



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

# REVISTA USHTARAKE

(edicioni i tretë)

INSTITUTI KËRKIMOR SHKENCOR USHTARAK © 2026



Botim i Akademisë së Forcave të Armatosura  
Miratuar me vendim nr. 03, datë 28.09. 2026  
të Bordit Drejtues të Revistës Ushtarake

**Bordi Drejtues i Revistës Ushtarake**

**Kryetari i bordit**

Gjeneralmajor **Ferdinant Dimo**

**Anëtarët e Bordit**

Gjeneral brigade **Fatmir Neziraj**

Prof. as. dr. **Etleva Smaçi**

Prof. as. dr. **Teki Kurti**

Kolonel (R) Dr. **Ahmet Leka**

Nënkolonel (R) Dr. **Enrik Ago**

Nënkolonel Dr. **Fitim Karasani**

**Përgatiti për botim:** Grupi i Redaktimit dhe i Publikimit, IKSHU

**Art design:** Engjellushe Llulla

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

Copyright © 2026 nga Instituti Kërkimor Shkencor Ushtarak në Akademinë e Forcave të Armatosura.

Akademia e Forcave të Armatosura zotëron liri akademike dhe respekton detyrimet ligjore të përcaktuara shprehimisht në ligjin për Arsimin e Lartë si dhe të gjitha aktet e tjera ligjore që janë të detyrueshme për institucionet publike.

Pikëpamjet dhe opinionet e shprehura në “Revista Ushtarake” janë të autorëve dhe nuk pasqyrojnë qëndrim zyrtar të Ministrisë së Mbrojtjes, Shtabit të Përgjithshëm të FARSH dhe Akademisë së Forcave të Armatosura. Autorët e shkrimeve nuk do të jenë subjekt i ndëshkimit për shprehjen e lirë të qëndrimeve dhe pozicioneve të tyre individuale, edhe sikur përmbajtja e tyre të mos jetë në përputhje me qëndrimet zyrtare të institucionit të mbrojtjes. Njëkohësisht, autori/autorët mbajnë përgjegjësi për shtrembërimet e fakteve si dhe kopjimet e pa referuara të krijimeve dhe mendimeve të autorëve të tjerë.

Akademia e Forcave të Armatosura  
Instituti Kërkimor Shkencor Ushtarak  
**Shtypur: shtator 2026**



# PËRMBAJTJA E REVISTËS USHTARAKE

## RUBRIKA E PARË

### Vlerësime dhe analiza në mjedisin e sigurisë

|                                                                                                                                                                            |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Nga Ankara 2026 drejt Tiranës 2027: Shqipëria në arkitekturën e re të sigurisë së krahut juglindor të NATO-s .....</b>                                                  | <b>9</b>  |
| <i>Kolonel (R) Dilaver Hoxha</i><br><i>Këshilltar Politik (POLAD)</i><br><i>Brigada Multinacionale e Evropës Juglindore (SEEBRIG)</i><br><i>Stamboll, Turqi</i>            |           |
| <b>Deri në çfarë mase Forcat Speciale kontribuojnë në luftën konjitive në konfliktet hibride? .....</b>                                                                    | <b>21</b> |
| <i>Kolonel Ramadan Karakushi</i><br><i>Shef i Departamentit të Operacioneve Ushtarake,</i><br><i>Kolegji i Mbrojtjes dhe i Sigurisë</i>                                    |           |
| <b>Arkitektura e cënueshmërisë dhe qëndrueshmëria kombëtare: përtej parashikimit drejt veprimit të koordinuar – Implikime për Shqipërinë dhe Forcat e Armatosura .....</b> | <b>37</b> |
| <i>Msc. Alqi Nikolla</i><br><i>Specialist në IKSHU</i>                                                                                                                     |           |

## RUBRIKA E DYTË

### Industria e mbrojtjes dhe kapacitetet operacionale

|                                                                                                                                     |           |
|-------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Parandalimi dhe mbrojtja në epokën digjitale: transformimi i FARSH nga burimet e mbrojtjes te kapacitetet operacionale .....</b> | <b>59</b> |
| <i>Kolonel (R) Msc. Agim Shahu</i><br><i>Shtabi i Përgjithshëm i Forcave të Armatosura</i>                                          |           |
| <b>Industria ushtarake përballë sfidave dhe mundësive të epokës digjitale .....</b>                                                 | <b>75</b> |
| <i>Kolonel (R) Hysni Gjergji</i><br><i>Agjencia e Industrisë së Mbrojtjes</i>                                                       |           |

## RUBRIKA E TRETË

### Arsimimi ushtarak, lidershipi dhe zhvillimi profesional

|                                                                                                                                                       |           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Mësimdhënia e terminologjisë ushtarake përmes materialeve autentike operacionale: një qasje e bazuar në Anglishten për Qëllime Specifike .....</b> | <b>91</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|

*Dr. Manjola Likaj*

*Dr. Alma Vladi*

*Departamenti i Shkencave të Komunikimit dhe Gjuhëve të Huaja,  
Fakulteti i Mbrojtjes dhe i Sigurisë, AFA*

|                                                                                                     |            |
|-----------------------------------------------------------------------------------------------------|------------|
| <b>Koncepti Platonian mbi edukimin ushtarak dhe integrimi në strukturat ushtarake moderne .....</b> | <b>107</b> |
|-----------------------------------------------------------------------------------------------------|------------|

*Dr. Blerina Kuqi*

*Msc. Marsida Minga*

*Fakulteti i Mbrojtjes dhe i Sigurisë, AFA*

|                                                                                                            |            |
|------------------------------------------------------------------------------------------------------------|------------|
| <b>Transformimi i edukimit ushtarak bashkëkohor përmes integritetit të inteligjencës artificiale .....</b> | <b>115</b> |
|------------------------------------------------------------------------------------------------------------|------------|

*Msc. Edgen Murati*

*Akademia e Forcave të Armatosura*

## RUBRIKA E KATËRT

### Zhvillimi i teknologjisë dhe inovacionit në fushën e mbrojtjes

|                                                                                        |            |
|----------------------------------------------------------------------------------------|------------|
| <b>Platformat parandaluese “proaktive” të sigurisë dhe mbrojtjes kibernetike .....</b> | <b>135</b> |
|----------------------------------------------------------------------------------------|------------|

*Kolonel Inxh. Gjergji Vasili*

*Shefi i Departamentit të Inovacionit dhe Teknologjisë, IKSHU*

|                                                                                                                                                                              |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Aplikimet e inteligjencës artificiale dhe “agjentëve” autonomë të saj në sistemet e mbrojtjes, avantazhet operacionale, rreziqet, sfidat dhe lufta e së ardhmes .....</b> | <b>157</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|

*Kolonel (R) Msc. Adi Ndoni*

*Oficer shtabi, kërkues I, specialist FT në IKSHU*

# **RUBRIKA E PARË**

## **VLERËSIME DHE ANALIZA NË MJEDISIN E SIGURISË**



# **Nga Ankara 2026 drejt Tiranës 2027: Shqipëria në arkitekturën e re të sigurisë së krahut juglindor të NATO-s**

---

**Kolonel (R) Dilaver HOXHA**

*Këshilltar Politik (POLAD)*

*Brigada Multinacionale e Evropës Juglindore (SEEBRIG)*

*Stamboll, Turqi*

## **Trajtesë e shkurtuar**

*Ky punim analizon rolin në zhvillim të Shqipërisë në arkitekturën e sigurisë së krahut juglindor të NATO-s, në një periudhë të karakterizuar nga përshkallëzimi i pasigurisë ndërkombëtare, nga lufta e zgjatur në Ukrainë deri te tensionet e reja në Lindjen e Mesme gjatë vitit 2026. Duke përdorur analizën strategjike dhe studimin e rastit, punimi shqyrton mënyrën se si një vend i vogël anëtar i Aleancës mund ta shndërrojë angazhimin institucional në kapital strategjik përmes kontributit operacional, diplomatik, industrial dhe infrastrukturor.*

*Samiti i NATO-s në Ankara (korrik 2026) trajtohet si pikë referimi për të analizuar transformimin e mjedisit të sigurisë në krahun juglindor të Aleancës dhe pozicionimin në rritje të Shqipërisë brenda tij. Argumentohet se pritja e Samitit të NATO-s në Tiranë në 2027 nuk përfaqëson një zhvillim të izoluar apo simbolik, por pasqyron një proces më të gjerë të konsolidimit të rolit shqiptar në strukturat e sigurisë kolektive euroatlantike. Rasti shqiptar ofron kështu një shembull se si vendet e vogla mund ta rrisin peshën e tyre strategjike përmes besueshmërisë institucionale, angazhimit afatgjatë dhe integritetit në mekanizmat e sigurisë rajonale dhe aleate.*

**Fjalë kyçe:** NATO; Shqipëria; siguria kolektive; vendet e vogla; Samiti i Ankarasë; Samiti i Tiranës; krahut juglindor; diplomacia e mbrojtjes; Korridori VIII.

## Hyrje

**R**endi gjeostrategjik euroatlantik po kalon në një periudhë përshkallëzimi të vazhdueshëm, më shumë sesa përmes zhvillimeve të papritura dhe të izoluar. Lufta në Ukrainë, e cila vazhdon prej vitit 2022, ka vendosur tashmë kornizën brenda së cilës NATO-ja po rimendon angazhimet e saj kolektive të sigurisë. Ndërkohë, kriza e re me Iranin në pranverën e vitit 2026, e shoqëruar me bllokadën detare në Ngushticën e Hormuzit dhe me rimobilizimin perëndimor në Gjirin Persik, dëshmon se hapësira gjeografike e sigurisë euroatlantike po zgjerohet përtej kufijve tradicionalë të kontinentit (RTSH, 2026). Në këtë kuadër përshkallëzimi, u zhvillua Samiti i NATO-s në Ankara, më 7 dhe 8 korrik 2026, i dyti i organizuar nga Turqia, pas Samitit historik të Stambollit në vitin 2004 (NATO, 2026).

Zgjedhja e Turqisë si vendi pritës nuk është rastësore, por pasqyron një vlerësim të ri të peshës strategjike të krahut juglindor të Aleancës, në kryqëzimin e Detit të Zi, Mesdheut Lindor dhe Kaukazit (Modern War Institute, 2026). Pikërisht në këtë kontekst duhet parë edhe vendimi për zhvillimin e Samitit të ardhshëm të NATO-s në Tiranë, në vitin 2027. Kjo e vendos Shqipërinë, për herë të parë që prej anëtarësimit të saj në Aleancë, në qendër të vëmendjes politike dhe strategjike të NATO-s.

Vendet e vogla brenda NATO-s përballen me një dilemë themelore: ato përfitojnë nga siguria kolektive pa qenë në gjendje të kontribuojnë në mënyrë proporcionale në barrën e mbrojtjes së Aleancës. Kjo krijon nevojën për të gjetur mjete alternative për të dëshmuar vlerën e tyre. Siç vëren Keohane (1969), “vendet e vogla në aleanca duhet të gjejnë mënyra për të kompensuar kufizimet e tyre materiale përmes pozicionimit strategjik, qëndrueshmërisë dhe angazhimit institucional” (cituar në disertacionin e D. Hoxha, 2026, Kap. VII). Forcat e Armatosura të Republikës së Shqipërisë, si ushtri e vogël në përmasa dhe burime, e ka ndjerë këtë dilemë drejtpërdrejt që në fillimet e procesit të integritit euroatlantik. Në këtë proces kam qenë pjesëmarrës aktiv, në role të ndryshme, si ekspert dhe drejtues. Megjithatë, zhvillimet më të rëndësishme nuk u shfaqën me anëtarësimin e Shqipërisë në NATO në vitin 2009, por gjatë viteve që pasuan dhe, veçanërisht, në periudhën e fundit pas fillimit të luftës në Ukrainë.

Ky punim shqyrton se si Shqipëria, si një vend i vogël anëtar i NATO-s, ka shndërruar angazhimin e saj institucional, operacional dhe industrial në kapital strategjik brenda Aleancës. Hipoteza që udhëheq analizën është se prania e vazhdueshme dhe e besueshme e Shqipërisë, jo thjesht kontributi i saj material, është faktori që ka çuar drejt përzgjedhjes së Tiranës si vendi pritës i Samitit të NATO-s në vitin 2027. Për ta testuar këtë hipotezë, punimi analizon katër drejtime të njëkohshme të angazhimit shqiptar gjatë vitit 2026: pjesëmarrjen

në strukturat e NATO-s dhe operacionet e drejtuara prej saj, përdorimin e platformave diplomatike rajonale, rivitalizimin e industrisë kombëtare të mbrojtjes, dhe zhvillimin e infrastrukturës kritike të lëvizshmërisë ushtarake.

Metodologjikisht, punimi mbështetet në analizën strategjike dhe studimin e rastit (case study), duke e trajtuar Shqipërinë si vend të vogël anëtar të NATO-s, dhe duke vlerësuar se si ndërveprimi i katër drejtimeve të sipërpërmendura, ndikon në pozicionimin e saj strategjik brenda Aleancës. Rasti i Shqipërisë paraqet interes të veçantë, pasi ilustron si një vend me burime relativisht të kufizuara mund ta rrisë profilin e tij strategjik përmes kontributit të qëndrueshëm në sigurinë kolektive.

## **I. Konteksti gjeostrategjik i ri**

Që prej pushtimit rus të Ukrainës në shkurt 2022, mjedisi i sigurisë euroatlantik ka njohur një përshkallëzim të vazhdueshëm, jo një seri ngjarjesh të veçuara. Deti i Zi, dikur korridor periferik, është shndërruar në një nga teatrot më kritikë strategjike të Evropës, ku përplasen siguria detare, energjia dhe infrastruktura nënujore (Atlas Institute for International Affairs, 2026). Fushata ukrainase me dronë kundër objektivave ruse në Novorossiysk dhe Kerç, si dhe incidentet e përsëritura me anije tregtare të goditura që prej vitit 2022, kanë detyruar NATO-n të përgjigjet me mekanizma të rinj të përhershëm: Baltic Sentry (janar 2025) dhe Eastern Sentry (shtator 2025) (Grosswald Research, 2026).

Rumania, e cila dikur perceptohej thjesht si vend krahu, tashmë vlerësohet zyrtarisht nga Sekretari i Përgjithshëm i NATO-s, Mark Rutte, si “spirancë e Detit të Zi” e Aleancës (NATO, cituar në Atlas Institute for International Affairs, 2026). Kjo logjikë e forcimit rajonal u zgjerua pikërisht gjatë ditëve të Samitit të Ankarasë. Më 8 korrik 2026, ministrat e mbrojtjes të Bullgarisë, Rumanisë dhe Turqisë nënshkruan, në Ankara, zgjerimin e mandatit të Grupit Detar Kundër Minave në Detin e Zi (EUalive, 2026). Nuk është rastësi që një vendim kaq konkret rajonal u firmos në të njëjtin vend dhe të njëjtën ditë me samitin e liderëve, duke treguar se Ankaraja shërbeu njëkohësisht si qendër simbolike dhe si qendër praktike vendimmarrjeje për krahun juglindor.

Paralelisht, në pranverën e vitit 2026, lufta e re e Iranit solli bllokadë detare në portet iraniane dhe rimobilizim të disa aleatëve perëndimorë në Gjirin e Omanit dhe Ngushticën e Hormuzit (RTSH, 2026). Kjo krizë e dytë, e shtrirë përtej kufijve tradicionale të Evropës, e ka kthyer Detin e Zi në rrugë tranzitimi energjetik dytësor me rëndësi të shtuar, saktësisht sepse rreziqet në Gjirin Persik e bënë më të brishtë rrugën kryesore (Maritime News, 2026).

Ky zgjerim i njëkohshëm i teatrove (Deti i Zi dhe Gjiri Persik) e ka rritur, jo ulur, vlerën relative të vendeve të vogla të besueshme brenda Aleancës.

Një raport i fundit i GLOBSEC mbi gatishmërinë luftarake të krahut lindor vëren se përparimi mes vendeve të para linjës është real, por i pabarabartë në shkallë rajonale, me boshllëqe që prekin disa prej tyre në mobilizim, logjistikë dhe kapacitet industrial (GLOBSEC, 2026), çka e bën qëndrueshmërinë institucionale, jo vetëm shpenzimet, faktorin që dallon aleatët e besueshëm nga ata thjesht të angazhuar në letër.

### ***Vështrim rajonal - Evropa Juglindore***

Kjo dinamikë e re prek në mënyra të ndryshme secilin vend të krahut juglindor. Turqia mban ushtrinë e dytë më të madhe të Aleancës dhe një pozicion të pazëvendësueshëm mes Detit të Zi, Mesdheut Lindor dhe Kaukazit (Modern War Institute, 2026). Greqia po kryen modernizimin më të madh ushtarak në historinë e saj, rreth 25 miliardë euro deri në fund të dekadës (World Socialist Web Site, 2026), ndërsa Rumania dhe Bullgaria kanë marrë role drejtuese në sigurinë detare të Detit të Zi (EUalive, 2026). Maqedonia e Veriut, nga ana e vet, u vlerësua drejtpërdrejt nga Sekretari i Përgjithshëm Rutte për arritjen e pragut 2% të PBB-së dhe kontributin rajonal (NATO, 2026).

