të IA-së është njohja e pasojave të mundshme dhe aftësia për t'i vlerësuar ato paraprakisht. Kjo kërkon një mentalitet të ri drejtues në nivel politik, ekonomik, ushtarak dhe të rendit publik, i cili është i aftë të menaxhojë veçoritë dhe pasojat specifike që shoqërojnë përdorimin e IA-së.

Sfidat e përdorimit të IA-së

Sipas ndarjes së Shkollës së Kopenhagës, sektori ushtarak përfshin detyrimet mbrojtëse të shtetit; sektori politik përfshin detyrat që lidhen me mbrojtjen e "rendit shoqëror" dhe ruajtjen e sovranitetit;[33] sektori ekonomik ka të bëjë me sigurimin e mbrojtjes së burimeve të nevojshme për funksionimin e shtetit; sektori mjedisor lidhet me rreziqet që burojnë nga mjedisi natyror ose që ndikojnë mbi të; ndërsa sektori shoqëror përfshin elementet e identitetit të komunitetit që duhen mbrojtur. Përpjekjet politike që minojnë stabilitetin e shtetit përbëjnë njëkohësisht edhe sulm ndaj sovranitetit të tij (madje edhe brenda kornizës së luftës hibride të gjeneratës së pestë – 5GH). Për këtë arsye, në çdo sektor sigurie, kërcënimet e identifikuara dhe masat mbrojtëse ndikojnë drejtpërdrejt edhe sektorin politik. Këto mbivendosje janë të vëzhgueshme në të gjithë sektorët e sigurisë.[34] Potenciali i zgjidhjeve të bazuara në inteligjencën

[31] Ontheloop → në rrethin e kontrollit *ose* mbikëqyrje njerëzore*:* Njeriu ka rol aktiv të monitorimit dhe ndërhyrjes, edhe pse sistemi kryen veprime autonome. Vendimet finale mund të modifikohen ose ndërpriten nga operatori njerëzor.

[32] Outoftheloop → jashtë rrethit të kontrollit ose pa mbikëqyrje njerëzore: Sistemi vepron plotësisht në mënyrë autonome pas aktivizimit. Sjellja e tij nuk është domosdoshmërisht e parashikueshme nga njeriu që e urdhëron përdorimin.

[33] Remek, É. (2014). *How large is the "shadow of our security" in our globalized world? (pp. 67–78)*

[34] Buzan – Wæver – De Wilde 1998: *Security: A new framework for analysis.* Boulder, CO: Lynne Rienner Publishers, 141–142.

artificiale në fushën e mbrojtjes dhe të sigurisë kombëtare – për përvetësim kompleks të të dhënave, gjenerim përmbajtjeje, si dhe për nisjen e operacioneve kibernetike dhe kinetike – mundëson kompromet imin e tërësisë së sektorëve të sigurisë me një shkallë efektiviteti që, në kushtet e një ekosistemi tradicional të IT-së dhe me varësi të lartë nga ndërhyrja njerëzore, nuk do të ishte i realizueshëm.

Media botërore, gjatë një episodi të luftës civile në Libi (Operacioni "Békevihar"[35]), e paraqiti përdorimin e UAV-ve turke Kargu-2 ("predhave që lëvizin në mënyrë të paparashikueshme ose që devijojnë nga kursi i caktuar") si një aplikim "vrasës" të IA dhe robotikës. Megjithatë, raporti i OKB-së, mbi të cilin u mbështetën këto artikuj, përmbante vetëm faktin e përdorimit të Kargu-2 dhe të dhënën teknike se ky dron është i aftë të kryejë sulme edhe pa ruajtur lidhje të të dhënave me operatorin.[36] Meqenëse raporti nuk specifikonte nëse gjatë operacioneve dronët kishin vepruar realisht pa mbikëqyrje njerëzore, ky rast nuk mund të përdoret si provë e përdorimit operacional autonom të IA-së.

Një situatë e ngjashme është shfaqur edhe në konfliktin ruso–ukrainas, ku media publikon rregullisht aplikimet ushtarake të IA-së dhe përpjekjet kërkimore-zhvillimore, kryesisht nga Ukraina dhe entitetet mbështetëse. IA mund t'u ofrojë dronëve mbështetje të rëndësishme për rritjen e rezistencës ndaj luftës elektronike, drejtimin e tufave të dronëve, identifikimin e objektivave të dukshme dhe mbështetjen e identifikimit multimodal. Megjithatë, ndonëse në nivel teorik identifikimi i objekteve të fshehura apo i personave të caktuar është i mundur, shkalla e pasigurisë mbetet e lartë, çka e bën ekzekutimin autonom të goditjeve potencialisht problematik në raport me të drejtën ndërkombëtare humanitare. Si shembull, identifikimi i fytyrës mund të jetë pothuajse 100% në kushte ideale, por në rrethana reale norma e gabimeve rritet ndjeshëm edhe te algoritmet më efikase.

Në rastin e objekteve të fshehura ekziston rreziku real që kundërshtari, duke përdorur mjetet e luftës elektronike, të vendosë objektiva të rreme ose të "maskojë" objektivat e palës që përdor dronët, në mënyrë që të provokojë "zjarr miqësor". Përsa u përket objektivave njerëzore, identifikimi i karakteristikave biometrike dhe i veshjes mbetet mjaft i pasigurt për të lejuar nisjen e një sulmi të ligjshëm vetëm mbi këto baza – pa miratim njerëzor.

[35]Operacioni i vitit 2020 i nisur nga Qeveria e Pajtimit Kombëtar kundër trupave të gjeneralit Haftar.
[36] *U.N. Panel of Experts on Libya. (2021). Letter dated 8 March 2021 from the Panel of Experts on Libya.*

Përfundime

Nga analiza e zhvilluar rezulton qartë se inteligjenca artificiale (IA), e marrë në vetvete, nuk përmbush kriteret klasike për t'u konsideruar armë e shkatërrimit në masë (WMD), as në aspektin e natyrës së saj teknike dhe as në përmasën e efekteve të drejtpërdrejta shkatërruese. Megjithatë, ky konstatim nuk duhet të çojë në nënvlerësimin e rolit të saj strategjik në arkitekturën bashkëkohore të sigurisë ndërkombëtare. Përkundrazi, brenda kornizës së Sistemeve Teknologjike komplekse (TS), ku inteligjenca artificiale ndërvepron me rrjetet e komunikimit të avancuara (5G/6G), ekosistemet IoT dhe kapacitetet ekzekutuese kinetike, kibernetike dhe informative, IA fiton potencialin për të prodhuar efekte të krahasueshme me ato të armëve të shkatërrimit në masë.

Ky potencial nuk buron nga fuqia shkatërruese e drejtpërdrejtë e IA-së, por nga aftësia e saj për të përshpejtuar, automatizuar dhe koordinuar procese komplekse vendimmarrjeje dhe veprimi në një shkallë dhe shpejtësi që tejkalojnë kapacitetet njerëzore. Në këtë kontekst, fenomeni i përshkallëzimit të inteligjencës artificiale përfaqëson një rrezik sistemik për stabilitetin ndërkombëtar, pasi krijon kushtet për lindjen e një dileme të fortë mbrojtjeje, të ngjashme – por jo identike – me atë të epokës bërthamore.

Analiza identifikon dy mekanizma kryesorë përmes të cilëve mund të materializohet përshkallëzimi i IA-së. Së pari, përmes ndërveprimit dinamik të modeleve të inteligjencës artificiale të përdorura nga palët kundërshtare, ku sistemet, duke analizuar në mënyrë reciproke sjelljen dhe reagimet e njëra-tjetrës, hyjnë në cikle përmirësimi dhe reagimi të përshpejtuar eksponencialisht, të ngjashme me logjikën e modeleve kundërshtuese (GAN). Së dyti, përmes veçorive të brendshme të modeleve të mëdha gjuhësore (LLM), të cilat, të trajnuara mbi një bazë masive të të dhënave historike dhe strategjike, mund të shfaqin prirje drejt rekomandimeve eskaluese, përfshirë edhe opsione kinetike ekstreme, nëse këto perceptohen si "racionale" nga këndvështrimi statistikor dhe historik.

Një rrezik shtesë buron nga fakti se bazat e të dhënave mbi të cilat trajnohen modelet e avancuara të IA-së mund të përmbajnë informacion të ndjeshëm, i cili potencialisht mund të shfrytëzohet për zhvillimin e armëve kibernetike me efikasitet të lartë, si dhe për përshpejtimin e kërkimeve në fushën e armëve kimike, biologjike dhe bërthamore. Kjo e zhvendos inteligjencën artificiale nga statusi i një teknologjie neutrale në atë të një multiplikatori strategjik rreziku.

Megjithëse autorë si Kissinger dhe Allison theksojnë vështirësinë pothuajse strukturore të kontrollit të armatimeve në fushën e inteligjencës artificiale – për shkak të ritmit të zhvillimit, natyrës dual-use dhe pamundësisë së verifikimit të besueshëm – përpjekjet për vendosjen e mekanizmave vetëkufizues dhe të komunikimit strategjik mbeten thelbësore. Edhe nëse marrëveshjet formale nuk arrijnë të prodhojnë kontroll efektiv në kuptimin klasik të Luftës së Ftohtë, ato mund të kontribuojnë në uljen e pasigurisë, rritjen e transparencës relative

dhe parandalimin e keqinterpretimit të veprimeve të palës kundërshtare.

Në përfundim, inteligjenca artificiale nuk duhet të kuptohet si një armë e shkatërrimit në masë, por si një faktor transformues i ekuilibrave të sigurisë globale, i cili ka potencialin të amplifikojë ndjeshëm kapacitetet shkatërruese ekzistuese dhe të riformësojë logjikën e parandalimit dhe eskalimit. Në mungesë të një qasjeje strategjike, etike dhe institucionale të koordinuar, zhvillimi i pakontrolluar i IA-së rrezikon të krijojë një mjedis sigurie më të paqëndrueshëm, ku shpejtësia e vendimmarrjes dhe automatizimi tejkalojnë aftësinë.

Në këtë kuadër, për shtete të vogla si Shqipëria, ndikimi i inteligjencës artificiale në sigurinë kombëtare pritet të shfaqet kryesisht në dimensionin konjitiv dhe informativ të konflikteve hibride, dhe më pak në atë kinetik. Për rrjedhojë, forcimi i kapaciteteve të mbrojtjes kibernetike, qëndrueshmërisë institucionale dhe besimit publik ndaj institucioneve shtetërore përbën një element kyç të qasjes kombëtare ndaj sfidave të sigurisë në epokën e inteligjencës artificiale.

Bibliografia

1. Aschenbrenner, Leopold (2024): Situational Awareness: The Decade Ahead. 2024. június. Online: https://situational-awareness.ai/
2. Buzan, Barry (2024): A New Cold War? The Case for a General Concept. International Politics, 61, 239–257. Online https://doi.org/10.1057/s41311-024-00559-8
3. Buzan, Barry – Wæver, Ole – De Wilde, Jaap (1998): Security: A New Framework for Analysis. Boulder, Colorado: Lynne Rienner. Caballero, William N. – Jenkins, Phillip R. (2024): On Large Language Models in National Security Applications. arXiv:2407.03453v1 [cs.CR]. Online: https://doi. org/10.48550/arXiv.2407.03453
4. Campbell, Jamal M. (2021): Psychological Effects on UAV Operators and Proposed Mitigation Strategies to Combat PTSD (Thesis). Monterey (Califronia, USA): Naval Postgraduate School. Online: https://apps.dtic.mil/sti/trecms/pdf/AD1150884.pdf
5. Cheung, Sunny (2024): PRC Adapts Meta's Llama for Military and Security AI Applications. China Brief, 24(21). Online: https://jamestown.org/program/prcsadaptation-of-open-source-llm-for-military-and-security-purposes/
6. Depp, Michael (2024): A Blueprint for a Functional China-US Working Group on AI. The Diplomat, 2024. április 27. Online: https://thediplomat.com/2024/04/ablueprint-for-a-functional-china-us-working-group-on-ai/
7. Friedman, Thomas L. (2005): It's a Flat World, After All. The New York Times Magazine, 2005. április 3. Online: https://www.nytimes.

com/2005/04/03/magazine/its-aflat-world-after-all.html

8. Gallagher, Shannon et al. (2023): A Retrospective in Engineering Large Language Models for National Security. Carnegie Mellon University Software Engineering Institute. Online: https://insights.sei.cmu.edu/library/a-retrospective-in-engineering-large-language-models-for-national-security/
9. Kissinger, Henry A. – Allison, Graham (2023): The Path to AI Arms Control. Foreign Affairs, 2023. október 13. Online: https://www.henryakissinger.com/articles/ the-path-to-ai-arms-control/
10. Kissinger, Henry A. – Schmidt, Eric – Huttenlocher, Daniel (2023): ChatGPT Heralds an Intellectual Revolution. The Wall Street Journal, 2023. február 24. Online: https:// www.henryakissinger.com/articles/chatgpt-heralds-an-intellectual-revolution/
11. Liu, Yang et at. (2024): Advancements in Brain-Machine Interfaces for Application in the Metaverse. Frontiers in Systems Neuroscience, (18). Online: https://doi. org/10.3389/fnins.2024.1383319
12. Maurer, John D. (2018): The Purposes of Arms Control. Texas National Security Review, 2(1), 8–27. Online: http://dx.doi.org/10.26153/tsw/870
13. Nitzberg, Alex (2024): Autonomous Systems and Weapons Company Anduril Announces Plan to Build Massive Manufacturing Facility in Ohio. FOXBusiness, 2025. január 16. Online: https://www.foxbusiness.com/fox-news-military/
14. Rein, David et al. (2023): GPQA: A Graduate-Level Google-Proof Q&A Benchmark. arXiv arXiv:2311.12022v1. Online: https://doi.org/10.48550/arXiv.2311.12022
15. Roy, Nicolas – Coll, Michel-Pierre (2024): Empathy: Exploring the Impact of Violence in Video Games. eLife, 13. Online: https://doi.org/10.7554/eLife.94949
16. Seewald, A. K. (2022): A Criticism of the Technological Singularity. In Dingli, A. et al. (szerk.): Disruptive Technologies in Media, Arts and Design. Springer, 91–119. Online: https://doi.org/10.1007/978-3-030-93780-5_8
17. Singh, P. R. et. al. (2023): 6G Networks for Artificial Intelligence-Enabled Smart Cities Applications: A Scoping Review. Telematics and Informatics Reports, 9. 100044. Online: https://doi.org/10.1016/j.teler.2023.100044 Schmidt, Eric (2023): Innovation Power: Why

Sfidat e mbrojtjes kibernetike të sistemeve ushtarake të komunikimit dhe shkëmbimit të informacionit përballë zhvillimeve teknologjike të sistemeve të komunikimit "5G dhe 6G"

Kolonel Inxh. Gjergji VASILI
Shef i Departamentit të Inovacionit dhe Teknologjisë, IKSHU

Trajtesë e shkurtuar

Zhvillimi i sistemeve dhe rrjeteve të komunikimit "5G" dhe perspektiva e afërt në "6G" ofrojnë kapacitete të mëdha teknologjike transformuese për sistemet ushtarake të komunikimeve dhe shkëmbimit të informacionit, mbi shpejtësinë tepër të lartë të realizimit të komunikimeve, "latencë"[1] ultra të ulët dhe lidhje masive të pajisjeve elektronike të sistemeve të ndryshme (p.sh., për C4ISR dhe sistemet autonome). Njëherësh, këto teknologji rrisin shumë "sipërfaqen" e sulmeve kibernetike, duke krijuar sfida të mëdha për sigurinë & mbrojtjen ushtarake të sistemeve të komunikimit.

Ky artikull analizon vulnerabilitetet kryesore, kërcënimet dhe risqet emergjente si dhe ndërtimi i masave mbrojtëse, me fokus në kontekstin ushtarak (duke përfshirë NATO-n dhe Forcat e Armatosura Shqiptare).

Përfitimet teknologjike: - teknologjia "5G" (Massive MIMO[2], networkslicing dhe MEC) mundësojnë komunikime taktike në kohë reale, mbështetje teknologjike për sistemet drone "Swarms" dhe "JADC2" (Joint All-DomainCommandandControl); - teknologjia "6G" (perspektivë 2030+): integrim me brezin e frekuencave në "THz", IA kognitive[3] dhe rrjete hapësinore - tokësore (STIN), duke ofruar shpejtësi transmetimi në nivelet "Tbps" dhe "inteligjencë" kolektive për sisteme autonome.

Sfidat kryesore të sigurisë:- sipërfaqe e zgjeruar e sulmeve: Open RAN dhe

[1] "Latencë": koha e vonesës midis dërgimit dhe marrjes së të dhënave është jashtëzakonisht e vogël; komunikim pothuajse në kohë reale.

[2] MIMO: teknologji "wireless" që shumëfishon kapacitetin e lidhjeve radio duke përdorur antena të shumëfishta transmetimi dhe marrjeje, teknologji për komunikimet me brez të gjerë, me standarde mobile WiMAX (802.16 e, m) & 5G NR dhe standardet Wi-Fi, IEEE 802.11n.

[3] "IA njohëse" i referohet IA që imiton të menduarit dhe vendimmarrjen njerëzore duke mësuar nga të dhënat, duke u përshtatur me informacionin si dhe duke rafinuar qasjen *(https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cognitive-ai*

arkitektura "cloud-native" rrisin rreziqet e aksesit të paautorizuar dhe DDoS (sulme në "corenetwork" deri në 40% degradim performancë); - kërcënime kuantike: algoritmet aktuale (AES) janë vulnerabël ndaj kompjuterëve kuantikë; 6G kërkon kriptografi post-kuantike (PQC); - sulme hibride ushtarake: "Jamming, spoofing GPS" dhe sulme "AI-adversarial" në sistemet autonome; - rreziqe zinxhiri furnizimi (p.sh., vendorë të huaj); - specifike ushtarake: rrjetet taktike (battlefield "5G") janë të ndjeshme ndaj ndërhyrjeve.

Masa mbrojtëse dhe inovacionet: - standarde aktuale: 3GPP TS 33.501 për autentikim (EAP-TLS) dhe "Zero Trust Architecture" (ZTA) për verifikim të vazhdueshëm; - për teknologjinë "6G": Quantum Key Distribution (QKD), blockchain për IDS dhe IA për zbulim anomalish; - rekomandime ushtarake: integrim i "rapid prototyping" (DIANA NATO) për zhvillim të shpejtë të moduleve të sigurta; trajnim specialistësh dhe sovranitet teknologjik. NATO ka adoptuar PQC në sistemet VPN dhe IFF (viti 2025) por kërkohet një qasje "proaktive" për mbrojtjen & sigurinë kibernetike. Kërkime të mëtejshme duhet të fokusohen në simulime të sulmeve kuantike dhe IA rezistente.

Fjalët kyçe: sisteme "5G"/"6G", C4ISR, Open RAN, IA, "cloud-native", "IoT", DDoS, kriptografi post-kuantike (PQC), kompjuteri kuantik, kriptografi, sistemet "autonome", Jamming, spoofing GPS, sulme "AI-adversarial", "Zero Trust Architecture", "blockchain", QuantumKeyDistribution (QKD).

▪ Rëndësia e teknologjive 5G dhe 6G në transformimin e komunikimeve ushtarake

Teknologjitë e sistemeve të komunikimit "5G dhe 6G" shënojnë një evolucion të madh në telekomunikacion, duke kaluar nga lidhjet e thjeshta në rrjete inteligjente, ultra-efikase dhe të integruara me IA. Teknologjia "5G", e lançuar komercialisht që nga viti 2019, ishte në fazën e maturimit përgjatë vitit 2025 me mbi 2.9 miliardë abonime globalë *(rreth një e treta e abonimeve mobile)*. Ndërkohë teknologjia "6G", ende në fazë kërkimore, parashikohet të debutojë rreth vitin 2030, duke premtuar shpejtësi 100 herë më të larta se teknologjia "5G" dhe aplikime revolucionare si komunikimet "holografike"[4]. Zhvillimet kryesore në teknologjinë 5G *(2020-2025)* kanë transformuar industrinë duke ofruar shpejtësi deri në 20 Gbps, latencë<1 ms dhe mbështetje për 1 milion pajisje/km², duke mundësuar aplikime masive të teknologjive si "IoT", pajisje-sisteme të lidhura dhe realitet i zgjeruar *(AR/VR[5])*. Përgjatë vitit 2025, fokusi ishte te niveli "5G-Advanced" *(release 18 i 3GPP),* i cili rrit me efikasitet kapacitetin e komunikimit, mobilitet të lartë dhe automatizim me "AI-native". Teknologjitë "5G dhe 6G" po revolucionarizojnë edhe sistemet

[4] Komunikimet holografike janë komunikime vizuale 3D që krijojnë iluzionin e pranisë reale në distancë.

[5] Audio-Visual/Virtual Reality, janë teknologji audio-vizuale të kombinuara me mjedise plotësisht virtuale, 3D, përmes pajisjeve speciale.

ushtarake të komunikimeve dhe shkëmbimit të informacionit, duke mundësuar operacione tepër efikase dhe të sigurta në fushëbetejë. Këto zhvillime teknologjike mbështesin fuqishëm sistemet si *C4ISR*[6] dhe JADC2[7] duke transformuar komunikimet tradicionale në rrjete inteligjente dhe rezistente.

Përfitimet kryesore të teknologjisë 5G në sistemet e komunikimeve ushtarake:

- **shpejtësi dhe latencë**: "bandwidth" i gjerë dhe latencë <1ms mundësojnë transmetim real-time të të dhënave nga sensorë, dronë dhe kamera, duke përmirësuar vendimmarrjen taktike & operacionale.

- **lidhje masive** të pajisjeve: mbështetje për lidhjen dhe integrimin e mijëra pajisje simultane *("IoT" ushtarak)*, si drones warms dhe sisteme autonome.

- **rezistencë ndaj ndërhyrjeve**: Frekuencat "mmWave" ofrojnë mbrojtje më të mirë kundër "jamming"-ut, duke rritur ndjeshëm sigurinë në ambiente & zona të kontestuara.

Perspektivat e zhvillimit të teknologjisë së sistemeve të komunikimeve "6G" *(2030 +)*:

- **avancime teknologjike tepër të mëdha**: shpejtësi transmetimi deri në 1 Tbps, latencë mikrosekonda, integrim me brezin THz, IA kognitive dhe shumë të ndjeshme "sensing", sisteme tepër të integruara *(ISAC*[8]*)* për zbulim dronësh ose kërcënimesh të spektrit të gjerë, kryesisht në sigurinë kibernetike.

- **transformim ushtarak**: mundëson inteligjencë kolektive në sisteme autonome, komunikime hapësinore-tokësore *(STIN)* dhe rezistencë kuantike.

SHBA-ja ka lançuar sistemin "Open6G" për Open RAN; NATO *(përmes DIANA)* po investon në teknologjinë "6G" për inovacione "dual-use"; Kina po zhvillon teknologjinë "6G" për aplikime ushtarake *(p.sh., hipersonike).* Këto teknologji paraqesin një ndikim të theksuar strategjik, rrisin avantazhin ushtarak duke integruar IA *(ML)* për analizë të shpejtë të të dhënave, por kërkojnë mbrojtje specifike kibernetike *(PQC, ZTA)*. NATO dhe SHBA po përshpejtojnë adoptimin e sistemeve të komunikimit në këto teknologji për të ruajtur superioritetin ndaj kërcënimeve hibride. Teknologjia "5G" po transformon komunikimet aktuale ushtarake, ndërsa teknologjia "6G" do të "ridefinojë" luftën e ardhshme me rrjete ultra-inteligjente dhe tepër rezistente. Zhvillimet kryesore në teknologjin "6G" janë një paradigmë e re: rrjete "AI-native, energy-aware", të integruara me ndjeshmëri "sensing", shpejtësi transmetimi deri në 1 Tbps, latencë mikrosekonda, mbulim me precizion centimetrik, duke mundësuar holograme, digital twins dhe operacione remote në kohë reale, rrjetet "6G" do të kombinojnë komunikimin me "sensing", duke

[6] Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance.
[7] Joint All-Domain Command and Control.
[8] Integrated Sensing and Communication.

krijuar rrjete "të zgjuara" për aplikime me pretendimin se teknologjia "6G" do të evoluojë pa nevojë për "hardware" të ri, por duke përdorur "upgrades software".

Përmirësimet e pritshme në teknologjinë 6G: Teknologjia 6G me katër përmirësimeve kryesore të specifikuar si: - IA të integruar, - përdorimi i frekuencave "Terahertz", - "hologramat" dhe rrjetet e adaptueshme, premton një revolucion në telekomunikacion, me përmirësimet e teknologjisë 5G drejt rrjeteve ultra-inteligjente, me integrim të thellë me IA që do të transformojnë aplikimet civile dhe ushtarake, duke mundësuar eksperienca immersive[9] dhe operacione autonome.

Inteligjenca Artificiale e Integruar - Teknologjia "6G" do të integrojë IA-në si element themelor të arkitekturës së rrjetit, duke e bërë atë "native" në vend të një shtese të jashtme. Kjo do të lejojë rrjete vetë-optimizuese dhe vetë-shërbuese, duke parashikuar dhe zgjidhur problemet para se të ndikojnë në përdoruesit[10]. IA do të menaxhojë alokimin e burimeve, "estimimin"[11] e kanaleve dhe adaptimin e valëve, duke përdorur teknika si "deep reinforcement learning" dhe "graphn eural networks" për mobilitet të shpërndarë (p.sh., në UAV relays ose edge servers). Kjo ul konsumimin e energjisë deri në 30% dhe krijon modele "AI-as-a-Service" *(AIaaS)* për shërbime si smart cities ose misionet e shpëtimit. Në ushtri, IA e integruar do të mundësojë vendimmarrje autonome në JADC2, duke reduktuar ndërhyrjen njerëzore dhe duke rritur rezistencën ndaj sulmeve[12].

Përdorimi i frekuencave "Terahertz" *(THz Communication*) - frekuencat THz (0.1-10 THz) do të jenë baza e teknologjisë 6G-së, duke ofruar bandwidth të pabesueshëm për transmetime ultra-shpejta dhe lokalizim precis[13]. Frekuencat do të arrijë shpejtësi Tbps, duke mundësuar aplikime si 3D holografi ose eksplorimi hapësinor. Në fushën e mbrojtjes, frekuencat në bandën THz do të lejojë komunikime të sigurta në mjedise të kontestuara, duke mbështetur zbulim të integruar *(ISAC)* për sensorë ushtarakë. Konsumimi i energjisë, i zgjidhur me IA-native është paradigm.

Hologramat *(holographic telepresence)* - Teknologjia "6G" do të mundësojë hologramat reale, duke bashkuar botën fizike me atë dixhitale përmes lidhjeve ultra-shpejta. Me shpejtësi Tbps dhe latencë <1 ns, hologramat do të integrohen me XR *(Extended Reality)* për telepresence immersive, duke krijuar "digital twins" për trajnime "remote". Në ushtri, hologramat do të revolucionarizojnë komandën taktike, duke lejuar simulime 3D të fushëbetejës

[9] Përvoja ku përdoruesi zhytet plotësisht në një mjedis digjital ose të kombinuar me realitetin, duke u ndjerë sikur është pjesë e tij.

[10] https://www.iotforall.com

[11] Procesi i vlerësimit të karakteristikave të kanalit të komunikimit *(rrugës që ndjek sinjali nga transmetuesi te marrësi)*, në mënyrë që komunikimi të jetë sa më i saktë dhe i besueshëm.

[12] https://www.fcc.gov

[13] https://www.iotforall.com

ose trajnime pa rrezik fizik.

Rrjetet e adaptueshme *(Adaptive Networks)* - Rrjetet "6G" do të jenë vetë-adaptuese, duke përdorur IA për të reaguar në kohë reale ndaj ndryshimeve mjedisore ose ngarkesës. Cell-freemassive MIMO heq kufijtë e "qelizave" tradicionale, duke përdorur antena të shpërndara për efikasitet spektral. Kjo do të integrojë NTN *(Non-Terrestrial Networks)* për mbulim "ubiquitous"[14], duke ulur ndikimin mjedisor me upgrades software. Në mbrojtje, rrjetet adaptive do të garantojnë rezistencë ndaj sulmeve hibride, duke mbështetur operacione në zona të vështira si detet ose hapësira. Përmirësimet në teknologjinë 6G do të krijojnë një ekosistem hiper-konektuar, duke mundësuar aplikime transformuese si "metaverse"[15], autonomi masive dhe siguri kuantike. Kërkimet e zhvilluara përgjatë vitit 2025-s tregojnë një tranzicion të shpejtë, por sfidat si siguria dhe energjia kërkojnë bashkëpunim ndërkombëtar.

Përdorimi ushtarak: dronë, komunikim në fushëbetejë, IA taktike, *Internet of Military Things.*

Teknologjia 5G/6G po transformon operacionet ushtarake me sisteme më autonome dhe rezistente.

Dronët *(UAV/drone swarms & sisteme autonome)* - Teknologjitë 5G & 6G mundësojnë koordinim real-time të dronëve, duke reduktuar latencën për navigim dhe transmetim video. Në teknologjinë 5G, "beamforming"[16] dhe URLLC[17] lejojnë streaming multi-gigabit të imazheve nga dronë, duke përmirësuar zbulimin në terren. Kjo rrit sigurinë duke minimizuar ekspozimin. Në teknologjinë 6G, THz do të lejojë swarms autonome me IA për formacion kontroll, duke reduktuar vulnerabilitetin e helikopterëve me eskortë dronësh dhe rritur efikasitetin taktike me 39% tregu të UAV-ve AI-driven.

Komunikimi në fushëbetejë *(tactical communications)* - Teknologjia 5G krijon rrjete private taktike *(portable 5G)* për komunikim të sigurtë midis automjeteve, sensorëve dhe personelit, duke mundësuar "situational awareness" reale. Tregu i 5G-së në mbrojtje parashikohet të rritet nga 1.36 miliardë USD në 5.23 miliardë USD deri në 2032 *(CAGR 21.3%)*, duke mbështetur C4ISR. Njëherësh redukton kohën e vendimmarrjes me "streaming video", multi-burim dhe sensor fusion, duke rritur koordinimin mes formacioneve ushtarake apo forcave të koalicionit. Në teknologjinë 6G, rrjetet adaptive me IA do të ofrojnë "network as a sensor" për vetë-shërim, duke siguruar komunikim në

[14] Mbulim të gjithanshëm / kudo-të-pranishëm, pra që sinjali ose shërbimi është i disponueshëm pothuajse në çdo vend.