Në këtë hartë rajonale, Shqipëria zë një vend të veçantë. Ndërsa disa aleatë investojnë kryesisht në modernizim financiar apo peshë ushtarake, kontributi i Shqipërisë buron nga një burim tjetër po aq i vlefshëm: qëndrueshmëria institucionale afatgjatë dhe besueshmëria politike e ndërtuar me kohë, të cilat, siç do të argumentohet më poshtë, po japin tashmë rezultate konkrete.

## **II. Samiti i Ankarasë 2026 dhe implikimet për sigurinë e krahut juglindor të NATO-s**

Samiti i 36-të i NATO-s u zhvillua në Kompleksin Presidential Beştepe të Ankarasë më 7-8 korrik 2026, me pjesëmarrjen e liderëve të 32 vendeve anëtare. Ishte samiti i dytë i organizuar nga Turqia pas atij historik të Stambollit në vitin 2004. Ai u zhvillua në një periudhë të karakterizuar nga sfida të vazhdueshme për sigurinë euroatlantike: vazhdimi i luftës në Ukrainë, tensionet e reja në Lindjen e Mesme dhe nevoja për forcimin e kapaciteteve mbrojtëse kolektive.

Rezultatet e samitit ishin domethënëse në disa drejtime. Aleatët riafirmuan angazhimin ndaj mbrojtjes kolektive sipas Nenit 5 të Traktatit të Uashingtonit dhe shpallën programe të reja investimesh: mbi 50 miliardë dollarë prokurime të reja mbrojtëse, 40 miliardë dollarë për mbrojtjen kundër dronëve dhe 70 miliardë euro ndihmë ushtarake për Ukrainën për periudhën 2026-2027 (NATO, 2026; Temnycky, 2026). Në Deklaratën e Ankarasë, krerët e shteteve dhe qeverive theksuan se “*our unity, solidarity and collective strength remain the foundation of peace, security and prosperity*” (uniteti, solidariteti

dhe forca jonë kolektive mbeten themeli i paqes, sigurisë dhe prosperitetit) (NATO, 2026), ndërsa Sekretari i Përgjithshëm Mark Rutte e përmbloodhi mesazhin kryesor të samitit me formulimin “*NATO delivers*”, duke nënvizuar se angazhimet politike të viteve të fundit po shndërrohen gradualisht në kapacitete konkrete ushtarake, industriale dhe infrastrukturore (NATO, 2026).

Disa vështrime analitike të pavarura ofruan një lexim më të kujdesshëm, duke vënë në dukje se vetë deklarata përfundimtare mbeti relativisht e shkurtër dhe nuk përfshiu një angazhim formal për samitin e vitit pasues (Atlantic Council, 2026). Kjo vërejtje nuk e vë në dyshim rezultatin e samitit, por shërben si kujtesë se Aleanca vazhdon të menaxhojë kompleksitet të brendshëm edhe teksa dëshmon kohezion në vendimmarrje.

Përtej vendimeve konkrete, rëndësia e Samitit të Ankarasë qëndron edhe në mesazhin strategjik që përcolli për krahun juglindor të Aleancës. Organizimi i tij në Turqi pasqyroi rëndësinë në rritje të kësaj hapësire gjeostrategjike, ku ndërthuren interesat e Detit të Zi, Mesdheut Lindor, Ballkanit Perëndimor dhe Lindjes së Mesme. Në këtë kuptim, rëndësia e vendeve të vogla brenda kësaj arkitekture nuk përcaktohet vetëm nga madhësia e kapaciteteve të tyre ushtarake, por gjithnjë e më shumë nga besueshmëria institucionale dhe gatishmëria për të kontribuar në mënyrë të qëndrueshme.

Është domethënëse që, ndër 17 vendet anëtare që deri më sot nuk kishin organizuar një samit të NATO-s, Shqipëria u përzgjodh të presë Samitin e Aleancës në 2027, menjëherë pas Ankarasë. Kjo vazhdimësi gjeografike, Stamboll 2004, Ankara 2026, Tiranë 2027, pasqyron një proces më të gjerë në të cilin krahu juglindor po fiton rëndësi të shtuar në arkitekturën e sigurisë euroatlantike dhe përbën një tregues të besimit institucional që Shqipëria ka fituar brenda Aleancës.

### **III. Angazhimi shqiptar në praktikë**

Angazhimi i Shqipërisë brenda NATO-s gjatë vitit 2026 nuk shprehet përmes një veprimi të vetëm të dukshëm, por përmes katër drejtimeve të njëkohshme, të ndërlidhura mes tyre.

#### ***1. Angazhimi në strukturat e NATO-s dhe operacionet e drejtuara prej saj***

Angazhimi ndërkombëtar ushtarak i Shqipërisë nis në vitin 1996, me pjesëmarrjen e parë historike në Bosnjë e Hercegovinë, në kuadër të përpjekjeve për stabilizim pas Dejtonit, prani që vazhdon edhe sot, në forma të reduktuara. Vitet në vijim sollën zgjerim të vazhdueshëm: misioni i NATO-s në Irak dhe, mbi të gjitha, Afganistani, ku Shqipëria mbajti kontingjentin e saj më të madh ndonjëherë të dërguar jashtë vendit, si dhe dy vëzhgues për shumë vite në misionin monitorues të Bashkimit Evropian në Gjeorgji. Mbyllja e

plotë e misionit në Afganistan në vitin 2021 solli rënien më të madhe në volumin e përgjithshëm të pranisë ushtarake shqiptare jashtë kufijve, por kjo rënie nuk shënoi tërheqje: Shqipëria e ka ruajtur gatishmërinë institucionale për t'u riaktivizuar aty ku Aleanca e kërkon, siç e dëshmoi rritja graduale e pranisë në krahun lindor pas fillimit të luftës në Ukrainë. Kjo vazhdimësi angazhimi u ripohua zyrtarisht edhe nga vetë komanda ushtarake: Shefi i Shtabit të Përgjithshëm të Forcave të Armatosura, Gjenerallejtënant Arben Kingji, gjatë një konference të komandantëve të krahut jugor të Aleancës në Napoli, riafirmoi angazhimin e Shqipërisë ndaj Planit Juglindor të NATO-s (Shtabi i Përgjithshëm i FA, 2025).

Sot, kjo traditë tridhjetëvjeçare shprehet në një hartë prezence të gjerë dhe të njëkohshme: forcat shqiptare gjenden njëherësh në Kosovë me KFOR-in; në Letoni, me Brigadën e Forcës së Përparuar; në Bullgari, në kuadër të Aktivitetit të Vigjilencës së Zgjeruar; në Detin Egje, me Operacionin Sea Guardian; dhe në Bosnjë e Hercegovinë, në kuadër të EUFOR Althea, krahas kontributeve në misionet e Kombeve të Bashkuara. Për një forcë të armatosur me përmasa aq të vogla sa ajo shqiptare, kjo shtrirje e njëkohshme në disa teatro të ndryshëm përfaqëson një raport pjesëmarrjeje ndaj madhësisë totale të ushtrisë që është dukshëm i lartë, tregues i qartë se pesha e një vendi të vogël nuk matet domosdoshmërisht me numra absolutë, por me shkallën e angazhimit relativ ndaj kapaciteteve që zotëron.

## ***2. Platformat diplomatike rajonale***

Paralelisht, Shqipëria ka investuar në diplomacinë e mbrojtjes përmes iniciativave rajonale si Adriatic Charter (A3), i zgjeruar që në 2008 në A5 me hyrjen e Malit të Zi dhe Bosnjë e Hercegovinës, kryesimin e OSBE-së në 2020, dhe anëtarësimin jo të përhershëm në Këshillin e Sigurimit të OKB-së për periudhën 2022 deri 2023. Këto janë instrumente që, siç argumentohet edhe në disertacionin tim, i shërbejnë kompensimit të kufizimeve materiale përmes ndërtimit të kapitalit politik (Hoxha, 2026, Kap. VII). Në këtë kuadër hyn edhe pjesëmarrja shqiptare në Brigadën Multinacionale të Evropës Juglindore (SEEBRIG), e sapo dislokuar këtë vit në Stamboll, e cila, pavarësisht kufizimeve efektive si strukturë operacionale, ka mbajtur për herë të dytë komandën shqiptare: Gjeneral Bilbil Bitri që nga 2023, pas Gjeneral Zyber Dushkut në 2009, me pjesëmarrje edhe të personelit tjetër shqiptar në përbërje të shtabit. Pavarësisht se SEEBRIG nuk përbën strukturë të NATO-s, vazhdimësia e bashkëpunimit në kuadër të Procesit të Takimeve të Ministrave të Mbrojtjes së Evropës Juglindore (SEDM) dëshmon se siguria rajonale mbështetet jo vetëm mbi strukturat formale të Aleancës, por edhe mbi mekanizma bashkëpunimi që ndërtojnë besim dhe kulturë të përbashkët strategjike.

### **3. Rivitalizimi i industrisë së mbrojtjes**

Drejtimi i tretë është ai industrial, dhe pasqyron një objektiv kombëtar afatgjatë: rikthimin e Shqipërisë si prodhuese, jo vetëm konsumatore, e kapaciteteve të veta mbrojtëse. Ky objektiv gjeti shprehjen e tij të parë konkrete në korrik 2024, kur Kuvendi miratoi dy ligje themeltare: Ligjin nr. 87/2024 “Për rregullimin e prodhimit, tregtimin, kërkimit dhe zhvillimit të armëve, municioneve, pajisjeve dhe teknologjive ushtarake”, dhe Ligjin nr. 88/2024 “Për krijimin e shoqërisë shtetërore për prodhimin dhe tregtimin e armëve, municioneve, pajisjeve dhe teknologjive ushtarake”, i cili themeloi shoqërinë shtetërore KAYO sh.a. Këto u shoqëruan më pas nga vendimet e qeverisë: Vendimi nr. 794/2024, që krijoi Agjencinë e Industrisë së Mbrojtjes, dhe Vendimi nr. 841/2024, që përcaktoi kriteret e lehtësirave për subjektet partnere.

Paralelisht me këtë institucionalizim, rritja e shpenzimeve të mbrojtjes i dha kësaj kornize ligjore mbështetje financiare reale. Buxheti i mbrojtjes arriti në 2,6% të PBB-së për 2026, duke e afruar ndjeshëm Shqipërinë me objektivin afatgjatë prej 5% të vendosur në Samitin e Hagës në 2025 (Ministria e Mbrojtjes, 2026). Rezultatet konkrete filluan të shfaqen shpejt pas kësaj kornize: nënshkrimi i marrëveshjes me kantierin naval italian Fincantieri, përmes shoqërisë KAYO, pritet të sjellë prodhim anijesh në Pashaliman me rreth 500 vende pune të reja, ndërsa kompani si TIMAK Defence dhe Guna Tactical po krijojnë kapacitete prodhuese vendase, kjo e fundit duke premtuar deri në 800 vende pune. Ajo që e dallon këtë fazë nga deklaratat e mëparshme të vullnetit politik është pikërisht kjo: sot ekzistojnë ligje të miratuara, struktura funksionale, dhe kontrata të nënshkruara, jo thjesht plane afatgjata.

### **4. Infrastruktura kritike: Kuçova, Porto Romano dhe Korridori VIII**

Drejtimi i katërt dhe, ndoshta, ai me pasojat më të prekshme afatgjata, është infrastrukturor. Baza Ajrore Taktike e Kuçovës shënoi hapin e parë të dukshëm në këtë drejtim: e rindërtuar me një investim prej rreth 50 milionë eurosh nga NATO përmes NSPA-s, u përfundua më 5 mars 2024 si baza e parë ajrore rajonale e Aleancës në Ballkanin Perëndimor.

Në ceremoninë e përfundimit, Presidenti Bajram Begaj e cilësoi atë “monument bashkëpunimi, solidariteti, kohezioni dhe uniteti mes aleatëve”, ndërsa Ministri i Mbrojtjes, Niko Peleshi, theksoi se baza do të ishte “pikë strategjike në operacionet e NATO-s për mbrojtjen e paqes” (NATO, 2024). Po në atë ceremoni, Kryeministri Edi Rama zbuloi hapin tjetër që do të vinte: përpjekjet për ta bërë gati sa më shpejt bazën e re detare të NATO-s në Porto Romano (Anadolu Agency, 2024).

Kjo bazë detare u përfshi më pas në një hartë shumë më të gjerë lëvizshmërie

ushtarake: Korridorin Pan-Evropian VIII, që lidh portet e Durrësit dhe Vlorës me Detin e Zi përmes Maqedonisë së Veriut dhe Bullgarisë. Korridori hyri zyrtarisht në planet ushtarake të NATO-s që në korrikun 2024, kur Shqipëria, Italia, Bullgaria dhe Maqedonia e Veriut nënshkruan Letrën e Qëllimit për lëvizshmëri ushtarake. Hapi vendimtar erdhi më 18 shkurt 2026, kur ministrat e jashtëm të pesë vendeve, duke shtuar edhe Rumaninë, miratuan në Tiranë Deklaratën e Përbashkët, që e lidh Korridorin VIII me planifikimin rajonal të NATO-s (Debuglies, 2026). Vetë Kryeministri Rama e konfirmoi këtë status brenda kuadrit zyrtar të Aleancës: duke komentuar vendimin e Ministerialit të Mbrojtjes së NATO-s të 18 shkurtit, ai deklaroi se “Korridori 8, me pikënisje në kompleksin detar Durrës-Porto Romano dhe dalje në Detin e Zi, u njoh zyrtarisht si korridor sigurie për mbrojtjen kolektive” (Rama, cituar në Faxweb, 2026).

Sot, kompleksi Durrës-Porto Romano është caktuar si pika kryesore e pritjes së forcave të NATO-s në Ballkanin Perëndimor (Ministria e Mbrojtjes, 2026). Në këtë kuadër, Kuçova, Porto Romano dhe Korridori VIII bashkohen kështu në një hartë të vetme. Në prag të vitit 2027-s, Shqipëria pozicionohet jo vetëm si vend pritës i një samiti të rëndësishëm të Aleancës, por edhe si pikë fizike kyçe për pritjen dhe ridislokimin e forcave aleate, rol që bashkon besueshmërinë operacionale, angazhimin diplomatik, dhe kapacitetin logjistik konkret.

### ***5. Katër drejtime, një sistem i ndërvuarur***

Analiza e mësipërme evidenton katër drejtime themelore të angazhimit shqiptar: operacional, diplomatik, industrial dhe infrastrukturor, pa pretenduar se këto janë të vetmet, por duke i konsideruar ato më domethënëset për argumentin e këtij punimi. Një vlerësim i drejtë kërkon të theksohet se këto katër drejtime nuk përparojnë me të njëjtin ritëm. Angazhimi industrial dhe infrastrukturor operon në një horizont kohor dukshëm më të gjatë sesa vendimmarrja politike dhe diplomatike që i shoqëron. Marrëveshje të tilla si ajo me Fincantieri apo realizimi i plotë i projekteve si Korridori VIII, janë procese me natyrë shumëvjeçare. Rreziku qëndron jo te mungesa e vullnetit politik, por te mundësia që drejtimet më të dukshme publikisht të krijojnë përshtypjen e një përparimi më të shpejtë sesa realiteti i kapaciteteve zbatuese dhe institucionale e lejon.

Megjithatë, pikërisht kjo ndërlidhje mes drejtimeve me ritme të ndryshme është ajo që i jep procesit vlerë kumulative: prania operacionale ndërton besueshmëri, besueshmëria krijon hapësirë për thellim të angazhimit diplomatik, ky i fundit tërheq investim industrial, dhe infrastruktura e re i integron të gjitha në një kapacitet konkret institucional. Në këtë kuptim, katër drejtimet nuk përbëjnë thjesht një listë arritjesh paralele, por një sistem të

ndërruar, ku qëndrueshmëria e tërësisë varet nga aftësia për t'i menaxhuar diferenat e ritmit ndërmjet pjesëve përbërëse.

Vetë Ministri i Mbrojtjes, Ermal Nufi, e ka përmbledhur këtë moment kalimtar në terma të qartë strategjikë: sipas tij, Shqipëria dhe NATO po hyjnë tashmë në një fazë të re marrëdhëniesh, të quajtur “*NATO 3.0*”, e karakterizuar nga një Aleancë “më e përgatitur, më e aftë dhe që kërkon më shumë përgjegjësi” nga çdo vend anëtar (Nufi, cituar në JavaNews, 2026). Katër drejtimit e trajtuara në këtë punim janë, në thelb, përgjigjja konkrete shqiptare ndaj kësaj faze të re dhe pikërisht ky efekt sinergjik shpjegon pse disa vende të vogla arrijnë të krijojnë ndikim strategjik disproporcional në raport me kapacitetet e tyre materiale.

#### IV. Drejt Tiranës 2027

Rruga që e çon Shqipërinë drejt pritjes së Samitit të NATO-s në vitin 2027 nuk fillon me vendimin formal si vend pritës, por me një dekadë e gjysmë angazhimi të vazhdueshëm, që nga kalimi konceptual i vitit 2009 nga logjika e marrjes së ndihmës drejt asaj të ofrimit të ndërveprueshmërisë, e deri te përsheptimi i ndjeshëm i vitit 2026. Ajo çka e bën këtë moment të veçantë nuk është një arritje e vetme e madhe, por bashkimi i njëkohshëm i katër drejtimeve të trajtuara më sipër, pikërisht në kohën kur vetë Aleanca po e rimendon peshën strategjike të krahut të saj juglindor.

Pritja e një samiti të NATO-s nuk është thjesht nder protokollar, por ushtrim konkret sigurie dhe logjistike: mbyllje ajrore dhe detare, koordinim i shërbimeve të inteligjencës mes dhjetëra vendeve, si dhe kapacitet pritjeje për delegacione, median dhe siguri të nivelit më të lartë shtetëror. Përvoja e Ankarasë në vitin 2026 tregoi qartë shkallën e kësaj ndërmarrjeje, edhe për një vend me kapacitete shumë më të mëdha se Shqipëria. Përgatitja shqiptare për vitin 2027 do të kërkojë, për rrjedhojë, jo vetëm gatishmëri diplomatike, por edhe një test të drejtpërdrejtë të kapaciteteve operationale e logjistike që ky punim i ka trajtuar si drejtime më vete.

Zgjedhja e Ankarasë si vendi pritës i samitit të vitit 2026, e ndjekur menjëherë nga Tirana në 2027, nuk është thjesht rotacion gjeografik rutinë mes 17 vendeve që ende s’kishin organizuar një samit. Është vazhdim i së njëjtës logjikë që solli forcimin e statusit të Rumanisë si “*spirancë e Detit të Zi*” dhe njohjen e Greqisë si mur mbrojtës i Mesdheut Lindor: një rikonceptim i krahut juglindor jo më si periferi e Aleancës, por si hapësirë me peshë vetjake strategjike. Në këtë hartë të re, Shqipëria hyn jo si përfituese pasive e vëmendjes së re, por si vend që, përmes katër drejtimeve të angazhimit të saj, e ka kultivuar me vetëdije këtë moment.

E rëndësishme është, megjithatë, të mos lexohet Samiti i Tiranës si pikë

mbërritjeje. Vlera e tij reale do të matet jo nga vetë zhvillimi i samitit, por nga objektivat e reja që ai do të hapë për periudhën pasuese: thellim i mëtejshëm i katër drejtimeve, jo ndalim tek arritja simbolike e vendit pritës. Kjo logjikë vlen edhe përtej vitit 2027: nëse periudha 2022-2026 u karakterizua nga rikthimi i mbrojtjes kolektive në qendër të planifikimit strategjik të NATO-s, periudha 2027-2030 pritet të karakterizohet nga konsolidimi i kapaciteteve të reja operacionale, industriale dhe infrastrukturore, ku Shqipëria ka mundësi të forcojë më tej rolin e saj si nyje logjistike dhe operacionale e krahut juglindor, veçanërisht përmes zhvillimit të mëtejshëm të bazës së Kuçovës, kompleksit Durrës-Porto Romano dhe integritetit të plotë të Korridorit VIII. Sfida kryesore nuk do të jetë kështu organizimi i samitit në vetvete, por aftësia për ta shndërruar këtë moment në një platformë të qëndrueshme për zgjerimin e rolit shqiptar brenda arkitekturës së sigurisë euroatlantike.

## **Përfundime**

Ky punim argumentoi se angazhimi shqiptar në NATO gjatë vitit 2026 nuk mund të kuptohet si seri veprimesh të veçanta, por si konvergencë e katër drejtimeve të njëkohshme: operacionale, diplomatike, industriale dhe infrastrukturore, që së bashku e kanë kthyer besueshmërinë institucionale në kapital strategjik të prekshëm.

Samiti i Ankarasë 2026 dëshmoi rëndësinë në rritje të krahut juglindor brenda planifikimit strategjik të NATO-s, ku qëndrueshmëria e vendeve më të vogla e të besueshme fitoi peshë të re, si plotësim i domosdoshëm i solidaritetit aleat, jo si zëvendësim i tij.

Pritja e Samitit të Tiranës në 2027 nuk është kështu shpërblim i papritur, por vazhdim logjik i një procesi që filloi më shumë se një dekadë e gjysmë më parë, dhe që u përshpejtua ndjeshëm gjatë vitit të fundit. Ai duhet parë, njëkohësisht, si pikënisje, jo si kulm përfundimtar: vlera e tij e vërtetë do të vijë nga objektivat që do të hapë për periudhën pas 2027-s, jo nga vetë fakti i organizimit. Përvoja shqiptare sugjeron se, në kushtet e mjedisit aktual të sigurisë, ndikimi i vendeve të vogla brenda NATO-s përcaktohet gjithnjë e më pak nga dimensionet sasiore të forcave të tyre dhe gjithnjë e më shumë nga besueshmëria, kontributi i vazhdueshëm dhe aftësia për të mbështetur objektivat kolektive të Aleancës.

Si dikush që e ka jetuar këtë proces që nga fillimet e tij institucionale, e sot e ndjek nga brenda vetë strukturave rajonale të Aleancës, e shoh këtë konvergencë jo si përfundim rrëfimi, por si kapitull të ri që sapo fillon të shkruhet.

## Rekomandime

Në përgatitje të Samitit të Tiranës 2027, rekomandohen tri drejtime konkrete veprimi.

*Së pari*, investimi i njëkohshëm në të katër drejtimet e trajtuara, operacional, diplomatik, industrial dhe infrastrukturor, duhet të vazhdojë pa u lënë asnjëri mbrapa, duke pasur parasysh diferencat e ritmit ndërmjet tyre të trajtuara më sipër.

*Së dyti*, Samiti i Tiranës duhet të konceptohet jo si moment përmbyllës, por si pikënisje objektivash të rinj afatgjatë. Institucionet përgjegjëse duhet të përcaktojnë përpara zhvillimit të Samitit, se cilat angazhime konkrete do të vijnë pas mbylljes së tij, në mënyrë që momenti të mos mbetet i izoluar.

*Së treti*, vëmendje e veçantë i duhet kushtuar ruajtjes së ritmit të angazhimit edhe pas mbylljes së Samitit, në një periudhë kur vëmendja ndërkombëtare zakonisht tërhiqet shpejt drejt krizës tjetër, në mënyrë që kapitali besueshmërie i ndërtuar deri në 2027 të mos zbehet po aq shpejt sa u ndërtua.

## Bibliografia

1. Anadolu Agency. (2024, 3 maj). NATO's first-ever tactical air base in Western Balkans inaugurated in Albania [Baza e parë taktike ajrore e NATO-s në Ballkanin Perëndimor u përrua në Shqipëri].
2. Atlantic Council. (2026, 9 korrik). Eleven takeaways from the NATO Summit in Ankara [Njëmbëdhjetë përfundime nga Samiti i NATO-s në Ankara].
3. Atlas Institute for International Affairs. (2026). The Black Sea in 2026: From contested waters to strategic opportunity [Deti i Zi në 2026: Nga ujëra të kontestuara në mundësi strategjike].
4. Debuglies. (2026, 27 korrik). From the Adriatic to the Black Sea: Corridor VIII transforms Italy into Europe's military rearguard [Nga Adriatiku në Detin e Zi: Korridori VIII e shndërron Italinë në krahun ushtarak mbrojtës të Evropës].
5. EUalive. (2026, 9 korrik). NATO allies expand Black Sea mission to protect critical underwater infrastructure [Aleatët e NATO-s zgjerojnë misionin në Detin e Zi për të mbrojtur infrastrukturën kritike nënujore].
6. Faxweb. (2026, 12 shkurt). "Korridori 8, korridor sigurie për NATO-n"/ Rama: E vendos Shqipërinë në zemër të infrastrukturës strategjike.
7. GLOBSEC. (2026). NATO Eastern Flank readiness 2026: Are frontline states battle ready? [Gatishmëria e krahut lindor të NATO-s 2026: A janë vendet e vijës së parë gati për luftë?].

8. Grosswald Research. (2026). NATO exercises 2026: The complete guide to allied readiness [Stërvitjet e NATO-s 2026: Udhëzuesi i plotë i gatishmërisë aleate].
9. Hoxha, D. (2026). Roli i vendeve të vogla në aleancat ushtarake dhe kontributi i Forcave të Armatosura në mbrojtjen kolektive: Rasti i Shqipërisë në NATO [Disertacion doktrature, Universiteti Ushtarak i Teknologjisë, Varshavë].
10. JavaNews. (2026, korrik). Shqipëria hyn në fazën “NATO 3.0”, Nufi njofton investime në mbrojtje.
11. Maritime News. (2026, 24 mars). NATO launches Sea Shield 2026 exercise in Black Sea amid heightened maritime security focus [NATO nis stërvitjen Sea Shield 2026 në Detin e Zi].
12. Ministria e Mbrojtjes, Republika e Shqipërisë. (2024). Akte ligjore për industrinë ushtarake: Ligji nr. 87/2024, Ligji nr. 88/2024, VKM nr. 794/2024, VKM nr. 841/2024.
13. Ministria e Mbrojtjes, Republika e Shqipërisë. (2026, 31 maj). Nufi: Porto Romano dhe Korridori VIII, investime strategjike për lëvizshmërinë e NATO-s.
14. Modern War Institute at West Point. (2026). NATO’s Turkey paradox [Paradoksi i Turqisë për NATO-n].
15. NATO. (2024, 5 mars). NATO completes modernisation of major airbase in Albania [NATO përfundon modernizimin e bazës kryesore ajrore në Shqipëri].
16. NATO. (2026, 3 mars). Joint press conference by NATO Secretary General Mark Rutte with the President of North Macedonia [Konferencë e përbashkët shtypi e Rutte-s me Presidentin e Maqedonisë së Veriut].
17. NATO. (2026, korrik). Overview: 2026 NATO Summit in Ankara [Përmbledhje: Samiti i NATO-s në Ankara, 2026].
18. RTSH. (2026, 3 qershor). SHBA ka ridrejtuar mbi 125 anije tregtare që nga fillimi i bllokadës detare të porteve iraniane.
19. Shtabi i Përgjithshëm i Forcave të Armatosura. (2025, nëntor). Gjenerallejtënant Arben Kingji në Napoli: Shqipëria riafirmon angazhimin ndaj Planit Juglindor të NATO-s. Gazeta Ushtria.
20. Temnycky, M. (2026, 9 korrik). What happened at the 2026 NATO Summit in Turkey? [Çfarë ndodhi në Samitin e NATO-s në Turqi, 2026?] Forbes.
21. World Socialist Web Site. (2026, 28 maj). Greece deepens role as Washington’s Eastern Mediterranean bulwark [Greqia thellon rolin si mburoja e Uashingtonit në Mesdheun Lindor].

# Deri në çfarë mase Forcat Speciale kontribuojnë në luftën konjitive në konfliktet hibride?

---

**Kolonel Ramadan KARAKUSHI**

*Shef i Departamentit të Operacioneve Ushtarake  
Kolegji i Mbrojtjes dhe i Sigurisë*

## **Trajtesë e shkurtuar**

*Lufta bashkëkohore po zhvillohet në një mjedis ku kufijtë ndërmjet paqes dhe konfliktit, si dhe ndërmjet dimensioneve fizike, informative dhe njohëse, janë gjithnjë e më pak të dallueshëm. Në këtë kontekst, lufta hibride synon jo vetëm dobësimin e kapaciteteve kritike të sigurisë, por edhe ndikimin mbi perceptimet, vullnetin e vendimmarrësve dhe shoqërinë në tërësi. Ky punim shqyrton masën në të cilën Forcat Speciale kontribuojnë në luftën konjitive në konfliktet hibride, duke u përqendruar në përpjekjet dhe kapacitetet e tyre në fushën njerëzore, zbulimin special, ndihmën ushtarake, angazhimin me partnerët dhe krijimin e avantazheve në procesin e vendimmarrjes. Vlera e tyre kryesore qëndron në aftësinë për të krijuar njohuri të thelluara mbi mjedisin njerëzor, për të ndërtuar besim dhe bashkëpunim me partnerët, për të ndikuar në perceptimin e rrezikut dhe për të mbrojtur procesin e vendimmarrjes.*

*Në të njëjtën kohë, efektet konjitive janë të vështira për t'u matur dhe për t'u atribuuar vetëm aktiviteteve të Forcave Speciale, për shkak të kompleksitetit dhe karakterit shumëdimensional të konflikteve hibride. Si përfundim, punimi e trajton konceptin e Forcave Speciale si një kapacitet strategjik në luftën konjitive, efektiviteti i të cilit rritet ndjeshëm kur aktivitetet e tyre integrohen me inteligjencën, komunikimin strategjik, diplomacinë, kapacitetet kibernetike, forcat konvencionale dhe partnerët lokalë.*

**Fjalë kyçe:** lufta konjitive; lufta hibride; Forcat Speciale; NATO FOS; domen njerëzor; zbulim special; ndihma ushtarake; vendimmarrja; komunikim strategjik

## Hyrje

Karakter i konfliktit bashkëkohor po ndryshon nga një model ku fitorja përcaktohet kryesisht nga kontrolli i territorit dhe shkatërrimi i kapaciteteve fizike, drejt një mjedisi ku perceptimi, vullneti, besimi dhe vendimarrja e aktorëve janë po aq të rëndësishme sa rezultatet në fushën fizike. Në këtë mjedis, lufta hibride kombinon instrumente ushtarake dhe joushtarake, të hapura dhe të fshehta, duke synuar shfrytëzimin e dobësive politike, sociale, ekonomike dhe informative të kundërshtarit. NATO e konsideron kërcënimin hibrid si një kombinim të mjeteve dhe metodave që mund të veprojnë nën prapenë e konfliktit të armatosur tradicional.<sup>1</sup> Kjo e zhvendos rëndësinë e konkurrencës strategjike nga pyetja se kush mund të prodhojë më shumë fuqi fizike drejt pyetjes se kush mund të ndikojë më efektivisht në mënyrën se si individët, grupet dhe institucionet e perceptojnë realitetin dhe marrin vendime. NATO e përshkruan luftën konjitive si përpjekje për të ndikuar, mbrojtur ose ndërprerë proceset njohëse në nivele individuale, grupe dhe shoqërore, me qëllim krijimin e avantazhit ndaj kundërshtarit.<sup>2</sup> Për rrjedhojë, dimension i konjitiv nuk duhet të trajtohet si një zëvendësim i luftës fizike, por si një hapësirë në të cilën efektet fizike, informative, politike dhe sociale marrin kuptim strategjik.<sup>3</sup>

Në këtë mjedis, Forcat e Operacioneve Speciale (FOS) paraqesin një instrument me karakteristika të veçanta. Ato janë të afta të veprojnë me gjurmë relativisht të kufizuara, të ndërtojnë marrëdhënie të qëndrueshme me partnerët, të grumbullojnë njohuri mbi mjedisin njerëzor dhe të ofrojnë opsione fleksibël për vendimmarrësit. NATO i lidh operacionet speciale me objektiva taktike, operacionale dhe strategjike dhe identifikon Goditjet Direkte (GD), Zbulimin Special (ZB) dhe Asistencën Ushtarake (AU) si profile kryesore të misionëve të FOS.<sup>4</sup> Në kushtet e konkurrencës “zonë-gri”, ky fleksibilitet mund të jetë veçanërisht i rëndësishëm sepse FOS mund të veprojnë në hapësirën midis paqes dhe luftës, ku përdorimi i forcës konvencionale mund të jetë politikisht ose strategjikisht disproporcional.<sup>5</sup> Megjithatë, ekziston një rrezik konceptual nëse çdo aktivitet i FOS etiketohet automatikisht si luftë konjitive.

<sup>1</sup> NATO, “Countering Hybrid Threats,” NATO, updated January 29, 2026. NATO – Countering Hybrid Threats

<sup>2</sup> NATO Allied Command Transformation, “Cognitive Warfare: Beyond Military Information Support Operations,” May 9, 2023. NATO ACT – Cognitive Warfare

<sup>3</sup> Robert Schmidle, “Understanding Cognitive Warfare: Beyond Information,” *PRISM* 11, no. 2 (2026).

<sup>4</sup> NATO, “Special Operations Forces,” NATO. NATO – Special Operations Forces

<sup>5</sup> Lohaus, Phillip. Special Operations Forces in the Gray Zone: An Operational Framework for Employing Special Operations Forces in the Space Between War and Peace. American Enterprise Institute, 2016. <http://www.jstor.org/stable/resrep03267>.