[15] Mjedis digjital virtual, i përbashkët, i vazhdueshëm, i ndërlidhur dhe gjithëpërfshirës.

[16] Teknikë transmetimi ku sinjali radio drejtohet qëllimisht drejt një pajisje të caktuar, në vend që të shpërndahet në të gjitha drejtimet.

[17] Ultra-Reliable Low-Latency Communication - do të thotë komunikim me besueshmëri shumë të lartë dhe vonesë jashtë zakonisht të ulët.

mjedise të "jamuara" dhe mundëson operacione hibride pa ndërprerje, duke ruajtur avantazhin strategjik ndaj armiqve.

Inteligjenca artificiale taktike *(tactical AI)* – teknologjia "5G" integron IA për analizë të shpejtë të të dhënave në fushëbetejë, duke mundësuar vendimmarrje autonome në sisteme si dronë ose robotë. Për shembull, IA + 5G në mbrojtje revolucionarizon operacionet me sensor fusion për kërcënime të parashikuara, rrit efikasitetin me procesim real-time të të dhënave, duke ulur gabimet njerëzore dhe duke mbështetur cyberwarfare. Në teknologjinë 6G, AI-native do të integrojë "predictive maintenance" dhe "decision networks", duke transformuar luftën me sisteme të pavarura. Kjo ndihmon në strategji moderne, duke ofruar avantazh taktik si p.sh. në stërvitjet e NATO-s.

IoMT *(Internet of MilitaryThings)* - IoMT lidh sensorë, veshje dhe pajisje ushtarake në rrjete 5G/6G për ndarje të menjëhershme të të dhënave në fushëbetejë[18]. IoMT mundëson monitorim vital për ushtarët dhe koordinim robotik. Për shembull, "5G private networks" integrojnë IoMT për "real-time intelligence" nga sensorë në tanke ose dronë. Përmirëson koordinimin me "mesh networks" rezistente, duke reduktuar kohën e reagimit dhe duke rritur sigurinë. Në teknologjinë 6G, IoMT do të integrojë ISAC për "sensing" të integruar, duke krijuar ekosisteme autonome, forcon mbrojtjen kolektive *(NATO)*, duke ulur kostot dhe duke rritur efikasitetin operacional. Përdorimi ushtarak i teknologjisë 5G dhe 6G rrit efikasitetin, sigurinë dhe autonominë, duke transformuar luftën hibride. Këto teknologji ofrojnë avantazh strategjik, por kërkojnë investime në siguri kibernetike për të minimizuar rreziqet.

2. Siguria kibernetike dhe masat mbrojtëse në epokën e teknologjive "5G/6G"

Rritja e sipërfaqes së sulmeve kibernetike për shkak të teknologjive të avancuara

Sipërfaqja e sulmeve kibernetike *(attack surface)* përfaqëson të gjitha pikat e mundshme të hyrjes për sulmuesit, si pajisje, rrjete dhe aplikacione *(software)*. Teknologjitë e avancuara si IA, IoT, 5G/6G, "edge computing" dhe "Industry 4.0" e zgjerojnë këtë sipërfaqe, duke rritur rreziqet për organizatat dhe sistemet ushtarake te komunikimit. Arsyet kryesore janë:

1. **Zgjerimi nga pajisjet IoT dhe lidhjet masive të pajisjeve elektronike**: IoT *(Internet of Things)* shton miliona pajisje të lidhura, si pajisje që vishen *(wearable devices)*[19] ose sensorë, duke krijuar pika të reja dobësie në rrjete. Kjo rrit sipërfaqen e sulmit, duke lejuar hyrje të paautorizuara dhe sulme DDoS. Sipas analizave statistikore dhe vlerësimeve të riskut janë mbi 200

[18] https://www.techaheadcorp.com

[19] Pajisje teknologjike që vishen në trup dhe mbledhin ose shfaqin të dhëna në kohë reale (ora-unaza-kufje inteligjente).

teknologji emergjente që zgjerojnë pikat e hyrjes kibernetike, duke bërë sistemet më të ndjeshme.

2. **Ndikimi i IA dhe automatizimit**: IA mundëson sulme më të sofistikuara, si "phishing" të avancuar ose zbulim automatik të vulnerabiliteteve, por vetë IA krijon sipërfaqe të reja sulmi duke ekspozuar modele të trajnuara ndaj manipulimeve.
3. **Nevoja për mbrojtje "proaktive":** pasi adoptimi i IA rrit ekspozimin e organizatave.
4. **Teknologjitë 5G/6G dhe "edge computing"**: rrjetet 5G/6G rrisin sipërfaqen duke shtuar pajisje dhe të dhëna të larta, ndërsa "edge computing" shpërndan sistemet, duke krijuar më shumë pika të dobëta ndaj sulmeve hibride dhe ky zgjerim i bën prodhuesit më të ekspozuar ndaj sulmeve kibernetike.
5. **Digjitalizimi global**: rritja e sulmeve vjen nga adoptimi masiv i IA dhe digjitalizimi, duke shtuar vlerën e të dhënave dhe duke krijuar më shumë objektiva për aktorë keqdashës. Teknologjitë e avancuara ofrojnë efikasitet, por zgjerojnë sipërfaqen e sulmit duke shtuar kompleksitet dhe pika hyrjeje, për rrjedhojë kërkohet mbrojtje e avancuara proaktive si IA për zbulim kërcënimesh.

Arkitektura të sigurisë "Zero-Trust" ***(ZT)*** - është një qasje revolucionare në mbrojtjen kibernetike, e cila supozon se asnjë entitet, brenda apo jashtë rrjetit, nuk mund të besohet automatikisht. Në epokën e 5G dhe 6G, ku rrjetet janë më të decentralizuara, me latencë ultra-të ulët dhe integrim të thellë me IA, ZT bëhet thelbësore për të mbrojtur sistemet kundër sulmeve të sofistikuara. Kjo arkitekturë kalon nga modeli tradicional "perimetër" *(ku mbrohet vetëm kufiri i rrjetit)* në një verifikim të vazhdueshëm të identitetit, aksesit dhe kontekstit. ZT pritet të jetë komponent kryesor i teknologjisë 6G, duke përmirësuar mbrojtjen në rrjetet ushtarake dhe infrastruktura kritike[20].

Parimet themelore të arkitekturës Zero-Trust në teknologjinë 5G/6G:

Arkitektura Zero Trust (ZT) bazohet në parimin "kurrë mos beso, gjithmonë verifiko", duke aplikuar kontrolle të vazhdueshme sigurie në çdo nivel të rrjetit. Në teknologjitë 5G dhe 6G, ku rrjetet janë cloud-native dhe të virtualizuara përmes Network Function Virtualization (NFV) dhe Software-Defined Networking (SDN), qasja Zero Trust integron sigurinë drejtpërdrejt në arkitekturën e rrjetit për të reduktuar sipërfaqen e sulmeve kibernetike[21].

Verifikimi i vazhdueshëm: Çdo kërkesë për akses verifikohet në kohë reale duke marrë parasysh faktorë të shumtë si identiteti i përdoruesit, vendndodhja, pajisja dhe konteksti i përdorimit. Në teknologjinë 5G kjo përfshin mekanizma

[20] https://www.osti.gov/ - Office of Scientific and Technical Information/U.S. Department of Energy.
[21] https://www. ericsson.com

të fortë autentikimi për *network slicing* (ndarja virtuale e rrjetit), duke izoluar segmente kritike, për shembull komunikimet ushtarake ose emergjente nga trafiku civil. Në teknologjinë 6G, rrjetet AI-native pritet të parashikojnë rreziqet në mënyrë proaktive dhe të zbatojnë parimet Zero Trust edhe në *edge computing*, duke mundësuar vendimmarrje të automatizuar dhe të decentralizuar.

Mikro-segmentimi *(micro-segmentation)*: Rrjeti ndahet në segmente të vogla, duke kufizuar lëvizjen laterale të sulmuesve. Në teknologjinë 5G, kjo mbron kundër sulmeve në "Open RAN", ku komponentë nga vendorë të ndryshëm mund të jenë vulnerabël. Në teknologjinë 6G, segmentimi do të jetë dinamik, duke përdorur inteligjencën artificiale për të përshtatur kufijtë e segmenteve në kohë reale sipas nivelit të rrezikut.

Kriptografia e avancuar: ZT kërkon kriptim "end-to-end", duke përfshirë PQC *(Post-Quantum Cryptography)* për të mbrojtur kundër kompjuterëve kuantikë. Në teknologjitë 5G/6G, kjo mbron të dhënat në transmetim, duke reduktuar rreziqet e "eaves dropping"[22].

Zbulimi dhe reagimi automatik: Inteligjenca artificiale (IA) dhe **Machine Learning (ML)** integrohen në arkitekturën e sigurisë për të zbuluar anomali në trafikun e rrjetit dhe për të reaguar automatikisht ndaj aktivitetit të dyshimtë. Në rrjetet 5G, standardet e zhvilluara nga **3GPP**[23] mbështesin implementimin e Zero Trust përmes mekanizmave të autentikimit të avancuar, si **EAP-TLS**[24], i cili përdor certifikata digjitale për verifikimin e përdoruesve ose pajisjeve, duke ofruar siguri më të lartë sesa autentikimi i bazuar vetëm në fjalëkalime.

Në epokën e teknologjisë 5G/6G, ku rrjetet janë më të decentralizuara dhe të lidhura (me IoT masive dhe "edgecomputing"), ZT ofron masa "proaktive" për të luftuar rritjen e sipërfaqes së sulmeve.

- Për teknologjinë 5G: ZT aplikohet në rrjete private ushtarake për të verifikuar çdo pajisje (p.sh., dronë ose sensorë IoMT), duke përdorur network "slicing" të sigurtë për të izoluar trafikun kritik. Masa përfshijnë: autentikim multi-faktor, logjim të vazhdueshëm dhe reagim automatik ndaj anomalive.

- **Për teknologjinë 6G**: si arkitekturë "AI-native", ZT do të integrohet natyrshëm, duke përdorur "blockchain" për identitet të decentralizuar dhe IA për parashikim sulmesh. Masa përfshijnë: kriptografi rezistente kuantike, "federated learning" për të mbrojtur modelet IA dhe "dynamicmicro-segmentation" për rrjete adaptive. ZT në tek. "6G" kërkon arkitekturë të shpërndarë për të luftuar sulmet në "edge"[25].

---

[22] https://www. research.samsung.com

[23] Third Generation Partnership Project: organizatë ndërkombëtare që standardizon teknologjitë e rrjeteve celulare në nivel global.

[24] Protokoll sigurie për autentikim në rrjete, pjesë e familjes EAP *(Extensible Authentication Protocol)*.

[25] https://www.ieeexplore.ieee.org

- Për aplikimet ushtarake: Gjatë aplikimeve në fushën e mbrojtjes (FA), ZT mbron kundër infiltrimit në IoMT, duke verifikuar çdo sensor ose dron. ATIS raporton se ZT në 5G/6G ul rrezikun në "cloud" ushtarake, duke kërkuar verifikim të vazhdueshëm për të shmangur sulme nga aktorë shtetërorë[26].

ZT ul mundësinë e lëvizjes laterale të sulmuesve, duke mbrojtur kundër "DDoS, spoofing" ose manipulimit të sinjaleve. Në teknologjinë 6G, kjo integrohet me IA për reagim automatik, duke ulur kohën e përgjigjes në mikrosekonda. Në mjedise të kontestuara, ZT siguron që edhe nëse një segment komprometohet, të tjerët mbeten të sigurtë. Në teknologjinë 5G, ZT kërkon modifikim të rrjeteve ekzistuese, duke rritur kostot dhe vonesat; kurse në teknologjinë 6G, integrimi me IA rrit rrezikun e sulmeve "adversarial" ndaj vetë modeleve ZT. Por verifikimi i vazhdueshëm mund të shtojë latencë në aplikime kritike ushtarake, si drones warms. Ndërsa "3GPP " mundëson ZT në 5G, 6G kërkon standarde të reja për të adresuar rreziqe kuantike dhe etike. Në ushtri, ZT duhet të balancojë sigurinë me shpejtësinë operative, duke kërkuar trajnim dhe teknologji të reja. Si përfundim, ZT është një mjet kyç për mbrojtjen kibernetike në teknologjitë 5G/6G, duke ofruar mbrojtje dinamike kundër rreziqeve në rritje. Implementimi i saj në rrjete ushtarake të komunikimit dhe infrastrukturën kritike kërkon investime në aplikimin IA dhe PQC për të ruajtur avantazhin strategjik[27].

Përdorimi i Inteligjencës Artificiale për zbulim të hershëm të sulmeve kibernetike

Në epokën e teknologjisë 5G dhe 6G, mbrojtja kibernetike mbështetet gjithnjë e më shumë në inteligjencën artificiale (IA) për zbulim të hershëm të sulmeve kibernetike. IA mundëson analizë në kohë reale të trafikut të rrjetit, duke identifikuar anomalitë para se të shndërrohen në sulme të plota, si "DDoS, spoofing" ose infiltrim. Kjo qasje "proaktive" kalon nga mbrojtja "reaktive" në atë "parashikuese", duke përdorur modele "machine learning" *(ML)*, "deep learning" *(DL)* dhe "generative AI" për të trajtuar kompleksitetin e rrjeteve të ardhshme të komunikimit & shkëmbimit të informacionit. Në 2025, raportet treguan se përdorimi i IA uli kohën e zbulimit të sulmeve nga orë në sekonda, duke reduktuar dëmet në infrastrukturë kritike dhe sisteme ushtarake[28].

- Mekanizmat e IA-së për zbulim të hershëm të sulmeve: IA funksionon duke analizuar modele të trafikut të rrjeteve, duke identifikuar devijime nga normat *(anomalitë)* që mund të sinjalizojnë sulme kibernetike. Në teknologjitë 5G/6G, ku volumi i të dhënave është masiv *(deri në Tbps)*, IA është i domosdoshëm për procesim të shpejtë pa ndërhyrje njerëzore.

[26] https://www.atis.org

[27] https://www. dl.acm.org

[28] https://www.upguard.com/ - kompani & platformë e cyber sigurisë dhe menaxhimit të rrezikut kibernetik - California/SHBA.

- Machine Learning (ML) dhe Deep Learning (DL): modelet ML si "Random Forest ose Support Vector Machines" trajnohen në të dhëna historike për të klasifikuar trafikun normal dhe të dyshimtë. DL, si "Convolutional Neural Networks" (CNN) ose "Recurrent Neural Networks" (RNN), analizojnë sekuenca të trafikut për zbulim të hershëm të sulmeve të sofistikuara, si ato në Open RAN ose edgecomputing. Për shembull, një sistem DL mund të zbulojë DDoS duke identifikuar rritje të papritur të kërkesave në rrjet, duke ulur kohën e reagimit në mikrosekonda. Në teknologjinë 6G, DL integrohet me ISAC *(Integrated Sensing and Communication)* për të zbuluar ndërhyrje fizike *(jamming)* përmes analizës së sinjaleve[29].

- **Reinforcement Learning (RL) dhe Graph Neural Networks (GNN)**: RL lejon sisteme që "mësojnë" nga simulime sulmesh kibernetike, duke optimizuar mbrojtjen në kohë reale *(p.sh., adaptim të rrjetit për të izoluar një segment të sulmuar).* GNN analizojnë strukturën e rrjetit si graf, duke zbuluar anomalitë në lidhje midis pajisjeve IoT, si infiltrimi në një droneswarm. Këto modele janë kritike për 6G, ku rrjetet janë dinamike dhe shumë të shpërndara.

- **Generative IA:** modelet si GAN *(Generative Adversarial Networks)* simulojnë sulme për të trajnuar sisteme mbrojtëse kibernetike, duke krijuar skenarë realë për zbulim të hershëm. Në teknologjinë 5G, "generative AI" zbulon kërcënime në kohë reale, si manipulim sinjalesh ose "helmim" të dhënash, duke ulur "false positives"[30] deri në 50%. Në teknologjinë 6G, ky mekanizëm GAN integrohet për të parashikuar sulme në rrjete THz, duke rritur mbrojten kundër kërcënimeve kibernetike kuantike.

Në teknologjinë 5G, IA përdoret për "Intrusion Detection Systems" *(IDS)* në "core network", duke zbuluar sulme në "network slicing" *(ndarje virtuale e rrjetit)*. Në sistemet e Forcave të Armatosura, IA integrohet në JADC2 për zbulim të hershëm të "jamming-ut ose spoofing" në drone, duke përdorur ML për të analizuar trafikun e rrjetit dhe të identifikojë modele sulmesh.

Në teknologjinë 6G, "AI-native networks" do të lejojnë zbulim autonom të sulmeve, duke integruar me PQC për mbrojtje kuantike dhe duke reduktuar rreziqet në "edge computing". Aplikime specifike përfshijnë zbulime të sulmeve në "smartcities", ku 6G lidh IoTmassive ose mbrojtje të rrjeteve ushtarake nga sulme "adversarial AI"[31].

Pavarësisht avantazheve të siguruara nga përdorimi i IA në mbrojtjen kibernetike, IA për zbulime të hershëme ka disa sfida: - false positives/ negatives: modelet e IA mund të gabojnë trafikun normal si sulm, duke shkaktuar

[29] https://www.sciencedirect.com/ - faqe e besueshme dhe shumë e njohur akademike për publikime shkencore.

[30] Alarm i rremë & reduktimi i rasteve kur një system sinjalizon gabimisht një problem që në fakt nuk ekziston.

[31] https://www. sciencedirect.com

ndërprerje të panevojshme, ose të mos zbulojnë sulme të sofistikuara. Në 5G, kjo ul efikasitetin në rrjete të dendura; - konsumimi i burimeve: IA kërkon fuqi llogaritëse të lartë, duke rritur latencën në pajisje të kufizuara *(p.sh. IoMT ushtarak)*, çka është kritike për teknologjinë 6G me latencë mikrosekonda; - sulme "adversarial" ndaj IA-së: sulmuesit mund të "helmojnë" modele ML duke injektuar të dhëna false, duke e bërë IA-në të paefektshme. Në teknologjinë 6G, kjo sfidë thellohet me integrim të thellë të IA; - mungesa e standardeve: Në vitin 2025, mungoi harmonizimi global për IA në siguri kibernetike, duke krijuar pabarazi midis vendeve. Në ushtri, kjo rrit rrezikun e ndërveprueshmërisë në aleanca si NATO.

Përdorimi i IA për zbulim të hershëm të sulmeve kibernetike është një masë kyçe kibernetike në teknologjitë 5G/6G, duke ofruar mbrojtje "proaktive" kundër kërcënimeve në rritje. Në vitin 2025, zhvillimet si ato në rrjetet telekomunikimit treguan se IA transformon sigurinë, por kërkon zgjidhje për sfida si "adversarialattacks" dhe burime të kufizuara për të ruajtur efektivitetin në mbrojtje ushtarake dhe infrastruktura kritike.

Ndërtimi i rrjeteve komunikimi të sigurta të mbrojtura nga "end-to-end encryption".

Ndërtimi i rrjeteve të sigurta, të mbrojtura nga "end-to-end encryption" *(E2EE)* është një nga masat kryesore kibernetike në epokën e teknologjive 5G dhe 6G, ku rrjetet janë më të decentralizuara, me shpejtësi ultra të lartë dhe integrim të thellë me teknologji IoT masive. E2EE siguron që të dhënat të kriptohen nga burimi *(dërguesi)* deri në destinacion *(marrësi)*, duke parandaluar aksesin e paautorizuar nga palë të treta, përfshirë operatorët e rrjetit. Kjo qasje kalon nga kriptimi tradicional (p.sh., AES në 5G) në një model "proaktiv", duke adresuar rritjen e sipërfaqes së sulmeve dhe kërcënimet kuantike.

Më poshtë, shpjegohet në detaje mbrojtja kibernetike, masat, sfidat dhe aplikimet, me fokus në kontekstin e sistemeve ushtarake të komunikimit dhe të infrastrukturës kritike.

Koncepti dhe mekanizmat e "E2EE" në teknologjinë 5G/6G.

E2EE është një formë kriptimi ku çelësat e kriptimit gjenerohen dhe menaxhohen vetëm nga dërguesi dhe marrësi, duke e bërë të pamundur decriptimin nga serverët intermediarë*(midis përdoruesit & klientit dhe serverit kryesor)* ose operatorët e rrjetit. Në teknologjinë 5G, E2EE integrohet me standardet 3GPP *(p.sh., release 18)*, duke përdorur algoritme si AES-256 ose ChaCha20 për të mbrojtur të dhënat në transmetim, ndërsa në teknologjinë 6G, ajo do të kombinohet me kriptografi post-kuantike *(PQC)* për të rezistuar kompjuterëve kuantikë.

- Mekanizmat kryesorë: Në teknologjinë 5G, E2EE aplikohet në shtresën e aplikacionit *(p.sh., për VoIP ose mesazhe të siguruara)*, duke përdorur protokolle si TLS 1.3 ose QUIC për të mbrojtur kundër "eavesdropping"

(përgjimit). Në teknologjinë 6G, E2EE do të jetë "AI-native", duke përdorur "machinelearning" për të adaptuar çelësat në kohë reale dhe për të zbuluar tentativat e thyerjes. Kjo mbron kundër sulmeve "man-in-the-middle" *(MITM)* dhe DDoS, duke siguruar integritetin e të dhënave në rrjete të shpërndara. Rrjetet ndërtohen duke integruar E2EE në arkitekturë nga fillimi *(secure by design)*, duke përdorur "networkslicing" në 5G për të izoluar segmente kritike *(p.sh., rrjetet ushtarake nga civile)* dhe duke aplikuar kriptim në çdo nivel: nga pajisja fundore *(end device)* deri në "cloud". Masa mbrojtëse si "encryption e avancuar" ulin rrezikun e interceptimit të të dhënave gjatë transmetimit në rrjete të distribuara.

Masat mbrojtëse kibernetike fokusohen në ndërtimin e rrjeteve rezistente, duke kombinuar E2EE me teknologji të tjera për mbrojtje gjithëpërfshirëse. E2EE forcon autentikimin *(p.sh., EAP-TLS*) dhe mbron kundër sulmeve në "Open RAN", ku komponentë të ndryshëm vendorësh mund të jenë vulnerabël. Masa përfshijnë: - kriptim të trafikut në shtresën e transportit, - "zero-trust access" për të verifikuar çdo pajisje, dhe integrim me IA për zbulim anomalish. Në rrjetet ushtarake, E2EE mbron komunikimet taktike në C4ISR, duke reduktuar rrezikun e "eaves dropping" në rrjete të shpërndara.

Në teknologjinë 6G, E2EE integrohet me PQC për të rezistuar sulmeve kuantike, duke mbrojtur kundër "harvestnow, decryptlater". Masa përfshijnë: - kriptim dinamik në frekuencat THz, "blockchain" për integritet të dhënash, dhe "federated learning" për të trajnuar modele IA pa ndarje të dhënash të ndjeshme. Në kontekstin ushtarak, këto masa mbrojnë kundër sulmeve në "droneswarms" ose hologramet taktike, duke ulur rrezikun e manipulimit të sinjaleve. Ndërtimi i rrjeteve kërkon auditime të vazhdueshme, "zero-trust architecture" për verifikim aksesi dhe simulime sulmesh me IA për të testuar E2EE. Kompjuterët kuantikë mund të thyejnë E2EE tradicionale, duke kërkuar tranzicion në PQC. Kjo është një sfidë kryesore për teknologjinë 6G, ku sulmet kuantike bëhen reale. Në sistemet ushtarake, E2EE duhet të balancojë sigurinë me shpejtësinë, duke kërkuar trajnime dhe investime.

Në përfundim, ndërtimi i rrjeteve të mbrojtura me E2EE është një masë esenciale kibernetike në teknologjitë 5G/6G, duke ofruar mbrojtje proaktive kundër rreziqeve në rritje.

"Virtualizimi" i funksioneve të rrjetit (NFV) dhe "segmentimi" i rrjeteve *(network slicing).*

Në epokën e teknologjive 5G dhe 6G, mbrojtja kibernetike mbështetet në "virtualizimin" e funksioneve të rrjetit *(NetworkFunctionVirtualization& NFV)* dhe "segmentimin" e rrjeteve *(networkslicing)*. Këto teknologji lejojnë krijimin e rrjeteve fleksibël dhe të izoluar, duke ulur sipërfaqen e sulmeve dhe duke mundësuar mbrojtje "proactive" kundër kërcënimeve si "DDoS, spoofing" ose infiltrim. NFV virtualizon funksionet "hardware" në "software", duke lejuar menaxhim dinamik, ndërsa "network slicing" krijon "fetë" virtuale

të rrjetit për shërbime të ndryshme, duke izoluar trafikun kritik. Në vitin 2025, këto masa ishin shumë sensitive për infrastrukturën kritike dhe ushtarake, duke siguruar reduktimin e rreziqeve në rritje nga densifikimi i pajisjeve dhe kërcënimet "kuantike".

Koncepti dhe mekanizmat e NFV-së në mbrojtjen kibernetike: NFV zëvendëson pajisjet fizike *(si routerë ose firewall)* me funksione "virtual" të ekzekutuara në serverë "cloud", duke lejuar "skalim" dinamik dhe menaxhim të centralizuar. Në teknologjitë 5G/6G, NFV integrohet me SDN *(Software-Defined Networking)* për të krijuar rrjete rezistente, duke mundësuar zbulim dhe reagim të shpejtë ndaj sulmeve. NFV lejon orkestrim të funksioneve të sigurisë virtuale *(Virtual Security Functions & VSF)*, si firewall virtuale ose IDS *(Intrusion Detection Systems)*, duke i vendosur ato në pika kritike të rrjetit. Në teknologjinë 5G, NFV përdoret për të izoluar dobësitë në "Open RAN", duke reduktuar rrezikun e sulmeve në komponentë të ndryshëm vendorësh[32].

Në teknologjinë 6G, NFV do të jetë "AI-native", duke përdorur "machine learning" për të adaptuar funksionet e sigurisë në kohë reale, si zbulim automatik të anomalive në "edge computing". Masat mbrojtëse përfshijnë: monitorim të vazhdueshëm të VSF-ve për të zbuluar sulme DDoS ose malware dhe "megrim" dinamik të funksioneve në serverë të sigurtë gjatë një kërcënimi. NFV ul kohën e reagimit ndaj sulmeve nga orë në sekonda, duke lejuar izolim të shpejtë të segmenteve të kompromentuara. Në infrastrukturë kritike, kjo mbron kundër "cross-layer" sulmeve, ku një dobësi në një shtresë ndikon në të tjera. Në ushtri, NFV mundëson rrjete taktike rezistente, duke mbrojtur kundër "jamming" ose sulmeve në C4ISR.

Koncepti dhe mekanizmat e "networkslicing" në mbrojtjen kibernetike: "Network slicing" krijon rrjete virtuale të pavarura *(slices)* brenda një infrastrukture fizike, duke alokuar burime *(bandwidth, latencë)* për shërbime të ndryshme. Në teknologjitë 5G/6G, "slicing" lejon izolim të trafikut, duke mbrojtur segmente kritike nga sulmet[33]. Çdo "slice" ka politikat e veta të sigurisë, duke përdorur autentikim të fortë *(EAP-TLS)*, kriptim dhe monitorim të dedikuar. Në teknologjinë 5G, "slicing" izolon sulmet "cross-slice", pra një sulm "DDoS" në një "slice" civile nuk ndikon në atë ushtarak[34]. Sikurse në teknologjinë 6G, "slicing" do të jetë dinamik dhe "AI-driven", duke adaptuar izolimin në kohë reale bazuar në kërcënime, si në rrjete THz ku një "slice" për dronë mund të izolohet automatikisht gjatë një anomalie. Masa përfshijnë: "slice orchestration" me SDN për të aplikuar rregulla sigurie, dhe integrim me "PQC" për të mbrojtur kundër sulmeve kuantike. "Slicing" redukton përhapjen e sulmeve, duke ulur dëmet nga 50-70% në rrjete të segmentuara. Në infrastrukturë kritike, mbron kundër "isolation failures ose monitoring gaps", duke e bërë të vështirë për sulmuesit

[32] https://link.springer.com/
[33] https://www. mdpi.com
[34] https://www.p1sec.com/

të kalojnë midis "slicesh". Në fushën ushtarake, "slicing mundëson rrjete të dedikuara për misione, duke u mbrojtur kundër sulmeve në IoMT.

Integrimi i NFV-së dhe networkslicing në mbrojtjen kibernetike: NFV dhe "slicing" punojnë së bashku për të krijuar një arkitekturë hibride. NFV virtualizon funksionet e sigurisë brenda "slicing", duke lejuar menaxhim dinamik dhe izolim të forte. Në teknologjinë 5G, kjo krijon një "distributedsecurityframework" me VSF në shtresa të ndryshme, duke përdorur IA për orkestrim. Në teknologjinë 6G, integrimi do të jetë më i avancuar, duke reduktuar rreziqet në rrjete të shpërndara. Masa përfshijnë: - "robust authentication", - "cryptographic", - "techniques" dhe "sliceisolation" për të luftuar "attack vectors" si "cross-slice" sulmet. Në ushtri, sfida përfshijnë rreziqet në rrjetet taktike, ku një "failure" në "slicing" mund të kompromentojë misione. Kjo kërkon integrim me PQC për të luftuar kërcënime kuantike. Në përfundim, NFV dhe "network slicing" janë masa esenciale kibernetike në teknologjitë 5G/6G, duke ofruar izolim dhe fleksibilitet për mbrojtje "proaktive".

Stërvitjet kibernetike ushtarake dhe ndërveprimi ndërkombëtar: Në epokën e teknologjive 5G dhe 6G, ku rrjetet kanë integrim të thellë me IoT masive dhe IA, mbrojtja kibernetike kërkon qasje proaktive. Stërvitjet kibernetike ushtarake dhe ndërveprimi ndërkombëtar, si p.sh. stërvitja e NATO-s "Locked Shields" luajnë një rol kyç në zhvillimin e aftësive mbrojtëse, duke simuluar sulme reale për të përmirësuar rezistencën kundër kërcënimeve kibernetike. Këto stërvitje jo vetëm testojnë teknologjitë, por edhe forcojnë bashkëpunimin midis vendeve, duke adresuar sfida si sulmet hibride, rreziqet kuantike dhe vulnerabilitetet e "supplychain".