Një operacion GD mund të ketë efekt fizik pa prodhuar domosdoshmërisht ndryshim konjitiv, një mision trajnimit mund të rrisë kapacitetin e partnerit pa ndryshuar perceptimet e tij dhe një marrëdhënie e mirë me një partner nuk është vetvetiu provë e ndikimit në vendimmarrje. Prandaj, kontributi i FOS duhet të vlerësohet përmes lidhjes midis aktivitetit, angazhimit njerëzor, mekanizmit të ndikimit, efektit konjitiv, ndryshimit në vendimmarrje dhe rezultatit operacional apo strategjik.<sup>6</sup>

Ky punim argumenton se FOS të NATO-s kontribuojnë në luftën konjitive në një masë të konsiderueshme, por të kushtëzuar. Kontributi i tyre nuk qëndron kryesisht në aftësinë për të zhvilluar propagandë ose operacione informative në kuptimin tradicional, por në kapacitetin për të ndikuar në kushtet që formojnë perceptimin, besimin, qëndrueshmërinë dhe vendimmarrjen. Fusha Njerëzore, Asistenca Ushtarake (AU), Zbulimi Special (ZB), marrëdhëniet me partnerët dhe aftësia për të gjeneruar njohuri lokale krijojnë një lidhje midis veprimit ushtarak dhe dimensionit konjitiv.<sup>7</sup> Në të njëjtën kohë, efektet më të rëndësishme shfaqen kur aktivitetet e FOS sinkronizohen me instrumente të tjera të fuqisë dhe me objektivat më të gjerë strategjike të NATO-s.<sup>8</sup> Prandaj, argumenti kryesor është se FOS duhet të kuptohen si strategji mundësuese në luftën konjitive, ato mund të krijojnë avantazh konjitiv, të forcojnë qëndrueshmërinë dhe besueshmërinë e partnerëve, të përmirësojnë vendimmarrjen dhe të ndikojnë në perceptimin e kundërshtarit, por rrallëherë mund të prodhojnë vetë, të izoluar, efektin strategjik përfundimtar.

## **Lufta hibride dhe dimensionit konjitiv**

Për të kuptuar kontributin e FOS, duhet, së pari, të kuptohet mjedisi në të cilin zhvillohet konkurrenca hibride. Lufta hibride nuk kufizohet në përdorimin e forcës ushtarake, por përfshin një kombinim të mjeteve politike, ekonomike, informative, kibernetike, ushtarake dhe sociale. NATO vëren se kundërshtarët mund të përdorin metoda të hapura dhe të fshehta për të krijuar pasiguri, për të shfrytëzuar ndarjet shoqërore dhe për të dobësuar kohezionin e kundërshtarit.<sup>9</sup> Për këtë arsye, objektivi i një fushate hibride mund të jetë më pak shkatërrimi i një njësie ushtarake dhe më shumë dobësimi i aftësisë së një shteti për të marrë vendime koherente dhe për të ruajtur vullnetin politik. Reisinger dhe Golts e vendosin qasjen ruse në një spektër ku aktivitetet ushtarake dhe

<sup>6</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>7</sup> Heather S. Gregg, "The Human Domain and Influence Operations in the 21st Century," *Special Operations Journal* 2, no. 2 (2016): 92–105. <https://doi.org/10.1080/23296151.2016.1239978>

<sup>8</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>9</sup> NATO, "Countering Hybrid Threats."

joushtarake kombinohen për të arritur objektiva politike duke shmangur, kur është e mundur, përshkallëzimin drejt konfliktit konvencional.<sup>10</sup> Cordesman gjithashtu thekson vështirësinë e ndarjes së prerë midis “zonë-gri”, hibrid dhe konkurrencë me shumë fusha, sepse këto aktivitete shpesh zhvillohen paralelisht dhe mbështesin njëra-tjetrën.<sup>11</sup> Kjo nënkupton se lufta konjitive duhet parë si një dimension i integruar i konkurrencës hibride dhe jo si një aktivitet i izoluar informativ.<sup>12</sup>

Në këtë mjedis, beteja për perceptimin bëhet një element i rëndësishëm i konkurrencës strategjike. NATO e përkufizon luftën konjitive si aktivitet që synon të ndikojë, mbrojë ose ndërpresë proceset konjitive të individëve, grupeve dhe popullatave për të fituar avantazh ndaj kundërshtarit.<sup>13</sup> Kjo qasje shkon përtej propagandës klasike sepse objektivi nuk është vetëm transmetimi i një mesazhi, por ndryshimi i mënyrës se si informacioni interpretohet dhe si ky interpretim ndikon në sjellje dhe vendimmarrje. Schmidle argumenton se lufta konjitive duhet dalluar nga *Operacioni Informues*, sepse fokusi i saj kryesor është te perceptimi, krijimi i bindjeve dhe mënyra se si njerëzit kuptojnë realitetin.<sup>14</sup> Në rastin e Rusisë, NATO Defense College ka evidentuar rëndësinë strategjike të kontrollit të perceptimeve historike dhe mënyrës se si narrativat mbi të kaluarën përdoren për të ndikuar në perceptimet e brendshme dhe të jashtme.<sup>15</sup> Burda, duke analizuar përvojat e Çekisë dhe Ukrainës, thekson se lufta konjitive duhet kuptuar si një sfidë shoqërore që kërkon jo vetëm përgjigje ushtarake, por edhe institucionale dhe shoqërore.<sup>16</sup> Prandaj, kontributi i FOS duhet të analizohet brenda këtij ekosistemi më të gjerë.

## Karakteristikat e FOS dhe rëndësia e tyre konjitive

Avantazhi i parë i FOS në këtë mjedis lidhet me mënyrën se si ato krijojnë dhe përdorin marrëdhënie njerëzore. Operacionet speciale nuk varen vetëm nga aftësia për të kryer veprime të sakta ushtarake, ato kërkojnë gjithashtu

<sup>10</sup> Heidi Reisinger and Aleksandr Golts, *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, NATO Defense College Research Paper no. 105 (2014). NATO Defense College – downloadable paper

<sup>11</sup> Anthony H. Cordesman and Grace Hwang, *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations* (Washington, DC: Center for Strategic and International Studies, 2020).

<sup>12</sup> Robin Burda, *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds* (The Hague Centre for Strategic Studies, 2023). HCSS – Cognitive Warfare as Part of Society

<sup>13</sup> NATO Allied Command Transformation, “Cognitive Warfare: Strengthening and Defending the Mind,” April 5, 2023. NATO ACT – Strengthening and Defending the Mind

<sup>14</sup> Schmidle, Robert. “Understanding Cognitive Warfare: Beyond Information.” *PRISM* 11, no. 2 (2026): 46–63. <https://www.jstor.org/stable/48873423>.

<sup>15</sup> Daniel Shultz, *Who Controls the Past Controls the Future: How Russia Uses History for Cognitive Warfare*, NATO Defense College Outlook no. 4 (2023). NATO Defense College – Shultz, Cognitive Warfare

<sup>16</sup> Burda, *Cognitive Warfare as Part of Society*.

kuptim të mjedisit, akses, besim dhe aftësi për të punuar me partnerë lokalë. Gregg e vendos fushën njerëzore në qendër të debatit mbi operacionet e ndikimit, duke argumentuar se qëllimi ushtarak është krijimi i ndikimit që mund të ndryshojë sjelljen e një popullate të synuar.<sup>17</sup> Kjo është veçanërisht e rëndësishme për FOS sepse Asistenca Ushtarake dhe angazhimi i vazhdueshëm mund të ndërtojnë marrëdhënie që zgjasin përtej një operacioni të vetëm. Lohaus argumenton se FOS kanë vlerë të veçantë në zonë gri për shkak të aftësisë së tyre për t'u përshtatur me mjedise ku kufiri midis paqes dhe luftës është i paqartë.<sup>18</sup> Stringer e lidh këtë karakteristikë me parandalimin e integruar dhe argumenton se FOS mund të ofrojnë një opsion të rëndësishëm në konkurrencën strategjike nën pragun e konfliktit tradicional.<sup>19</sup> Prandaj, marrëdhënia e FOS me fushën njerëzore nuk është vetëm një çështje taktike, por mund të krijojë kushtet për rezultate konjitive më afatgjata.

Megjithatë, marrëdhënia njerëzore nuk duhet barazuar automatikisht me ndikimin konjitiv. Ekzistenca e një marrëdhënieje me partnerin nuk provon se partneri ka ndryshuar perceptimin ose sjelljen e tij. Për këtë arsye, duhet të bëhet dallimi midis angazhimit, ndikimit dhe efekt. Angazhimi nënkupton aktivitetin dhe marrëdhënien, ndikimi nënkupton mekanizmin përmes të cilit marrëdhënia ndryshon perceptimin ose sjelljen, ndërsa efekt nënkupton rezultatin e identifikueshëm të këtij ndryshimi.<sup>20</sup> Ky dallim është i rëndësishëm sepse në konfliktet hibride ekzistojnë shumë faktorë konkurrues që ndikojnë në sjelljen e një individi, institucioni ose shteti. NATO e lidh luftën konjitive me ndikimin në qëndrime dhe sjellje, ndërsa fusha njerëzore fokusohet në kuptimin e aktorëve dhe marrëdhënieve që mund të krijojnë ndikim.<sup>21</sup> Në këtë kuptim, FOS kanë avantazh sepse mund të jenë të pranishme në mjedise ku njohuritë mbi aktorët lokalë, rrjetet sociale dhe perceptimet politike janë të rëndësishme për vendimmarrjen.<sup>22</sup> Por ky avantazh duhet të konvertohet në rezultate të matshme për të argumentuar se ekziston një efekt konjitiv.

## **Zbulimi Special dhe avantazhi në njohuri**

Një nga mënyrat më të rëndësishme përmes të cilave FOS mund të kontribuojnë në luftën konjitive është krijimi i avantazhit në vendimmarrjeje

---

<sup>17</sup> Gregg, "The Human Domain and Influence Operations," 92–105.

<sup>18</sup> Lohaus, Phillip. *Special Operations Forces in the Gray Zone*, 8-10.

<sup>19</sup> Stringer, Kevin D. "A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF)." *PRISM* 10, no. 4 (2024): 123–32. <https://www.jstor.org/stable/48785859>.

<sup>20</sup> Gregg, "The Human Domain and Influence Operations," 92–105.

<sup>21</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>22</sup> Lohaus, Phillip. *Special Operations Forces in the Gray Zone: An Operational Framework for Employing Special Operations Forces in the Space Between War and Peace*. American Enterprise Institute, 2016. <http://www.jstor.org/stable/resrep03267>.

përmes ZS dhe njohjes së mjedisit. Në një konflikt hibrid, avantazhi nuk varet vetëm nga sasia e informacionit, por nga aftësia për ta kuptuar informacionin, për ta vlerësuar dhe për ta përdorur në kohën e duhur. NATO e lidh superioritetin e njohjes me aftësinë për të kuptuar, vendosur dhe vepruar në mënyrë më efektive se kundërshtari.<sup>23</sup> Kjo e bën ZS të rëndësishme sepse FOS mund të sigurojnë njohuri mbi aktorët, rrjetet, dobësitë dhe zhvillimet lokale që nuk janë gjithmonë të dukshme për strukturat që veprojnë nga distanca. Në konfliktet hibride, informacioni mbi qëndrimet e popullsisë, strukturat lokale të pushtetit, rrjetet e ndikimit dhe narrativat dominuese mund të jetë po aq i rëndësishëm sa informacioni mbi kapacitetet fizike të kundërshtarit.<sup>24</sup> Kështu, kontributi konjitiv i ZS nuk është domosdoshmërisht ndikimi i drejtpërdrejtë mbi mendjen e kundërshtarit, por përmirësimi i aftësisë së NATO-s dhe partnerëve për të kuptuar mjedisin dhe për të marrë vendime më të mira.<sup>25</sup>

Kjo lidhje midis informacionit, kuptimit dhe vendimmarrjes krijon një nga dallimet më të rëndësishme midis luftës konjitive dhe luftës së informacionit. Lufta e informacionit mund të synojë kontrollin, manipulimin ose mbrojtjen e informacionit, ndërsa lufta konjitive synon ndikimin në mënyrën se si informacioni perceptohet dhe përdoret.<sup>26</sup> NATO thekson se kundërshtarët po përdorin teknologjitë e komunikimit, lajme të rreme dhe manipulimin e perceptimeve për të dobësuar besimin në burimet e informacionit dhe për të ndikuar në opinionin publik.<sup>27</sup> Në këtë mjedis, FOS mund të kontribuojnë duke siguruar kuptim kontekstual që ndihmon komandantët dhe vendimmarrësit të dallojnë informacionin e rëndësishëm nga zhurma informative. Kjo mund të reduktojë pasigurinë, të përmirësojë ritmin e vendimmarrjes dhe të krijojë mundësi për reagim më të shpejtë ndaj veprimeve të kundërshtarit.<sup>28</sup> Për këtë arsye, ZS duhet parë si një burim i mundshëm i avantazhit konjitiv, edhe kur nuk ka një operacion të drejtpërdrejtë për ndikimin e perceptimit të popullsisë.

## Asistenca Ushtarake, besimi dhe qëndrueshmëria

Asistenca Ushtarake, është një tjetër mekanizëm përmes të cilit FOS mund të prodhojnë efekte konjitive, veçanërisht nëpërmjet ndërtimit të besimit dhe qëndrueshmërisë së partnerëve. Ndryshe nga një operacion i vetëm, asistenca e vazhdueshme krijon mundësi për ndërveprim, mësim reciprok dhe zhvillim

<sup>23</sup> NATO, "Why Cognitive Superiority Is an Imperative," *NATO Review*, February 6, 2024. NATO Review – Cognitive Superiority

<sup>24</sup> Gregg, "The Human Domain and Influence Operations," 92–105.

<sup>25</sup> NATO, "Why Cognitive Superiority Is an Imperative."

<sup>26</sup> Schmidle, Robert. "Understanding Cognitive Warfare

<sup>27</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>28</sup> NATO, "Why Cognitive Superiority Is an Imperative."

të kapaciteteve institucionale. NATO e identifikon asistencën ushtarake si një nga profilet kryesore të misioneve FOS, ndërsa përvoja e operacioneve speciale tregon se partneriteti është një komponent i rëndësishëm i aftësisë së tyre për të vepruar në mjedise komplekse.<sup>29</sup>

Në dimensionin konjitiv, rëndësia e AU nuk qëndron vetëm në rritjen e kapaciteteve ushtarake të partnerit, por në mënyrën se si këto kapacitete ndikojnë në perceptimin e tij për sigurinë, aftësinë dhe mundësinë për të rezistuar presionit. Stringer e lidh përdorimin e FOS në zonën gri me konceptin e parandalimit të integruar, ku partneriteti dhe prania e vazhdueshme mund të rrisin koston e veprimeve agresive dhe të ndikojnë në kalkulimin e kundërshtarit.<sup>30</sup> Në këtë mënyrë, asistenca ushtarake mund të prodhojë një efekt të dyfishtë: të rrisë kapacitetin fizik të partnerit dhe, njëkohësisht, mund të forcojë besimin dhe vullnetin e tij për të vepruar.

Ky mekanizëm është veçanërisht i rëndësishëm në konfliktet hibride sepse një nga objektivat e kundërshtarit mund të jetë krijimi i ndjenjës së pasigurisë, pafuqisë ose varësisë. Nëse një partner bindet se nuk është në gjendje të mbrojë institucionet e veta ose të përballojë presionin e jashtëm, ai mund të bëhet më i prirur për kompromis ose për pranimin e narrativave të kundërshtarit. Në të kundërt, kapaciteti i ndërtuar përmes asistencës mund të forcojë reziliencën dhe të ruajë autonominë e vendimmarrjes.<sup>31</sup> Burda thekson se mbrojtja ndaj luftës konjitive kërkon angazhim të aktorëve të ndryshëm shoqërorë dhe ndërtimin e politikave që forcojnë reziliencën e shoqërisë.<sup>32</sup> Në të njëjtën mënyrë, NATO e lidh luftën konjitive me nevojën për të ruajtur lirinë e veprimit dhe vendimmarrjes.<sup>33</sup> Kjo tregon se AU mund të ketë vlerë konjitive jo sepse FOS “kontrollojnë” perceptimin e partnerit, por sepse ndihmojnë në krijimin e kushteve ku partneri mund të marrë vendime të pavarura nën presion.<sup>34</sup>

## **Besueshmëria, shkurajimi dhe perceptimi i kundërshtarit**

Një dimension tjetër i kontributit të FOS është aftësia e tyre për të ndikuar në perceptimin e rrezikut dhe shkurajimit. Në konfliktet hibride, kundërshtari mund të mos jetë i interesuar vetëm të vlerësojë se sa trupa apo armë ka NATO,

<sup>29</sup> NATO, “Special Operations Forces.”

<sup>30</sup> Stringer, Kevin D. “A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF).”

<sup>31</sup> Burda, *Cognitive Warfare as Part of Society*.