Stërvitjet kibernetike simulojnë skenarë luftë kibernetike për të trajnuar ekipet në mbrojtjen e rrjeteve, duke përfshirë simulime të sulmeve në teknologjitë 5G/6G si DDoS, jamming ose manipulim sinjalesh. Këto stërvitje përmirësojnë masat kibernetike duke identifikuar dobësitë para se të ndodhin sulme reale, duke integruar teknologji si: "Zero-Trust Architecture (ZTA), Post-Quantum Cryptography (PQC) dhe IA për zbulim anomalish. "Locked Shields" është stërvitja më i madh kibernetik në botë, organizuar nga Qendra e Ekselencës së Mbrojtjes Kibernetike të NATO-s që nga viti 2010. Në vitin 2025, kjo stërvitje përfshiu 41 vende në 17 ekipe, duke simuluar një luftë kibernetike ku ekipet mbrojnë infrastrukturën kritike nga sulme të sofistikuara.

3. Perspektivat strategjike: siguria dhe sovraniteti teknologjik

Kontrolli i teknologjive 5G dhe 6G është bërë një faktor kyç strategjik në fuqinë ndërkombëtare, duke ndikuar në ekonomi, siguri dhe influencë gjeopolitike. Këto teknologji nuk përfaqësojnë thjesht avancime në sistemet e telekomunikacionit, por shërbejnë si mjete për dominim digjital, duke mundësuar mbledhjen masive të të dhënave, operacione autonome dhe mbrojtje kibernetike. Kontrolli i tyre ofron avantazh në industritë e ardhshme

si inteligjenca artificiale (IA), Interneti i Gjërave (IoT) dhe qytetet inteligjente ("smart cities"), duke krijuar varësi ekonomike. Teknologjitë 5G/6G sigurojnë avantazh ushtarak, duke mbështetur komunikimet taktike, operacionale dhe inteligjencën reale, dhe konsiderohen "high ground" digjital për mbrojtjen kundër sulmeve hibride. Politikat e "sovereign 5G" synojnë zhvillimin e rrjeteve 5G të pavarura nga furnitorë të huaj, duke garantuar sovranitetin teknologjik dhe reduktuar varësinë nga zinxhirët globalë të furnizimit.

Roli i institucioneve ndërkombëtare: NATO, ITU, BE dhe SHBA

Në epokën e teknologjive 5G dhe 6G, institucionet ndërkombëtare kanë një rol vendimtar në formësimin e peizazhit strategjik dhe gjeopolitik, duke balancuar inovacionin teknologjik me sigurinë kombëtare dhe bashkëpunimin global, si dhe konkurrencën midis fuqive të mëdha.

NATO: Për NATO-n, teknologjitë 5G/6G janë element kyç i transformimit digjital ushtarak. Samiti i Hagës (24–26 qershor) theksoi përgatitjen e Aleancës për epokën e teknologjisë së lartë (5G/6G, AI, kibernetikë, hapësirë), duke e kthyer nga një organizatë e mbrojtjes konvencionale në një aleancë teknologjikisht superiore. Strategjia e NATO-s drejt 2030-s synon të ndikojë në standardet IMT (International Mobile Telecommunications), për të përshtatur teknologjitë 5G/6G me kërkesat e mbrojtjes dhe për të mundësuar adoptimin efektiv nga ushtritë aleate[35]. Prioritetet përfshijnë sigurinë kibernetike dhe interoperabilitetin midis 32 vendeve anëtare, përdorimin e 5G/6G për përmirësimin e C4ISR dhe JADC2, dhe integrimin e inteligjencës artificiale (IA) dhe kriptografisë post-kuantike (PQC) për mbrojtje kuantike në qendrën e ekselencës kibernetike (CCDCOE). Strategjikisht, kjo redukton varësinë nga teknologjia civile dhe rrit efikasitetin e operacioneve multinacionale.

International Telecommunication Union (ITU): Si agjenci e OKB-së, ITU ka rol kryesor në standardizimin e teknologjive 5G/6G, duke koordinuar alokimin e spektrit dhe zhvillimin e standardeve globale (p.sh., IMT-2030 për 6G). ITU promovon standarde neutrale për të siguruar interoperabilitet dhe zhvillim të qëndrueshëm të teknologjive për aplikime si "smart cities" dhe mbrojtje kibernetike. Ky rol redukton fragmentimin teknologjik dhe mundëson mbrojtje të unifikuar kundër kërcënimeve si jamming ose sulme DDoS. Strategjikisht, ITU ndihmon në alokimin e spektrit "mid-band" për përdorime ushtarake, duke balancuar nevojat civile dhe mbrojtëse.

Bashkimi Evropian (BE): BE luan rol kyç në promovimin e sovranitetit digjital, duke zhvilluar politika që balancojnë inovacionin me sigurinë. Prioriteti është mbrojtja e infrastrukturës kritike, integrimi i 5G/6G për ekonomitë inteligjente ("smart economies") dhe mbrojtje kibernetike. Programi "Digital Decade 2030" investon miliarda euro për "sovereign 5G",

[35] https://www.ncia.nato.int/

duke përdorur IA dhe PQC për mbrojtje kundër sulmeve hibride. Kjo strategji forcon rezistencën ekonomike dhe redukton rreziqet nga furnitorë të huaj.

SHBA: SHBA e konsideron teknologjinë 5G/6G si një komponent strategjik për mbrojtjen kombëtare, duke e integruar në strategjinë e sigurisë. Raporti "Forging the 5G Future" i Atlantic Council (2025) e thekson 5G si shtyllë të sigurisë, prosperitetit dhe influencës gjeopolitike[36]. SHBA promovon programin "Clean Network" për të larguar furnitorët kinezë nga aleatët, duke forcuar aleancën transatlantike me NATO dhe BE.

Në përmbledhje, institucionet ndërkombëtare luajnë rol kyç për të balancuar inovacionin me sigurinë, duke krijuar një botë multipolare ku teknologjitë 5G/6G shndërrohen në mjete të fuqisë strategjike.

Rekomandimet

Rekomandimet fokusohen në një qasje "proactive", duke integruar sigurinë që nga faza e dizajnit *(security-by-design)*.

Adoptimi i arkitekturave zero-trust *(ZTA)*: Implementimi i arkitekturës "zero-trust" në të gjitha shtresat e rrjetit, duke kërkuar autentikim të vazhdueshëm për pajisje, përdorues dhe të dhëna. Kjo është kritike për teknologjinë 5G/6G ushtarake, ku rrjetet publike dhe private bashkëveprojnë për të eliminuar besimin e nënkuptuar dhe për të validuar çdo interaksion. Integrimi i ZTA me IA për monitorim të lartë të rrjetit dhe mbrojtje konfidenciale, veçanërisht në mjedise taktike ku kërcënimet janë dinamike.

Mbrojtja e zinxhirit të furnizimit dhe integriteti i harduerit dhe softuerit: Kryerja e auditimeve të rrepta për furnitorët e "hardware & software", duke përdorur përditësime të nënshkruara kriptografikisht dhe procese transparente prodhimi. Për sistemet ushtarake, zhvilloni strategji për zinxhir furnizimi të besueshëm, duke përfshirë certifikim të komponentëve sipas standardeve NATO dhe BE, dhe testime gjithëpërfshirëse për kërcënime kibernetike.

Integrimi i kriptografisë post-kuantike dhe mbrojtjeve "AI-driven": Aplikimi i "kriptografi post-kuantike" që nga fillimi për të mbrojtur të dhënat ndaj kompjuterëve kuantikë, veçanërisht në teknologjinë 6G ku të dhënat e enkriptuara mund të ruhen për de-enkriptim të ardhshëm. Përdorimi i IA për detektim të anomalive, automatizim të përgjigjeve dhe mbrojtje në nyjet "core" dhe "edge". Në kontekstin ushtarak, IA duhet të jetë rezistente ndaj manipulimit *(adversarial attacks)* dhe poisoning të të dhënave, duke mbështetur operacione si "swarming" të droneve ose "sensim real-time". Rekomandohet zhvillimi i kontrolleve të sigurisë të bazuara në "machinelearning" për orkestrim të shpejtë të rrjetit.

Bashkëpunimi ndërkombëtar dhe standardizimi: Forcimi i partneriteteve

[36] https://www.atlanticcouncil.org/

midis agjencive publike, institucioneve kërkimore dhe prodhuesve të sistemeve të telekomunikacionit për zhvillimin e kërkimeve të sigurta në teknologjinë 6G, me fokus në autonominë strategjike të Europës. NATO dhe BE duhet të zhvillojnë platforma testimi ('testbeds') për të garantuar ndërveprueshmërinë multi-vendor, për të vendosur standarde të përbashkëta sigurie dhe për të lehtësuar transferimin e teknologjisë. Gjithashtu, duhet të kryhen analiza periodike të rreziqeve duke përdorur metoda të prioritetizimit, si dhe të zhvillohen matrica të personalizuara të sulmeve për rrjetet taktike.

Edukimi dhe trajnimi i strukturave ushtarake në siguri kibernetike: Në kontekstin e zhvillimeve të shpejta të rrjeteve teknologjike 5G dhe 6G, edukimi dhe trajnimi i strukturave ushtarake në fushën e sigurisë kibernetike janë elemente kyçe për mbrojtjen e sistemeve të komunikimeve ushtarake. Këto rrjete ofrojnë avantazhe të tilla si shpejtësi e lartë, latencë e ulët dhe integrim me teknologji si inteligjenca artificiale, Interneti i Gjërave (IoT) dhe sisteme të integruara të ndarjes së informacionit (ISAC), por gjithashtu zgjeron sipërfaqen e rrezikut ndaj sulmeve kibernetike, duke përfshirë jamming, spoofing, sulme në zinxhirin e furnizimit dhe manipulim të të dhënave.

Bashkëpunimi me Akademinë, universitetet, agjensitë, industrinë dhe partnerët ndërkombëtarë për identifikimin e talenteve – burimeve njerëzore të kualifikuara: Zhvillimi i planeve të kapitalit njerëzor duke bashkëpunuar me universitetet, laboratorët dhe industrinë për të identifikuar nevojat në sigurinë kibernetike për teknologjinë 5G/6G. Kjo përfshin programe STEM *(Shkencë, Teknologji, Inxhinieri dhe Matematikë)*, bursa, internship-e dhe programe post-doktorale të përshtatura për nevojat ushtarake, si mbrojtja e rrjeteve taktike dhe integrimi i IA-së në sistemet e komunikimit.

Përdorimi i "testbeds dhe simulimeve reale për trajnim praktik: Përdorimi i rrjeteve 5G/6G të stacionuara dhe "testbeds" për trajnime reale, duke simuluar skenarë ushtarakë si operacione "multidomain", lëvizje taktike *(p.sh., smartports dhe smartroads)* dhe komunikime në fushëbetejë. Trajnimi duhet të mbulojë menaxhimin e sigurisë "end-to-end", duke përfshirë mbrojtjen nga sulmet si DoS*(DenialofService)*, "spoofing" dhe "informacion disclosure" në aplikacione si V2X *(Vehicle-to-Everything) dhe ProSe (Proximity Services)*. Për teknologjinë 6G, integrimi i trajnimit me simulime "AI-driven" për të trajtuar kërcënime adversariale, si "poisoning" i të dhënave ose manipulim i modeleve të "machinelearning" në rrjete taktike autonome *("bubbles" taktike)*. Rekomandohet zhvillimi i programeve multinacionale pilote për co-zhvillim të sistemeve 5G/6G, duke përfshirë "interaksion" ushtarak-privat për të ndërtuar njohuri organizative dhe për të testuar vulnerabilitete në praktikë.

Trajnim në praktikat e sigurisë së komunikimeve dhe higjienës kibernetike: Promovimi i trajnimeve në përdorimin e kanaleve të enkriptuara, protokolleve të sigurt dhe raportimit të incidenteve për të minimizuar rreziqet e përgjimit në rrjetet 5G/6G. Kjo përfshin praktika në krijimin e fjalëkalimeve

të forta, shmangien e faqeve të pabesueshme dhe simulime real-world për të trajtuar kërcënime si IA në sulmet kibernetike ose siguria e pajisjeve IoT në operacionet ushtarake. Përditësimi i moduleve të trajnimit për të adresuar rreziqet emergjente, si integrimi i teknologjisë 5G në "smart seaports" *(p.sh., AGV – Automated Guided Vehicles)* dhe "smart roads" *(p.sh., platooning C-V2X)*, duke kryer analiza rreziku sistematike për çdo rast përdorimi.

Angazhimi në organizata standardizuese ndërkombëtare: Rritja e pranisë së industrisë në organet e standardeve si 3GPP, ITU dhe IEEE për të influencuar adoptimin e standardeve të besueshëm. Kjo përfshin kontribute të përbashkëta në ITU për standardet IMT-2030, duke integruar parime të sigurisë-by-design në specifikat globale të teknologjisë 6G. Promovimi i arkitekturave të hapura si "Open RAN" në "O-RAN Alliance" dhe "3GPP", duke bashkëpunuar për ndërfaqe të hapura, diversitet të furnitorëve dhe integrim të IA-së për siguri, duke synuar një arkitekturë "Day 0" për teknologjinë 6G. Kjo ndihmon në fleksibilitet dhe koekzistencë me teknologjinë 5G, duke zvogëluar fragmentimin dhe duke siguruar ndërveprueshmëri.

Bashkëpunimi ndërkombëtar është kyç për të shndërruar rreziqet e teknologjive 5G/6G në avantazhe strategjike, duke siguruar sovranitet teknologjik dhe aftësi për t'u përballur me vështirësi, për t'u rikuperuar pas goditjeve dhe për të vazhduar përpara, madje edhe duke u forcuar nga përvojat e vështira në kontekst gjeopolitik. Pa standarde të unifikuara, integrimi i këtyre rrjeteve në sistemet ushtarake mund të çojë në dobësi kritike, si ekspozim ndaj spiunazhit ose humbje kontrolli në operacione taktike. Harmonizimi përmes NATO-s, BE-së dhe ITU-së siguron ndërveprueshmëri, duke promovuar inovacionin dhe sigurinë kolektive, veçanërisht në aplikime si ISAC për zbulim të kërcënimeve dhe rrjetet autonome. Në fund, investimet në këto bashkëpunime, do të forcojnë mbrojtjen ndaj kërcënimeve emergjente, duke kërkuar veprime urgjente për tranzicionin drejt teknologjisë "6G" rreth vitit 2030.

Bibliografia:

1. NATO Science & Technology Reports – Security in 5G Military Use.
2. ITU Reportson 6G Standardization.
3. IEEE Paperson 5G/6G Network Security.
4. Brookings Institute – The Geopolitics of 5G.
5. MITRE ATT&CK – Framework for Threat Modeling.
6. Russell, Stuart J.; Norvig, Peter (2021). Artificial Intelligence: A Modern Approach (4th ed.). Hoboken: Pearson. fq.1-4. ISBN 978-0-1346-1099-3.
7. Grumbling, Emily; Horowitz, Mark, eds. (2019). Quantum Computing. ISBN 978-0-309-47970-7.

8. https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/.
9. https://www.ibm.com/think/topics/intrusion-detection-system.
10. Rose, Scott; Borchert, Oliver; Mitchell, Stu; Connelly, Sean. “Zero Trust Architecture” (PDF).
11. https://www.nsa.gov/Cybersecurity/.
12. NATO – NCIA: https://www.ncia.nato.int/; https://www.ncia.nato.int/newsroom/news.
13. NATO CCDCOE: https://ccdcoe.org/.
14. Cyber Security Global Alliance: https://www.csga-global.org/.
15. https://www.sto.nato.int/Pages/default.aspx (NATO Science&Tech. Org.).
16. https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/.
17. https://www.nsa.gov/Cybersecurity/.
18. Cyber Security and Information Systems Information Analysis Center (https://www.cisa.gov/).

Zbatimi i Inteligjencës Artificiale në planifikimin e operacioneve ushtarake

Nënkolonel Dashnor BETA
Oficer Shtabi/specialist/kërkues për Studime dhe Analizë Strategjike IKSHU

Trajtesë e shkurtuar

Çelësi i suksesit të një operacioni ushtarak qëndron në planifikimin e tij. Aktivitetet e planifikimit në NATO kryhen në përputhje me procesin e planifikimit të operacioneve (OPP) dhe zbatohen nga grupet e planifikimi të operacioneve (OPG). Ritmi i progresit teknologjik ka një ndikim të madh në mënyrën se si kryhet procesi i planifikimit në ushtri. Në këtë kontekst, përparimet në sistemet e sensorëve dhe Inteligjencën Artificiale (IA) luajnë një rol të madh. Ushtritë tashmë përdorin mjete të drejtuara nga IA që ndihmojnë hapat dhe fazat e ndryshme në procesin e planifikimit. Po kështu ushtritë ndajnë tashmë buxhete të konsiderueshme për të çuar përpara kërkimin dhe për të zhvilluar asete të IA, siç janë sistemet e automatizuara të armëve dhe asistentët e planifikimit të automatizuar. Megjithatë, një aplikimi i gjerë i kërkimit të IA-së dhe aseteve të saj ende nuk është i pragmatizuar.

Nga një perspektivë tjetër, IA në aspektin e planifikimit shihet shpesh si një mjet i mundshëm për të ndihmuar operatorët njerëzorë. Veçanërisht, përparimet në IA mund të çojnë në futjen e asistentëve të planifikimit, të pajisur me kapacitete të pakrahasueshme me ato të operatorëve njerëzorë. Këto zhvillime ndikojnë në OPP-në. Integrimi i IA në planifikimin ushtarak përfaqëson një ndryshim transformues në mënyrën se si konceptohet dhe ekzekutohet lufta. Ndërsa sot përballemi me kompleksitetet e konfliktit modern, IA shfaqet si një mjet i rëndësishëm që rrit vendimmarrjen strategjike dhe efikasitetin operacional. Të kuptuarit e IA në planifikimin ushtarak përfshin shqyrtimin e aftësive të saj në fusha të ndryshme, nga ndërgjegjësimi e vlerësimi i situatës deri te analizat parashikuese. Implikimet e shfrytëzimit të teknologjisë së IA shtrihen përtej avantazheve të thjeshta operacionale duke formësuar peizazhin e ardhshëm të strategjive të sigurisë e mbrojtjes.

Fjalë kyçe: planifikim operacionesh, Inteligjencë Artificiale, mjete planifikimi, vendimmarrje ushtarake, sistemet autonome/gjysmë të armëve, C2, mjete të drejtuara nga IA, algoritme.

Hyrje

Aktualisht sot një nga temat kryesore e literaturës bashkëkohore shkencore është aplikimi i AI në fusha të ndryshme të aktiviteteve të përditshme. IA duhet të shihet në kontekstin e inteligjencës njerëzore, pasi në fillimet e veta ishte ky modeli të cilin studiuesit u përpoqën të kopjonin. Inteligjenca njerëzore mund të ndahet në tre nivele: inteligjenca llogaritëse, perceptuese dhe njohëse (cognitive)[1]. Në fushën llogaritëse dhe perceptuese të inteligjencës kompjuterët priren të jenë më të shpejtë dhe më të plotë për shkak të shpejtësisë së tyre dhe algoritmeve të aplikuara. Të shkëlqesh në fushën njohëse është një sfidë më e madhe. Përdorimi më i thjeshtë i IA në ushtri është në sistemet autonome të armëve të cilat mund të zbulojnë e shkatërrojnë vetë armikun, pa mbikëqyrjen njerëzore. Sistemet gjysmë autonome të armëve kanë nevojë për një njeri, t'i urdhërojë dhe/ose autorizojë dhe të ofrojë mbikëqyrje gjithashtu. Një shembull i njohur i sistemit të armëve gjysmë autonome është versioni Block II i raketës Tomahawk nga vitet 1980 që përdori një IA fillestare për të lundruar të quajtur Dixhital Scene Matching Area Correlator[2].

Lloje të ndryshme robotësh, pajisje vetëdrejtuese, municione inteligjente janë vetëm disa shembuj që tregojnë se shume vende alokojnë buxhete kërkimi dhe zhvillimi të industrisë së mbrojtjes. Përveç këtyre, IA ka potencial të madh për të ofruar ndihmë në fazat e planifikimit dhe ekzekutimit të operacioneve ushtarake (OU).

Që nga v.1960, SHBA dhe B. Sovjetik (BS) punuan për automatizimin e sistemeve të fushëbetejës, duke krijuar sisteme kompjuterike për të ndihmuar komandim-kontrollin e forcave në operacione. Këto sisteme të hershme dështuan kryesisht sepse nuk u përmbush pritshmëria e ushtrisë për shkak të gjendjes së teknologjisë në atë kohë[3], por pas viteve '80 situata ndryshoi. Sistemet C2 në fushëbetejë avancuan dhe njohuritë e fituara ofruan një bazë solide për futjen e teknologjive të reja. Planifikimi i OU bashkëkohore po bëhet gjithnjë e më kompleks dhe duhet të marrë parasysh një numër të madh faktorësh. Komandim-kontrolli (C2) i avancuar ofron nivele të paprecedentë të dhënash për komandantët dhe shtabet. Aftësia e IA për të përfituar sa më shumë nga të dhënat e disponueshme në një kohë të shkurtër, mund të jetë zgjidhja për të hartuar plane më të detajuara mes këtij kompleksiteti. Zbulimi

[1] Imre Négyesi-Péter Török: The Relationship between Human Intelligence and Artificial Intelligence I. American Journal of Research, Education and Development, no. 2 (2020). 7-10.

[2] Geoffrey B. Irani-James P. Chirst: Image Processing for Tomahawk Scene Matching. Johns Hopkins APL Technical Digest, 15, no. 3 (1994). 250-264

[3] For more information see Elizabeth A. Stanley: Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System. Carlisle, Strategic Studies Institute, 1998; Imre Négyesi: A csapatvezetési rendszerek automatizálásának első eredményei az USA fegyveres erőinél I. Hadtudomány, E-szám (2015). 139-151

bashkëkohor për "makinat e të menduarit" është parë herët me optimizëm dhe kërkimi për të vazhdoi të arrinte qëllime më realiste. Në të njëjtën kohë me zhvillimet e algoritmeve dhe metodave të IA u zhvilluan edhe metodat e planifikimit ushtarak.

Në dekadat e fundit të shekullit XX, qasja holistike[4] (qasja e trajtimit të një gjëje si një tërësi e integruar - qasja ku sisteme të ndryshme shihen si tërësi dhe jo thjesht si koleksion pjesësh), ndryshoi proceset e planifikimit të operacioneve, duke kërkuar analiza dhe mënyra të reja të të menduarit për të zhvilluar plane. Me rritjen e sasisë së punës së nevojshme për të hartuar një plan të arsyeshëm, u konsiderua në planifikim përdorimi i aplikacioneve të sofistikuara kompjuterike. Disa programe kompjuterike të hershme të drejtuara nga IA u zhvilluan për të lehtësuar planifikimin e OU. Meqenëse kjo fushë kërkimore po përparon vazhdimisht dhe aplikimet ushtarake vlerësohen sekrete, materiali ofron një pamje të të dhënave aktuale nga burime të hapur bazuar në metodën e analizës së dokumenteve. Zbatimi i IA në planifikimin e OU është një nga funksionet kryesore të shtabeve ushtarake. Kompleksiteti në rritje i mjedisit bashkëkohor operacional kërkon një qasje të re për të kuptuar situatën dhe për të realizuar një plan të zbatueshëm. Pyetja kryesore është nëse IA në gjendjen aktuale mund të zbatohet në planifikimin e OU. Analizimi i kësaj çështje na jep një pasqyrë të kësaj mënyre të mundshme të rritjes së efektivitetit të grupeve të planifikimit, duke kontribuar në gjetjen e zgjidhjeve më efektive për problemet komplekse dhe gjithëpërfshirëse të shfaqura.

Kuptimi i IA-së në planifikimin ushtarak.

IA në planifikimin e OU përfshin zbatimin e teknologjive të kësaj inteligjence në funksion të rritjes së efikasitetit operacional, zhvillimit strategjik dhe proceset e vendimmarrjes brenda kornizave ushtarake. Ky integrim synon të përmirësojë efektivitetin e misioneve dhe të optimizojë ndarjen e burimeve, duke çuar në fund të fundit në rezultatet më të mira në OU të ndryshme. Përmes analizës së grupeve të mëdha të të dhënave, algoritmet e IA ndihmojnë planifikuesit ushtarakë të informohen në hartimin e strategjive. Këto teknologji analizojnë modelet me të dhënat historike të konfliktit, duke mundësuar parashikime më të sakta të skenarëve të ardhshëm. Përdorimi i IA në planifikimin ushtarak kontribuon në përgjigje më të shpejta e të adaptueshme ndaj kërcënimeve në zhvillim. Për më tepër, sistemet e IA mund të automatizojnë detyrat rutinë, duke i lejuar personelit ushtarak të përqendrohet në procese vendimmarrjeje komplekse, të cilat kërkojnë gjykim njerëzor. Kjo sinergji lehtëson një strategji ushtarake më kohezive, ku ekspertiza njerëzore dhe efikasiteti i makinerive punojnë në unison. Ndërsa organizatat ushtarake në të gjithë botën pranojnë teknologjitë e IA, të kuptuarit e implikimeve të saj në planifikimin ushtarak bëhet një faktor kritik. Ky kuptim do të formësojë jo

[4] Termi "holizëm" u shpik nga Jan Smuts në librin e tij "Holism and Evolution", viti 1926.

vetëm aftësitë operacionale, por edhe udhëzimet etike dhe metodat e trajnimit për personelin e ngarkuar me shfrytëzimin e këtyre inovacioneve.

Roli i IA-së në procesin e vendimmarrjes

Në planifikimin ushtarak IA përmirëson ndjeshëm procesin e vendimmarrjes duke ofruar njohuri të bazuara në të dhëna dhe në analiza parashikuese. Kjo teknologji u mundëson drejtuesve ushtarakë të informohen dhe të bëjnë zgjedhje bazuar në analizën gjithëpërfshirëse të të dhënave, duke përmirësuar ndërgjegjësimin për situatën dhe efikasitetin operacional. Përmes përpunimit të të dhënave në kohë reale, sistemet e IA-së mund të identifikojnë modele dhe trende që analistët njerëzorë mund t'i anashkalojnë. Kjo aftësi lejon vlerësim të shpejtë të skenarëve kompleks, dhe mundëson përgjigje më të shpejta ndaj kërcënimeve në zhvillim. Si rezultat, vendimmarrësit mund të vlerësojnë opsione dhe rezultate të shumta brenda pak sekondave, duke optimizuar planifikimin ne nivele taktik deri në atë strategjik. Për më tepër, IA në planifikimin ushtarak zvogëlon ngarkesën njohëse mbi personelin, duke i lejuar ata të përqendrohen në çështje të nivelit strategjik, në vend të përpilimit të të dhënave. Duke automatizuar analizat rutinë, IA lehtëson komunikimin më të qartë midis njësive ushtarake, dhe siguron që informacioni në kohë dhe i saktë të rrjedhë në të gjithë strukturën komanduese. Integrimi i teknologjive të IA-së në vendimmarrje transformon metodat tradicionale, duke nxitur një peizazh ushtarak më dinamik, më të shkathët dhe më të përgjegjshëm. Ndërsa IA vazhdon të evoluojë, roli i saj në planifikimin ushtarak mund të bëhet edhe më kritik në arritjen e suksesit operacional.

Pasqyra e planifikimit të operacioneve ushtarake

Planifikimi është një detyrë e domosdoshme e çdo organizate. Planifikimi i operacioneve është një aktivitet i kryer nga organizatat ushtarake në të tre nivelet e luftës.[5] Përmbajtja dhe detyrat e tij ndryshojnë në çdo nivel; një planëzim operacioni në nivel strategjik ndryshon nga planëzimi i operacionit në nivel taktik, kryesisht në fokusin e planifikimit. Në nivel taktik, fokusi i planifikimit është; përdorimi i trupave dhe mjeteve të disponueshme për arritjen e misionit të caktuar, ndërsa në nivelin strategjik fokusi kryesor është; identifikimi i mënyrave ushtarake për të arritur qëllimet politike. Lidhja midis nivelit strategjik dhe taktik sigurohet nga niveli operacional, i cili përkthen objektivat gjithëpërfshirëse të nivelit strategjik në objektiva të nivelit operacional dhe identifikon detyrat e ekzekutueshme për njësitë taktike të caktuara. Prandaj, në një proces planifikimi, nivelet strategjike dhe operacionale, dhe ato operacionale e taktike punojnë ngushtë për të hartuar një plan.

Metoda e planifikimit mund të jetë sekuenciale, paralele ose bashkëpunuese

[5] NATO Standardization Office: AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A, Version 2. 2019a.

varësisht kohës në dispozicion dhe shtabit që e zbatojnë atë[6]. Përveç kësaj, ekzistojnë dy filozofi kryesore përgjatë të cilave zhvillohen proceset e planifikimit dhe metodat e udhëheqjes. Njëra është qasja e stilit perëndimor, tjetra është ajo e stilit rus. Në stilin perëndimor, komandanti është një figurë qendrore, por ai ka një shtab për ta ndihmuar në vendimmarrje. Kjo metodë ngarkon shtabin me përgjegjësinë për të bërë vlerësime, rekomandime dhe për të zhvilluar kurse të ndryshme veprimi nga të cilat komandanti zgjedh më të përshtatshmin. NATO ofron një qasje të planifikimit e pranuar përgjithësisht dhe e vërtetuar shkencërisht që quhet Procesi i Planifikimit të Operacioneve (OPP). Ai përbëhet nga aktivitete kyçe si: fillimi i planifikimit, analiza e misionit, zhvillimi i kurseve së veprimit (KV), analiza e KV, vlerësimi dhe krahasimi i KV, vendimi i komandantit dhe jo më pak e rëndësishme, zhvillimi i planit. Këto aktivitete kanë shumë aktivitete të varura, të cilat duhet të realizohen për të arritur qëllimin e planifikimit[7].

Metodat e planifikimit në nivele të ndryshme të luftës ose të vendeve të ndryshme mund të ndryshojnë në ekzekutim, por logjika e planifikimit dhe e rezultatit përcaktohet nga kuadri i OPP, p.sh., Procesi i Planifikimit Taktik (PPT) në NATO për Forcat Tokësore (FT) është një proces i gatshëm për përdorim i projektuar për selinë taktike të NATO. Ai ndjek skemën e OPP pasi ka gjithashtu këto hapa kryesorë: marrja e misionit, analiza e misionit, zhvillimi i KV, analiza e KV, krahasimi i KV, vendimi i komandantit dhe urdhri, prodhimi, shpërndarja dhe tranzicioni. Ka disa dallime në emrat e hapave, por ideja është e njëjtë[8]. Procesi i Vendimmarrjes Ushtarake (PVU) që përdor ushtria e SHBA në thelb është i njëjtë. Planifikimi i nivelit operacional të NATO ka faza dhe emërtime të ndryshme nga OPP, por idetë kryesore nuk ndryshojnë: duhet të analizohet misioni, të zhvillohen KV dhe pas vendimit duhet të hartohet një plan. Megjithatë, ky proces i planifikimi dhe zbatimi i tij ka disa mangësi. Së pari, kuptimi i detyrës së komandës eprore, analiza e misionit është një proces që kërkon kohë në të cilin janë të angazhuar të gjithë ekspertët funksionalë të shtabit. Dështimi për të kuptuar problemin dhe misionin në mënyrë korrekte mund të çojë në zgjidhje të gabuara ose humbje kohe dhe rianalizim të situatës. Nëse komandanti nuk i miraton KV, shtabi duhet të punojë për kurse të reja, gjë që kërkon kohë dhe ndoshta kalon nën presionin e kohës. Po kështu, nëse ndonjë nga shefat në shtab ka mangësi në njohuri për fushën e vet, atëherë të metat e fshehura mund të prishin planifikimin që në fazat e hershme.

Ndërsa qasja e punës në grup (planifikim i stilit perëndimor) përpiqet të përfitojë nga njohuritë e përbashkëta të ekipit të planifikimit, rezultati mund të

[6] For more information, see NATO Standardization Office (2019a): op. cit. Chapter 2.
[7] NATO Standardization Office (2019a): op. cit. 4-1.
[8] NATO Standardization Office: APP-28 Tactical Planning for Land Forces, Edition A, Version 1. 2019b. 1-7.

mos jetë gjithmonë i pranueshëm. Shuma e njohurive të anëtarëve të shtabit është më shumë se njohuritë e vetëm të komandantit, por fërkimet, keqkuptimet midis shtabit dhe keqkuptimet rreth misionit mund të çojnë lehtësisht në gabime dhe të rrezikojnë përpjekjen. Procesin aktual të vendimmarrjes ruse ne nuk e dimë në detaje, por ka disa mendime se si ai duket. Në këtë qasje komandanti vendos se si dëshiron të përmbushë misionin, përcakton kursin e veprimit, ndërsa shtabi ndihmon vetëm në zhvillimin e tij në detaje. Është një lloj vlerësimi i komandantit, në të cilin ai harton planin pasi analizon situatën dhe më vonë kryet zbulimi i terrenit për të verifikuar qëndrueshmërinë e planit. Paralelisht me zbulimin, shtabi fillon procesin për të verifikuar planin dhe për ta rregulluar atë nëse është e mundur. Pasi përfundon kjo lëshohet urdhri tek vartësve. Ky proces është mjaft i drejtpërdrejtë, konciz dhe kërkon më pak kohë se ai perëndimor[9]. Duke kuptuar kohën e shkurtër për vendimmarrjen e stilit rus dhe duke u mbështetur në mësimet e nxjerra nga angazhimet e dekadave të mëparshme, mendimtarë ushtarakë të SHBA dhe NATO nxorën metoda për të shkurtuar proceset e planifikimit. PPT të NATO për FT sugjeron që nën presionin e kohës, detajet e kurseve të veprimit duhet të reduktohen me qëllim analizimin dhe krahasimin më të shpejtë të tyre[10]. SHBA propozon disa zgjidhje në mjedisin me kohë të kufizuar, në PVU të FT, ku njëra është metoda që vetëm një kurs veprimi zhvillohet nga një ekip i vogël i drejtuar nga komandanti - shumë e ngjashme me atë ruse[11]. Duke i studiuar hollësisht këto procese planifikimi, mund të vlerësohet se ekzistojnë tre hapa që kërkojnë kohë të konsiderueshme: analiza e misionit, zhvillimi i kurseve të veprimit dhe analiza e tyre.

Këta hapa përfshijnë disa procese të tjera që duhet të kryhen për të hartuar një plan të mirë dhe të ekzekutueshëm. Pjesa më e qenësishme e analizës së misionit është analiza e mjedisit operacional. Këtu duhet të merren parasysh faktorët e armikut, terreni dhe mjedisi, të cilat kërkojnë analiza të plota dhe kohë. Analiza e KV zakonisht përmban një lloj luftimi, d.m.th., të gjitha veprimet që duhet të ndërmerren gjatë ekzekutimit duhet të modelohen për të identifikuar mangësitë ose përplasjet e mundshme. Mjetet ekzistuese të IA në planifikimin e OU janë shumë përtej qëllimit të kësaj pune për të përcaktuar se çfarë është IA. Ka disa qasje për të kuptuar vetë thelbin e IA nga këndvështrime të ndryshme, si arsyetimi apo sjellja[12]. Lidhur me këtë, IA konsiderohet një degë e shkencës kompjuterike, e cila merret me automatizimin e aktiviteteve si përpunimi i të dhënave, zgjidhja e problemeve dhe vendimmarrja. Si e tillë, AI mund të konceptohet vetëm në një mjedis digjital.

[9] Roger N. McDermott- Charles K. Bartles: The Russian Military Decision-Making Process and Automated Command and Control. Hamburg, German Institute for Defence and Strategic Studies, 2020. 29-32.

[10] NATO Standardization Office (2019b): op. cit. F-1-F-3.

[11] Department of the Army: FM 6-0 Commander and Staff Organization and Operations. 2014. 9-44-9-46.

[12] Stuart Russel- Peter Norvig: Artificial Intelligence. Englewood Cliffs, Prentice Hall, 1995. 4-5

Vetë origjina e IA mund të lidhet me aktivitetet ushtarake. Në fazat e hershme, financimi ushtarak nxiti kërkimin me shpresën e arritjes së teknologjisë së fundit për të ruajtur epërsinë ndaj armikut. Sikurse është përmendur, sistemet gjysmë autonome dhe autonome janë fusha me prioritet të lartë të kërkimit të IA. Shumica e fushave të kërkimit të IA mund të lidhen me disa zbatueshmëri ushtarake. Kërkimi fillestar i projekteve kërkimore të IA u zhvillua në laboratorë dhe universitete kërkimore, të financuara pjesërisht nga institucione qeveritare dhe ushtria siguronte një pjesë të konsiderueshme të financimit, që ishte kryesisht për projektet në aplikime në jetën reale në një afat të arsyeshëm të shkurtër. Kur kërkesat harduerike të një IA të mundshme, universale, filluan të rriten, u bënë përpjekje për të ndërtuar një gjeneratë të re kompjuterësh, në gjendje të punojnë paralelisht me probleme të ndryshme. Këto sisteme të reja me shumë procesorë u ndërtuan posaçërisht për aplikimin e IA dhe kontribuuan shumë në kërkim dhe kjo bashkë me përparimet në teknologjinë kompjuterike duket se e afruan arritjen e IA të vërtetë.

Qëllimi përfundimtar i kërkimit të IA është një kompjuter që mund të veprojë e të mendojë të paktën po aq mirë sa një njeri. Pothuajse është konsensuale që ky qëllim nuk është i arritshëm me mundësitë aktuale[13]. Aktualisht në epokën e re të konkurrencës të fuqive të mëdha, SHBA, Kina dhe BE po investojnë miliarda dollarë në kërkimin e IA[14] me fokus kryesor në fushën industriale dhe ekonomike, ku dhe ushtria ka një pjesë në të. Shpesh ushtria është përfitues i teknologjive të zhvilluara për përdorim civil dhe IA mund të jetë po ashtu një shembull i mirë për këtë. Planifikimi i OU ushqehet me informacionin e duhur për të bërë një plan të guximshëm e të zbatueshëm. Prandaj, fushat kryesore për shfrytëzimin e IA janë aktivitetet e grumbullimit të informacionit, e quajtur Inteligjenca, Mbikëqyrja dhe Zbulimi (ISR). Kur nevojiten efekte të dëshiruara, duhet të konsiderohet dhe përdorimi i sistemit të mbështetur nga IA në fushat e operacioneve të hapësirës kibernetike dhe të operacioneve të informacionit. Sistemet e C2 të mbështetur nga IA mund të japin një kontribut të paçmuar për suksesin në operacion kur fillon përgatita për ekzekutim ose ekzekutimi i planit[15].

Forcimi i sektorit privat ishte impulsi i ri i nevojshëm i IA sidomos në SHBA dhe në perëndim ku aktorë/lojtarë me ndikim në industri arritën nivele të reja në kërkime e progres gjë që ushtria u përpoq të përdorte. Disa kompani private bashkëpunuan me ushtrinë e SHBA, veçanërisht Google, ekspertiza e së cilës ishte parësore në ngritjen e të ashtuquajturit Ekip i Ndërfunksionit Algorithmic Warfare të Departamentit të Mbrojtjes, ose Projekti Maven, qëllimi

[13] Nils J. Nilsson: The Quest for Artificial Intelligence. New York, Cambridge University Press, 2010

[14] Neil Savage: The Race to the Top among the World's Leaders in AI. Nature, 10 December 2020. S102-S104.

[15] Daniel S. Hoadley-Kelley M. Sayler: AI and National Security. Washington, Congressional Research Service, 2020. 9-16

i të cilit ishte të zhvillonte një sistem të drejtuar nga IA që mund të ndihmonte në përpjekjet e inteligjencës terroriste dhe agjentëve ushtarakë. Fokusi kryesor ishte përpunimi, shfrytëzimi e shpërndarja e pamjeve dhe e videove të lëvizjeve, të bëra nga sistemet ajrore pa pilot të cilat ishin në gjendje të zbulonin dhe klasifikonin objekte e të jepnin sinjale për raste specifike[16].

Projekti Maven ishte një sukses sepse ndihmoi në identifikimin e kryengritësve dhe terroristëve të mundshëm të ISIS në Irak e Siri. Google e braktisi projektin për shkak të shqetësimeve të punonjësve të saj në lidhje me etikën e përdorimit ushtarak të IA. Disa kompani të mëdha private të SHBA e ndoqën shembullin dhe deklaruan se nuk miratonin aplikimin ushtarak të IA. Kompanitë rivale të SHBA në Kinë, nuk e bënë një gjë të tillë, pasi mundet që ky vend do të fitojë më shumë nga aplikimi i IA në fushën ushtarake. Por nga ana tjetër algoritmet e njohjes së fytyrës të aplikuara nga Kina për të kontrolluar popullsinë patën një diskutim në nivel etik. Njohja e fytyrës për identifikimin e luftëtarëve të mundshëm armik nga ana tjetër ka përfitime të paçmueshme[17].

Projekti i Programit Strategjik të Kompjuterisë Strategjike të SHBA dha një kontribut të madh në kërkimin e IA, në valën e re të kërkimeve të IA që filloi në v.'80. Projekti tjetër "Përpunimi i gjuhës natyrore", u zhvillua në SHBA rezultoi me një softuer të përdorshëm për njohjen e të folurit[18] dhe shënoi arritje të mëdha. Ky projekt u avancua nga një kompani private kineze me bazë në SHBA duke mundësuar njohje efikase të të folurit. Kjo mundësoi analizimin e një sasie të madhe komunikimi të radiove armike dhe regjistrimeve të thirrjeve telefonike për të marrë informacione të rëndësishme operacionale ose për të identifikuar persona të rëndësishëm. Të gjitha këto aplikacione mund të shfrytëzohen nga njësi të inteligjencës ushtarake në çdo shtab.

Grumbullimi i informacionit dhe analiza e të dhënave

Grumbullimi i informacionit dhe analiza e të dhënave përfshijnë mbledhjen dhe shqyrtimin sistematik të informacionit për të përmirësuar planifikimin ushtarak dhe efektivitetin operacional. Teknologjitë e IA e lehtësojnë këtë proces duke përpunuar sasi të mëdha të dhënash nga burime të ndryshme, përfshi imazhet satelitore, mediat sociale e rrjete sensorësh. IA nëpërmjet algoritmeve të përparuara mund të identifikojë modele dhe anomali në të dhëna që analistët njerëzorë mund t'i anashkalojnë. Kjo aftësi u lejon drejtuesve ushtarakë të kenë informacion kritik mbi lëvizjet kundërshtare, kërcënimet e mundshme etj., duke mundësuar vendimmarrje më të informuara. Po kështu, IA rrit shpejtësinë me të cilën planëzuesit ushtarakë mund t'u përgjigjen situatave në zhvillim. Analiza e të dhënave në kohë reale mundëson përshtatje të shpejta

[16] Pentagon: DoD Memorandum. 2017.
[17] Forrest E. Morgan et al.: Military Applications of Artificial Intelligence. Santa Monica, RAND Corporation, 2020. 25-26.
[18] Nilsson (2010): op. cit. 370-371.

të strategjive, duke siguruar që forcat të operojnë shpejt në mjedise dinamike. Integrimi i IA në planifikimin ushtarak, çon në grumbullim informacionit më efikas dhe më të saktë. Por, pavarësisht këtyre avantazheve, mbetet sfidë interpretimi i të dhënave dhe sigurimi i besueshmërisë së burimeve të informacionit. Prandaj, kërkimet e vazhdueshme mbi analizën e të dhënave të drejtuara nga IA janë jetike për përmirësimin e efikasitetit të operacioneve të inteligjencës ushtarake në skenarë kompleksë.

Integrimi i IA-së me sistemet ekzistuese ushtarake

Integrimi i IA-së në sistemet ushtarake ekzistuese kupton krijimin e një marrëdhënieje sinergjike mes teknologjive të reja dhe kornizave tradicionale operacionale. Ky integrim është jetik për rritjen e efektivitetit të strategjive ushtarake, duke siguruar që aftësitë e IA në planifikimin ushtarak të shfrytëzohen plotësisht. Përputhshmëria me teknologjitë aktuale paraqitet si mundësi dhe si sfidë gjithashtu. Shumë sisteme ushtarake kanë komponentë të trashëguar që mund të mos ndërveprojnë lehtësisht me zgjidhjet e drejtuara nga IA. Përmirësimi i këtyre sistemeve është i nevojshëm, por shpesh paraqet pengesa logjistike e financiare që mund të vonojnë zbatimin. Sfidat e integrimit përfshijnë jo vetëm mospërputhjet teknologjike, por edhe çështjet e ndërveprimit mes forcave aleate. Vendosja e standardeve dhe protokolleve për ndarjen e të dhënave është thelbësore për të siguruar që vendimet e drejtuara nga IA të mund të ekzekutohen shpejt e me besueshmëri në nivele të ndryshme ushtarake dhe vende aleate, duke ruajtur kështu një strategji operacionale kohezive. Pra, integrimi i suksesshëm kërkon një qasje sistematike, përfshi programet e trajnimit dhe faktorët njerëzorë. Kjo siguron që personeli të jetë i njohur për të përdorur IA në mënyrë efektive brenda sistemeve ekzistuese ushtarake dhe të optimizojnë potencialin e IA-së në planifikimin ushtarak.

Pajtueshmëria me teknologjitë aktuale

Integrimi i IA-së në planifikimin ushtarak kërkon një pajtueshmëri të përsosur me teknologjitë ekzistuese. Meqenëse forcat ushtarake mbështeten në një gamë sistemesh të sofistikuara, zbatimi i suksesshëm i IA varet nga aftësia e saj për të punuar në mënyrë kohezive brenda këtyre kornizave. Sfidat e pajtueshmërisë përfshijnë çështje që lidhen me sistemet e trashëguara, të cilat mund të mos mbështesin algoritmet e avancuara apo aftësitë e përpunimit të të dhënave që kërkon IA. Pajisjet dhe softuerët ushtarakë duhet t'i nënshtrohen përmirësimeve dhe zëvendësimeve për të lehtësuar këtë integrim, i cili mund të jetë i kushtueshëm dhe të kërkojë kohë.

Disa konsideratat kryesore për pajtueshmërinë përfshijnë: vlerësimin e ndërveprimit me sistemet aktuale të C2; sigurimin e harmonizimit të formateve të të dhënave e protokolleve të komunikimit; vlerësimin e shkallëzueshmërisë të mjeteve të IA-së dhe të sistemeve të trashëguara. Pajtueshmëria efektive siguron që IA të mund të rrisë efikasitetin dhe efektivitetin operacional pa dëmtuar

funksionalitetin e teknologjive ekzistuese ushtarake, harmonizim i cili është themelor për arritjen e avantazheve strategjike në operacionet ushtarake.

Sfidat e integrimit

Integrimi i IA në planifikimin ushtarak paraqet sfida të shumta që duhen adresuar për të shfrytëzuar plotësisht potencialin e saj. Këto sfida rrjedhin nga aspektet teknologjike dhe nga ato operacionale, duke ndikuar në efikasitetin e zbatimit të IA. Një sfidë kryesore është përputhshmëria e sistemeve të IA me infrastrukturën ekzistuese ushtarake. Shumë teknologji aktuale mund të mos kenë fleksibilitetin e nevojshëm për integrim të përsosur, duke penguar vendosjen efektive të aplikacioneve të IA. Përshtatja e sistemeve të vjetra për të punuar me aftësitë e përparuara të IA shpesh kërkon investime të konsiderueshme. Për më tepër, ndërveprimi mes degëve të ndryshme ushtarake paraqet një pengesë tjetër. Standardet dhe protokollet e ndryshme të përdorura në të gjitha shërbimet mund ta ndërlikojnë procesin e integrimit, duke çuar në joefikasitet dhe rreziqe operacionale. Sigurimi i komunikimit koheziv midis sistemeve të IA dhe operatorëve njerëzorë është jetik për integrim të suksesshëm. Po kështu ka çështje që lidhen me cilësinë dhe menaxhimin e të dhënave. IA mbështetet shumë në grupe të dhënash të sakta dhe të gjera, dhe çdo mangësi mund të kufizojë performancën. Vendosja e kornizave të forta të mënyrës së administrimit të të dhënave është thelbësore për të mbështetur IA-në në planifikimin ushtarak në mënyrë efektive.

Siguria kibernetike dhe trajnimi i personelit për përdorimin e IA në OU

Integrimi i IA brenda OU ka implikime të thella për sigurinë kibernetike. Teknologjitë e IA rrisin aftësinë për të zbuluar dhe për t'iu përgjigjur kërcënimeve kibernetike në kohë reale. Kjo aftësi është thelbësore, pasi sistemet ushtarake bëhen gjithnjë e më të ndërlidhura dhe të varura nga infrastruktura digjitale. IA mund të analizojë sasi të mëdha të dhënash me shpejtësi përtej kapacitetit njerëzor, duke identifikuar modele dhe anomali që tregojnë ndërhyrje kibernetike. Duke shfrytëzuar algoritmet e të mësuarit automatik, personeli ushtarak mund të parashikojë shkelje të mundshme të sigurisë dhe të zbatojë kundërmasa në mënyrë proaktive, duke minimizuar rreziqet për integritetin operacional. Megjithatë, përdorimi i IA gjithashtu sjell dobësi të reja. Sulmet kundërshtare ndaj sistemeve të IA mund të çojnë në dezinformata, gjë që mundëson gjykime të gabuara në skenarë të ndryshëm. Sigurimi i masave të forta të sigurisë rreth teknologjive të IA është i domosdoshëm për të mbrojtur planet dhe operacionet e ndjeshme ushtarake dhe kjo kërkon që sinergjia midis IA dhe sigurisë kibernetike të jetë thelbësore. *Trajnimi i personelit* për përdorimin e IA kërkon një qasje gjithëpërfshirëse në kuptimin teorik, zbatimin praktik dhe zhvillimin e vazhdueshëm të aftësive. Personeli duhet të njohë teknologjitë specifike të IA që po vendosen, përfshi aftësitë dhe kufizimet e tyre, për t›i integruar ato në mënyrë efektive në OU.

Trajnimi praktik të mund të përfshijnë simulime të cilat u lejojnë përdoruesve të mësojnë se si IA ndihmon në planifikimin ushtarak, duke i mundësuar ata të marrin vendime të informuara shpejt dhe saktë. Ky trajnim është thelbësor për ndërtimin e besimit në përdorimin e këtyre sistemeve. Edukimi dhe zhvillimi i vazhdueshëm janë thelbësorë në kohën që teknologjia e IA evoluon me shpejtësi. Kurset online dhe pjesëmarrja në ushtrime të fokusuara në IA ndihmojnë në ruajtjen e kompetencës në përdorimin e IA në planifikimin ushtarak. Ky investim siguron shfrytëzimin në mënyrë efektive të njohurive të drejtuara nga IA dhe mbështet gatishmërinë operacionale. Së fundmi, bashkëpunimi midis degëve të ndryshme ushtarake edhe me partnerët e sektorit privat rrit iniciativat e trajnimit, pasi ndan njohuritë dhe praktikat më të mira, kupton më mirë zbatimet shumëplanëshe të IA në mjediset ushtarake dhe mundëson një zbatim sa më efektiv të IA-së në planifikimin ushtarak.

Efekti i mundshëm i IA në planifikimin e operacioneve të ardhshme

E ardhmja e planifikimit të OU vendoset sot ndërsa procesi i aplikimit të IA në procesin e planifikimit vijon të përparoj në vende të ndryshme. Në ditët e sotme, ushtria e SHBA po punon për sistemet mbështetëse të C2, siç është C2 i përbashkët i gjithë domenit (JADC2), i cili synon të centralizojë planifikimin dhe ekzekutimin e operacioneve në tokë, ajër, det, hapësirë dhe hapësirë kibernetike. Të gjithë fuqitë e mëdha ushtarake, si SHBA, Kina, Rusia vlerësojnë se në vendimmarrje duhet të përdoret potenciali i IA. Kërkimi, zhvillimi dhe testimi bashkëkohor në progres në terren po hapin rrugën për vendimmarrjen inteligjente dhe të përmirësuar. Edhe pse kërkesat për aktivizimin e sistemeve të IA mund të ndryshojnë në varësi të fushës së aplikimit, vendit, krahut ushtarak që e zbaton atë, mund të identifikohen disa kritere të përbashkëta. *Së pari,* IA mbështet planifikimin i cili duhet të jetë në gjendje të kryejë detyrën e vet për analizimin e të dhënave, apo kurset e veprimit në kohë reale. *Së dyti,* informacioni përfundimtar duhet të jetë i këmbyeshëm me sistemet e tjera të IA, dhe me planifikuesit njerëzorë, kështu që rezultati duhet të jetë i qartë, konciz dhe i kuptueshëm për planifikuesit qofshin këta dhe pa njohuri të veçanta në teknologjitë e informacionit. *Së treti,* procesi që zbaton IA duhet të jetë transparent për t'i bërë planifikuesit njerëzorë të kuptojnë mënyrën se si i ka marrë vendimet. Kriteri më i rëndësishëm është që: makina duhet të jetë në gjendje të shpjegojë mënyrën e saj të të menduarit.

Mjedisi operacional është kompleks nga vetë natyra e tij dhe sfidat e reja e bëjnë atë më komplekse në vazhdimësi. IA në gjendjen e saj aktuale funksionon në mënyrë të ngjashme me njohjen njerëzore: ndan problemet komplekse në nën probleme të zgjidhshme. Natyra kaotike e mjedisit operacional, mbushur me sisteme komplekse adaptive e bën pothuajse të pamundur parashikimin se çfarë do të ndodhë më pas, por të paktën ka përpjekje për këtë. Marrja në konsideratë e planifikimit të OU, analiza e misionit, zhvillimi i KV dhe analiza

e tyre janë hapat që kërkojnë shumë kohë, por ato mund të përshpejtohen dhe përmirësohen duke aplikuar IA. Gjatë analizës së misionit, pavarësisht se për çfarë niveli operacioni diskutohet, hapi më i rëndësishëm është të kuptuarit e mjedisit operacional. NATO në nivele të ndryshme ka emërtime të ndryshme si; përgatitja e mjedisit operacional të përbashkët të zbulimit, përgatitja zbuluese e luftimit. Kjo analizë ofron informacione për kundërshtarin dhe terrenin që duhet të merren parasysh gjatë përgatitjes së planit. Janë dy faktorë që kufizojnë analizën: *informacioni* dhe koha në dispozicion. Sasia e të dhënave të grumbulluara në një mjedis operacional bashkëkohor është aq e madhe sa analistët njerëzorë nuk janë në gjendje t'i përballojnë ato në kohë. Sistemet e bazuar në IA do të jenë gjithnjë e më kompetentë në përkthimin e të dhënave përkatëse në informacion, duke lehtësuar në këtë mënyrë vendimmarrjen në kohë. Hartimi i KV është një proces që ndërtohet mbi informacionin e marrë gjatë analizës së misionit. IA ka treguar aftësinë e saj për të përpunuar të dhënat të besueshme dhe shpejt, kështu që aplikimi i një kursi veprimi të drejtuar nga IA është një mundësi.

Ekspertët e sistemeve të sofistikuara duhet të zgjedhin informacionin në mënyrë që të shmangin mbingarkimin e planifikuesve njerëzorë, kapaciteti njohës i të cilëve duhet të fokusohet diku tjetër. Informacioni i detajuar i terrenit në jetën reale mund të përdoret për të krijuar modele 3D dhe me mjetet e IA mund të përdoren për të planifikuar KV, duke ofruar ndihmë në përcaktimin e drejtimit të zjarrit etj. Zbatimi i një data bazë të angazhimeve, manovrave dhe ushtrimeve të mëparshme mund të fuqizojë një mjet mbështetës vendimesh për të sugjeruar KV në varësi të shembujve të mëparshëm të suksesshëm. Analiza e KV përbëhet nga disa teste, në të cilat "luhen" kundër njëri-tjetrit drejtimet e ndryshme të veprimeve të forcave tona dhe atyre armike. Një metodë e pranuar për analizë është loja luftarake, një proces që është "një simulim i një operacioni ushtarak në të cilin pjesëmarrësit kërkojnë të arrijnë një objektiv të caktuar, bazuar në burimet dhe kufizimet e paracaktuara"[19]. Në varësi të madhësisë dhe zonës së operacionit, këto simulime kërkojnë kohë. Ngjashëm me IA që mund të aplikohet për të krijuar KV, analiza d.m.th. procesi i lojës luftarake mund të përshpejtohet duke përdorur sisteme të IA të dizajnuara për këtë qëllim.

Dihet që koha është faktor i rëndësishëm në planifikim. Në mjedisin operacional me teknologji të lartë, çdo moment është i çmuar dhe shpejtësia e vendimeve mund të jetë çelës suksesi. Kjo është tema kryesore e luftës së parashikuar në qendër të vendimit[20]. Kur informacioni është i disponueshëm,

[19] NATO Standardization Office: AAP-06 NATO Glossary of Terms and Definitions (English and French) Edition 2021. 137.

[20] Bryan Clark et al.: Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations. Washington, Center for Strategic and Budgetary Assessments, 2020. 17–25.

koha për përpunimin e tij dhe për të prodhuar urdhra për vartësit është e çmuar. Kushdo që mund të zvogëlojë kohën midis hapave të ciklit të vendimit vëzhgo-oriento-vendos-vepro do të ketë përparësi ndaj kundërshtarit. IA mund të ndihmojë në nxjerrjen në pah të aseteve të disponueshme në kohë të shkurtër, duke krijuar zgjidhje për lëvizjet e trupave, misionet e zjarrit, të përshpejtojë llogaritjet e fuqisë luftarake dhe mund të bëjë rekomandime për lëvizjet e trupave. FA të SHBA aktualisht mendojnë idenë e operacioneve me shumë domene. Çelësi i konceptit është efekte të shumta nga fusha të ndryshme të përqendruara në kohë dhe hapësirë për të mbingarkuar e prishur sistemet e C2 të kundërshtarit. Planifikimi i këtyre efekteve dhe gjetja e asaj pike në kohë kur këto efekte duhet të grumbullohen kundër kundërshtarit është një proces kaq delikat saqë kërkon ndihmë nga sistemet e mbështetjes së vendimeve nga IA. Instalimi dhe inkorporimi i sistemeve të IA jo vetëm që ndihmon në përshpejtimin e ciklit të vendimit, por disa e shohin atë edhe si një mënyrë për të reduktuar numrin e personelit ushtarak në shtabe. Ndërkohë që përdorimi i IA i shpejton proceset, aktualisht kërkohen specialistë për mirëmbajtjen dhe trajtimin e tij, gjë që mund të nënkuptojë një rritje të lehtë të personelit, pasi një shtab duhet të jetë i përgatitur për të përmbushur misionin pa IA, kështu që specialistët ekzistues nuk duhet të hiqen nga lista.

Një kërkesë tjetër për llojet e ndryshme të AI është energjia elektrike. Kompjuterët që përdorin këto aplikacione të rënda për llogaritje kërkojnë sasi të madhe energjie elektrike që nuk mund të sigurohet gjithmonë në terren. Në të ardhmen e afërt, vlerësohet se niveli operacional e strategjik ka më shumë gjasa të përdorin mjete të IA, krahasuar me ato të nivelit taktik për shkak të këtij kufizimi. Përmirësimet në akumulatorë dhe teknologjia kuantike mund të ndihmojnë në kapërcimin e këtij kufizimi. Një zgjidhje tjetër mund të jetë përdorimi i mjeteve të IA të vendosura në një vendndodhje të largët dhe transferimi i të dhënave, por kjo kërkon komunikime të mbrojtura të vazhdueshme e të besueshme dhe vlerësohet se arritja e kësaj është një sfidë e vështirë.