<sup>32</sup> Po aty

<sup>33</sup> NATO Allied Command Transformation, “Cognitive Warfare: Strengthening and Defending the Mind.”

<sup>34</sup> Stringer, Kevin D. “A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF).”

por edhe sa është e gatshme Aleanca të përdorë aftësitë e saj dhe sa të besueshme janë këto aftësi. FOS mund të kontribuojnë në këtë perceptim përmes pranisë, ushtrimeve, angazhimit me partnerët dhe aftësisë për të operuar në mjedise ku përdorimi i forcës konvencionale do të kishte pasoja të tjera politike. Lohaus argumenton se FOS kanë një rol të veçantë në hapësirën midis paqes dhe luftës për shkak të përshtatshmërisë së tyre ndaj mjediseve të paqarta strategjike.<sup>35</sup> Stringer e zgjeron këtë argument duke i parë FOS si një element të parandalim i integruar, ku kapacitetet speciale mund të krijojnë opsione të ndryshme për t'iu përgjigjur konkurrencës nën prapësinë e konfliktit.<sup>36</sup> Nëse kundërshtari beson se këto aftësi ekzistojnë dhe se ato mund të përdoren në mënyrë efektive, perceptimi i kostos dhe riskut mund të ndryshojë.<sup>37</sup> Prandaj, efekti konjitiv këtu ndodh në nivelin e kalkulimit të kundërshtarit.

Megjithatë, shkurrëimi nuk mund të reduktohet në prapësinë fizike të FOS. Efekti i saj varet nga mënyra se si kundërshtari e interpreton sinjalin dhe nga besueshmëria e mesazhit strategjik. Një aktivitet i FOS që interpretohet si demonstrim i aftësisë mund të rrisë shkurrëimin, ndërsa një aktivitet që interpretohet si provokim mund të rrisë tensionin dhe të shkakttojë përshkallëzim.<sup>38</sup> Kjo është arsyeja pse lufta konjitive kërkon sinkronizim midis veprimit ushtarak dhe instrumenteve të tjera të fuqisë. NATO Allied Command Transformation (ACT) thekson se aktivitetet konjitive duhet të zhvillohen në koordinim me instrumentet e tjera të fuqisë për të ndikuar në qëndrime dhe sjellje dhe për të fituar avantazh ndaj kundërshtarit.<sup>39</sup> Në këtë kuptim, FOS mund të ofrojnë një sinjal të fuqishëm, por kuptimi strategjik i këtij sinjali varet nga konteksti politik, komunikimi dhe perceptimi i audiencave.<sup>40</sup> Kjo e bën besueshmërinë një faktor ndërmjetësues midis aktivitetit të FOS dhe efektit konjitiv.

## FOS dhe lufta për narrativën

Një tjetër mënyrë për të vlerësuar kontributin e FOS është marrëdhënia e tyre indirekte me narrativën strategjike. Lufta konjitive nuk kufizohet në shpërndarjen e informacionit, por përfshin mënyrën se si aktorët ndërtojnë kuptimin e realitetit. NATO Defense College ka analizuar përdorimin e historisë

<sup>35</sup> Phillip Lohaus, "Special Operations Forces in the Gray Zone, 75-91.

<sup>36</sup> Kevin D. "A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF)." 123-129

<sup>37</sup> Po aty

<sup>38</sup> NATO, "Countering Hybrid Threats."

<sup>39</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>40</sup> Shultz, Daniel. *Who Controls the Past Controls the Future: How Russia Uses History for Cognitive Warfare*. NATO Defense College, 2023. <http://www.jstor.org/stable/resrep58203>.

nga Rusia si instrument për të formuar perceptime dhe për të mbështetur objektiva strategjike.<sup>41</sup> Kjo tregon se narrativa mund të ketë efekt më të madh kur lidhet me identitetin, historinë, legjitimitetin dhe perceptimin e kërcënimit. Në këtë mjedis, FOS mund të kontribuojnë në mënyrë indirekte përmes marrëdhënieve të tyre me partnerët dhe aktorët lokalë, duke siguruar njohuri mbi narrativat që ekzistojnë në një shoqëri dhe mbi mënyrën se si ato ndikojnë në sjellje.<sup>42</sup> Gregg argumenton se kuptimi i fushës njerëzore është i rëndësishëm për të kuptuar se si ndikimi mund të prodhohet përmes marrëdhënieve njerëzore dhe kontekstit social.<sup>43</sup> Prandaj, FOS nuk duhet të konsiderohen domosdoshmërisht si aktori kryesor që ndërton narrativën strategjike, por si një burim i rëndësishëm i njohurive dhe marrëdhënieve që mund të ndihmojnë aktorët e tjerë të zhvillojnë komunikim më të besueshëm dhe më të përshtatshëm ndaj audiencës.<sup>44</sup>

Kjo qasje e bën të domosdoshëm dallimin midis narrative influence dhe propagandës. Nëse FOS ndërtojnë marrëdhënie të besueshme me partnerët, veprimet e tyre mund të shërbejnë si dëshmi konkrete e angazhimit të NATO-s. Nëse, përkundrazi, veprimet e tyre perceptohen si të papërshtatshme, ato mund të krijojnë materiale për narrativën e kundërshtarit. NATO ACT thekson se lufta konjitive synon të ndryshojë perceptimet e realitetit dhe të shfrytëzojë dobësitë konjitive në nivel shoqëror.<sup>45</sup> Prandaj, çdo aktivitet i FOS mund të ketë edhe efekte të paqëllimshme në informacion dhe perceptim. Ky është një aspekt i rëndësishëm për vlerësimin e kontributit të tyre: një operacion nuk duhet të konsiderohet sukses konjitiv vetëm sepse objektivi fizik u arrit.<sup>46</sup> Nëse rezultati fizik prodhon humbje besimi, perceptim negativ ose përçarje midis partnerëve, efekti strategjik mund të jetë negativ.<sup>47</sup> Për këtë arsye, planifikimi i operacioneve speciale duhet të marrë në konsideratë jo vetëm efektin e menjëhershëm, por edhe efektet njohëse në vazhdimësi.

## FOS dhe avantazhi në vendimmarrje

Kontributi më i rëndësishëm i FOS në luftën konjitive qëndron në lidhjen ndërmjet njohurive, perceptimit dhe vendimmarrjes. NATO e konsideron superioritetin konjitiv të lidhur me aftësinë për të kuptuar, vendosur dhe vepruar më shpejt dhe më efektivisht se kundërshtari.<sup>48</sup> Në këtë kuptim, lufta

---

<sup>41</sup> Po aty.

<sup>42</sup> Heather S. Gregg, "The Human Domain and Influence Operations in the 21st Century,"

<sup>43</sup> Po aty.

<sup>44</sup> Robin Burda, *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds*.

<sup>45</sup> NATO Allied Command Transformation, "Cognitive Warfare: Beyond Military Information Support Operations."

<sup>46</sup> Heather S. Gregg, "The Human Domain and Influence Operations in the 21st Century,"

<sup>47</sup> NATO, "Countering Hybrid Threats."

<sup>48</sup> NATO, "Why Cognitive Superiority Is an Imperative."

konjitive nuk kufizohet vetëm në ndryshimin e opinioneve apo qëndrimeve; ajo merr rëndësi strategjike kur ndikon në procesin e vendimmarrjes dhe në sjelljen e aktorëve. Zbulimi Special mund të sigurojë njohuri, Asistenca Ushtarake mund të rrisë besimin dhe kapacitetin e partnerit, ndërsa prania dhe besueshmëria e FOS mund të ndryshojnë perceptimin e riskut. Kur këto elemente ndërthuren, ato mund të ndikojnë në mënyrën se si një aktor e vlerëson situatën dhe zgjedh kursin e veprimit.<sup>49</sup> Kjo krijon një lidhje të drejtpërdrejtë midis aktiviteteve të FOS dhe modelit “vëzhgoj, orientoj, vendos, veproj, (OODA observe, orient, decide, act,)” ku avantazhi kërkohet përmes përmirësimit të ritmit dhe cilësisë së ciklit të vendimmarrjes.<sup>50</sup>

Në këtë aspekt, kontributi i FOS mund të jetë i dyfishtë, ato mund të përpiqen të përmirësojnë ciklin konjitiv të partnerit dhe, njëkohësisht, të dobësojnë ciklin e kundërshtarit. Një partner që ka më shumë besim, më shumë informacion dhe më shumë kapacitet mund të vendosë më shpejt dhe me më pak pasiguri. Një kundërshtar që përballet me pasiguri, me perceptim të ndryshuar të riskut ose me vështirësi për të kuptuar qëllimet e NATO-s mund të ngadalësojë vendimmarrjen e vet. NATO Allied Command Transformation e përshkruan luftën konjitive si një qasje që synon të ndikojë në qëndrime dhe sjellje për të krijuar avantazh ndaj kundërshtarit.<sup>51</sup> Kjo e mbështet argumentin se vlera e FOS nuk matet vetëm me numrin e operacioneve të kryera, por me aftësinë e tyre për të krijuar kushte ku NATO dhe partnerët marrin vendime më efektive dhe kundërshtari përballet me më shumë pasiguri.<sup>52</sup> Avantazhi në vendimmarrje përbën urën ndërmjet aktivitetit taktik të FOS dhe efektit konjitiv-operacional.

## **Integrimi i SOF me instrumentet e tjera të fuqisë**

Pavarësisht potencialit të tyre, FOS nuk mund të konsiderohen instrumenti kryesor ose i vetëm i luftës konjitive. Vetë NATO e paraqet luftë konjitive si një aktivitet që duhet të sinkronizohet me instrumente të tjera të fuqisë.<sup>53</sup> Kjo është veçanërisht e rëndësishme në konfliktet hibride, ku kundërshtari mund të veprojë në të njëjtën kohë në dimensionin politik, ekonomik, kibernetik, informativ dhe ushtarak.<sup>54</sup>

<sup>49</sup> Kevin D. “A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF), 123-128.

<sup>50</sup> Schmidle, Robert. “Understanding Cognitive Warfare

<sup>51</sup> NATO Allied Command Transformation, “Cognitive Warfare: Beyond Military Information Support Operations.”

<sup>52</sup> NATO, “Why Cognitive Superiority Is an Imperative.”

<sup>53</sup> NATO Allied Command Transformation, “Cognitive Warfare: Beyond Military Information Support Operations.”

<sup>54</sup> Reisinger, Heidi, and Aleksandr Gol’c. “Hybrider Krieg in Der Ukraine: Russlands Intervention Und Die Lehren Für Die NATO.” *Osteuropa* 64, no. 9/10 (2014): 119–34. <http://www.jstor.org/stable/44937050>.

FOS mund të sigurojnë akses, njohuri dhe marrëdhënie, por këto duhet të lidhen me diplomacinë, inteligjencën, komunikimin strategjike, aftësitë kibernetike, forcat konvencionale dhe instrumentet civile. Schnaubelt argumenton se qasja shumë-domenëshe kërkon integrimin e instrumentit ushtarak me instrumentet joushtarake dhe një qasje gjithëpërfshirëse ndaj konkurrencës strategjike.<sup>55</sup> Stringer arrin në një përfundim të ngjashëm duke e vendosur vlerën e FOS brenda konceptit më të gjerë të parandalimit të integruar.<sup>56</sup> Për rrjedhojë, ndikimi konjitiv i FOS rritet kur aktivitetet e tyre janë pjesë e një fushate të sinkronizuar dhe zvogëlohet kur ato zhvillohen si aktivitete të izoluar.

Kjo nënkupton se modeli më i përshtatshëm analitik nuk është ai i FOS si instrument i drejtpërdrejtë i prodhimit të efektit konjitiv, por ai që e sheh aktivitetin e FOS si pjesë të një zinxhiri ndikimi: angazhimi njerëzor mundëson përdorimin e mekanizmave të ndikimit, të cilët synojnë të sjellin ndryshime në perceptim dhe sjellje, të ndikojnë në shpejtësinë dhe cilësinë e vendimmarrjes dhe, në fund, të kontribuojnë në krijimin e një efekti operacional me rëndësi strategjike. Ky zinxhir e bën të mundur vlerësimin e kontributit të FOS pa pretenduar se ato janë shkaku i vetëm i një rezultati strategjik.

Në një konflikt kompleks, një ndryshim në perceptim mund të jetë rezultat i veprimit disa aktorëve njëkohësisht. Për këtë arsye, vlerësimi i kontributit të FOS duhet të mbështetet në triangulim dhe në analizën e kontributit.<sup>57</sup> Një nivel i lartë kontributi do të kërkonte prova se aktiviteti i FOS lidhet me një mekanizëm të qartë ndikimi dhe se ky mekanizëm lidhet më pas me një ndryshim të identifikueshëm në perceptim, sjellje ose vendimmarrje. Në të kundërt, një nivel më i ulët kontributi do të ekzistonte kur aktiviteti është i dokumentuar, por lidhja e tij me efektin konjitiv mbetet e paqartë.<sup>58</sup>

Ky model shmang dy gabime: ekzagjerimin e rolit të FOS dhe, në të kundërt, nënvlerësimin e rolit të tyre si mundësues brenda një fushate më të gjerë hibride.

## Kufizimet dhe rreziqet

Megjithatë, kontributi i FOS në luftën konjitive përballat me kufizime të rëndësishme. *Së pari*, efektet konjitive janë të vështira për t'u matur sepse

<sup>55</sup>Christopher M. Schnaubelt, *Anyplace, Anywhere, Anytime: NATO and Multi-Domain Operations*, NATO Defense College, 2023.

<sup>56</sup>Stringer, Kevin D. "A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF)." 123-128.

<sup>57</sup>Cordesman, Anthony H., and Grace Hwang. "Broadening the Definition of Gray Area, Hybrid, Irregular and Multi-Domain Operations." In *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*. Center for Strategic and International Studies (CSIS), 2020. <http://www.jstor.org/stable/resrep27622.5>.

<sup>58</sup>Po aty

perceptimet, besimet dhe proceset e vendimmarrjes nuk janë gjithmonë të dukshme. *Së dyti*, konfliktet hibride përfshijnë një gamë të gjerë aktorësh, çka e bën të vështirë atribimin e veprimeve dhe efekteve të caktuara. Siç vëren Cordesman, aktivitetet në zonën gri dhe ato hibrid janë shpesh të ndërlydhura, ndërsa përpjekjet për t'i kategorizuar ato në mënyrë të ngurtë mund të çojnë në keqinterpretimin e natyrës dhe dinamikës së konkurrencës.<sup>59</sup> *Së treti*, burimet zyrtare mund të kenë tendencë të theksojnë suksesin operacional, ndërsa kundërshtari mund të manipulojë informacionin mbi rezultatet. NATO Defense College, në analizën e luftës konjitive ruse, nënvizon rëndësinë e kuptimit të objektivave konjitivë dhe dobësive të kundërshtarit përpara se të bëhet vlerësimi i ndikimit.<sup>60</sup> Këto kufizime kërkojnë që çdo pretendim mbi efektin e FOS të mbështetet në më shumë se një burim dhe të bëhet dallimi midis korrelacionit dhe shkakësisë.<sup>61</sup>

Një rrezik tjetër është që përpjekja për të prodhuar efekt konjitiv mund të krijojë efekt të kundërt. Nëse veprimet e FOS perceptohen si manipulim, shkelje e autonomisë lokale ose përdorim i tepruar i forcës, besueshmëria mund të dëmtohet. Në një mjedis ku besimi është vetë një objektiv i konkurrencës, humbja e legjitimitetit mund të prodhojë më shumë dëm sesa përfitim. NATO e vendos luftën konjitive në kontekstin e mbrojtjes së lirisë së veprimit dhe vendimmarrjes, çka nënkupton se efektet duhet të vlerësohen edhe nga perspektiva e mbrojtjes së vetë Aleancës dhe partnerëve.<sup>62</sup> Prandaj, suksesi i një operacioni FOS nuk duhet të matet vetëm me objektivin e tij imediat, por edhe me pasojat e tij konjitive, narrative dhe politike.<sup>63</sup> Kjo kërkon që komandantët dhe planifikuesit të analizojnë jo vetëm “çfarë ndodh?”, por edhe “si u perceptua?”, “çfarë ndryshoi?” dhe “a ndikoi ky ndryshim në sjelljen ose vendimmarrjen?”.<sup>64</sup>

## Përfundime

Analiza e mësipërme tregon se Forcat Operacionale Speciale të NATO-s kontribuojnë në luftën konjitive në konfliktet hibride në një masë të konsiderueshme. Megjithatë ky kontribut është i kushtëzuar nga konteksti operacional, integrimi dhe aftësia për të transformuar aktivitetin ushtarak në efekte konjitive të matshme. FOS nuk duhet të konceptohen si një instrument që

---

<sup>59</sup> Po aty

<sup>60</sup> Shultz, Daniel. *Who Controls the Past Controls the Future: How Russia Uses History for Cognitive Warfare*. NATO Defense College, 2023.

<sup>61</sup> Robin Burda, *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds*

<sup>62</sup> NATO Allied Command Transformation, “Cognitive Warfare: Strengthening and Defending the Mind.”

<sup>63</sup> Heather S. Gregg, “The Human Domain and Influence Operations in the 21st Century,” *Special Operations Journal* 2, 92-105.

<sup>64</sup> NATO, “Why Cognitive Superiority Is an Imperative.”

zëvendëson Operacionet Informuese, Komunikimin Strategjik, inteligjencën, diplomacinë ose instrumentet e tjera të fuqisë. Përkundrazi, vlera e tyre qëndron në aftësinë për të lidhur dimensionin fizik të operacioneve me marrëdhëniet njerëzore, perceptimin dhe vendimmarrjen. NATO e përkufizon luftën konjitive si një aktivitet që synon të ndikojë, mbrojë ose ndërpresë proceset konjitive për të krijuar avantazh ndaj kundërshtarit.<sup>65</sup> Në këtë kuptim, FOS kanë një pozicion të veçantë sepse veprojnë në mjedise ku marrëdhënia me njerëzit, njohuritë lokale dhe besueshmëria janë pjesë e vetë aftësisë operacionale.<sup>66</sup> Kjo i bën ato më shumë se një instrument taktik: ato mund të funksionojnë si mundësues strategjikë brenda një fushate hibride më të gjerë.

Kontributi i parë i rëndësishëm lidhet me **avantazhin konjitiv**. Zbulimi Special (ZS) dhe angazhimi me aktorët lokalë mund të sigurojnë njohuri që përmirësojnë kuptimin e mjedisit dhe cilësinë e vendimmarrjes.<sup>67</sup> Kontributi i dytë lidhet me forcimin e partneritetit dhe qëndrueshmërisë (*resilience*). Asistenca Ushtarake (AU) mund të rrisë jo vetëm kapacitetet ushtarake të partnerëve, por edhe besimin e tyre në aftësinë për t'u përballur me presionin dhe për të ruajtur autonominë e vendimmarrjes.<sup>68</sup> Kontributi i tretë lidhet me **besueshmërinë dhe parandalimin**. Prania dhe aftësitë e FOS mund të ndryshojnë perceptimin e kundërshtarit lidhur me kapacitetet, qëllimet dhe kostot e veprimit.<sup>69</sup> Kontributi i katërt **lidhet me kuptimin e mjedisit njerëzor**, përmes të cilit FOS mund të identifikojnë marrëdhënie, rrjete, perceptime dhe dobësi që mund të jenë të rëndësishme për një fushatë më të gjerë konjitive.<sup>70</sup> Këta mekanizma nuk janë të barasvlershëm me luftën konjitive në vetvete, por krijojnë kushtet në të cilat efektet konjitive mund të zhvillohen.

Prandaj, përgjigjja më e saktë ndaj pyetjes “deri në çfarë mase?” nuk është se FOS janë instrumenti dominues i luftës konjitive, por se ato janë një kapacitet i rëndësishëm dhe shumëfishues i fuqisë kur përdoren në mënyrë të integruar. Stringer e vendos vlerën e FOS në zonë gri brenda konceptit të parandalim i integruar, ndërsa Lohaus thekson përshtatshmërinë e tyre për konkurrencën në hapësirën midis paqes dhe luftës.<sup>71</sup> NATO, nga ana tjetër,

---

<sup>65</sup> NATO Allied Command Transformation, *Cognitive Warfare: Beyond Military Information Support Operations*.

<sup>66</sup> NATO, *Special Operations Forces*.

<sup>67</sup> NATO, “Why Cognitive Superiority Is an Imperative.”

<sup>68</sup> Stringer, Kevin D. “A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF).”

<sup>69</sup> Lohaus, Phillip. *Special Operations Forces in the Gray Zone: An Operational Framework for Employing Special Operations Forces in the Space Between War and Peace*.

<sup>70</sup> Heather S. Gregg, “The Human Domain and Influence Operations in the 21st Century,”

<sup>71</sup> Stringer, Kevin D. “A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF).”

thekson nevojën për sinkronizimin e luftës konjitive me instrumentet e tjera të fuqisë.<sup>72</sup> Kjo çon në përfundimin se efekti më i madh i FOS nuk arrihet kur ato veprojnë të izoluara, por kur aktivitetet e tyre lidhen me inteligjencë, komunikime strategjike, diplomaci, kibernetikë, forca konvencionale dhe partnerët lokalë.<sup>73</sup> Për këtë arsye, modeli Aktiviteti- Angazhimi -Ndikimi - Efekti Njohës - Efekti i Vendimmarrjes - Efekti Operacional - Kontributi Strategjik ofron një mënyrë më të saktë për të vlerësuar kontributin e tyre.

Në konfliktet hibride, megjithatë, është jashtëzakonisht e vështirë të provohet se një ndryshim në perceptim ose vendimmarrje është shkaktuar vetëm nga FOS. Shumë aktorë dhe instrumente veprojnë njëkohësisht dhe disa nga efektet më të rëndësishme konjitive mund të shfaqen shumë kohë pas aktivitetit fillestar.<sup>74</sup> Nëse aktiviteti është i dokumentuar, por lidhja me rezultatin konjitiv mbetet e dobët, atëherë kontributi duhet të vlerësohet si limited ose i pasigurt.<sup>75</sup> Përfundimisht, FOS të NATO-s kontribuojnë në luftën konjitive jo sepse janë një “armë e mendjes” të pavarur, por sepse aftësitë e tyre në fushën njerëzore, Zbulimi Special, Ndihma Ushtarake, angazhimi i partnerëve, besueshmëria, qëndrueshmëria dhe avantazhi i vendimmarrjes mund të krijojnë kushtet për të fituar konkurrencën konjitive. Forca e tyre strategjike qëndron pikërisht në aftësinë për t'i lidhur këto kapacitete me një qasje gjithëpërfshirëse dhe të sinkronizuar ndaj luftës hibride.

## Bibliografia

1. Burda, Robin. *Conjitive Warfare as Part of Society: Never-Ending Battle for Minds*. The Hague: The Hague Centre for Strategic Studies, 2023. <https://hcss.nl/report/conjitive-warfare-as-part-of-society-never-ending-battle-for-minds/>.
2. Cordesman, Anthony H., and Grace Hwang. “Broadening the Definition of Gray Area, Hybrid, Irregular and Multi-Domain Operations.” In *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*. Washington, DC: Center for Strategic and International Studies, 2020. <http://www.jstor.org/stable/resrep27622.5>.
3. *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*. Washington, DC: Center for Strategic and International Studies, 2020.

---

<sup>72</sup> NATO Allied Command Transformation, “Cognitive Warfare: Beyond Military Information Support Operations.”

<sup>73</sup> Schnaubelt, Christopher M. “Strategy and Multi-Domain Operations.” In *How to Write a Strategy*. NATO Defense College, 2024. <http://www.jstor.org/stable/resrep60913.12>.

<sup>74</sup> Cordesman, Anthony H., and Grace Hwang. “Broadening the Definition of Gray Area, Hybrid, Irregular and Multi-Domain Operations.”

<sup>75</sup> Po aty

<http://www.jstor.org/stable/6190d37f-c0e6-3e8d-bd47-3366bc6ef4aa>.

4. Gregg, Heather S. "The Human Domain and Influence Operations in the 21st Century." *Special Operations Journal* 2, no. 2 (2016): 92–105.
5. Lohaus, Phillip. *Special Operations Forces in the Gray Zone: An Operational Framework for Employing Special Operations Forces in the Space Between War and Peace*. Washington, DC: American Enterprise Institute, 2016. <http://www.jstor.org/stable/resrep03267>.
6. NATO. "Countering Hybrid Threats." NATO. Updated January 29, 2026. <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>.
7. NATO. "Special Operations Forces." NATO. <https://www.nato.int/en/what-we-do/deterrence-and-defence/special-operations-forces>.
8. NATO. "Why Conjitive Superiority Is an Imperative." *NATO Review*, February 6, 2024. <https://www.nato.int/docu/review/articles/2024/02/06/why-conjitive-superiority-is-an-imperative/index.html>.
9. NATO Allied Command Transformation. "Conjitive Warfare: Beyond Military Information Support Operations." May 9, 2023. <https://www.act.nato.int/article/conjitive-warfare-beyond-military-information-support-operations/>.
10. NATO Allied Command Transformation. "Conjitive Warfare: Strengthening and Defending the Mind." April 5, 2023. <https://www.act.nato.int/article/conjitive-warfare-strengthening-and-defending-the-mind/>.
11. Reisinger, Heidi, and Aleksandr Gol'c. "Hybrider Krieg in Der Ukraine: Russlands Intervention Und Die Lehren Für Die NATO." *Osteuropa* 64, no. 9/10 (2014): 119–34. <http://www.jstor.org/stable/44937050>.
12. Reisinger, Heidi, and Aleksandr Golts. *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*. NATO Defense College Research Paper no. 105. Rome: NATO Defense College, 2014.
13. Schmidle, Robert. "Understanding Conjitive Warfare: Beyond Information." *PRISM* 11, no. 2 (2026): 46–63. <https://www.jstor.org/stable/48873423>.
14. Schnaubelt, Christopher M. *Anyplace, Anywhere, Anytime: NATO and Multi-Domain Operations*. Rome: NATO Defense College, 2023.
15. "Strategy and Multi-Domain Operations." In *How to Write a Strategy*. Rome: NATO Defense College, 2024. <http://www.jstor.org/stable/resrep60913.12>.
16. Shultz, Daniel. *Who Controls the Past Controls the Future: How Russia Uses History for Conjitive Warfare*. Rome: NATO Defense College,

2023. <http://www.jstor.org/stable/resrep58203>.

17. Stringer, Kevin D. "A Gray Zone Option for Integrated Deterrence: Special Operations Forces (SOF)." PRISM 10, no. 4 (2024): 123–32. <https://www.jstor.org/stable/48785859>.

# Arkitektura e cënueshmërisë dhe qëndrueshmëria kombëtare: përtej parashikimit drejt veprimit të koordinuar – Implikime për Shqipërinë dhe Forcat e Armatosura

---

Msc. Alqi NIKOLLA

Specialist në Institutin Kërkimor Shkencor Ushtarak

## Trajtesë e shkurtuar

*Bllokimi i Kanalit të Suezit (2021) tregoi se si cënueshmëria e njohur e një nyjeje kritike (chokepoint) mund të shndërrohet në tronditje globale logjistike. Dëmtimi i kabllave nënujore në Detin Baltik (2024) evidentoi kufizime në koordinimin institucional dhe në përcaktimin e përgjegjësive, ndërsa ndërprerja e qarkullimit në Ngushticën e Hormuzit (2026) nxori në pah vështirësitë e reagimit të koordinuar ndaj pasojave në tregjet globale të energjisë. Në të tria rastet, sfida nuk lidhej me mungesën e parashikimit, por me vështirësinë për ta shndërruar informacionin në veprim të shpejtë e të koordinuar.*

*Ky punim argumenton se kufizimi kryesor i qëndrueshmërisë qëndron në një mospërputhje strukturore midis mënyrës si organizohen mekanizmat e saj dhe mënyrës si ndërprerjet përhapen përmes sistemeve të ndërlidhura. Duke u mbështetur në raste nga nyjet kritike detare, sistemet energjetike, infrastruktura nënujore dhe hapësira kibernetike, tregohet se si ngjarje relativisht të kufizuara gjenerojnë pasoja të gjera në sektorë të pa projektuar për t'u përgjigjur në mënyrë të integruar.*

*Analiza zgjerohet te rasti i Shqipërisë, duke shqyrtuar implikimet që ndërvarësitë mes infrastrukturës energjetike, porteve, rrjeteve digjitale dhe sigurisë kanë për qëndrueshmërinë kombëtare. Për një shtet të vogël anëtar të NATO-s, ndërtimi i qëndrueshmërisë kërkon jo vetëm forcim sektorial, por koordinim mes institucioneve civile, operatorëve të infrastrukturës kritike dhe Forcave të Armatosura të Republikës së Shqipërisë – kjo e fundit e parë jo vetëm si instrument mbrojtjeje, por si komponent kyç i arkitekturës kombëtare*

*të qëndrueshmërisë. Në qendër të rikonceptimit të propozuar qëndron nocioni i arkitekturës së cenueshmërisë, që zhvendos vëmendjen nga origjina e kërcënimit drejt rrugëve strukturore të përhapjes së tij. Qëndrueshmëria kuptohet kështu si funksion sistemik, jo karakteristikë sektoriale, me implikime të drejtpërdrejta për politikën e sigurisë, qeverisjes dhe mbrojtjes së infrastrukturës kritike në Shqipëri dhe në mjedisin euroatlantik.*

**Fjalë kyçe:** qëndrueshmëria kombëtare, arkitektura e cenueshmërisë, infrastruktura kritike, rreziku sistemik, ndërvarësia, kërcënimet hibride, Shqipëria, FARSH.

## Hyrje

Qëndrueshmëria është shndërruar në një koncept qendror në diskutimet mbi sigurinë, infrastrukturën dhe qeverisjen – veçanërisht për Shqipërinë, e cila si vend anëtar i NATO-s dhe kandidat për në BE është e ekspozuar njëkohësisht ndaj presioneve gjeopolitike rajonale dhe kufizimeve strukturore të kapaciteteve të saj institucionale. Gjatë dekadës së fundit, qeveritë dhe organizatat ndërkombëtare kanë investuar ndjeshëm në përmirësimin e aftësisë për të parashikuar ndërprerjet, për të vlerësuar përhapjen e tyre dhe për të identifikuar pasojat e mundshme në sistemet e ndërlidhura përmes analizës perspektive, vlerësimit të rrezikut dhe sistemeve të paralajmërimit të hershëm. Shqipëria vetë ka ndërtuar disa prej këtyre instrumenteve, prej kuadrit ligjor për infrastrukturën kritike deri te strukturat e reagimit kibernetik, por siç do të argumentohet, ekzistenca e instrumenteve të parashikimit nuk garanton vetvetiu aftësinë për t'i shndërruar ato në veprim të koordinuar.

Ngjarjet e viteve të fundit tregojnë një problem të vazhdueshëm: ndërprerjet shpesh mund të parashikohen, por pasojat e tyre mbeten të vështira për t'u menaxhuar sapo materializohen. Nga bllokimi i Kanalit të Suezit te kufizimet e Kanalit të Panamasë nga thatësira, e deri te incidentet që prekin infrastrukturën nënujore, shfaqet një model i përbashkët: ndërprerja e ka origjinën në një vend specifik, por efektet përhapen nëpër sisteme të ndërlidhura që tejkalojnë kapacitetet e mekanizmave sektorialë të reagimit. Ky model nuk është i huaj për Shqipërinë: sulmi kibernetik i korrikut 2022 ndaj sistemeve qeveritare, i lidhur me Iranin, tregoi se si një ndërprerje në infrastrukturën digjitale mund të gjenerojë efekte zinxhir përtej sektorit fillestar, duke cenuar funksionimin e institucioneve shtetërore. Këto dinamika sfidojnë supozimin se qëndrueshmëria mund të arrihet duke forcuar sektorë individualë të izoluar – supozim që në rastin shqiptar shfaqet qartë në varësinë pothuajse të plotë nga hidroenergja, e cila e bën sektorin energjetik të cenueshëm jo vetëm ndaj goditjeve klimatike, por edhe ndaj goditjeve që mund të shfaqen njëkohësisht në sektorët e ndërlidhur me të.

Argumenti kryesor i këtij punimi është se kufizimi i qasjeve aktuale ndaj qëndrueshmërisë ka natyrë strukturore dhe nuk buron nga mungesa e informacionit. Në këtë kuadër, zhvillohet koncepti i arkitekturës së cenueshmërisë për të shpjeguar si ndërvarësitë ndërmjet sistemeve ndikojnë në përhapjen e çrregullimeve dhe pse mekanizmat ekzistues hasin vështirësi në shndërrimin e parashikimit në veprim të koordinuar. Për Forcat e Armatosura të Shqipërisë kjo ka rëndësi të drejtpërdrejtë: FA vepron në një kuadër ku përcaktimi më i qartë i pragjeve të aktivizimit për skenarë hibridë dhe kibernetikë do të kontribuonte në rritjen e efektivitetit të koordinimit ndërinstitucional dhe të reagimit në kohë.