Megjithatë përdorimi i IA ka disa pengesa të nënkuptuara. Duke lejuar që IA të zgjedhë të dhënat dhe të prodhojë informacion, askush nuk mund të garantohet se të dhëna të rëndësishme janë lënë jashtë. Një zgjidhje mund të jetë inteligjenca artificiale e shpjegueshme, pra operatorët mund të ndjekin arsyetimin logjik që ka çuar makineritë në vendimmarrje. IA e këtij lloji është ende në zhvillim e sipër[21]. Nga ana tjetër, është faktori njerëzor. Është e diskutueshme nëse një oficer, një shtab apo një komandant do të pranonte rekomandimet ose faktet nga një IA nëse nuk kuptojnë se cilat janë metodat me të cilat është siguruar rekomandimi dhe në cilat fakte është bazuar. Kërkimet aktuale sugjerojnë një besim relativisht të lartë në algoritme për të marrë

[21] Sherrill Lingel et al.: Joint All-Domain C2 for Modern Warfare. Santa Monica, RAND Corporation, 2020. 44-45.

këshilla kur një detyrë bëhet e vështirë[22]. Kjo nënkupton se puna e shtabit ushtarak perëndimor që aktualisht bazohet në punën bashkëpunuese mund të jetë e njëanshme kur IA hyn në lojë. Po kështu besimi në IA do të varet nga përvojat personale gjatë trajnimeve dhe operacioneve. Nëse nuk ka besim mes njeriut dhe IA, atëherë kjo do të rrezikonte misionin dhe jetën e njerëzve. Zhvillimi dhe implementimi i IA ngre disa pyetje të tjera. Aktualisht nuk ka asnjë rregullore ligjore ndërkombëtare që përcakton kufijtë e IA. Zbatimi i rregulloreve të pranuara globalisht mund të jetë po ashtu një sfidë për një IA, metodat e punës dhe motivet e të cilit pas vendimeve nuk janë mjaft të qarta[23].

Trendet e ardhshme të IA-së në planifikimin ushtarak

Përparimet në të mësuarit automatik pritet të revolucionarizojnë IA në planifikimin ushtarak. Algoritmet e përmirësuara po mundësojnë analiza parashikuese më të sakta, duke përmirësuar aftësitë e vlerësimit të kërcënimeve. Ky evolucion u lejon drejtuesve ushtarakë të parashikojnë konflikte të mundshme dhe optimizojnë shpërndarjen efikase të burimeve. Për më tepër, integrimi në rritje i teknologjive të IA mund të riformësojë dinamikën gjeopolitike. Vendet që investojnë në IA për aplikime ushtarake mund të fitojnë avantazhe të konsiderueshme strategjike. Kjo mund të çojë në një garë armatimi të përqendruar rreth aftësive të IA, duke ndikuar në strukturat globale të fuqisë dhe aleancat. Ndërsa sistemet e IA bëhen më të sofistikuara, bashkëpunimi mes sektorëve ushtarakë, akademikë dhe privatë bëhet më i domosdoshëm. Përpjekjet e përbashkëta mund të lehtësojnë zhvillimin e mjeteve të sigurta të IA, të adaptueshme dhe të harmonizuara etikisht. Kjo qasje kolektive është thelbësore për të siguruar që IA në planifikimin ushtarak të përfitojë kornizat ndërkombëtare të sigurisë, duke adresuar dhe shqetësimet etike.

Përfundime

- Përvojat e kaluara tregojnë se gjithmonë ka pasur pritshmëri të mëdha në lidhje me ndikimin e mundshëm të përmirësimeve teknologjike, por teknologjia aktuale zakonisht ka mbetur prapa në përmbushjen e këtyre pritshmërive.
- Ekziston një rrezik potencial në mbivlerësimin e aftësive të aseteve të disponueshme të IA. Teknologjitë aktuale të IA nuk përfshijnë arsyetim të nivelit të lartë dhe nuk mendojnë, nuk arrijnë në konkluzione që lidhet me kuptimin e gjuhës ose logjikës që njerëzit janë të aftë të bëjnë, nuk janë në gjendje të arsyetojnë në mënyrë abstrakte për situatat e jetës reale, por ata

[22] Eric Bogert et al.: Humans Rely more on Algorithms than Social Influence as a Task Becomes more Difficult. Nature Scientific Reports, 11, no. 8028 (2021)

[23] For more on legal and ethical issues see Imre Négyesi: A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. Honvédségi Szemle, 149, no. 1 (2021). 133-144; James Butcher-Irakli Beridze: What is the State of Artificial Intelligence Governance Globally? The RUSI Journal, 164, no. 5-6 (2019). 88-96.

shkëlqejnë në gjetjen e modeleve dhe përpunimin e të dhënave[24].

- Planifikimi i operacioneve duhet të përshpejtohet, duhet të bëhet më i plotë dhe kjo do të mund të arrihet duke përfshirë zgjidhjet më të fundit të inteligjencës artificiale në të ardhmen duke shfrytëzuar aftësitë ekzistuese e të provuara si çelës për aplikim të suksesshëm në planifikim.
- Ushtria ka qenë gjithmonë nxitës dhe përfitues i kërkimit të IA dhe ende është ndër përkrahësit kryesorë të tij në të gjithë botën. Injorimi i IA do të thotë t'i japësh dorën kundërshtarit cilido qoftë ai. Ushtritë kryesore në botë: SHBA, Rusia dhe Kina po investojnë shumë në kërkimet ushtarake të IA sidomos në aplikimin e saj në drejtim të C2.
- IA në gjendjen aktuale nuk është ende në gjendje të formulojë plane ushtarake dhe pse është shumë i dobishëm në përshpejtimin e nënproceseve të ndryshme.
- Planifikimi i operacioneve të NATO mbështetet në analiza të ndryshme që kërkojnë shumë kohë kur planifikohen operacione në shkallë të gjerë, sidomos planifikimi i reagimit ndaj krizës mund të marrë muaj dhe javë derisa të formulohet një plan në nivel strategjik dhe operacional.
- Futja gjerësisht e IA në procesin e planifikimit kërkon kompjuterë më të avancuar, teknologji të besueshme dhe të sigurt dhe metoda të lidhjes në distanca të gjata me shpejtësi të lartë.
- Hapat e procesit të planifikimit të operacioneve kanë detyra që mund të lehtësohen me ndihmën e mjeteve mbështetëse të bazuara në IA. Disa nga këto mjete janë në përdorim ose në testim, disa janë në format konceptual ose në zhvillim, por ndikimi i tyre nuk mund të neglizhohet.
- Shtabet duhet të trajnohet tërësisht për të adoptuar mentalitetin e kërkuar për të punuar me IA në organizatat e mundshme hibride njeri-kompjuter të së ardhmes.

Bibliografia:

1. Imre Négyesi-Péter Török: The Relationship between Human Intelligence and Artificial Intelligence I. American Journal of Research, Education and Development, no. 2 (2020). 7-10.
2. Geoffrey B. Irani-James P. Chirst: Image Processing for Tomahawk Scene Matching. Johns Hopkins APL Technical Digest, 15, no. 3 (1994). 250-264
3. Elizabeth A. Stanley: Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System. Carlisle, Strategic Studies Institute, 1998;

[24] Kathy Pretz: Stop Calling Everything AI, Machine-Learning Pioneer Says. IEEE Spectrum, 31 March 2021; Yasmin Afina: Rage Against the Algorithm: The Risks of Overestimating Military Artificial Intelligence. Chatham House, 27 August 2020.

4. NATO Standardization Office: AJP-5 Allied Joint Doctrine for the Planning of Ops, Ed. A, Ver.2. 2019a.
5. NATO Standardization Office (2019a): op. cit. Chapter 2.
6. NATO Standardization Office (2019a): op. cit. 4-1.
7. NATO Standardization Office: APP-28 Tactical Planning for Land Forces, Edition A, Vers.1. 2019b. 1-7.
8. Roger N. McDermott-Charles K. Bartles: The Russian Military Decision-Making Process and Automated Command and Control. Hamburg, German Institute for Defence and Strategic Studies, 2020. 29-32.
9. NATO Standardization Office (2019b): op. cit. F-1-F-3.
10. Department of the Army: FM 6-0 Commander and Staff Organization and Operations. 2014. 9-44-9-46.
11. Stuart Russel- Peter Norvig: Artificial Intelligence. Englewood Cliffs, Prentice Hall, 1995. 4-5
12. Nils J. Nilsson: The Quest for Artificial Intelligence. New York, Cambridge University Press, 2010
13. Neil Savage: The Race to the Top among the World's Leaders in AI. Nature, 10 Dec. 2020. S102-S104.
14. Daniel S. Hoadley-Kelley M. Sayler: AI and National Security. Congressional Research Service, 2020. 9-16
15. Pentagon: DoD Memorandum. 2017.
16. Forrest E. Morgan et al.: Military Applications of AI. Santa Monica, RAND Corporation, 2020. 25-26.
17. Nilsson (2010): op. cit. 370-371.
18. NATO Standardization Office: AAP-06 NATO Glossary of Terms and Definitions. Edition 2021. 137.
19. Bryan Clark et al.: Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations. Washington, Center for Strategic and Budgetary Assessments, 2020. 17–25.
20. Sherrill Lingel et al.: Joint All-Domain C2 for Modern Warfare. Santa Monica, RAND Corporation, 2020. 44-45.
21. Eric Bogert et al.: Humans Rely more on Algorithms than Social Influence as a Task Becomes more Difficult. Nature Scientific Reports, 11, no. 8028 (2021)
22. For more on legal and ethical issues see Imre Négyesi: A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. Honvédségi Szemle, 149, no. 1 (2021). 133-144; James Butcher-Irakli Beridze: What is the State of Artificial Intelligence Governance Globally? The RUSI Journal, 164, no. 5-6 (2019). 88-96.
23. Kathy Pretz: Stop Calling Everything AI, Machine-Learning Pioneer Says. IEEE Spectrum, 31 March 2021; Yasmin Afina: Rage Against the Algorithm: The Risks of Overestimating Military Artificial Intelligence. Chatham House, 27 August 2020.

RUBRIKA E TRETË

ARSIMIMI USHTARAK, LIDERSHIPI DHE ZHVILLIMI PROFESIONAL

Etika profesionale dhe kultura e sigurisë

Prof. Asoc. Dr. Edmond BRANESHI
Shef grupi, Departamenti i MNDLH, FMS

Trajtesë e shkurtuar

Etika profesionale dhe kultura e sigurisë përbëjnë dy shtylla themelore në zhvillimin e organizatave bashkëkohore dhe në ruajtjen e integritetit të individëve brenda tyre. Etika profesionale nënkupton respektimin e parimeve morale, transparencës, përgjegjësisë dhe ndershmërisë në veprimtarinë e përditshme. Ajo krijon besueshmëri dhe nxit marrëdhënie të shëndosha brenda organizatës. Nga ana tjetër, kultura e sigurisë lidhet me ndërtimin e një mjedisi pune ku mbrojtja e jetës, shëndetit dhe mirëqenies së anëtarëve është përparësi absolute. Kjo kulturë nuk kufizohet vetëm në respektimin e rregullave përkatëse, por përfshin edhe ndërgjegjësimin, edukimin dhe angazhimin e vazhdueshëm të çdo individi për të parandaluar rreziqet dhe për të promovuar sjellje të sigurta. Ndërthurja e etikës profesionale me kulturën e sigurisë krijon një bazë të fortë për zhvillim të qëndrueshëm, rrit produktivitetin dhe siguron një klimë pune të drejtë e të përgjegjshme. Madje, në literaturën ndërkombëtare, siguria shihet si një element i pandashëm i efektivitetit operacional dhe i mbrojtjes së jetës njerëzore. Në këtë kuadër, ky shkrim synon të analizojë rolin e këtyre dy koncepteve (veçanërisht në Forcat e Armatosura, ku rreziku është i pranishëm në çdo veprim), ndikimin e tyre në organizata dhe rëndësinë e integrimit të tyre në praktikat e përditshme profesionale.

Fjalë kyçe: etika profesionale, etika ushtarake, kultura e sigurisë, kultura e organizatës, forcat e armatosura, morali, vlerat, lidershipi, anëtar, organizatë, parime.

Hyrje

Në shoqërinë bashkëkohore, ku profesionet po bëhen gjithnjë e më komplekse dhe kërkesat për cilësi janë gjithnjë e më të larta, etika profesionale dhe kultura e sigurisë zënë një vend qendror në funksionimin e çdo organizate. Ato nuk janë thjesht koncepte teorike, por parime praktike që ndikojnë drejtpërdrejt në mënyrën se si individët ndërveprojnë me njëri-tjetrin,

me bashkëpunëtorët, me teknologjinë dhe me mjedisin e punës. Ndërtimi i një kulture të përgjegjshme dhe të sigurt kërkon një etikë të fortë, dhe po ashtu etika nuk mund të zbatohet plotësisht pa garancinë e një mjedisi të sigurt. Kjo lidhje e dyanshme e bën të domosdoshme analizimin dhe kuptimin e tyre të ndërlidhur.

Forcat e Armatosura janë të lidhura pazgjidhshmërisht me çështjet morale që kanë ndikim në motivimin e personelit. Motivimi nuk është një efekt i mirëqenies materiale apo i njohjes së të drejtave vetjake, ai është i lidhur me kodin e sjelljes dhe qëndrimit: me etikën ushtarake. Ajo përfaqëson një bashkësi parimesh morale dhe profesionale që udhëheq sjelljen e ushtarakëve në shërbim dhe në jetën e tyre publike. Ajo synon të sigurojë që forcat e armatosura të veprojnë me integritet, disiplinë dhe respekt ndaj ligjit, shoqërisë dhe njerëzimit. Etika është një shtyllë e fuqishme në themelin e lidershipit dhe organizatës e cila kur funksionon siç duhet, garanton një kulturë sigurie të qëndrueshme.

1. Etika profesionale në Forcat e Armatosura

1.1. Etika si koncept

Studime të shumta rreth moralit, etikës dhe lidershipit, për nivele të ndryshme të drejtimit e të komandimit kanë nxjerrë në pah domosdoshmërinë e një formimi sa më të plotë të fushës së moralit dhe etikës. Bazuar në faktin se etika është shkenca që studion moralin, që përcakton rregullat dhe normat e sjelljes së njerëzve, detyrimet ndaj njëri-tjetrit, ndaj shoqërisë, ndaj shtetit dhe atdheut, vërejmë se vlerat etike janë thelbësore për të gjithë ushtarakët. Në etimologjinë e fjalës, etika dhe morali janë ekuivalente (*ethos* në greqisht dhe *mores* në latinisht) dhe përcaktojnë mënyrën e qëndrimit të njerëzve, zakonet e tyre, karakterin, normat rregulluese, si ato natyrore, dhe ato ligjore[1]. Pra, etika është shkenca që përcakton rregullat dhe normat e sjelljes së njerëzve, detyrat ndaj njëri-tjetrit, organizatës, shoqërisë, vendit, duke i frymëzuar njëherësh njerëzit për t'i zbatuar e kryer këto norma, rregulla, detyra apo detyrimet përkatëse.

Etika ekziston qysh në lindjen dhe formimin e shoqërisë njerëzore dhe përcaktohet në radhë të parë nga zhvillimi ekonomik. Nisur nga kushtet e jetës së shoqërisë, ajo u kthye praktikisht në një sërë normash të caktuara të sjelljes së njerëzve, qofshin edhe të pashkruara, por të detyrueshme. Dhe kështu, shkallë-shkallë marrëdhëniet e individit me komunitetin, me të afërmit, me familjen, me vetë proceset e jetës, u përforcuan dhe u transformuan në parime psikologjike të pranuara nga të gjithë, u bënë morali i shoqërisë. Në qoftë se njerëzit do të ishin krejt të pavarur në veprimtarinë e tyre, atëherë do të kishim një kaotizëm të paparë, sepse individët do të pengonin njëri-tjetrin dhe do të rrënohej vetë shoqëria. Mirëpo qeniet njerëzore, për nga natyra, janë të shoqërueshëm dhe shoqërizimi është veçori e tyre. Për këtë arsye, etika me

[1] Grup autorësh, *Etika ushtarake dhe arti i komandimit*, (Tiranë: Publikim i QD në KDS, 2013), ISBN: 978-9928-171-02-3, f. 9.

vlerat e saj, "portretizon" normat e sjelljes së individëve. Këto norma janë parime të përcaktuara ose rregulla që njerëzit duhet t'i respektojnë, pasi ato përfaqësojnë çfarë duhet bërë mirë e shumë mirë dhe çfarë nuk duhet bërë në jetën shoqërore.

Individi nuk duhet të shihet thjesht si një njeri i veçuar dhe kaq. Ai është pjesëtar i një grupi, organizate, shoqërie dhe, në marrëdhënie me të tjerët, ai duhet të rrezatojë norma etike. Në këtë kuadër, çdo njeri ka individualitetin e tij, brenda një shoqërie të caktuar. Prandaj vullneti i individit nuk mund të jetë në kundërshtim, e aq më tepër, t'i kundërvihet vullnetit të shoqërisë normale. Individit i duhet të parashtrojë kërkesat e tij deri në atë masë sa nuk e shmangin nga interesat e përgjithshme të shoqërisë. Etika, duke u bërë një nga format e ndërgjegjes shoqërore, niset nga motive të brendshme, motive që e shtyjnë njeriun të mbajë në jetë një qëndrim apo sjellje të caktuar për të mirën e të keqen, të drejtën e të padrejtën, të vërtetën e gënjeshtrën, nderin e turpin, çiltërsinë dhe hipokrizinë[2] etj., gjithnjë kjo në raport me vetë qëllimet dhe idealet morale që e karakterizojnë.

Brenda qëllimit e idealit moral që karakterizon individin, është profesioni ai që ka ndikimin më të drejtpërdrejtë mbi jetën e përditshme e mbi mënyrën e jetesës së tij, rrjedhimisht ka ndikimin më të madh mbi konceptin e këtij individi për moralin dhe etikën.

1.2. Etika profesionale në Forcat e Armatosura dhe veçoritë e saj

Etika profesionale përkufizohet si një grup parimesh dhe rregullash morale që udhëheqin sjelljen e individëve në veprimtaritë e tyre të punës. Ajo është një udhërrëfyese që orienton profesionistin drejt veprimeve të drejta, të përgjegjshme dhe të ndershme. Një profesionist etik duhet të tregojë integritet, respekt, objektivitet dhe përgjegjësi në çdo proces të punës. Kjo do të thotë se vendimet e tij nuk duhet të ndikohen nga interesat vetjake, presionet e jashtme apo konfliktet e mundshme të interesit. Etika profesionale është baza e besueshmërisë në çdo profesion, pasi garanton se shërbimet apo objektivat e përmbushur janë rezultat i punës së ndershme dhe profesionale.

Kodet e etikës profesionale janë dokumente që përcaktojnë udhëzime dhe standarde sjelljeje për profesionistët në fusha specifike, duke i udhëzuar ata se si të veprojnë në situata etike komplekse dhe të ndjeshme. Këto kode shërbejnë si një udhëzues për të siguruar që vendimet dhe veprimet në organizatë të jenë në përputhje me vlerat dhe parimet etike të profesionit.

Etika profesionale është thelbësore për të nxitur besimin, për të krijuar dhe mbajtur një frymë të lartë kohezive në strukturat e organizatës, duke kontribuar

[2] Bashkim Kozeli, Ilir Spahiu, *Edukimi qytetar dhe etika në Forcat e Armatosura*, (Tiranë: SHBU, 2000), f. 216.

në zhvillimin vetjak dhe profesional të individëve dhe në ndërtimin e një shoqërie më të drejtë dhe etike.

Profesioni i ushtarakut përcakton një etikë disi ndryshe nga ajo e një profesioni civil. Është ndryshe sepse profesioni i ushtarakut nënkupton një ndjeshmëri edhe më të madhe ndaj qenieve të tjera njerëzore dhe se veprimtaria e tij është me pasoja për njerëzit e tjerë dhe për mjedisin. Sipas Huntington-it, ndërsa të gjitha profesionet janë të rregulluara ose të kontrolluara në një farë mënyre nga shteti, profesioni ushtarak është monopol i shtetit. Aftësia e mjekut është të diagnostikojë dhe të mjekojë; përgjegjësia e tij është shëndeti i klientit të tij. Aftësia e oficerit është drejtimi i forcës ushtarake; përgjegjësia e tij është sigurimi ushtarak i klientit të tij, shoqërisë. Marrja e kësaj përgjegjësie kërkon zotërimin e përgatitjes që bën të nevojshme e të mundur pranimin e përgjegjësisë.[3] Pra, përgjegjësia dhe përgatitja, e dallojnë oficerin nga tipat e tjerë socialë. Në këtë kuadër, Forcat e Armatosura janë shembulli i institucionit profesional me rol të veçantë e specifika të ndryshueshme nga ato të mjedisit rrethues dhe shoqërisë në tërësi. Shoqëria e di mirë se çfarë do të thotë të kryesh një mision të karakterit luftarak, paqeruajtës apo humanitar, kur ndërmerren nga Forcat e Armatosura.

Etika shpalos kuadrin moral për t'i shërbyer kombit dhe ndihmon në kuptimin e qëllimit të domosdoshëm për mbrojtjen e vendit, madje duke përdorur dhe forcën ushtarake. Elementet thelbësorë të etikës profesionale të Forcave të Armatosura përmbajnë vlerat kryesore që udhëheqin rrugën që duhet të ndjekë gjithsecili dhe ato janë: besnikëria ndaj atdheut; detyra si një detyrim ligjor për të bërë atë çfarë duhet bërë pa ta diktuar kush; shërbimi vetëmohues (sakrifica) për t'u shërbyer në radhë të parë interesave të kombit dhe integriteti[4].

- *Besnikëria ndaj atdheut, Forcave të Armatosura dhe organizatës*. Me termin "besnikëri" kuptojmë të qenët besnik, ndjenjë e qëndrueshme e dashurisë për dikë, qëndrueshmëri e patundur në marrëdhëniet e në lidhjet me dikë, kështu kemi besnikërinë ndaj Atdheut, besnikërinë ndaj shokut, familjes etj. Besnikëri është edhe qëndrimi i pandryshueshëm kundrejt detyrave dhe angazhimeve të marra, ndjekja dhe zbatimi në vijimësi e me këmbëngulje i parimeve, ideve, vendimeve, udhëzimeve apo urdhrave të ndryshëm. Besnikëria është zhvilluar si përkushtim për familjen, farefisin dhe shokët, ajo vjen më natyrshëm ndërmjet grupeve të vogla.

Betimi që bën çdo ushtarak përmban ato kërkesa që kanë të bëjnë me besnikërinë. Ai përcakton një detyrim sublim për ushtarët që të mbrojnë kushtetutën e atdheun deri në sakrifikimin e jetës së tyre. Duke cituar B. Tracy-in, besnikëria është pjesë e rëndësishme e karakterit. Kur jeni besnik, ju kurrë

[3] Samuel Huntington, *Ushtaraku dhe shteti*, (Tiranë: SHBU, 1995), faqe 18.

[4] *Udhëheqja Ushtarake, studime nga ushtarakë të lartë amerikanë*, (Tiranë: SHBU, 1995), faqe 82.

nuk ankoheni, dënoni ose kritikoni organizatën tuaj, drejtuesin tuaj, shërbimet tuaja ose ndonjë gjë tjetër në lidhje me punën tuaj. Edhe nëse jeni të pakënaqur për ndonjë arsye, ju e mbani atë për veten tuaj. Ju gjithmonë mbështesni njerëzit me të cilët punoni dhe tregoni besnikëri të plotë ndaj personit "bosit" tuaj.[5] Në këtë kuadër, besnikëria ndaj Forcave të Armatosura nënkupton mbështetjen e zinxhirit të komandimit ushtarak dhe civil. Besnikëria ndaj organizatës shpreh si detyrimin midis atyre që drejtojnë e të drejtuarve, ashtu dhe angazhimin e përbashkët të vartësve për njëri tjetrin. Besnik është ai që mbështet drejtuesin dhe del në mbrojtje të shokëve të tij. Duke kryer detyrën e ngarkuar, ju tregoni besnikërinë ndaj grupit (ekipit) apo organizatës tuaj.

Ushtarakët profesionistë janë mbrojtës të idealeve të kombit të vet, gjithnjë të gatshëm të luftojnë për këto ideale, me qëllim që të tjerët të jetojnë në një shoqëri të lirë e të drejtë. Për të plotësuar këtë detyrë, ata duhet të jenë ekspertë në drejtimin e njerëzve gjatë zhvillimit të luftimit. Drejtuesi ushtarak, që vlerëson thellë besnikërinë ndaj kombit të vet e sheh vetveten si një individ që gjithnjë do të bëjë më të mirën e mundshme për mbrojtjen e idealeve kombëtare.

Organizata është pjesa juaj e veprimtarisë së përditshme në Forcat e Armatosura. Duke kontribuar për misionin dhe gatishmërinë luftarake të organizatës, ju kontribuoni për mbrojtjen e vendit tuaj. Ajo është familja juaj, është ekipi juaj. Besnikëria për organizatën nënkupton që ju të vendosni qëllimet dhe nevojat e saj mbi ato vetjake.

- *Detyra* është një detyrim ligjor ose moral për kryerjen e veprimeve të duhura me nismën tuaj, pa qenë e nevojshme që kjo të kërkohet nga eprori i juaj. Detyra nënkupton plotësimin e të gjitha detyrimeve të ngarkuara, duke përdorur sa më mirë të gjitha aftësitë tuaja mendore dhe fizike. Detyra kërkon gatishmëri për të pranuar përgjegjësinë e plotë si për veprimet e kryera nga ju, ashtu dhe për nivelin e performancës së vartësve. Ajo kërkon një drejtues që të tregojë nismë dhe aftësi për të parashikuar nevojat në përgjigje të situatës së dhënë. Njëkohësisht kërkon drejtues që ka aftësi t'i frymëzojë njerëzit që të veprojnë. Ata që e kanë këtë aftësi, u japin njerëzve një ndjenjë përkushtimi, e cila nuk ka lidhje fare me asnjë nxitës të jashtëm, apo përfitim të mundshëm. Ata që mund të frymëzojnë, krijojnë një grup ndjekësish, të cilët veprojnë në të mirë të të gjithëve, jo ngaqë duhet, por ngaqë duan.[6] Si profesionist, përgjegjësia e juaj është të përmbushni detyrën e dhënë duke bërë më të mirën e mundshme.

- *Shërbimi vetëmohues* është një term që nënkupton një "shërbim i cili kryhet pa pritur ndonjë shpërblim për të". Vetëmohimi është flijim i vetes dhe

[5] Brian Tracy, *Fito atë për të cilën ti vlen*, (Tiranë: Reklama, 2023), ISBN: 978-9928-308-59-7, faqe 190.

[6] Simon Sinek, *Fillo me pse, si liderët e mëdhenj frymëzojnë këdo që të veprojë*, (Tiranë: Minerva, 2019), ISBN: 978-9928-261-16-1, faqe 7.

interesave vetjake për të mirën e përgjithshme, është qëndrim heroik, pa kursyer vetveten kur e kërkon nevoja për mbrojtjen e kauzës së përbashkët. Shërbimi vetëmohues, bashkë me besnikërinë dhe vlerat e tjera themelore të Forcave të Armatosura janë instrumente morale që na udhëheqin në jetën tonë të përditshme. Ato përbëjnë bazën e angazhimit të ushtarakëve në shërbim vetëmohues ndaj kombit, Forcave të Armatosura, organizatës dhe kolegëve të tyre. Në një vend demokratik, profesioni i ushtarakut nënkupton ekzistencën e një marrëveshjeje morale midis ushtarakut dhe shoqërisë ku ai i shërben. Kjo "kontratë" ka në bazë besimin e përbashkët, sigurinë dhe mbështetjen e ndërsjellë. Kjo kërkon nga shoqëria që anëtarëve të Forcave të Armatosura, në shkëmbim të shërbimit që ata ofrojnë dhe përgjegjësisë së pakufizuar që marrin përsipër, t'u sigurohen mjetet dhe burimet e nevojshme për përmbushjen e detyrave të ngarkuara.

Në këtë mënyrë, pjesëtarët e Forcave të Armatosura realizojnë detyrimet apo objektivat përkatëse pa marrë parasysh vështirësitë, rreziqet dhe në fund të fundit të jenë të gatshëm të bëjnë edhe sakrificat më sublime, në qoftë se këtë e kërkon situata e dhënë. Ushtarakët nuk janë të përfshirë në ndonjë angazhim tjetër, përveç ushtrimit të profesionit të tyre. Profesionistëve ushtarakë u është besuar mbrojtja e vendit. Në këtë mënyrë, me shërbimin tyre, ata janë mbrojtës të së ardhmes së shtetit, atdheut dhe popullit të tyre. Ky mision fisnik kërkon që të vënë kurdoherë interesat e kombit, të Forcave të Armatosura, të organizatës para interesave vetjakë, pra detyrimi i tyre si profesionistë është vënia e interesit të përgjithshëm mbi çdo gjë.

- *Integriteti* është domosdoshmëri në zbatimin e etikës profesionale të Forcave të Armatosura. Ai nënkupton të jesh i drejtë dhe i ndershëm, të shmangësh mashtrimin dhe të jetosh në bazë të vlerave që ju i sugjeroni vartësve tuaj. Brian Tracy, duke folur për rëndësinë e padiskutueshme të integritetit e cilëson atë si "*...vlera themel në të cilën bazohen gjithë vlerat e tjera. Të pasurit e një integriteti të vërtetë do të thotë që ju gjithmonë jetoni dhe veproni në mënyrë të qëndrueshme me vlerat tuaja. Nëse keni mungesë të integritetit, ju duhet të bëni kompromis me vlerat e tjera tuaja me tundimin më të vogël*."[7] Integriteti kërkon që të veproni në përputhje me vlerat e tjera etike të Forcave të Armatosura. Si drejtues, ju duhet të jeni i sinqertë, i ndershëm, i drejtë dhe i paanshëm dhe të evitoni sjelljet e pahijshme. Integriteti përbën bazën e besimit dhe mbështetjes që duhet të ekzistojë midis anëtarëve të organizatës. Gjithashtu, drejtuesi duhet të demonstrojë integritet në jetën e tij vetjake. Në qoftë se me sjelljen e tij do të kompromet integritetin, atëherë ai ka cenuar besimin e krijuar ndaj vartësve dhe eprorit të tij.