Punimi sugjeron një rishikim të mënyrës se si konceptohet qëndrueshmëria në kushtet e stresit sistemik, duke e parë atë përmes ndërvarësive që formojnë arkitekturën e cenueshmërisë dhe ndikojnë në mënyrën se si organizohen qeverisja, siguria dhe infrastruktura. Për Shqipërinë, këto implikime lidhen veçanërisht me ndarjen e roleve dhe mekanizmat e bashkëpunimit ndërmjet institucioneve civile dhe strukturave të mbrojtjes, si dhe me vendin që zë FA brenda arkitekturës më të gjerë të sigurisë kombëtare. Argumenti zhvillohet përmes analizës konceptuale të mbështetur në raste të përzgjedhura mbi baza teorike, që përfaqësojnë fusha strukturalisht të ndryshme por të ndërvarura të infrastrukturës kritike. Fokusi nuk është matja krahasuese e qëndrueshmërisë së shteteve, por identifikimi i mekanizmave të cenueshmërisë strukturore dhe i mospërputhjeve institucionale – mekanizma që gjejnë shprehje konkrete edhe në rastin shqiptar, nga Porti i Durrësit e deri te kabllo të nënujore të komunikimit që lidhin Shqipërinë me rrjetin rajonal.

Punimi ndjek konceptin e arkitekturës së cenueshmërisë në rastet e përzgjedhura si nyje të ndërvarësisë sistemike: nyjet kritike detare (ku Porti i Durrësit, si nyja kryesore e tregtisë detare dhe komponent i lëvizshmërisë ushtarake të Korridorit VIII, shërben si shembull konkret<sup>1</sup>), infrastruktura nënujore, sistemet energjetike dhe infrastruktura digjitale; më pas shqyrton pse strukturat institucionale kufizojnë reagimin efektiv pavarësisht paralajmërimeve të hershme; rikonceptimin e qëndrueshmërisë si funksion sistemik; dhe implikimet strategjike e të politikëbërjes që burojnë prej tij, përfshirë ato specifike për rolin e Forcave të Armatosura.

---

<sup>1</sup> Më 18 shkurt 2026 është nënshkruar Deklarata e Përbashkët e Tiranës nga ministrat e Jashtëm të Italisë, Shqipërisë, Bullgarisë, Maqedonisë së Veriut dhe Rumanisë, e cila e përcakton Korridorin VIII si “infrastrukturë sigurie evropiane” duke ju referuar angazhimit të marrë në Samitin e NATO-s në Uashington (2024) për një korridor të harmonizuar të lëvizshmërisë ushtarake. <https://www.ilssole24ore.com/art/energia-porti-e-corridoio-viii-balcani-vera-frontiera-adriatica-AJa8DLY>

## I. Kuadri konceptual: Arkitektura e cenesshmërisë

Qasjet bashkëkohore të qëndrueshmërisë nuk lidhen me mungesën e parashikimit, por me sfidat që shfaqen në kalimin nga paralajmërimi në veprim. Në këtë drejtim, sistemet që duhet ta përkthejnë parashikimin në masa konkrete reagimi dhe përgatitjeje nuk kanë evoluar gjithmonë me të njëjtin ritëm si sistemet që synojnë të mbrojnë. Një sfidë e tillë vërehet edhe në rastin shqiptar, ku kuadri ligjor për infrastrukturën kritike ekziston, por pragjet konkrete të aktivizimit institucional, përfshirë ato që lidhen me rolin e FA-së, mbeten ende për t'u përcaktuar më qartë.

Kur anija *Eagle S* dëmtoi kabllo të nënujore në Detin Baltik në vitin 2024, incidenti evidentoi sfida në përcaktimin e shpejtë të juridiksionit dhe të autoritetit përgjegjës për reagim. Po kështu, kur thatësira uli kapacitetin e Kanalit të Panamasë në vitin 2023, kufizimet në kalimin e anijeve kërkuan përshtatje të flukseve të trafikut dhe nxorën në pah rëndësinë e mekanizmave të koordinuar për menaxhimin e ndërvarësive logjistike. Në të dyja rastet, institucionet dhe mekanizmat e reagimit u përballën me sfidën e menaxhimit të një niveli të lartë ndërvarësie. Një perspektivë e ngjashme mund të merret në konsideratë edhe për Shqipërinë, veçanërisht në lidhje me kabllo të nënujore me fibër optike që e lidhin vendin me rrjetet rajonale dhe evropiane të telekomunikacionit në Detin Adriatik.<sup>2</sup>

Në praktikë, planifikimi i qëndrueshmërisë vazhdon të organizohet kryesisht sipas sektorëve: energjia veçmas nga transporti, ndërsa telekomunikacioni veçmas nga logjistika. Kjo pasqyron edhe mënyrën se si janë ndërtuar institucionet, ku ministritë dhe agjencitë organizohen sipas fushave të përgjegjësisë dhe veprojnë përmes proceseve dhe mekanizmave të tyre përkatës. Një logjikë e tillë karakterizon edhe arkitekturën institucionale shqiptare, ku përgjegjësitë janë të shpërndara ndërmjet institucioneve si Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK), Shërbimi Informativ Shtetëror (SHISH), Ministria e Mbrojtjes (MM), Agjencia Kombëtare e Mbrojtjes Civile (AKMC), Enti Rregullator i Energjisë (ERE), Ministria e Infrastrukturës dhe Energjisë dhe Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) etj., sipas fushave përkatëse të kompetencës. Megjithatë kjo ndarje lehtëson administrimin dhe përcaktimin e përgjegjësisë, ajo mund të mos pasqyrojë plotësisht shkallën e ndërlidhjes reale ndërmjet sektorëve. Pikërisht këto lidhje ndërsektoriale përbëjnë kanalet përmes të cilave ndërprerjet mund

---

<sup>2</sup> Shqipëria është e lidhur me rrjetet rajonale dhe evropiane të telekomunikacionit përmes kabllove nënujore me fibër optike në Detin Adriatik. Këto lidhje mbështesin komunikimet elektronike ndërkombëtare dhe përbëjnë një komponent të rëndësishëm të infrastrukturës kritike të vendit.

të përhapen dhe të prodhojnë efekte zinxhir, duke e bërë forcimin e mekanizmave të koordinimit ndërinstitucional një element të rëndësishëm të qëndrueshmërisë kombëtare.

Ky fragmentim ndikon edhe në mënyrën se si kuptohet rreziku: ndërprerjet në sektorin energjetik trajtohen si probleme të energjisë, ndërsa incidentet kibernetike si rreziqe digjitale – pikërisht kështu u trajtua fillimisht edhe sulmi kibernetik i korrikut 2022, si një çështje thjesht digjitale, përpara se pasojat institucionale të bëheshin të qarta. Studimet mbi infrastrukturën kritike tregojnë prej kohësh se dështimet rrallë mbeten të kufizuara brenda një sistemi,<sup>3</sup> ndërsa rritja e ndërlikohjes e bën përhapjen më të shpejtë e më të vështirë për t'u parashikuar.<sup>4</sup>

Planifikimi aktual ndërtohet rreth kategorive të njohura kërcënimesh (kibernetike, motit ekstrem, ushtarake), duke supozuar se krizat do t'u përshtaten këtyre kategorive. Në realitet, krizat zhvillohen njëkohësisht në disa fusha – dinamikë që për Shqipërinë do të thotë se një goditje klimatike të hidroenergji mund të përhapet njëkohësisht te qëndrueshmëria energjetike, infrastruktura digjitale dhe kapaciteti operacional i vetë FA-ve. Literatura e përshkruan këtë me konceptin e polikrizës (polycrisis), ku faktorë të ndryshëm stresi ndërveprojnë dhe përforcojnë njëri-tjetrin.<sup>5</sup>

Sistemet e infrastrukturës kritike organizohen në mënyra që krijojnë nivele të pabarabarta ekspozimi: disa pika shërbejnë si ura lidhëse, të tjera përqendrojnë flukse kryesore, siç është rasti i Portit të Durrësit, i cili funksionon njëkohësisht si nyje tregtare civile dhe komponent i lëvizshmërisë ushtarake të Korridorit VIII, pa u trajtuar gjithnjë si i tillë në planifikimin sektorial. Këtë gjendje punimi e përkufizon si arkitekturën e cenueshmërisë: konfigurimi strukturor që përcakton ku hyn ndërprerja, si amplifikohet dhe nëpër cilat sisteme përhapet. Kur thatësira kufizoi Kanalin e Panamasë, cenueshmëria buroi nga mënyra se si ishte konfiguruar sistemi – logjikë e krahasueshme me varësinë e Shqipërisë nga hidroenergji, ku vetë konfigurimi i sektorit, jo thjesht ekspozimi ndaj motit, e bën atë pikë kritike.

Kjo arkitekturë rrjedh nga mënyra se si infrastruktura është zhvilluar ndër vite: sistemet janë projektuar për të maksimizuar efikasitetin dhe për të funksionuar përtej kufijve shtetërorë, shpesh në kurriz të kapaciteteve rezervë dhe rrugëve alternative të operimit. Këto zgjedhje rrisin performancën në kushte

<sup>3</sup> Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine, 21(6), 11–25. <https://doi.org/10.1109/37.969131>

<sup>4</sup> Helbing, D. (2013). *Globally networked risks and how to respond*. Nature, 497, 51–59. <https://doi.org/10.1038/nature12047>

<sup>5</sup> Tooze, A. (2022). *Shutdown: How Covid shook the world's economy*. Allen Lane.

normale, por ulin aftësinë e sistemeve për të përballuar ndërprerjet dhe për të ruajtur funksionalitetin nën stres. Të njëjtat lidhje që mundësojnë efikasitetin krijojnë edhe rrugët përmes të cilave përhapet stresi, duke e bërë cenueshmërinë po aq produkt të organizimit të brendshëm sa edhe të goditjeve nga jashtë.

Strukturat institucionale e përforcojnë këtë dinamikë: koordinimi ndërsektorial mbështetet shpesh në marrëveshje të përkohshme, ndërsa përgjegjësitë dhe nivelet e aktivizimit mbeten të shpërndara. Kjo mospërputhje vërehet edhe në kuadrin ligjor shqiptar, ku përcaktimi i pragjeve dhe procedurave të aktivizimit të FA-së mund të qartësohet më tej. Studimet mbi menaxhimin e krizave tregojnë se dështimet në koordinim, më shumë sesa mungesa e informacionit, përcaktojnë shkallën e ndikimit<sup>6</sup> – dhe kjo shpjegon pjesërisht rezultatin e Shqipërisë në shtyllën e rezistencës ndaj goditjeve të matur nga EARI 2025.<sup>7</sup> Prandaj, kuptimi i cenueshmërisë kërkon zhvendosjen e vëmendjes nga dështimet e izoluar drejt strukturës që i lidh ato – parim që ka pasoja të drejtpërdrejta për mënyrën si duhet të riorganizohet roli i FA-ve brenda arkitekturës tonë të sigurisë.

## **II. Analiza empirike: Pikat e stresit në një botë të ndërlidhur**

Goditjet ndaj infrastrukturës kritike shfaqen në nyje të caktuara të ndërvarësisë dhe efektet përhapen në sisteme që nuk janë projektuar për të reaguar në mënyrë të integruar. Shqipëria, si vend me ekonomi të hapur detare, nuk qëndron jashtë këtij modeli, edhe pse nyjet e saj kritike janë të një shkalle më të vogël. Nyjet kritike detare ofrojnë ilustrimin më të qartë. Ngushtica e Hormuzit është shembulli më domethënës, pasi përmes saj kalon një pjesë e konsiderueshme e eksporteve botërore të naftës dhe gazit. Si rrjedhojë, çdo ndërprerje e qarkullimit në këtë ngushticë shkakton pasoja të menjëhershme për tregjet globale të energjisë, zinxhirët e furnizimit dhe ekonominë ndërkombëtare. Ajo përqendron një pjesë të konsiderueshme të flukseve globale të energjisë<sup>8</sup> ku edhe incidente të kufizuara kanë shkaktuar paqëndrueshmëri në tregjet energjetike dhe presione mbi zinxhirët e furnizimit.<sup>9</sup> Luhatje të tilla transmetohen pothuajse menjëherë edhe te Shqipëria, e cila,

<sup>6</sup> Boin, R. A., & ‘t Hart, P. (2010). *Organising for effective emergency management: Lessons from research*. Australian Journal of Public Administration, 69(4), 357–371. <https://doi.org/10.1111/j.14678500.2010.00694.x>

<sup>7</sup> *Enhanced Analytic Resilience Index 2025 - Central Euro-Atlantic pentru Reziliență - E-ARC*, EARI2025.pdf fq.26

<sup>8</sup> International Energy Agency. (2024). *World energy outlook 2024*. <https://www.iea.org/reports/world-energy-outlook-2024>

<sup>9</sup> Ghosal, A., & Olingo, A. (2026, March 30). *The war in Iran sparks a global fertilizer shortage and threatens food prices*.

pavarësisht hidroenergjisë vendase, mbetet e lidhur me tregjet rajonale të energjisë përmes importeve. Sipas IEA,<sup>10</sup> kufizimi i trafikut përmes Hormuzit prodhoi humbje kumulative mbi një miliard fuçi, ndërsa çmimet arritën përkohësisht mbi 144 dollarë/fuçi.

Kjo qasje është në përputhje me argumentin e Farrell dhe Newman,<sup>11</sup> të cilët theksojnë se ndërvarësia ndërkombëtare krijon kanale përmes të cilave ndërprerjet mund të projektohen përtej pikës së tyre fillestare. Ky punim e zgjeron këtë koncept drejt analizës së infrastrukturës fizike, duke argumentuar se përhapja dhe përforcimi i krizave nuk përcaktohen vetëm nga veprimet apo synimet e aktorëve, por edhe nga arkitektura strukturore e rrjeteve dhe pozicioni i nyjeve kritike brenda tyre.

Bllokimi i Kanalit të Suezit në vitin 2021 e përforcoi këtë model: një ndërprerje në një pikë të vetme prodhoi menjëherë grumbullim global anijesh dhe vonesa të konsiderueshme, me pasoja të matshme në kostot e transportit dhe faktorë që nxitën inflacionin në disa ekonomi.<sup>12</sup> Sulmet ndaj transportit tregtar në Detin e Kuq treguan gjithashtu se aktorë asimetrikë mund të shfrytëzojnë cenueshmërinë e nyjeve kritike pa pasur kontroll mbi vetë hapësirën detare, duke detyruar ridrejtimin e rrugëve dhe rritjen e kostove në zinxhirët globalë të furnizimit. Sipas IMO,<sup>13</sup> dhe UNCTD<sup>14</sup> në 2024 u raportuan 146 incidente piraterie dhe grabitjeje të armatosur ndaj anijeve në nivel global, të përqendruara në korridore si Ngushtica e Malakës dhe Oqeani Indian. Ridrejtimet e trafikut detar që rrjedhin prej këtyre ngjarjeve prekin edhe rrugët drejt Adriatikut dhe si pasojë, volumin dhe kohët e mallrave përmes Portit të Durrësit – nyja kryesore tregtare e vendit dhe njëkohësisht komponent i lëvizshmërisë ushtarake të Korridorit VIII, çka e vendos këtë port njëherësh në rrjedhën e efekteve të zinxhirëve globale dhe në qendër të planifikimit logjistik të FA-ve. Edhe sulmet e kufizuara rezultuan të mjaftueshme për të ndryshuar modelet globale të transportit detar, duke konfirmuar se ndikimi varet më pak nga përmasat e incidentit e më shumë nga pozicioni strukturor i infrastrukturës së prekur.

---

<sup>10</sup> International Energy Agency. (2026). *Oil Market Report: May 2026*. IEA.

<sup>11</sup> Farrell, H., & Newman, A. L. (2019). *Weaponized interdependence: How global economic networks shape state coercion*. *International Security*, 44(1), 42–79. [https://doi.org/10.1162/isec\\_a\\_00351](https://doi.org/10.1162/isec_a_00351)

<sup>12</sup> Carrière-Swallow, Y., Deb, P., Furceri, D., Jiménez, D., & Ostry, J. D. (2022). *Shipping costs and inflation (IMF Working Paper No. WP/22/61)*. International Monetary

<sup>13</sup> International Maritime Organization. (2025). *Reports on acts of piracy and armed robbery against ships: Annual report 2024 (MSC.4/ Circ.269)*.

<sup>14</sup> United Nations Conference on Trade and Development. (2024). *Navigating troubled waters: Impact to global trade of disruption of shipping routes in the Red Sea, Black Sea and Panama Canal*. UNCTAD

Kanali i Panamasë ilustron të njëjtën dinamikë pa origjinë armiqësore: thatësira kufizoi kapacitetin, duke shkaktuar vonesa dhe ndryshime në rrugët tregtare. Shkalla e ndikimit u përcaktua nga pozicioni i kanalit në arkitekturën globale, jo nga origjina e ndërprerjes. Infrastruktura nënujore shfaq dinamikë të lidhur: rasti i Eagle S nxori në pah vështirësinë e qasjeve ligjore për të përcaktuar në kohë juridiksionin dhe përgjegjësinë.<sup>15</sup> E njëjta sfidë vërehet te kabllot nënujore të Adriatikut, ku përgjegjësitë ndahen ndërmjet autoriteteve civile, detare dhe të mbrojtjes, ndërsa procedurat për aktivizimin e FA-së mund të qartësohen më tej. Këto kërcënime ndërthurin cenueshmërinë teknike me paqartësinë strategjike, ndërsa infrastruktura kritike dhe qeverisja mbeten të fragmentuara.