Duke parë elementet përkatës të etikës profesionale në FA, nënkuptohet që misioni i ushtarakut është t'i shërbejë shoqërisë dhe vendit të tij, duke

[7] Brian Tracy, *Ndryshoni të menduarit tuaj, ndryshoni jetën tuaj, si të zbulosh potencialin tënd për sukses e arritje*, (Tiranë: Elta BS, 2009), ISBN; 987-9951-544-08-5, faqe 263.

vlerësuar rëndësinë e grupit (organizatës) kundrejt individit. Prandaj suksesi në çdo veprimtari kërkon nënshtrimin e vullnetit të tij ndaj atij të grupit. Kështu, oficeri më shumë, por edhe nënoficeri, ushtari profesionist apo civili që punon në FA, duke humbur jo pak nga personaliteti dhe individualiteti i tyre, si pasojë e "shkrirjes" brenda së tërës (organizatës), i drejtojnë interesat e shërbimet vetjake në atë çfarë është e nevojshme për të mirën e shërbimit (FA). Kjo pa dyshim bie në kundërshtim me atë që me të drejtë vë në dukje filozofi Franc Kuco kur thekson se "… *moralisht kërkohet të respektohet pavarësia dhe liria e individit e të trajtohet me drejtësi, duke mos harruar se morali i është dhënë drejtuesit për të mirën e jetës së individëve dhe jo për të ndërhyrë në jetën e tyre më tepër se sa është e nevojshme, sepse morali ndërtohet për njeriun dhe jo njeriu për moralin*."[8]

Por në Forcat e Armatosura, individit i duhet ta vendosë veten në një kornizë morale dhe etike që e rrezikon së tepërmi kuptimin e vetë respektit e të autonomisë. Vënia e theksit te ndershmëria, vetëmohimi, bindja, detyra, besnikëria etj., krijon antagonizmin në raportet individ – profesion. Domethënë, ndërsa ndershmëria individuale kërkon ndjenjën e vetë respektit, të sinqeritetit e të nderit, nevojat profesionale (të ushtarakut) kërkojnë nënshtrimin e këtyre për hir të integritetit profesional. Nderi i ushtarakut nënkupton jetën në kolektiv, kryerjen bashkërisht të të njëjtave privacione të shërbimit, përdorimin kolektiv të së njëjtës armë, deri shkuarjen së bashku drejt rrezikut për jetën etj., që tregon më shumë se çdo gjë tjetër besnikërinë ndaj "vëllazërisë" së oficerëve, nënoficerëve, ushtarëve, sjellje fisnike dhe sakrificë vetjake për hir të tyre. Koloneli gjerman, Kolmar fon der Golt, në librin e tij "Kombi nën armë" shkruan: "*Ushtaraku duhet të hedhë poshtë psikologjinë e përfitimeve dhe të mirëqenies personale. Egoizmi është padyshim, armiku më i madh i cilësive thelbësore të korpusit të oficerëve*"[9]. Kurse Sharl De Gol, në veprën e tij "Ushtria e së ardhmes" thekson: "*Etika ushtarake është në thelb, një frymë bashkëpunimi. Ajo është thellësisht anti-individuale*"[10]. Pikërisht, nga këto mendësi përcaktohet në forcat e armatosura edhe etika, ajo që quhet etika profesionale në Forcat e Armatosura ose etika ushtarake, e cila përfshin parimet dhe normat që udhëheqin ushtarakun në atë që duhet bërë dhe që në FA, e ndoshta vetëm në FA, quhet e moralshme për t'u bërë.

1.3. Përgjegjësitë etike

Profesionit të ushtarakut i duhet të përcaktojë modele të qarta morale dhe etike, të lidhura këto me modelet më të mira morale dhe etike të shoqërisë. Modeli më i qartë etiko – moral në kushtet e shërbimit në një organizatë ushtarake realizohet nëse formojmë bindjet morale, shprehitë dhe zakonet e

[8] Diana Liçi, *E drejta në Forcat e Armatosura* (pjesa e dytë), (Tiranë: Filara, 2023), ISBN: 978-9928-279-99-6, f. 82.

[9] Samuel Huntington, *Ushtaraku dhe shteti*, (Tiranë: SHBU, 1995), faqe 68.

[10] Po aty, faqe 68.

sjelljes morale. Gjithashtu, individët që janë në zinxhirin e komandimit duhet të jenë të vetëdijshëm se aftësia drejtuese nuk është sinonim me autoritetin. Në një masë të konsiderueshme ajo është një vlerë e veçantë e barabartë me besimin e vartësve ndaj eprorit. Ajo mishëron një investim emocional shpirtëror, virtytin e besimit. Në këtë raport është vartësi ai që përcakton kushtet për dhënien e besimit. Ai i di dhe i percepton ato cilësi, karakteristika dhe vlera, që duhet të zotërojë eprori i tij për të qenë e për t'u pranuar si drejtues. Por sidoqoftë, është drejtues me të vërtetë i zgjuar ai, që kupton e vlerëson, që ushqen e mban të gjallë lidhjen midis tij si epror dhe vartësve[11]. Pothuaj, gjithë drejtuesit e suksesshëm kanë të përbashkët kapacitetin e jashtëzakonshëm për t'u lidhur me të tjerët, talentin për të ndërtuar marrëdhënie me njerëz nga një sërë sferash e bindjesh. Fuqinë e lidhjes e pohon dhe Dav Sidman në librin e tij me titull provokues: "Si: Pse...", ku shkruan: "*Në një botë që përparon me shpejtësi, fitojnë individët dhe organizatat të cilat krijojnë lidhjet më të forta... Sot na dallon mënyra se si sillemi dhe ndërveprojmë me të tjerët. Cilësitë që dikur dukeshin si të "buta" – integriteti, pasioni, përulësia dhe e vërteta – janë bërë etaloni i suksesit të sipërmarrjes dhe shtysat më të fuqishme drejt emrit të mirë të organizatës dhe suksesit*."[12] Pra, marrëdhëniet e ushtarakëve janë në themel të organizatës ushtarake. Dhe reflektimi serioz i secilit ushtarak mbi këtë të vërtetë për pranimin e moralit dhe të etikës ushtarake, rrit personalitetin individual e profesional të tij.

Në këtë këndvështrim, që eprori të krijojë marrëdhënie të drejta e korrekte me një vartës, duhet të ketë të qartë, (qoftë ky edhe drejtues pedant apo megaloman), se vartësi që ka përpara e nën urdhrat e tij nuk është thjesht një objekt, mekanizëm apo një gjë e ngurtë, dhe se personaliteti i tij nuk përcaktohet nga fakti se ky vartës është i detyruar të zbatojë urdhra, ta përsërisë dhjetë herë një veprim taktik, të hiqet zvarrë, të vrapojë, të pastrojë dyshemenë apo territorin etj., etj., por se është një njeri me botë, me zemër, me emocion dhe me dinjitet, që duhet respektuar e ndihmuar. Pra, një epror i mirë e ka të hequr nga vetja gjykimin e ngushtë: eprori vetëm urdhëron, vartësi vetëm bindet. Ai duhet të ndjejë disa përgjegjësi etike[13] ndaj vartësit dhe, më të rëndësishmet janë:

Së pari, të jetë shembull model për vartësit. Autoriteti i eprorit nuk përcaktohet vetëm nga grada apo posti, por edhe nga gjykimi që ai ka, nga puna, nga dituria dhe përvoja që shpalos, nga sjelljet etj., duke u bërë kështu model edukimi dhe imitimi. Sipas Lee Bolman-it, "*thelbi i udhëheqjes nuk është të japësh gjëra apo edhe të ofrosh vizione. Ajo është të ofrosh veten dhe*

[11] Perry M. Smith, *Taking Charge, a practical guide for leaders*, (Washington, D.C: National Defense University Press, 1986), faqe 152.

[12] Dale Carnegie, *Arti për t'u bërë i paharrueshëm*, (Tiranë: Pegi, 2018), ISBN: 978-9928-233-24-0, faqe 54.

[13] *Udhëheqja Ushtarake, studime nga ushtarakë të lartë amerikanë*, (Tiranë: SHBU, 1995), faqe 86.

shpirtin tënd."[14] Pra, në qoftë se ju jeni shembull model, atë do ta shprehni gjatë gjithë kohës. Veprimet flasin më shumë se fjalët tuaja. Vartësit ju shohin ju me shumë kujdes, gati ju vëzhgojnë në çdo kohë dhe ata imitojnë sjelljet tuaja. Sjelljet tuaja do t'ju prijnë sjelljeve të anëtarëve të tjerë në organizatë. Jeni ju ai që vendosni shembullin dhe ata do ta ndjekin këtë shembull. Albert Shvajcer ka thënë: "Ju duhet t'i mësoni njerëzit me anën e metodës së shembullit sepse ata nuk do të mësojnë nga askush tjetër"[15]. Ju keni detyrimin për të qenë një shembull model dhe kurrë nuk duhet të harroni ndikimin që sjellja juaj ka tek të tjerët. Ju duhet të jeni të gatshëm për të bërë atë që ju kërkoni të bëjnë ushtarët tuaj dhe të ndani rrezikun e vuajtjet me ta.

Së dyti, të kultivojë e të zhvillojë te vartësit ndjenjat etike, me qëllim që të formohen tek ai koncepte e përfytyrime të sakta mbi rregullat, veprimet e sjelljet morale në shoqërinë ushtarake si dhe të dallojë kështu të mirën nga e keqja, atë që lejohet dhe atë që është e ndaluar. Drejtuesi duhet të formojë vlerat shpirtërore dhe bindjet e ushtarëve të tij, me qëllim që ata të mbështesin vlerat e kombit, të forcës së armatosur dhe të organizatës. Ai i edukon vartësit jo vetëm nëpërmjet karakterit vetjak, por edhe nëpërmjet mësimit që u jep se si të arsyetojnë rreth problemeve etike. Të qenit i ndjeshëm është një pjesë e rëndësishme për zhvillimin etik të vartësve. Synimi i drejtuesit është të zhvillojë një ndjenjë etike të thellë, me qëllim që vartësit (ushtarët) të veprojnë në mënyrë të saktë në çdo sfidë apo përballje dhe në situatat e pasigurta të luftës.

Së treti, të shmangë krijimin e pasigurive etike te vartësit. Përderisa vartësit ju pranojnë juve si drejtues ushtarak, mos u kërkoni atyre që të bëjnë gjëra të cilat shkaktojnë sjellje joetike, pasiguri apo e thënë ndryshe, zbehje të etikës.[16] Zbehja e Etikës nënkupton strukturën e një kulture që i lejon njerëzit të veprojnë në mënyrë joetike, në mënyrë që të plotësojnë interesat e tyre, shpesh në kurriz të të tjerëve, teksa besojnë në mënyrë të gabuar se nuk kanë shkelur parimet e tyre morale. Zbehja etike shpesh fillon me shkelje të vogla, në dukje të padëmshme, të cilat, kur lihen jashtë kontrollit, fillojnë të rriten dhe të ndërlikohen. Pasiguritë etike kanë ndikime negative dhe janë veçanërisht të ndjeshëm ndaj venitjes etike. Peter Drucker-i, një nga mendimtarët dhe shkrimtarët më të shquar të fushës së menaxhimit, jep një këshillë të vlefshme për drejtuesit: *"Njerëzit nuk menaxhohen. Detyra jote është t'i drejtosh ata. Qëllimi yt është t'i bësh produktive fuqitë dhe dijet specifike të gjithsecilit"*[17].

Në këto tri përgjegjësi mund të përmblidhet, një kod i tërë etiko-moral, si më poshtë: të tregosh vazhdimisht interes për vartësit e tu; të veprosh me ta jo

[14] Kevin Cashman, *Leadership from the inside out (*second edition*)*, (San Francisco, California: Berrett-Koehler Publishers, Inc., 2008), ISBN 978-1-57675-599-0, faqe 24.
[15] Brian Tracy, *Lidershipi*, (Prishtinë: Damo, 2014), ISBN: 978-9951-642-27-9, faqe 70.
[16] Simon Sinek, *Loja e pafundme*, (Tiranë: Minerva, 2020), ISBN: 978-9928-265-26-5, faqe 147.
[17] Steve Chandler, Duane Black, *Mos i gjyko punonjësit*, (Tiranë: Max, 2014), ISBN 978-99956-23-37-1, faqe 18.

vetëm si komandant, por edhe si shok apo kujdestari i tyre; të jesh në vijimësi në shërbim të organizatës tuaj.

2. Kultura e sigurisë

2.1. Kultura e sigurisë, si pjesë e kulturës së organizatës

Natyra e lidershipit është e tillë që ndikimi i drejtuesve nuk është vetëm tek individët por edhe tek sistemet dhe proceset e përdorura nga organizatat për të arritur rezultatet e dëshiruara. Një prej këtyre metodave jo të drejtpërdrejta të udhëheqjes është ajo nëpërmjet kulturës së organizatës. Kultura e organizatës është "**...***një sistem hamendësish themelore të përbashkëta që grupi i ka mësuar gjatë zgjidhjes së problemeve të tij të përshtatjes së jashtme dhe integrimit të brendshëm, të cilat kanë funksionuar mjaft mirë për t'u konsideruar të dobishme dhe për rrjedhojë për t'ua mësuar anëtarëve të rinj si një mënyrë korrekte për të perceptuar, gjykuar dhe menduar në lidhje me këto probleme*".[18] Gjithashtu, kultura në shumë raste është përcaktuar thjesht si "forma ose mënyra se si ne i bëjmë gjërat". Kultura është koncept i fuqishëm, në këtë mënyrë shumë individë të përfshirë në proceset i shohin metodat ose rrugët aktuale si mundësinë e bërjes së gjërave "saktë" dhe "drejtë". Drejtuesit të cilët kuptojnë kulturën janë në gjendje të kuptojnë individët e pozicionuar dhe të përfshirë në "aktivitete, ngjarje" ose në çështjet e drejtimit. Kultura përcakton rregullat dhe standardet e funksionimit të organizatës. Në këtë kuadër, kultura trajtohet si një element i domosdoshëm për ndryshimin e suksesshëm të organizatës dhe rritjen në maksimum të vlerës dhe dobisë së kapitalit njerëzor.[19] Kjo është veçanërisht e rëndësishme në njohjen e organizatave të fuqishme, ku bëjnë pjesë edhe Forcat e Armatosura.

Një sfidë e rëndësishme për drejtuesit është të përcaktojnë se cila është kultura më efektive për organizatën e tyre dhe, si të ndryshojnë kulturën e organizatës në mënyrë efektive kur është e nevojshme. Kultura e organizatës zhvillohet në përputhje me vlerat, bindjet e hamendësitë e shoqërisë ku bën pjesë organizata. Ajo transmetohet përmes qëndrimit dhe sjelljes kolektive të anëtarëve si dhe përmes proceseve të komunikimit. Ajo krijohet si kontribut i çdo anëtari të organizatës por edhe udhëheq sjelljen e gjithsecilit.

Në kuptimin bazë, kultura ekziston kur individët ndajnë së bashku një kornizë referimi për të interpretuar dhe vepruar ndërmjet tyre dhe në raport me botën në të cilën jetojnë. Kjo kornizë e përbashkët referimi përfshin gjuhën, vlerat, besimet, krijimet dhe interpretimet e përvojës. Ajo pasqyrohet në zakonet, traditat dhe komunikimin si edhe në karakteristika të tjera të vrojtueshme

[18] E. H. Schein, *Organizational Culture and Leadership*. (San Francisco: Jossey-Bass, 1988).

[19] Grup autorësh, *Udhëheqja Strategjike*, (Tiranë: GEER, 2010), ISBN: 978-9928-105-15-8, faqe 252.

të komunitetit.[20] Në këtë kuadër, kultura ndihmon në ndërtimin e sistemit të duhur imunitar (mbrojtës, të sigurisë) të organizatës, ofron kuadrim brenda të cilit, punonjësit ndërveprojnë me njëri-tjetrin dhe me grupet e interesit. Është filtër për përzgjedhjen e punonjësve të rinj por edhe një avantazh për të tërhequr më të mirët. Ajo na ndihmon në krijimin e harmonisë mes vlerave që mbartin Forcat e Armatosura, vlerave që shfaqin ushtarakët e punonjësit civilë dhe vlerave që perceptojnë rekrutët dhe njerëzit që kërkojnë t'i bashkohen asaj.

Kultura e sigurisë, si pjesë përbërëse e kulturës së organizatës, shquhet nga disa elemente kyç përbërës. Këto elemente janë pjesë e vlerave dhe normave në përditshmërinë organizative. Ajo që e bën të dallueshme një kulturë sigurie të efektshme për organizatën janë: së pari, *lidershipi i angazhuar* (drejtuesit duhet të demonstrojnë përkushtim të vërtetë ndaj sigurisë, duke vendosur standardet e nevojshme); së dyti, *pjesëmarrja aktive e anëtarëve* (secili individ duhet të ndjejë përgjegjësi për identifikimin e rreziqeve, raportimin e incidenteve dhe respektimin e procedurave); së treti, *komunikimi i hapur* (një kulturë e fortë e sigurisë nxit komunikimin e lirë rreth problemeve dhe gabimeve, pa frikë nga ndëshkimi apo stigmatizimi); së katërti, *trajnimet e rregullta dhe edukimi i vazhdueshëm* (njohuritë për sigurinë duhet të përditësohen dhe praktikat duhet të përforcohen vazhdimisht); së pesti, *raportimi dhe analiza e incidenteve* (mësimi nga gabimet dhe incidentet është thelbësor për të përmirësuar sigurinë dhe për të parandaluar përsëritjen e tyre); së gjashti, *përmirësimi i vazhdueshëm* (kultura e sigurisë duhet të evoluojë duke u përshtatur me teknologjitë e reja, ndryshimet në organizatë dhe përvojat e mëparshme).

Çdo individ është "rojtar" i kulturës dhe i sigurisë së saj, është përgjegjësi dhe e drejtë e gjithsecilit të mos lejojë askënd që ta shkelë atë. Kultura ka një ritual: sa më shumë vlerësohet dhe reflektohet në punën tonë, aq më shumë rritet vlera e saj, aq më e pakopjueshme dhe unike bëhet ajo.[21] Me kalimin e kohës, kultura rrënjoset kaq shumë brenda organizatës dhe anëtarëve të saj, sa që një pjesë e mirë e kësaj kulture bëhet natyrë e dytë dhe shpesh merret si e sigurtë. Kultura krijon kuptimin (gjykimin) kryesor në lidhje me atë se çfarë përfaqëson organizata dhe mënyrën se si funksionon ajo. Kultura ndikon gjithashtu edhe në mënyrën se si anëtarët e organizatës perceptojnë, mendojnë e veprojnë në lidhje me njëri-tjetrin si dhe ndaj sfidave.

Së fundi, në mjedisin e brendshëm të karakterizuar nga paqëndrueshmëria, pasiguria, kompleksiteti dhe paqartësia, kultura e sigurisë, si pjesë e kulturës së organizatës, ndikon në sjelljen e vartësve, sidomos kur ata përballen me një

[20] Michael J. Papa, Tom D. Daniels, Barry K. Spiker, *Kominikimi organizativ, qasjet dhe prirjet*, (Tiranë: UET Press, 2009), ISBN: 978-99956-39-12-9, faqe 108.

[21] Vasil Naçi, Alma Bici, është rruga jonë, rruga e suksesit në Agna group, (Tiranë: Agna Leadership Academy, 2013), f. 13.

situatë të veçantë ku mungojnë procedurat "standarde" të veprimit. Zakonet dhe traditat e llojit të forcës, doktrinat e bëra të njohura nëpërmjet manualeve, politikat e shprehura në rregullore, procedurat standarde të veprimit, si dhe filozofia e deklaruar që udhëheq organizatën, janë disa nga mënyrat më të rëndësishme që e bëjnë kulturën të dukshme dhe të kapshme. Të gjithë këto çështje mbartin disa aspekte të kulturës në përgjithësi dhe kulturës së sigurisë në veçanti në strukturat e Forcave të Armatosura.

2.2. Kultura e sigurisë në organizatat ushtarake

Në çdo organizatë ku rreziku është i pranishëm, kultura e sigurisë përbën themelin e funksionimit të saj. Në Forcat e Armatosura, ky koncept merr një rëndësi të veçantë, pasi ushtarakët përballen çdo ditë me situata që mund të rrezikojnë jetën e tyre dhe suksesin e misioneve. Kultura e sigurisë nuk është thjesht një grup rregullash teknike, por një sistem vlerash, besimesh dhe sjelljesh që formësojnë mënyrën se si individët dhe grupet perceptojnë rreziqet dhe i menaxhojnë ato. Siç thekson Reason-i, *siguria është rezultat i ndërgjegjësimit kolektiv dhe i disiplinës institucionale, jo vetëm i masave teknike*.[22] Kultura e sigurisë në Forcat e Armatosura është e lidhur ngushtë me disiplinën ushtarake dhe respektimin e procedurave standarde. Ajo përfshin ndërgjegjësimin e çdo individi për rreziqet, si dhe përgjegjësinë kolektive për t'i shmangur ato. Studimet e NATO-s (2020) tregojnë se një kulturë e fortë sigurie rrit besueshmërinë e trupave dhe ul ndjeshëm numrin e incidenteve gjatë stërvitjeve dhe operacioneve. Për më tepër, siguria ndikon drejtpërdrejt në moralin e trupave: kur ushtarakët ndihen të mbrojtur, ata janë më të motivuar dhe më të përkushtuar ndaj misionit.

Kultura e sigurisë, për të qenë e qëndrueshme dhe efektive, duhet të mbështetet mbi disa shtylla bazë. Së pari, trajnimi i vazhdueshëm është i domosdoshëm për të përgatitur ushtarakët ndaj çdo rreziku, duke përfshirë simulime dhe ushtrime praktike. Së dyti, komunikimi i hapur është një faktor kyç: raportimi i çdo gjëje që nuk shkon (gabime, devijime, incidente etj.), pa frikë nga ndëshkimi ndihmon në nxjerrjen e mësimeve dhe përmirësimin e procedurave. Së treti, drejtuesit e përgjegjshëm luajnë rol vendimtar, pasi ata duhet të japin shembull në respektimin e rregullave të sigurisë. Teknologjia moderne (pajisjet mbrojtëse, sistemet e monitorimit etj.), është një tjetër element që ul rreziqet. Gjithashtu, disiplina institucionale garanton që rregullat të zbatohen pa kompromis, duke shmangur devijimet që mund të sjellin pasoja fatale. Kultura e sigurisë nuk shpërfaqet vetëm në teori, por reflektohet edhe në praktikë. Kështu për shembull, në operacionet paqeruajtëse të NATO-s në Afganistan dhe Kosovë, respektimi i protokolleve të sigurisë ka ulur ndjeshëm humbjet joluftarake.[23] Ministria e Mbrojtjes ka integruar standardet e sigurisë

[22] J. Reason, *Managing the risks of organizational accidents*. (Aldershot: Ashgate, 1997).
[23] NATO, *Lessons learned from peacekeeping missions*. (Brussels: NATO HQ, 2015).

të NATO-s në stërvitjet kombëtare, duke përmirësuar menaxhimin e rreziqeve dhe reagimin ndaj emergjencave (Ministria e Mbrojtjes, 2021). Një fushë e re ku kultura e sigurisë mbetet jetike është siguria kibernetike, pasi të tilla sulme mund të paralizojnë sistemet ushtarake dhe të rrezikojnë misionet.[24] Parë në këtë kontekst, natyrshëm lind pyetja: cilat janë sfidat e kulturës së sigurisë në të ardhmen? Mendoj që më të rëndësishmet mund të jenë: së pari, rreziqet e reja, si kërcënimet kibernetike, biologjike dhe teknologjike, sepse ato kërkojnë përshtatje të vazhdueshme; së dyti, ndërgjegjësimi i vijueshëm, pasi siguria nuk duhet parë si një detyrë e përkohshme, por si pjesë e identitetit ushtarak; dhe së treti, integrimi ndërkombëtar i cili është i domosdoshëm, sepse kërkon një harmonizim të praktikave kombëtare me standardet e NATO-s dhe BE-së për të siguruar bashkëpunim efektiv.

Në këtë kuadër, kultura e sigurisë në Forcat e Armatosura mbetet një element themelor për mbrojtjen e jetës, suksesin e misioneve dhe forcimin e besimit publik. Ajo kërkon përkushtim të vazhdueshëm, disiplinë dhe bashkëpunim. Vetëm përmes një kulture të fortë sigurie, Forcat e Armatosura mund të përmbushin me dinjitet dhe profesionalizëm misionin e tyre madhor: mbrojtjen e atdheut dhe kontributin në paqen ndërkombëtare. Siç dëshmojnë praktikat e NATO-s dhe përvoja e forcave tona të armatosura, siguria nuk është një opsion, por një domosdoshmëri.

3. Ndërthurja midis etikës profesionale dhe kulturës së sigurisë

Në shoqërinë moderne, ku dinamika e punës dhe teknologjisë po zhvillohet me ritme të shpejta, etika profesionale dhe kultura e sigurisë përbëjnë një domosdoshmëri për funksionimin e shëndetshëm të organizatave. Nëse etika profesionale lidhet me normat morale dhe standardet që udhëheqin sjelljen e individëve në profesionin e tyre, kultura e sigurisë ka të bëjë me krijimin e një mjedisi pune të mbrojtur, të përgjegjshëm dhe të qëndrueshëm. Ky kombinim siguron jo vetëm cilësi dhe besueshmëri në punë, por edhe mbrojtjen e sigurinë e organizatës dhe anëtarëve të saj.

Ndërthurja midis etikës profesionale dhe kulturës së sigurisë është e natyrshme dhe e domosdoshme. Pa një etikë të fortë profesionale, kultura e sigurisë nuk mund të ekzistojë. Një individ, që vepron me përgjegjshmëri dhe ndershmëri nuk do të neglizhojë rregullat e sigurisë, nuk do të fshehë gabimet dhe nuk do të rrezikojë veten apo të tjerët për përfitime afatshkurtra. Po ashtu, një lidership etik krijon mjedisin e duhur ku siguria vlerësohet, promovohet dhe zbatohet në mënyrë konsekuente. Në këtë mënyrë, etika profesionale bëhet themeli mbi të cilin ndërtohet dhe zhvillohet kultura e sigurisë. Kjo do të thotë që etika profesionale kërkon ndershmëri dhe përgjegjësi, ndërsa kultura e sigurisë e përforcon këtë duke e orientuar drejt mbrojtjes së jetës dhe

[24] P. W. Singer, & A. Friedman, *Cybersecurity and cyberwar: What everyone needs to know*. (Oxford University Press, 2014).

mjedisit; një profesionist etik nuk e neglizhon sigurinë, sepse e konsideron atë si pjesë të detyrës morale; organizatat që investojnë në kulturën e sigurisë, në fakt, po investojnë edhe në etikën profesionale, duke krijuar një mjedis pune ku respekti dhe përgjegjshmëria janë vlera të përbashkëta.

Duke e parë në këtë këndvështrim, etika profesionale dhe kultura e sigurisë nuk janë koncepte të ndara, por pjesë e së njëjtës filozofi pune që synon të mbrojë jetën, dinjitetin dhe profesionalizmin. Organizatat dhe individët që i vënë në qendër këto vlera, ndërtojnë një mjedis pune më të sigurt, më efikas dhe më të drejtë, duke kontribuar në përparimin e qëndrueshëm të shoqërisë. Raporti midis etikës profesionale dhe kulturës së sigurisë është thelbësor dhe i pazgjidhshëm. Etika profesionale garanton që punonjësit të veprojnë me përgjegjësi dhe me integritet, ndërsa kultura e sigurisë siguron kushtet praktike që këto parime të zbatohen në mënyrë efektive. Është e rëndësishme të theksohet se pajtueshmëria me kodin e etikës nuk duhet të shihet si një detyrim, por më tepër si një përgjegjësi e çdo individi.

Etika profesionale dhe kultura e sigurisë kanë ndikime të ndërsjella. Punonjësit etikë respektojnë procedurat dhe standardet e sigurisë, sepse e shohin këtë si një detyrim moral, jo thjesht ligjor. Profesionistët me integritet nuk bëjnë kompromis me sigurinë, edhe kur ndodhen nën presion për të kursyer kohë apo burime. Ata promovojnë komunikim të hapur dhe të sinqertë, duke ndihmuar organizatën të mësojë dhe të përmirësohet. Gjithashtu, një mjedis i sigurt dhe i mirëorganizuar u jep anëtarëve mundësinë të veprojnë si profesionistë të vërtetë. Kultura e sigurisë krijon besim tek strukturat dhe midis anëtarëve e lidershipit. Kur punonjësit shohin se siguria vlerësohet, ata ndihen më të motivuar të ruajnë standarde të larta etike. Kultura e sigurisë shërben si një kujtesë e përditshme se veprimet e tyre kanë ndikim të drejtpërdrejtë në jetën e të tjerëve.

Në këtë kuadër, kultura e sigurisë duke qenë një grup vlerash, besimesh dhe standardesh brenda organizatës inkurajon njerëzit të veprojnë me sigurinë si përparësinë kryesore. Në një organizatë me një kulturë aktive sigurie, individët zgjedhin lirisht dhe vullnetarisht të ndërmarrin veprime të sigurta dhe të shmangin rreziqet (gabimet) dhe kur ata nuk mbikëqyren drejtpërdrejt ose nuk u thuhet se çfarë të bëjnë. Kultura e sigurisë është e rëndësishme sepse modulon sjelljen e anëtarëve në organizatë. Kjo bën të mundur rritjen e mundësive që të gjitha masat paraprake të sigurisë të ndiqen dhe të ekzekutohen siç duhet.

Përfundime

Etika profesionale dhe kultura e sigurisë janë dy dimensione që shkojnë krah për krah dhe forcojnë njëra – tjetrën. Etika profesionale krijon bazën morale dhe parimore, ndërsa kultura e sigurisë siguron mjedisin praktik për zbatimin e këtyre parimeve. Organizatat që i japin rëndësi të vërtetë këtyre dy elementeve ndërtojnë mjedise pune më të sigurta, më efikase dhe më të

qëndrueshme. Në këtë mënyrë, ato kontribuojnë jo vetëm në mirëqenien e anëtarëve, por edhe në zhvillimin e përgjithshëm të shoqërisë.

Etika profesionale dhe kultura e sigurisë nuk janë thjesht rregulla të shkruara, por janë filozofi e të menduarit dhe të vepruarit në mjedisin profesional. Ato garantojnë jo vetëm suksesin e individëve dhe organizatave në FA, por edhe mbrojtjen e shoqërisë në tërësi. Një profesionist i vërtetë është ai që vepron me integritet, përgjegjësi dhe kujdes, duke e vendosur sigurinë dhe etikën në qendër të çdo veprimi. Vetëm përmes këtij kombinimi mund të ndërtohet një kulturë pune e qëndrueshme, e besueshme dhe e respektuar. Të kesh një kod etik të përcaktuar mirë, i cili ndahet gjerësisht midis të gjithë anëtarëve të organizatës, është bazë për promovimin e vlerave etike dhe forcimin e kulturës organizative. Prandaj, është thelbësore që organizatat të investojnë në zhvillimin dhe zbatimin e udhëzimeve të qarta dhe objektive etike që drejtojnë apo orientojnë sjelljen e njerëzve të tyre. Krijimi i një kulture sigurie të qëndrueshme është faktor i rëndësishëm në edukimin dhe veprimin praktik të personelit në përputhje me kërkesat përkatëse.

Jetëgjatësia e një organizate dhe siguria e saj varen nga vizioni i lidershipit dhe bashkëpunimi i anëtarëve me njëri-tjetrin për të arritur qëllimet. Drejtuesit janë përgjegjës për krijimin e normave që e mbështesin këtë lloj bashkëpunimi.

Bibliografia

1. Dale Carnegie, "Arti për t'u bërë i paharrueshëm", Shtëpia Botuese "Pegi", Viti 2018, ISBN: 978-9928-233-24-0.
2. Kevin Cashman, "Leadership from the inside out" (second edition), Berrett-Koehler Publishers, Inc., San Francisco, California, 2008), ISBN 978-1-57675-599-0.
3. Steve Chandler, Duane Black, "Mos i gjyko punonjësit", Shtëpia Botuese "Max", 2014, ISBN 978-99956-23-37-1.
4. R. Gjatoja, A. Lala, K. Xharo, E. Braneshi, "Udhëheqja Strategjike", Shtëpia Botuese "GEER", Tiranë 2010, ISBN: 978-9928-105-15-8.
5. Samuel Hantigton, "Ushtaraku dhe shteti", Shtëpia Botuese e ushtrisë, Tiranë 1995.
6. Bashkim Kozeli, Ilir Spahiu, "Edukimi qytetar dhe Etika në Forcat e Armatosura", Shtëpia Botuese e Ushtrisë, Tiranë 2000.
7. Diana Liçi, "E drejta në Forcat e Armatosura" (pjesa e dytë), Shtëpia Botuese "Filara", Tiranë 2023, ISBN: 978-9928-279-99-6.
8. Vasil Naçi, Alma Bici, "Është rruga jonë, rruga e suksesit në Agna group", Agna Leadership Academy 2013.
9. Michael J. Papa, Tom D. Daniels, B. K. Spiker "Kominikimi organizativ,

qasjet dhe prirjet", Shtëpia Botuese UET Press, viti 2009, ISBN: 978-99956-39-12-9.

10. Dr. Guri Pashaj, Dr. Ahmet Leka, Bardhyl Hoxha, Msc Valbona Zeka, "Etika ushtarake dhe arti i komandimit", Publikim i Qendrës së Doktrinës në Komandën e Doktrinës dhe Stërvitjes, Tiranë 2013, ISBN: 978-9928-171-02-3.
11. Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.
12. Schein, E. H. 1988. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.
13. Simon Sinek, "Fillo me pse, si liderët e mëdhenj frymëzojnë këdo që të veprojë", Shtëpia Botuese "Minerva", Viti 2019, ISBN: 978-9928-261-16-1.
14. Simon Sinek, "Loja e pafundme", Shtëpia Botuese "Minerva", Viti 2020, ISBN: 978-9928-265-26-5.
15. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
16. Perry M. Smith, "Taking Charge, a practical guide for leaders", National Defense University Press, Washington, D.C. 1986.
17. Brian Tracy, "Fito atë për të cilën ti vlen", Botime "Reklama", Tiranë 2023, ISBN: 978-9928-308-59-7.
18. Brian Tracy, "Lidershipi" Shtëpia Botuese "Damo", Prishtinë 2014, ISBN: 978-9951-642-27-9.
19. Brian Tracy, "Ndryshoni të menduarit tuaj, ndryshoni jetën tuaj, si të zbulosh potencialin tënd për sukses e arritje", Botimet Elta BS, Viti 2009, ISBN; 987-9951-544-08-5.
20. NATO. (2015). *Lessons learned from peacekeeping missions*. Brussels: NATO HQ.
21. "Udhëheqja Ushtarake (Studime nga ushtarakë të lartë amerikanë)" Shtëpia Botuese e Ushtrisë, Tiranë 1995.

Operacionet me shumë fusha: pikë kthese dhe sfidë për arsimin profesional ushtarak

Nënkolonel Mazllum ALLA
Oficer shtabi/specialist/kërkues për studime dhe analizë strategjike, IKSHU

Trajtesë e shkurtuar

Ky shkrim trajton konceptin e Operacioneve me Shumë Fusha (MDO) si një evolucion doktrinar në luftën moderne dhe ndikimet e tij për Arsimimin Profesional Ushtarak. Ai përqendrohet në origjinën dhe veçoritë e operacioneve me shumë fusha, si dhe identifikon sfidat që lidhen me arsimimin profesional për përgatitjen për operacionet e të ardhmes. Shkrimi bazohet në teorinë dhe përvojën e deritanishme, duke ju referuar dokumenteve dhe publikimeve nga studiues dhe ekspertë të vendeve të NATO-s dhe më gjerë. Përmes analizës krahasimore, shqyrton shkurtimisht qasjet e ndryshme të integrimit të MDO-ve në kurrikulat e arsimimit profesional të tre institucioneve arsimore—Kolegji i Mbrojtjes së NATO-s (NDC), Kolegji i Luftës së Ushtrisë Amerikane (USAWC) dhe Kolegji Mbretëror i Mbrojtjes së Danimarkës (RDDC). Gjetjet e këtij studimi tregojnë se përfshirja e MDO-ve në arsimin profesional është një proces i domosdoshëm për përgatitjen e forcave të armatosura ndaj sfidave të së ardhmes, duke theksuar nevojën për rishikim të kurrikulave, zhvillim të metodave pedagogjike ndërdisiplinore dhe kultivim të kapaciteteve analitike tek oficerët e ardhshëm. Në përfundim, artikulli thekson rëndësinë e zhvillimit të një moduli të dedikuar për operacionet me shumë fusha në arsimin tonë profesional, duke luajtur një rol të rëndësishëm në përshtatshmërinë e doktrinës, lidershipit dhe personelit në të ardhmen.

Fjalët kyçe: operacione me shumë fusha; arsimi profesional ushtarak; zhvillimi i kurrikulës; evolucioni doktrinar; arti operativ

Hyrje

Ndryshimet dinamike në mjedisin e sigurisë të ndodhura në dekadën e fundit kanë ndikuar ndjeshëm mënyrën e të menduarit dhe të kryerjes së operacioneve luftarake. Forcat ushtarake përballen me një hapësirë beteje

të gjerë dhe nivele lufte të ngjeshur duke vepruar në një mjedis kompleks shoqëror, teknologjik dhe ekonomik. Teknologjia po bëhet një nga aspektet më të shpejta në ndryshim të mjedisit të sigurisë. Ajo po ndryshon edhe mjedisin e operacioneve. Kjo është veçanërisht e vërtetë për teknologjitë e reja dhe lehtësisht të disponueshme si – dronët, robotët dhe sistemet autonome. Mësimet e nxjerra nga konfliktet dhe operacionet ushtarake në vitet e fundit vërtetojnë vlerën e të kuptuarit të dimensioneve të këtyre ndryshimeve.

Nga ana tjetër, *mjedisi i operacioneve* karakterizohet nga një kompleksitet në rritje dhe nga zbehja e kufijve tradicionalë ndërmjet fushave. Ai po zgjerohet përtej kufijve ushtarakë, me konkurrencën midis aktorëve të ndryshëm që po bëhet më e fortë në të gjitha instrumentet e fuqisë. Ky mjedis gjithashtu paraqet aktorë më të larmishëm, me armë dhe teknologji të reja të përdorura në mënyra të reja. Si rrjedhojë, përmbushja me sukses e objektivave në këtë mjedis veprimi kërkon balancimin e përpjekjeve të instrumentit ushtarak të fuqisë në të gjitha kontekstet formësuese, konkurruese dhe konfliktit. Madje, konkurrenca ushtarake ka tendencë të ndryshojë në mënyrën se si zhvillohen luftërat, si dhe me *konceptet operacionale* dhe teknologjitë e reja që lidhen me këto ndryshime.[1] Për më tepër, kjo sjell pasoja mbi forcat ushtarake për të kuptuar luftën moderne.

Në të njëjtën kohë, nocionet e rëndësishme të Artit Ushtarak - si hapësira dhe koha, fronti, thellësia dhe prapavija - kanë evoluar dhe mjedisi i operacioneve të sotme është zgjeruar dhe ngjeshur njëkohësisht, duke rritur kompleksitetin me të cilin mund të zhvillohet lufta. Kështu, faktori distancë/hapësirë mund të zvogëlojë efektin kufizues të armëve vdekjeprurëse dhe jo-vdekjeprurëse nga kudo në botë. Ky është rasti i rritjes së rëndësisë së *aftësive hapësinore dhe kibernetike*, të cilat mund të gjenerojnë pasoja vdekjeprurëse dhe jo-vdekjeprurëse në çdo cep të globit. Efektet e tyre kanë ndikime pothuajse të menjëhershme pa marrë parasysh hapësirën gjeografike dhe kufijtë politikë të shteteve.

Historikisht, ushtritë janë përpjekur të përshtatin strategjitë e tyre me zhvillimet më të fundit, qofshin ato taktike, teknologjike apo organizative. Por, përparimet teknologjike që po ndodhin tani kërkojnë koncepte dhe metoda të reja rreth të cilave do të organizohet dhe do të zhvillohet lufta në të ardhmen. Në këtë kuadër, Operacionet me Shumë Fusha (*Multi-Domain Operations*) është termi që po diskutohet gjerësisht dhe që i jep rëndësi konceptit në zhvillim të integrimit të aftësive në *fushat tokësore, ajrore, detare, kibernetike dhe hapësinore* për të krijuar avantazhin dhe epërsinë operacionale në konfliktet e ardhshme.

Është për t'u theksuar se operacionet me shumë fusha përfaqësojnë një ndryshim të rëndësishëm në qasjen e NATO-s dhe vendeve anëtare ndaj luftës.

[1] Michael J. Mazarr, Bryan Frederick, etj., Understanding a New Era of Strategic Competition, Santa Monica, California: RAND Corporation, 2022; në https://www.rand.org/pubs/research_reports/RRA290-4.html.

Zëvendësshefi i Shtabit të Komandës Aleate për Transformimin, Gjenerallejtënant Thomas J. Sharpy, në një Seminar Vjetor të Qendrës së Ekselencës për Komandim-Kontrollin (C2COE), për '*operacionet me shumë fusha dhe të ardhmen e luftës'*, shprehej se: "…kushdo që është i pari që zotëron Operacionet me Shumë Fusha (MDO) mund të mos e kontrollojë botën, por do të ketë një avantazh të rëndësishëm në të."[2] Edhe pse shumë shkurtimisht, kjo pikëpamje e tij është e rëndësisë së veçantë sepse ngërthen në vete dy aspekte të rëndësishme të këtyre operacioneve: aftësitë dhe përparësitë e tyre.

Kjo tregon se në peizazhin dinamik të luftës moderne, koncepti i operacioneve me shumë fusha shfaqet si një imperativ strategjik – në përgjigje ndaj ndryshimeve në mjedisin e sigurisë, zhvillimit teknologjik dhe evolucionit të luftës. Duke ndërthurur shumë fusha këto operacione riformësojnë paradigmat tradicionale në një qasje gjithëpërfshirëse që rrit fuqinë operacionale, shpejtësinë e reagimit dhe thellësinë strategjike. Për këtë arsye, koncepti i operacioneve me shumë fusha zgjeron kërkesat për përgatitjen e forcave të armatosura, duke sjellë ndryshime si në mjedisin akademik, ashtu edhe në atë operacional. Ky tranzicion nuk është thjesht një ndryshim metodologjik, por një *pikë kthese*, që kërkon një transformim themelor të kurrikulave, metodave të mësimdhënies dhe mentalitetit institucional për arsimin profesional.

Ky shkrim trajton konceptin e operacioneve me shumë fusha dhe ndikimin e tyre në arsimimin profesional nga një qasje perspektive, duke i kushtuar vëmendje të veçantë ndryshimeve që kanë ndodhur në dekadën e fundit, rolit të inovacionit të shpejtë teknologjik dhe shpërndarjes së informacionit në zhvillimin e tyre. Ai përshkruan origjinën dhe karakteristikat e MDO-ve, identifikon sfidat e përgatitjes për operacionet e së ardhmes dhe nxjerr në pah rolin e arsimit profesional ushtarak. Qëllimi është të ofrohet një kuadër analitik fillestar, i cili mund të shërbejë si nxitje për reformimin e arsimit tonë ushtarak në epokën e operacioneve me shumë fusha.

1. Vështrim i përgjithshëm mbi konceptin e operacioneve me shumë fusha (MDO) të SHBA-ve dhe NATO-s

Operacionet me shumë fusha janë tashmë koncepti mbizotërues brenda ushtrisë amerikane, NATO-s dhe vendeve të tjera të përparuara nga ana teknologjike. Në veprimtarinë e aleancës nuk mund të gjesh një aktivitet ushtarak pa hasur këtë koncept. Studiues dhe analistë të shumtë pothuajse të gjithë kanë një perspektivë. Disa thonë se është një "libër i vjetër në një mbështjellje të re". Dhe disa të tjerë e klasifikojnë atë si diçka të re dhe të nevojshme. Por, si lindi koncepti i MDO-ve? Pse janë ato të rëndësishme?

[2] General Leitnant Thomas J. Sharpy, "*Multi-Domain Operations: The Future of Warfare*" (C2 COE, Utrecht, Holland, 2020); p. 1; në, https://c2coe.org/seminar-read-ahead-multi-domain-operations-the-future-of-warfare/

Ngjarjet komplekse dhe të paparashikuara që ndodhën veçanërisht pas vitit 2014, kur Rusia aneksoi Krimenë, demonstruan nevojën për të ndryshuar mënyrën e të menduarit dhe të drejtimit të operacioneve ushtarake. Kështu, që nga viti 2015, udhëheqja ushtarake amerikane arsyetoj se ishte koha për një strategji të re për luftërat e ardhshme, një strategji për të arritur fitoren edhe në një konflikt me shkallë të gjerë. Për këtë, në vitin 2017 ushtria amerikane publikoj konceptin *"Beteja me Shumë Fusha: Evolucioni Gjitharmësh* për Shekullin e 21-të,"[3] për të ndryshuar mënyrën e zhvillimit të operacioneve të ardhshme. Ky koncept fillestar u hartua për të paraqitur një perspektivë të re se si lufton ushtria amerikane, si në qëllim ashtu edhe në formë, për t›iu përgjigjur sfidave të përfshirjes dhe përhapjes së teknologjive të reja.

Narrativa e betejës në shumë fusha (*Multi-Domain Battle*) erdhi si rezultat i drejtpërdrejtë i strukturave kërkimore amerikane që ofruan një përfytyrim, përshkrim dhe kuptim të qartë të asaj që nevojitej për të fituar në luftërat e ardhshme. Në fakt, origjina e konceptit të betejës në shumë fusha mund të gjurmohet që në prill të vitit 2015 në Kolegjin e Luftës të Ushtrisë Amerikane, ku zëvendëssekretari i Mbrojtjes i atëhershëm, Bob Work, në fjalimin e tij përshkroi problemet që do të krijojë lufta e shekullit 21-të dhe zgjidhjet që do të kërkojë. Sipas fjalëve të Work:

"Do të na duhet të mendojmë për luftën kundër armiqve që kanë shumë raketa të drejtuara, raketa balistike, artileri, mortaja, dhe që do përdorin luftë të informatizuar për të ndërprerë plotësisht forcën tonë të rrjetëzuar... kombinimi i municioneve të drejtuara dhe luftës së informatizuar - është një ndryshore kritike për suksesin e forcave ushtarake në luftën e shekullit të njëzet e një."[4]

Në Konceptin 1.0 "*Beteja me Shumë Fusha: Evolucioni Gjitharmësh* për Shekullin e 21-të", arti i realizimit të sinergjisë ndërmjet fushave lidhej me konvergjencën dhe integrimin e të gjithë sistemeve, në kohë dhe hapësirë, duke u përqendruar jo vetëm te njerëzit dhe proceset, por edhe te zgjidhjet teknologjike të nevojshme për të arritur një qëllim të caktuar. Për më tepër, koncepti i betejës me shumë fusha përshkruante një strukturë të zgjeruar të fushëbetejës për të luftuar në të gjithë gjerësinë dhe thellësinë e kapaciteteve të armikut, duke u shtrirë nga vija e frontit në venddislokimet bazë dhe nëpër shumë fusha.[5]

Ndërsa në vitin 2018, termi "*betejë*" u zëvendësua me termin "*operacion*"[6],

[3] *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century*, Version 1.0, dhjetor 2017, në https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo129084/pdf/GOVPUB-D101-PURL-gpo129084.pdf

[4] Kelly McCoy, *The Road to Multi-Domain Battle: An Origin Story*, (Modern War Institute, 2017), në: https://mwi.westpoint.edu/road-multi-domain-battle-origin-story/.

[5] David G. Perkins, *Multi-Domain Battle: Driving Change to Win in the Future,* Military Review; Fort Leavenworth Vol. 97, Iss. 4, (Jul/Aug 2017): fq. 6-12.

[6] The Association of the United States Army, *Multi-Domain Battle Gets a New Operational Name*, 23 maj 2018, në https://www.ausa.org/news/multi-domain-battle-gets-new-operational-name

pasi kjo ishte më në përputhje me mënyrën se si ushtria amerikane e parashikonte luftimin e përbashkët. Me fjalë të tjera, megjithëse ushtria amerikane zgjodhi një term të ri për betejën në shumë fusha, ideja mbeti e njëjtë: si e integron ushtria amerikane fuqinë luftarake kundër kundërshtarëve pothuajse të barabartë. Zyrtarisht, termi *multi-domain operations*, u përdor për herë të parë si një koncept doktrinar në vitin 2018, të titulluar – *Ushtria Amerikane në Operacione me Shumë Fusha 2028*.[7] Ky koncept u ngrit mbi doktrinën e viteve 1980 "Beteja Ajrore-Tokësore" (*Air-Land Battle*), e cila u përcaktua si një përgjigje ndaj kërcënimit nga ushtria sovjetike në teatrin evropian të kohës.[8]

Në fakt, koncepti i "Operacioneve me Shumë Fusha" kërkon njësi ushtarake të mëdha vërtet të integruara, elastike dhe të dislokueshme me shpejtësi, të organizuara për të zhvilluar manovra dhe zjarre ndër-domene, të afta të veprojnë së bashku dhe në një konvergjencë që shkon përtej sinkronizimit. Sipas doktrinës amerikane, *Divizioni* është zakonisht *niveli më i ulët taktik* që përdor aftësi nga fusha të shumëfishta për të arritur konvergjencën gjatë operacioneve luftarake në shkallë të gjerë. [9] Madje, manuali *FM 3-0 Operacionet*, thekson angazhimin e ushtrisë amerikane për operacione në shkallë të gjerë dhe përshkruan se si i zhvillojnë MDO-të brenda një kuadri të përbashkët dhe shumëkombësh.

Nga ana tjetër, NATO ka ndjekur konceptin Amerikan të MDO-ve për të përshtatur më mirë aftësitë e saj me kthimin e kërcënimit të konfliktit shtet-me-shtet në dekadën e fundit. Për këtë më 19 maj 2023, të gjitha vendet e NATO-s miratuan Konceptin e Aleancës për MDO-të.[10] Ky koncept sinjalizoi zyrtarisht transformimin e NATO-s nga një qasje e bashkuar (joint), e fokusuar në tre shërbimet ushtarake, në një qasje me shumë fusha. NATO i ka përkufizuar operacionet me shumë fusha (MDO) si *'orkestrimin e aktiviteteve ushtarake, në të gjitha fushat dhe mjediset, të sinkronizuara me aktivitete jo-ushtarake, për t'i mundësuar Aleancës të krijojë efekte konvergjente me shpejtësinë e kërkuar*'.[11] Ky përkufizim për MDO-të u hartua duke mbajtur parasysh se aktivitetet në pesë fushat operacionale krijojnë efekte konvergjente në tre dimensione (fizik, virtual, konjitiv). Pra, koncepti i Aleancës për MDO-të pasqyron një zhvendosje drejt një qasjeje më gjithëpërfshirëse dhe të ndërlidhur

[7] TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 6 dhjetor 2018, në https://info.publicintelligence.net/USArmy-MultidomainOps2028.pdf

[8] Dennis Wille, *The Army and Multi-Domain Operations: Moving Beyond AirLand Battle* (New America, 2019), në https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Army_and_Multi-Domain_Operations_Moving_Beyond_AirLand_Battle_2019-09-23_175932.pdf

[9] Field Manual 3-0 *Operations*, US Army, 2022. fq. 2-19, paragrafi 2.89

[10] *The Status of MDO in NATO*, NATO Multi-Domain Operation Conference 2023, 10-11 Tetor, Kopenhagen, Danimarkë, fq.9, në https://www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Report-LR.pdf

[11] *"Alliance Concept for Multi-Domain Operations",* 19 Maj 2023, fq.9.

ndaj luftës, duke theksuar se konfliktet moderne shtrihen përtej fushave tradicionale ushtarake.[12] Kjo qasje e NATO-s ndaj MDO-ve thekson sinkronizimin e veprimit ushtarak me instrumente të tjera të fuqisë, duke nënvizuar njëkohësisht rëndësinë themelore të 'transformimit digjital' për aleancën.

Ky koncept përshkruan katër parimet që janë themelore për orientimin e suksesshëm të NATO-s drejt një Aleance të aftë për MDO: *Uniteti, Ndërlidhshmëria, Kreativiteti* dhe *Shkathtësia*.[13] Gjithashtu, identifikon edhe faktorët për të mundësuar zhvillimin e MDO-ve, që janë: *të dhënat*, *avantazhi teknologjik*, *komandimi dhe kontrolli* (C2) në shumë-fusha, "*njerëzit e duhur, aftësitë e duhura*" dhe *trajnimi kolektiv*.[14] Si një koncept i fokusuar në zhvillim, ai nuk përshkruan veprime që forcat ushtarake mund të ndërmarrin. Megjithatë, koncepti i operacioneve me shumë fusha është një evolucion i operacioneve të përbashkëta dhe kalimi drejt tyre filloi kur Aleanca përfshiu fushat kibernetike dhe hapësinore… të cilat po ndryshojnë mënyrën se si vepron Aleanca".[15]

Natyrisht, koncepti i NATO-s për operacionet me shumë fusha nuk është vetëm përmirësimi i operacioneve të përbashkëta thjesht duke shtuar fusha të reja. Qasja e NATO-s lidhet kryesisht me një ndryshim të mentalitetit gjatë planëzimit dhe zhvillimit të operacioneve moderne me qëllim orkestrimin e efekteve në të gjitha dimensionet (fizike, virtuale dhe kognitive), në të gjitha fushat (detare, tokësore, ajrore, hapësinore dhe kibernetike), në të gjitha nivelet e komandës dhe duke përdorur të gjitha Instrumentet e Fuqisë (IoP) të aleancës – ushtarake, informative, politike dhe ekonomike.[16] Sidoqoftë, synimi kryesor i MDO-ve është krijimi i efekteve konvergjente; këto efekte mund të ndodhin në dimensione fizike (trupa në terren, bomba në objektiv), virtuale (operacione informacioni ose efekte kibernetike) ose konjitive (ku ndikohen qëndrimet dhe sjelljet).

Operacionet me shumë fusha përfaqësojnë një evolucion doktrinar në luftën moderne, duke kërkuar nga forcat e armatosura të integrojnë aftësitë tokësore, ajrore, detare, kibernetike dhe hapësinore. Karakteristikat dalluese i veçojnë MDO-të nga operacionet tradicionale të përbashkëta dhe shtrojnë kërkesa të reja ndaj arsimimit ushtarak profesional. Karakteristikat kryesore të MDO-ve janë *integrimi në të gjitha fushat* (tokë, ajër, det, kibernetikë, hapësirë), *veprimi*

[12] NATO Allied Command Transformation, *Multi-Domain Operation Conference Report*, 10-11 Tetor 2023, Kopenhagen, Danimarkë, fq. 12, parë 4 Maj 2025, në https://www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Report-LR.pdf

[13] "*Alliance Concept for Multi-Domain Operations*", 19 Maj 2023, fq. 14

[14] Po aty fq.15

[15] AJP-01 *Allied Joint Doctrine* Edicioni F Versioni 1, Dhjetor 2022, Fq.93

[16] Shaun Cannon, *The Alliance's Transition to Multi-Domain Operations*, Journal of the JAPCC, Edicioni 37, Maj 2024, fq.17, në: https://www.japcc.org/wp-content/uploads/JAPCC_J37_screen.pdf

i njëkohshëm, konvergjenca, përshtatshmëria ndaj ndryshimeve të shpejta, ndërveprueshmëria, inovacioni teknologjik, planëzimi ndër-nivelor, qëndrueshmëria dhe dominimi konjitiv.[17] Së bashku, këto tipare i bëjnë MDO-të një qasje gjithëpërfshirëse ndaj luftës moderne.

Është e rëndësishme të mbahet parasysh se zhvillimi i operacioneve me shumë fusha (MDO) të NATO-s kërkon orkestrimin e Instrumenteve Ushtarake të Fuqisë (IoP)[18] të *tridhjetë e dy vendeve anëtare* për të vepruar së bashku – pavarësisht dallimeve – duke sinkronizuar aktivitetet ushtarake me instrumentet e tjera jo-ushtarake, partnerët si dhe palët e interesuara nga akademia dhe industria.

Sidoqoftë, përveç SHBA-ve, akoma nuk është e qartë se si një vend aleat do ti zbatojë MDO-të brenda forcave të tij ushtarake dhe agjencive të tjera. Madje, duhet theksuar se pavarësisht vëmendjes në rritje ndaj operacioneve me shumë fusha nga disa vende të aleancës, ata janë shumë larg nga Shtetet e Bashkuara. Ndërsa shumë qasje të vendeve aleate mbeten konceptuale, Ushtria Amerikane po ngre në mënyrë aktive struktura për MDO-të me synim – të krijojë një forcë të aftë për MDO-të deri në vitin 2028 dhe një forcë të gatshme për MDO-të deri në vitin 2035.[19] Megjithatë, ajo që i dallon Shtetet e Bashkuara nga aleatët e tjerë, janë përparësitë e tyre për ta operacionalizuar këtë koncept dhe për të integruar aftësitë e MDO-ve në nivelin operacional dhe taktik.

Jashtë ushtrisë amerikane, konkretisht në vendet evropiane, termi "*operacioneve me shumë fusha"* është më i përgjithshëm dhe është e qartë se do të thotë gjëra të ndryshme për vende të ndryshme. Kjo shërben për të nxjerrë në pah se, edhe pas disa vitesh përpjekjesh ushtarake dhe akademike në shtetet aleate, idetë kryesore mbeten shumë të diferencuara. Por, pavarësisht se si përdoret termi MDO në NATO ose në ushtrinë amerikane, mund të nënvizojmë një element të përbashkët. Ky element është vendosmëria e Aleancës dhe vendeve anëtare për tu ballafaquar me sfidën e imponuar nga lufta komplekse e së ardhmes, përmes shfrytëzimit të teknologjisë. Në fund të fundit, *zbatimi i operacioneve me shumë fusha,* sido që të përcaktohen*, ka të bëjë me të gjithë vendet e NATO-s*.

Në të njëjtën kohë, vlen të theksohet fakti se, ndërsa baza teorike e MDO-ve

[17]Dokumenti i SHBA-ve "Multi-Domain Operations 2028", thekson njëkohshmërinë, konvergjencën dhe përshtatshmërinë si tre tipare përcaktuese të MDO-ve. Ndërsa, Koncepti i Operacioneve Multi-Domain, i NATO-s përshkruan integrimin ndërmjet fushave dhe ndërveprueshmërinë si tipare kryesore.

[18]Instrumentet kombëtare të fuqisë (IoP) ndahen në katër kategori sipas konceptit DIME (diplomacia, informacioni, ushtria, ekonomia).

[19] *The US Army in Multi-Domain Operations 2028,* u publikua në dhjetor 2018, me synim arritjen e "kapacitetit fillestar operacional" deri në vitin 2028 dhe "kapacitetit të plotë operacional" deri në vitin 2035.

është maturuar, sfidat kryesore të zbatimit mbeten – veçanërisht përputhja e qëllimit strategjik me realitetin operacional, ndaj forcat e armatosura dhe strukturat e tyre do të duhet të përshtaten me këtë realitet të ri. Në fund të fundit, *koncepti i Operacioneve me Shumë Fusha* kërkon studim dhe reflektim të kujdesshëm për të trajtuar në mënyrë të arsyeshme kompleksitetin e mjedisit të ardhshëm të sigurisë. Për më tepër, tashmë po zhvillohen sisteme me teknologji të lartë, bazuar në automatizim, veprimit automatik dhe Inteligjencën Artificiale (AI) me qëllim përdorimin e tyre në konfliktet e ardhshme – ndjekur nga dilema se kush do të jetë në krye brenda ekipit me personel/pa personel: njerëzit apo makina.[20]

2. Roli i arsimit profesional ushtarak në përgatitjen për Operacionet me Shumë Fusha

Arsimi Profesional Ushtarak (APU) ka qenë gjithmonë një komponent kritik në zhvillimin e udhëheqësve ushtarakë. Për breza me radhë, synimi i arsimit profesional ka qenë përgatitja dhe zhvillimi i drejtuesve të aftë, të cilët zotërojnë aftësitë teknike dhe taktike të nevojshme për kryerjen e detyrave të tyre, për të marrë vendime dhe për të udhëhequr. Ky synim mbetet thelbësor, por në mjedisin e sotëm të sigurisë, nuk është më i mjaftueshëm.

Ushtarakët sot veprojnë në një mjedis të ndryshëm, me kërcënime të ndryshme dhe mënyra të ndryshme të reagimit. Për shembull, në Ukrainë, improvizimi shpesh ka mposhtur doktrinën, përballë realitetit të kushteve luftarake komplekse dhe me ndryshime të shpejta, duke na mësuar se fushëbeteja nuk i përket vetëm kompleksit ushtarako-industrial, por njerëzve të përkushtuar, të lirë të improvizojnë aty ku është e nevojshme.[21] Ndërsa operacionet në zonën gri – *të cilat kombinojnë mjete joushtarake dhe ushtarake nën pragun e konfliktit të armatosur* – po minojnë parandalimin konvencional.[22] Nga ana tjetër, operacionet kibernetike zhvillohen në mënyra jolineare, pothuajse të padukshme duke mohuar në mënyrë të besueshme përfshirjen e aktorit/ve, dhe duke u bërë një veprimtari në rritje si për aktorët e fuqishëm ashtu edhe për ata të dobët.[23] Këto nuk janë më skenarë hipotetikë— *janë realitete të përditshme në konfliktet e sotme*— veçanërisht në mjediset me

[20] *Army Robotics and Autonomous Systems (RAS) Strategy*, në http://www.arcic.army.mil/App_Documents/RAS_Strategy.pdf

[21] Paul Schwennesen, "*Improvised Genius: Could the United States Match Ukraine's Scrappy Innovation Culture*?" Modern War Institute, 2 tetor 2025, në: https://mwi.westpoint.edu/improvised-genius-could-the-united-states-match-ukraines-scrappy-innovation-culture/

[22] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (US Army War College Press, 2015), në: https://press.armywarcollege.edu/monographs/428

[23] Richard L. Manley, "*Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert*," Joint Force Quarterly 106 (3rd Quarter, July 2022): 64–71, National Defense University Press, në: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3101556/cyber-in-the-shadows-why-the-future-of-cyber-operations-will-be-covert/

shumë fusha dhe kërkon oficerë që dinë të balancojnë njohuritë doktrinare me aftësinë për t'u përshtatur.

Në këtë kontekst, drejtuesit ushtarakë nuk mund të kufizohen vetëm në arsimimin për adresimin e problemeve tradicionale të sigurisë, por duhet të pajisen me aftësinë për të kuptuar dhe vlerësuar kompleksitetet e mjedisit operacional bashkëkohor, të mishëruar në konceptin e Operacioneve me Shumë Fusha. Ky koncept ka nxitur një sërë analizash dhe studimesh, të cilat kanë sjellë në vëmendje nevojën për *ndryshime në arsimin profesional ushtarak*.[24] Rekomandimet e dala nga këto studime variojnë nga reforma të thella dhe strukturore të kurrikulës deri te përshtatja e qasjeve proaktive që synojnë nxitjen e mendimit kritik, zhvillimin e aftësive analitike dhe promovimin e inovacionit si elemente thelbësore për përgatitjen e oficerëve të aftë të përballen me sfidat e sigurisë në shekullin e njëzet e një.

Arsimi profesional ushtarak përbën themelin e përgatitjes për operacionet me shumë fusha dhe krijimin e një kuptimi bashkëkohor mbi luftën. Madje, *arsimi dhe trajnimi janë dy nga mundësuesit kryesorë të operacioneve me shumë fusha*, [25] duke zhvendosur fokusin e NATO-s drejt përgatitjes së përbashkët, shumëkombëshe dhe ndërinstitucionale të drejtuesve të aftë për të integruar instrumentet politike, ushtarake, ekonomike dhe informative të fuqisë për të përballuar sfidat e ardhshme të sigurisë. Mund të tingëllojë e çuditshme, por MDO-të i japin arsimit profesional ushtarak një rol shumë më të rëndësishëm, ndonëse të ndryshëm, në peizazhin e ardhshëm të mjedisit të sigurisë.

Si rrjedhojë, arsimimi për operacionet me shumë fusha është bërë një temë qendrore në arsimin ushtarak, veçanërisht brenda NATO-s dhe mjaft institucioneve arsimore të vendeve anëtare. Kompleksiteti gjithnjë në rritje i luftës moderne në *—tokë, ajër, det, kibernetikë dhe hapësirë*—kërkon që oficerët të trajnohen jo vetëm në fushat tradicionale, por edhe në qasjen e integruar ndër-dimensionale. Progresi drejt operacioneve me shumë fusha do të kërkojë investime në arsim dhe trajnim si në nivelin e NATO-s ashtu edhe në nivel kombëtar, pasi MDO-të kërkojnë aftësi për të sinkronizuar kapacitetet në disa fusha njëkohësisht.[26] Ndaj, integrimi i MDO-ve në arsimin profesional përfaqëson jo vetëm një evolucion konceptual por edhe një domosdoshmëri praktike, duke e përshtatur arsimimin e oficerëve me kërkesat e luftës moderne.

---

[24] Katrine Lund-Hansen and Jeff Reilly, "*The Multi-Domain Operations Approach to Intermediate PME*," War Room – U.S. Army War College, 1 nëntor 2024, në: https://warroom.armywarcollege.edu/articles/the-multi-domain-operations-approach-to-intermediate-pme

[25] NATO Allied Command Transformation, *"Multi-Domain Operations in NATO – Explained,"* 5 tetor 2023, parë më 19 Janar 2026, në: https://www.act.nato.int/articles/multi-domain-operations-in-nato-explained

[26] Andrea Gilli, Mauro Gilli, and Gorana Grgić, *"NATO, Multi-Domain Operations and the Future of the Atlantic Alliance," Comparative Strategy* 43, no. 1 (2024), fq.5–7, në: https://doi.org/10.1080/01495933.2024.2445491

Në shkurt të vitit 2024, ushtria amerikane publikoi konceptin e transformimit të arsimit dhe trajnimit për periudhën 2030–2040 (The Army Learning Concept for 2030–2040*),* i cili thekson se arsimi i ardhshëm profesional duhet të kultivojë *kompetenca të reja, përshtatshmëri dhe mendim kritik* për të përgatitur drejtuesit për operacionet me shumë fusha.[27] Madje kërkon aftësi analitike shkak-pasojë, modelim matematikor dhe dinamikë sistemesh për të parashikuar efektet ndër-fusha. Kërkon kreativitet në parashikimin e veprimeve të reja të kundërshtarit dhe përgjigjeve inovative në disa fusha.

Vlen të theksohet se edhe pse MDO-të ende nuk janë operacionalizuar, tashmë ekziston një koncentrim akademik i dedikuar për arsimimin dhe trajnimin e oficerëve për një mjedis me shumë fusha. Ato janë integruar në kurrikulat e disa universiteteve dhe kolegjeve, në shumë vende si Kolegji i Luftës në SHBA, Akademia e Udhëheqjes në Hamburg, Gjermani, Universiteti i Studimeve të Luftës në Varshavë, Kolegji Mbretëror i Mbrojtjes së Danimarkës, Kolegji i Mbrojtjes së NATO-s në Romë, etj. Për më tepër, Komanda e Transformimit e NATO-s (ACT) ofron një kurs online mbi MDO-të përmes platformës së saj "Joint Advanced Distributed Learning (JADL)". Ndërsa në Kolegjin e Komandës dhe Shtabit të Forcave Ajrore të SHBA-ve *(U.S. Air Force Command and Staff College)* që prej vitit 2018 *zhvillohet një kurs i veçantë i dedikuar për MDO-të* i quajtur*,* Strategu i Operacioneve me Shumë Fusha (*Multi-Domain Operational Strategist* - MDOS)[28]. Ky kurs është një program akademik 10-mujor i krijuar për të trajnuar oficerët në planëzimin dhe zbatimin e operacioneve në të pesë fushat — tokësore, ajrore, detare, hapësinore dhe kibernetike. Ai shihet si një nga programet më inovative të Departamentit të Mbrojtjes, i cili përgatit drejtuesit të mendojnë dhe të veprojnë në mënyrë strategjike në mjedisin e ardhshëm të operacioneve. Sidoqoftë, kursi zhvillohet në nivel tepër sekret dhe nuk pranohen studentë ndërkombëtarë.[29]

Më poshtë përshkruhen shkurtimisht qasjet e tre institucioneve arsimore: Kolegji i Mbrojtjes së NATO-s (NDC), Kolegji i Luftës së Ushtrisë Amerikane (USAWC) dhe Kolegji Mbretëror i Mbrojtjes së Danimarkës (RDDC), duke nxjerrë në pah veçantitë e tyre në trajtimin e MDO-ve.

- *Kolegji i Mbrojtjes së NATO-s* në Romë: shërben si qendra intelektuale për arsimin strategjik të aleancës. Ai filloi të përfshijë operacionet me shumë fusha në kurrikulën e tij në fillim të viteve 2020, pas direktivës së Komitetit Ushtarak të NATO-s për të përcaktuar dhe zhvilluar një Koncept të Aleancës

[27] U.S. Army Training and Doctrine Command, *TRADOC Pamphlet 52582: The Army Learning Concept for 2030–2040* (Fort Eustis, VA: TRADOC, 2024). Fq. iii–iv.

[28] Reilly, Jeff. "*Over the Horizon: The Multi-Domain Operational Strategist (MDOS)*", 8 *nëntor 2018*. Në: https://othjournal.com/2018/11/08/oth-mdos-reilly/

[29] Kimberly Underwood, *Joint All-Domain Warfighting Takes Leadership,* AFCEA International*,* 30 mars 2021*,* në: https://www.afcea.org/signal-media/education/joint-all-domain-warfighting-takes-leadership

për MDO-të. NDC filloi të integrojë zyrtarisht MDO-të në kurrikulën e tij të viteve 2021–2022, dhe në vitin 2023 ato ishin të përfshirë plotësisht në kurse dhe botime si një prioritet arsimor në nivel strategjik, duke shënuar kështu integrimin e plotë të tyre në arsimin strategjik të NATO-s.[30] Qasja e këtij Kolegji ndaj MDO-ve thekson ndërveprimin dhe sinkronizimin e aleancës në të gjitha fushat. Në aspektin arsimor, NDC nxit mendimin strategjik, kohezionin e aleancës dhe ndërfaqen politike-ushtarake, duke siguruar që liderët e lartë të kuptojnë dimensionet doktrinare dhe politike të MDO-ve.[31]

- *Kolegji i Luftës së Ushtrisë Amerikane:* është i ankoruar në zhvillimin doktrinar dhe lidershipin strategjik, duke shërbyer si një institucion qendror për avancimin e qasjes së Ushtrisë Amerikane ndaj operacioneve me shumë fusha (MDO). Kurrikula e tij bazohet në konceptin *Multi-Domain Operations 2028*,[32] që parashikon veprimin në mjedise të kontestuara tokësore, ajrore, detare, hapësinore dhe kibernetike kundër kundërshtarëve të barabartë. Brenda këtij kuadri, kolegji i luftës u mëson oficerëve se si të integrojnë forcat tokësore me forcat e përbashkëta dhe multinacionale, duke siguruar ndërveprim dhe efektivitet nëpër të gjitha fushat. Ky kolegj funksionon si një "laborator mendimi" për inovacionin doktrinar, duke përgatitur drejtues të lartë për të zbatuar konceptet e MDO-ve si në kontekstin amerikan, ashtu edhe në atë të aleancës.[33]

Vlen të theksohet se integrimi i MDO-ve në Kolegjin e Luftës ka marrë një theks të fortë në vitet e fundit, duke reflektuar nevojën për përgatitjen e liderëve për luftën e ardhshme në mjedise shumë-dimensionale. Kështu, Operacionet e Luftës në Shkallë të Gjerë (LSCO) kanë riorientuar kurrikulat për të përgatitur oficerët dhe liderët për konflikte me intensitet të lartë kundër kundërshtarëve të barabartë, duke përfshirë fushat tokësore, ajrore, detare, kibernetike dhe hapësinore.[34] Kjo vëmendje dedikuar MDO-ve siguron arsimim të strukturuar dhe gjithëpërfshirës, duke nxjerrë në pah rëndësinë e aftësive të lidershipit në luftën moderne. Nga ana tjetër, gjatë tre viteve të fundit, arsimi profesional ka ndërmarrë një përpjekje të gjerë për të vlerësuar dhe rishikuar në mënyrë

[30] NATO Defense College. *Anyplace, anywhere, anytime – NATO and multi-domain operations*. Research Paper No. 27. Rome: NATO Defense College, korrik 2023. Në: https://www.ndc.nato.int/research/research.php?icode=0

[31] NATO Defense College. *NATO's Approach to Multi-Domain Operations*. Rome: NDC Publications, 2022.

[32] U.S. Army Training and Doctrine Command. *The U.S. Army in Multi-Domain Operations 2028*. Fort Eustis, VA: TRADOC Pamphlet 525-3-1, 2018.

[33] Mark Balboni, John A. Bonin, Robert Mundell, and Doug Orsi. *Mission Command of Multi-Domain Operations*. Carlisle, PA: U.S. Army War College Press, 2020. Në: https://press.armywarcollege.edu/monographs/918

[34] U.S. Army War College. *Large-Scale Combat Operations and Professional Military Education*. Carlisle, PA: U.S. Army War College Press, 2019. Në: https://press.armywarcollege.edu/monographs/610

progresive strukturën e kurrikulës për të pakësuar përmbajtjen joluftarake dhe për të rritur përmbajtjen luftarake.[35] Elementi kryesor i këtij rishikimi përfshin riformulimin e përmbajtjes luftarake nga një fokus i ngushtë mbi operacionet kundër kryengritjeve (COIN) dhe Operacionet e Stabilitetit drejt një fokusi më të madh mbi luftën në shkallë të gjerë kundër kërcënimeve të barabarta në mjedise të kontestuara.

- *Kolegji Mbretëror i Mbrojtjes së Danimarkës* (RDDC): përfaqëson perspektivën e një shteti të vogël mbi MDO-të. Ai po përshtat konceptin e operacioneve me shumë fusha me nevojat e arsimit profesional ushtarak të shteteve të vogla. Kurrikula e këtij kolegji integron MDO-të në arsimin e oficerëve duke theksuar përshtatshmërinë dhe inovacionin si kompetenca thelbësore për luftën moderne [36], kritike për shtetet me burime të kufizuara. Mësimdhënia dhe kërkimi që zhvillohen në Kolegjin e Mbrojtjes synojnë të kontribuojnë në zhvillimin konceptual dhe në zbatueshmërinë praktike të MDO-ve, duke lidhur teorinë me nevojat e operacioneve bashkëkohore.[37] Në mënyrë dalluese, ky kolegj i jep përparësi pajisjes së oficerëve danezë me aftësinë për të vepruar në mënyrë efektive në kontekste multinacionale, duke siguruar që Danimarka të kontribuojë në mënyrë domethënëse në operacionet e NATO-s dhe koalicioneve pavarësisht kufizimeve të burimeve kombëtare.[38]

Këto tre qasje pasqyrojnë një angazhim institucional në rritje për integrimin e MDOve, megjithëse ato ndryshojnë në nivelin e përfshirjes, burimeve dhe përafrimit doktrinar. Në thelb: Kolegji i Mbrojtjes së NATO-s i trajton MDO-të si një koncept të aleancës, Kolegji i Luftës së Ushtrisë Amerikane i trajton ato si doktrinë amerikane, ndërsa Kolegji i Mbrojtjes i Danimarkës i trajton si një përshtatje të fokusuar për shtetet e vogla. Sidoqoftë, koncepti për këto operacione po zhvillohet gjithnjë e më shumë, dhe arsimi shfaqet si faktor vendimtar për përgatitjen e profesionistëve ushtarakë të ardhshëm.

Duke u mbështetur në zhvillimet doktrinare dhe përvojat krahasuese të aleatëve, më poshtë hulumtohet nevoja për qartësi konceptuale, ndryshim kulturor dhe përgatitjen e një moduli të veçantë në të treja nivelet e arsimit tonë profesional (APU). Integrimi tashmë i MDO-ve në programet arsimore të institucioneve të NATO-s dhe vendeve aleate përforcon argumentin se operacionet

[35] U.S. Army Combined Arms Center and Army University. *Reforming Professional Military Education for Large-Scale Combat Operations*. Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2020. Në: https://armyuniversity.edu/PME-Reform

[36] Royal Danish Defence College. *Forsvarsakademiet forbereder sig på fremtidens militære operationer*. Copenhagen: FAK, 10 gusht 2023. Parë më16 janar 2026, në: https://www.fak.dk/da/nyheder/2023/forsvarsakademiet-forbereder-sig-pa-fremtidens-militare-operationer/

[37] Royal Danish Defence College. *About the Royal Danish Defence College*. Copenhagen: RDDC, 2022. Parë më 17 janar 2026. https://www.fak.dk

[38] Henrik Breitenbauch. *Small States and Military Education: Danish Approaches to Innovation*. Copenhagen: Centre for Military Studies, University of Copenhagen, 2019.

me shumë fusha nuk janë më një temë opsionale ose periferike, por një kompetencë thelbësore për komandim dhe vendimmarrje efektive në konfliktet e sotme dhe të ardhshme. Në fund të fundit, kjo qasje përgatit profesionistët ushtarakë të veprojnë në mjedise të karakterizuara nga ndryshime të shpejta teknologjike, kërcënime të ndërlidhura dhe nevoja për veprime të sinkronizuara nëpër fusha të shumta.[39] Ndaj, institucionalizimi i MDO-ve si një modul i veçantë në arsimin tonë profesional, gjithashtu sinjalizon rëndësinë e MDO-ve, duke e ngritur atë në të njëjtin nivel me vendet e aleancës.

Vlen të theksohet se arsimi ynë profesional ka pasur prirjen të integrojë koncepte të reja brenda kurrikulave ekzistuese, megjithatë, MDO-të ende nuk janë bërë pjesë e institucioneve tona arsimore, veçanërisht në kursin e lartë të oficerit (KLO). Ndaj, *zhvillimi i një moduli të dedikuar për operacionet me shumë fusha përfaqëson një element të domosdoshëm në arsimin tonë profesional, duke luajtur një rol të rëndësishëm në formësimin dhe përshtatshmërinë e doktrinës, lidershipit dhe personelit në të ardhmen.* Një modul i tillë do të siguronte një qasje të strukturuar dhe të qëndrueshme, duke u ofruar oficerëve bazat teorike mbi konceptin e MDO-ve, evolucionin historik dhe praktikat krahasuese të aleatëve. Përmes rasteve studimore, oficerët do të mësonin të kuptojnë efektet zinxhir ndërmjet fushave tokësore, detare, ajrore, kibernetike dhe hapësinore, si dhe të zhvillonin aftësi analitike e kreative për të adresuar dilemat komplekse ndërmjet fushave. Zhvillimi i një moduli të veçantë për MDO-të jo vetëm që e përshtat këtë koncept në nivelin e duhur, por siguron që oficerët të marrin njohuri të plota dhe të vazhdueshme për sfidat e operacioneve të ardhshme. Ky modul gjithashtu do të nxisë bashkëpunimin ndërinstitucional dhe me aleancën, duke i përgatitur oficerët me një qasje gjithëpërfshirëse.

Në fakt, më së shumti pjesa e operacioneve në arsimimin profesional, deri vonë, ishte përqendruar pothuajse ekskluzivisht në *operacionet e paqes dhe terrorizmin*, duke krijuar një perceptim tjetër të misionit doktrinar dhe roleve të forcave tona të armatosura. Por, as koncepti i MDO-ve, as ky studim, nuk sugjerojnë të shpërfillen përvojat dhe mësimet e nxjerra nga dy dekadat e kryerjes së operacioneve në mbështetje të paqes dhe angazhimeve të tjera të njësive të FA-ve. Pa dyshim, konfliktet me intensitet të ulët, terrorizmi dhe kryengritjet nuk janë diçka e së kaluarës dhe sigurisht që mbeten një kërcënim për sigurinë. Gjithsesi, NATO dhe vendet anëtare tashmë po përqendrohen tek *konfliktet në shkallë të gjerë dhe kërcënimet pothuajse të barabarta shtet me shtet*, sipas konceptit të ri të operacioneve me shumë fusha.

Është e rëndësishme të theksohet se operacionet me shumë fusha nuk duhet thjesht të integrohen në arsimin tonë profesional, apo të mësohen si një temë opsionale ose leksion i izoluar; përkundrazi, ato duhet të përshkojnë të gjithë

[39]Katrine Lund-Hansen dhe Jeff Reilly, *"The Multi-Domain Operations Approach to Intermediate PME,"* War Room – U.S. Army War College, 1 nëntor 2024.

nivelet arsimore. Oficerët duhet të përvetësojnë konceptin e MDO-ve me qëllim që të ndikojnë natyrshëm në mënyrën se si analizojnë problemet, planëzojnë operacionet dhe drejtojnë shtabet dhe komandat. Nga oficerët e gradës së ulët deri te drejtuesit e lartë, MDO-të duhet të integrohen progresivisht në çdo fazë të arsimit dhe trajnimit profesional ushtarak, duke siguruar që të formësojnë të menduarit, planëzimin dhe drejtimin në një mjedis me shumë fusha. [40]

Integrimi i operacioneve me shumë fusha (MDO) në lëndët bazë të arsimit profesional ushtarak kërkon një qasje sistematike dhe ndërdisiplinore. Për shembull, në *fushën e artit operativ*, kjo nënkupton përfshirjen e dimensioneve kibernetike, hapësinore dhe të informacionit në analizën e qendrës së rëndesës, me qëllim zhvillimin e një planëzimi sa më të plotë. Në *disiplinën e zbulimit*, është e domosdoshme që oficerët të aftësohen për mbledhjen e informacionit nga shumë fusha, duke mundësuar një kuptim të integruar të kapaciteteve dhe synimeve të kundërshtarit. Nga ana tjetër, *logjistika* duhet të fokusohet në sfidat e dislokimit dhe në ndërtimin e qëndrueshmërisë, duke përgatitur oficerët për të ruajtur vazhdimësinë e operacioneve në të gjitha fushat. *Sulmet kibernetike* nuk janë më thjesht një veprim kriminal—ato po shndërrohen në mjete të luftës moderne, duke sfiduar kornizat ekzistuese ligjore dhe etike. Ndaj çështja ligjore dhe e etikës duhet të përfshijnë analizën e autoriteteve, atribuimit, dinamikave të përshkallëzimit dhe zbutjes së dëmit ndaj civilëve në kontekste kibernetike, hapësinore dhe të informacionit.[41]

Përfundime

Ky shkrim shqyrtoi konceptin e Operacioneve me Shumë Fusha (MDO) në kontekstin e mjedisit të ardhshëm të sigurisë. Ai dha informacion mbi zhvillimin e konceptit dhe qasjeve të përshtatura nga NATO dhe disa vendeve anëtare të saj, si dhe nxori në pah rëndësinë e përfshirjes në kurrikulat e arsimimit profesional, të cilat mundësojnë përgatitjen ndaj sfidave të reja të sigurisë si dhe rrisin rolin e FA-ve në sigurinë kolektive.

Ndërsa MDO-të po zënë një vend kryesor brenda NATO-s, për shkak të rëndësisë së tyre në rritje, është domosdoshmëri për FA-në dhe strukturat e saj të kuptojë sfidat që ato paraqesin. Si një koncept operacional, operacionet me shumë fusha (MDO) do ndikojnë në llojet e sistemeve të armëve dhe pajisjeve që do blihen nga FA, llojet dhe numrin e forcave që nevojiten, strukturën organizative dhe llojin e arsimimit dhe trajnimit që kërkohet - të gjitha të rëndësishme për të ardhmen e FA-ve. Si rrjedhojë, ky shkrim është më shumë sesa thjesht një përshkrim i operacioneve me shumë fusha; është një thirrje për

[40]Katrine Lund-Hansen and Jeff Reilly,*"The Multi-Domain Operations Approach to Intermediate PME,"* War Room – U.S. Army War College, November 1, 2024.

[41]Michael N. Schmitt, "*The Law of Cyber Operations: A 2023 Update*," Journal of National Security Law & Policy 13, no. 2 (2023): faqe 145–178, në: https://jnslp.com/2023/07/15/the-law-of-cyber-operations-a-2023-update/ (parë më 18 janar 2026).

të shqyrtuar këto sfida nën dritën e këtyre zhvillimeve të reja.

Duhet mbajtur parasysh se ndryshimi konceptual në Forcat e Armatosura dhe përgatitja e tyre për operacionet e ardhshme nuk është aq e thjeshtë sa riformulimi i doktrinës dhe blerja e pajisjeve të reja. Ndaj, në të ardhmen, do të ishte e vlefshme të kryheshin studime të thelluara mbi përgatitjen dhe zbatimin e MDO-ve, si dhe të hulumtoheshin qasjet e shteteve të vogla të aleancës, për të përshtatur më tej konceptin e MDO-ve për forcat tona të armatosura. Përveç kësaj, këto studime do të mundësonin një vlerësim më objektiv për të matur efektivitetin dhe ndikimin e MDO-ve në skenarë të ndryshëm të angazhimit të FA-ve.

Në varësi të nivelit të komandimit, si dhe llojit të operacioneve, drejtuesit dhe komandantët e ardhshëm do të kenë nevojë për një përzierje të ndryshme të njohurive operacionale dhe teknologjike. Ndaj, kurrikula e arsimit profesional ushtarak do të duhet të rishikohet për t'i mësuar brezit të ardhshëm zhvillimin dhe drejtimin e operacioneve në të gjitha fushat. Për më tepër, sfidat në pabarazitë teknologjike, kufizimet buxhetore dhe strukturat e komandimit dhe kontrollit tregojnë nevojën që FA të hulumtojë modele për të zhvilluar një forcë luftarake të aftë për këtë epokë të re operacionesh.

Është e rëndësishme të theksohet se operacionet me shumë fusha nuk janë një koncept "mirë ta dish", janë sistem operativ për të ardhmen luftarake të NATO-s. Ndërsa Aleanca përparon drejt synimit për t'u bërë e aftë për MDO deri në vitin 2030-të, atëherë përshtatja nga FA e një qasje ndaj MDO-ve nuk është vetëm domosdoshmëri, por edhe urgjencë. Kjo qasje ndaj MDO-ve duhet të përfshijë «*të menduarit në shkallë të gjerë, hedhjen e hapave të vogël dhe shkallëzimin sipas nevojës*". Cilado qoftë qasja jonë ndaj MDO-ve, ne kemi një rol për të luajtur në konceptin e ri të NATO-s. Nuk është vetëm një koncept i së ardhmes - po ndodh tani, është rrënjësisht i ndryshëm dhe ne duhet të përgatitemi.

Në fund të fundit, pyetja që shtrohet nuk është nëse FA-të mund të zhvillojnë apo jo aftësitë për operacionet me shumë fusha, por nëse njësitë tona dhe – *drejtuesit e tyre* – do të jenë të pajisur me njohuritë e nevojshme për t'u përballur me një gamë të gjerë operacionesh në të ardhmen. Vlen të përmendet këtu shprehja e Gjeneral Stanley McChrystal, që është aktuale edhe sot: – *Aftësia për t'u përshtatur me kompleksitetin dhe ndryshimin e vazhdueshëm është bërë një imperativ*.[42] Ndaj, integrimi i plotë i MDO-ve në kurrikulat e kurseve të karrierës dhe thellimi i njohurive në fushën operacionale është domosdoshmëri, dhe institucionet e arsimit profesional duhet të vlerësojnë nevojën për të përgatitur drejtuesit e ardhshëm të FA-ve për t'u përballur me këto sfida që shtrihen përtej angazhimeve të sotme.

[42]Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World,* New York: Penguin Publishing Group, 2015, fq.5

E lidhur me këtë është efektiviteti i kostos së investimit në njohuri dhe kapital njerëzor. Ndërsa aftësitë për MDO-të janë pothuajse të paarritshme për shtete të vogla si ne, ato mund të maksimizohen përmes shpërndarjes së mençur të burimeve - veçanërisht në arsim, mjedise simulimi dhe kualifikime jashtë vendit. Një investim relativisht modest në arsimimin profesional mund të sjellë përfitime në përshtatshmërinë dhe përgatitjen e personelit. Kjo do të thotë se arsimimi dhe trajnimi nuk janë çështje periferike për MDO-të – ato janë themeli mbi të cilin duhet të ndërtohet e gjithë kompetenca për operacionet luftarake. Për shkak të këtij elementi, "avantazhi asimetrik" numër një i vendeve të vogla është personeli i tyre. Pra, "*nëse nuk mund të kemi teknologji, duhet të kemi njerëzit e arsimuar*."

Bibliografia:

1) "*Alliance Concept for Multi-Domain Operations,*" North Atlantic Council approved Version, 19 Maj 2023.
2) Allied Command Transformation, *Empowering NATO's Multi-Domain Operations Through Digital Transformation* (2023), në https://www.act.nato.int/article/empowering-nato-mdo-through-digitaltransformation/.
3) Franklin D. Kramer, Ann Marie Dailey, etj, *NATO multi-domain operations: Near- and medium-term priority initiatives*, Atlantic Council, 2024, në https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/
4) Gjeneral Lejtnant Thomas J. Sharpy, "*Multi-Domain Operations: The Future of Warfare*" (Seminar Read Ahead, NATO Command and Control Centre of Excellence, Utrecht, 2020);
5) Katrine Lund-Hansen, and Jeff Reilly. "T*he Multi-Domain Operations Approach to Intermediate PME*", War Room – U.S. Army War College, 1 Nëntor 2024.
6) Ludovico Caprio, Melanie Garcia Flores, etj, *NATO Multi- Domain Operations: challenges for the European Land Forces*, UK Land Warfare Centre, 2024, në https://finabel.org/wp-content/uploads/2024/10/FFTPersonal-Paper-Format-copia-1.pdf
7) Matthew Willis and Daniel Cochran, "*Transitioning NATO to an All-Domain Mindset*," The Journal of the JAPCC: Transforming Joint Air and Space Power 32, no. 1 (2021): faqe 56–61;
8) NATO Defense College. *Anyplace, Anywhere, Anytime – NATO and Multi-Domain Operations*. Research Paper No. 27. Rome: NATO Defense College, Korrik 2023.
9) NATO *Multi-Domain Operation Conference Report*, tetor 2023,

Copenhagen, Denmark, në https://www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Report-LR.pdf

10) NATO Multi-Domain Operations Conference: Driving Success Across All Domains, Ankara Turqi, 2025, në: https://www.act.nato.int/article/2025-mdo-conference/

11) Royal Danish Defence College. *About the Royal Danish Defence College*. Copenhagen: RDDC, 2022.

12) The U.S. Army War College. *Large-Scale Combat Operations and Professional Military Education*. Carlisle, PA: U.S. Army War College Press, 2019.

13) U.S. Army Combined Arms Center and Army University. *Reforming Professional Military Education for Large-Scale Combat Operations*. Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2020.

14) The U.S. Army, *Concept for Maneuver in Multi-Domain Operations*, *2028-2040*, Version 1.0, 2020, në https://apps.dtic.mil/sti/pdfs/AD1118627.pdf

15) TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 6 Dhjetor 2018.