Sistemet energjetike shfaqin të njëjtën logjikë: ndërprerja e flukseve të gazit e lidhur me luftën në Ukrainë tregoi se si një goditje sektoriale transmetohet gjerësisht<sup>16</sup> – dinamikë që në Shqipëri merr formë specifike, pasi varësia pothuajse e plotë nga hidroenergja e bën sektorin të cenueshëm jo vetëm ndaj thatësisirës, por ndaj çdo ndërprerjeje paralele në tregjet rajonale prej të cilave vendi plotëson mangësitë sezonale.

Digjitalizimi i thellon më tej ndërvarësitë: qendrat e të dhënave dhe sistemet e IA-së rrisin varësinë nga energjia dhe rrjetet e transmetimit. Sulmet me dronë ndaj infrastrukturës *cloud* në Lindjen e Mesme tregojnë se qendrat e të dhënave konsiderohen tashmë pjesë e shtyllës operacionale civile dhe ushtarake. Sulmi kibernetik i korrikut 2022 ndaj Shqipërisë ilustron të njëjtën zbehje kufijsh: një ndërprerje e nisur si incident digjital u përhap shpejt drejt funksionimit bazë të shtetit, duke kërkuar reagim që tejkalonte kapacitetet e vetë sektorit kibernetik.<sup>17</sup>

Në tërësi, këto raste konfirmojnë se krizat zakonisht fillojnë në pika të caktuara kritike – nyje detare, rrjete komunikimi, korridore energjetike ose infrastruktura të tjera strategjike – por pasojat e tyre përhapen përtej sektorit fillestar duke prekur funksione të tjera kombëtare. Mekanizmat e reagimit, të ndërtuar kryesisht mbi ndarje sektoriale, juridiksionale dhe institucionale, nuk janë gjithmonë të përshtatur me natyrën ndërsektoriale të këtyre krizave. Hendeku kryesor nuk qëndron më në mungesën e njohurive mbi rreziqet, por në aftësinë për ta shndërruar këtë njohuri në veprim të koordinuar përpara se efektet zinxhir të cenojnë funksionet kritike të shtetit.

<sup>15</sup> Wilbur, C. (2026). *Dragging Anchor, Dodging Jurisdiction: Rethinking Deterrence for Hybrid Maritime Threats*. Small Wars Journal.

<sup>16</sup> International Energy Agency. (2024). *World energy outlook 2024*. <https://www.iea.org/reports/world-energy-outlook-2024>

<sup>17</sup> Raporti i plotë i sulmit kibernetik të 15 korrikut 2022 | PDF

### III. Analiza diagnostikuese: Pse qëndrueshmëria dështon nën stresin sistematik

Rastet e mësipërme evidentojnë një prirje që shkon përtej kompleksitetit të ndërprerjeve individuale: megjithëse sistemet kanë përmirësuar ndjeshëm aftësinë për të identifikuar dhe vlerësuar rreziqet e mundshme, strukturat vendimmarrëse jo gjithmonë janë të përshtatura me shpejtësinë, shkallën dhe natyrën ndërsektoriale të krizave moderne. Kjo çështje ka rëndësi të veçantë edhe për Shqipërinë, ku kapacitetet e parashikimit dhe monitorimit janë zhvilluar, por sfida mbetet shndërrimi i këtij informacioni në koordinim dhe aktivizim efektiv institucional, veçanërisht në mbështetje të rolit të Forcave të Armatosura. Kjo pjesë analizon tre mekanizma kryesorë që ndikojnë në hendekun ndërmjet paralajmërimit dhe veprimit të koordinuar.

#### 1. Iluzioni i gatishmërisë

Gjatë dy dekadave të fundit, qeveritë dhe organizatat ndërkombëtare kanë zgjeruar ndjeshëm kapacitetet për të parashikuar ndërprerjet përmes analizës perspektive, vlerësimit të rrezikut dhe sistemeve të paralajmërimit të hershëm. Rreziqet klimatike, kërcënimet kibernetike dhe tensionet gjeopolitike jo vetëm monitorohen, por vlerësohen në mënyrë të përsëritur brenda kuadrove institucionale. Problemi qëndron në atë që ndodh më pas: institucionet kanë përmirësuar kapacitetet e vlerësimit të rrezikut, por këto procese shpesh mbeten të shkëputura nga mekanizmat e zbatimit.<sup>18</sup> Studimet mbi qeverisjen e orientuar nga e ardhmja, konfirmojnë se institucioneve u mungojnë rrugët për ta shndërruar parashikimin në veprim të koordinuar,<sup>19</sup> ndërsa UNDRR<sup>20</sup> ka dokumentuar se informacioni mbi rrezikun nuk çon automatikisht në reduktimin e tij, kur sistemet institucionale nuk janë organizuar për të identifikuar, përgatitur dhe vepruar paraprakisht ndaj rreziqeve. Parashikimi rrit dukshmërinë e rrezikut; dukshmëria, në vetvete, nuk prodhon veprim.

Kushtet e thatësirës në Panama u parashikuan kohë përpara krizës, megjithatë vendimet mbetën në duart e operatorëve individualë. Ndërprerja e qarkullimit të cisternave përmes Ngushticës së Hormuzit u zhvillua gjithashtu në një kontekst ku rreziku rajonal ishte i njohur dhe i dokumentuar prej kohësh.

<sup>18</sup> Casajus Valles, A., Marin Ferrer, M., Poljanšek, K., & Clark, I. (Eds.). (2020). *Science for disaster risk management 2020: Acting today, protecting tomorrow*. Publications Office of the European Union. <https://doi.org/10.2760/438998>

<sup>19</sup> Organisation for Economic Co-operation and Development. (2020). *Anticipatory innovation governance: Shaping the future through proactive policy making*. OECD Observatory of Public Sector Innovation.

<sup>20</sup> United Nations Office for Disaster Risk Reduction. (2022). *Global Assessment Report on Disaster Risk Reduction 2022: Our World at Risk*. UNDRR. [https://digitallibrary.un.org/record/3969846/files/GAR2022\\_EN.pdf](https://digitallibrary.un.org/record/3969846/files/GAR2022_EN.pdf)

Megjithatë, reagimi kërkoi një koordinim emergjent që mekanizmat ekzistues të qeverisjes nuk ishin të organizuar për ta siguruar me shpejtësinë e kërkuar. Në të dyja rastet, u dëshmuar se përgatitja ishte e paplotë: sistemet dispononin informacion dhe plane, por nuk kishin kapacitetin për të vepruar në mënyrë të koordinuar në momentin kur kjo ishte më e nevojshme. I njëjti “iluzion gatishmërie” gjendet te sulmi kibernetik i korrikut 2022 kundër Shqipërisë: rreziku ishte njohur më parë në terma të përgjithshëm, por mungesa e një procedure aktivizimi të përcaktuar qartë vonoi kalimin nga identifikimi te reagimi i koordinuar.

## 2. Vështirësitë e vendimmarrjes nën stres

Kur paralajmërimi dhe parashikimi nuk përkthehen në veprim të koordinuar, pengesa shpesh nuk qëndron te mungesa e strukturave institucionale, por te vështirësitë e procesit vendimmarrës nën kushte pasigurie dhe presioni. Kërkimet mbi vendimmarrjen në pasiguri tregojnë se kufizimet njohëse dhe organizative ndikojnë në zgjedhje më shumë sesa vlerësimi racional, veçanërisht kur presioni kohor kombinohet me informacion të paplotë.<sup>21</sup> Racionaliteti i kufizuar i Simon<sup>22</sup> përshkruan pikërisht këtë: aktorët veprojnë mbi bazën e informacionit dhe kapaciteteve të kufizuara për ta përpunuar.

Raste si dëmtimi i kabllove në Baltik dhe reduktimi i kapacitetit të Kanalit të Panamasë tregojnë se paqartësitë mbi juridiksionin dhe koordinimin mund të ndikojnë në shpejtësinë e reagimit. Një sfidë e ngjashme mund të vërehet edhe në Shqipëri, ku përfshirja e FA-së në skenarë hibridë kërkon koordinim të ngushtë ndërinstitutional dhe procedura të mirëpërcaktuara. Strukturat organizative mund të filtrojnë ose dobësojnë sistematikisht sinjalet e hershme përpara se ato të arrijnë te vendimmarrësit – efekt që në kontekstet hibride përforcon më tej kufizimet vendimmarrëse.<sup>23</sup>

Në kontekstet e ndërprerjeve hibride, ku kërcënimet veprojnë pikërisht përmes paqartësisë dhe vonësës, ky efekt filtrues thellon më tej kufizimet vendimmarrëse të përshkruara më sipër. Analizat praktike të mjediseve bashkëkohore të sigurisë kanë evidentuar një fenomen të lidhur, të përshkruar përmes konceptit të “cenueshmërisë paraprake njohëse” (*cognitive pre-fracture*): akumulimin gradual të dobësimit të legjitimitetit, fragmentimit të narrativave dhe mbingarkesës institucionale, të cilat ndikojnë në aftësinë e

<sup>21</sup> Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux. Boin, R. A., & ‘t Hart, P. (2010). *Organising for effective emergency management: Lessons from research*. *Australian Journal of Public Administration*, 69(4), 357–371.

<sup>22</sup> Simon, H. A. (1955). *A behavioral model of rational choice*. *The Quarterly Journal of Economics*, 69(1), 99–118. <https://doi.org/10.2307/1884852>

<sup>23</sup> Boin, A., ‘t Hart, P., Stern, E., & Sundelius, B. (2005). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.

një sistemi për të reaguar përpara se paqëndrueshmëria të bëhet e dukshme.<sup>24</sup> Të marra së bashku, këto dinamika krijojnë atë që ky punim e përkufizon si “vështirësitë në procesin e vendimmarrjes” (*decision friction*): një gjendje në të cilën aftësia për të vepruar ngadalësohet ose fragmentohet, pavarësisht ekzistencës së paralajmërimit të hershëm.

### 3. *Fragmentimi institucional*

Nëse ‘vështirësia në procesin e vendimmarrjes’ shpjegon pse aktorët individualë hasin vështirësi, struktura institucionale përcakton nëse kjo vështirësi mund të kapërcehet kolektivisht – dhe në praktikë kjo ndodh rrallë. Qasjet e qëndrueshmërisë funksionojnë përmes organizimeve të fragmentuara, ku përgjegjësitë shpërndahen mes sektorëve dhe juridiksioneve që nuk janë projektuar të veprojnë bashkërisht.

Ky fragmentim shfaqet gjerësisht: Qasja e Reagimit të Integruar Politik të BE-së (IPCR) varet nga harmonizimi vullnetar mes shteteve anëtare; kërkesat bazë të qëndrueshmërisë së NATO-s zbatohen në mënyrë të pabarabartë – Shqipëria vetë ilustron këtë pabarazi, siç e evidenton EARI 2025 në rezistencën ndaj goditjeve. Në Hemisferën Perëndimore, qasjet e OAS/CICTE dhe vlerësimet e BID evidentojnë boshllëqe të ngjashme koordinimi.<sup>25</sup> Modeli strukturor mbetet i njëjtë: ekzistojnë qasje me pritshmëri të përbashkëta, por efektiviteti operacional varet nga harmonizimi vullnetar, i cili dobësohet pikërisht kur stresi arrin nivelin më të lartë. Në Shqipëri, kjo varësi shfaqet në bashkëpunimin ndërmjet institucioneve dhe strukturave të ndryshme shtetërore, të cilat veprojnë mbi bazën e kuadrove të tyre ligjore dhe institucionale, ndërsa mekanizmat e koordinimit dhe aktivizimit ndërsektorial mund të harmonizohen më tej.

Siç thekson Susan Strange,<sup>26</sup> pushteti në sistemet globale është i strukturuar dhe jo i shpërndarë në mënyrë të barabartë, duke ndikuar cenueshmërinë dhe kapacitetin për reagim. Në infrastrukturat kritike, kjo vështirësi përforcohet nga mbivendosja e juridiksioneve, siç dëshmoi rasti i Eagle S<sup>27</sup> – dhe siç do ta

<sup>24</sup> Brad, N. 2026. *Cognitive prefracture: Early indicators of domestic instability in hybrid conflict*. LinkedIn article March 23.

<sup>25</sup> Organization of American States, Inter-American Committee against Terrorism (CICTE). (2018). *Critical infrastructure protection in Latin America and the Caribbean 2018*. Fisher, M. K., & Gamper, C. (2017). Policy evaluation framework on the governance of critical infrastructure resilience in Latin America. Inter-American Development Bank.

<sup>26</sup> Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge University Press.

<sup>27</sup> Wilbur, C. (2026). *Dragging Anchor, Dodging Jurisdiction: Rethinking Deterrence for Hybrid Maritime Threats*. Small Wars Journal. <https://smallwarsjournal.com/2026/04/02/dragging-anchor-dodging-jurisdiction>

gjente veten Shqipëria nëse do të ndodhte një incident i ngjashëm në kabllo të Adriatikut.

Rezultati është një model qëndrueshmërie që nuk është plotësisht i përshtatur me natyrën e sistemeve komplekse që synon të mbrojë. Fragmentimi institucional nuk sjell vetëm vonesa në koordinim, por ndikon edhe në cilësinë e reagimit, duke prodhuar ndërhyrje të pjesshme dhe jo gjithmonë të sinkronizuara në fusha që janë të ndërlidhura. Edhe kur rreziku është i identifikuar, ai nuk përkthehet domosdoshmërisht në veprim të përbashkët, nëse institucionet nuk disponojnë mekanizma për të vepruar përtej kufijve tradicionalë sektorialë. Për këtë arsye, sfida strategjike për Shqipërinë nuk është vetëm rritja e aftësisë për të parashikuar krizat, por ndërtimi i një arkitekture kombëtare që mundëson veprim të koordinuar ndërmjet FA-ve, institucioneve civile dhe operatorëve të infrastrukturës kritike.

#### **IV. Kontributi teorik: Rikonceptimi i qëndrueshmërisë si funksion i integruar**

Analiza e mësipërme evidenton një çështje themelore: mospërputhjen strukturore ndërmjet mënyrës se si konceptohet qëndrueshmëria dhe mënyrës se si shfaqen dhe përhapen ndërprerjet në praktikë. Qasjet ekzistuese trajtojnë qëndrueshmërinë si mbrojtje dhe rikuperim të komponentëve individualë, duke supozuar se stabiliteti ruhet duke forcuar pjesët. Megjithatë, ndërprerjet nuk veprojnë brenda këtyre kufijve; përhapen përmes lidhjeve, ku ndikimi përcaktohet nga mënyra se si sistemet ndërveprojnë nën presion. Kjo mbështetet në mendimin sistematik (systems thinking): sjellja e sistemeve të ndërlidhura shpjegohet përmes marrëdhënieve dhe konfigurimeve strukturore, jo vetëm komponentëve individualë.<sup>28</sup> Cenueshmëria dhe qëndrueshmëria janë, në këtë kuptim, veti që varen jo vetëm nga kapacitetet individuale të institucioneve, por edhe nga cilësia e bashkëpunimit dhe koordinimit ndërmjet tyre. Për Shqipërinë, kjo nënkupton se forcimi i kapaciteteve institucionale duhet të shoqërohet me qartësimin dhe konsolidimin e mekanizmave të koordinimit ndërinstitutional.

Koncepti i kapacitetit adaptues<sup>29</sup> dhe ai i qëndrueshmërisë sistematike<sup>30</sup> përqendrohen në vetitë e brendshme të sistemeve, jo në qeverisjen e ndërveprimeve gjatë stresit. Arkitektura e cenueshmërisë e zgjeron këtë fokus:

<sup>28</sup> Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.

<sup>29</sup> Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). *Resilience, adaptability and transformability in social-ecological systems*. *Ecology and Society*, 9(2), 5. <https://www.ecologyandsociety.org/vol9/iss2/art5/>

<sup>30</sup> Folke, C. (2006). *Resilience: The emergence of a perspective for social ecological systems analyses*. *Global Environmental Change*, 16(3), 253–267.

problemi kryesor është nëse marrëdhëniet mes sistemeve mund të qeverisen kur ndërprerja kalon njëkohësisht kufijtë e tyre.

Qëndrueshmëria në kushtet e stresit sistemik nënkupton aftësinë e sistemeve të ndërlidhura për të parashikuar, përballuar dhe përshtatur ndaj ndërprerjeve dhe efekteve të tyre zinxhir. Kjo e zhvendos fokusin nga rezistenca e sektorëve të veçantë të ruajtja e funksionalitetit dhe koordinimi ndërmjet tyre, duke e parë qëndrueshmërinë si një funksion të integruar. Në këtë kuptim, edhe FA-të vlerësohen jo vetëm për kapacitetet e tyre operacionale, por edhe për aftësinë për të bashkëpunuar dhe ndërvepruar në mënyrë efektive me strukturat civile.

Specializimi sektorial mbetet i domosdoshëm për shkak të ekspertizës dhe përgjegjësi të përcaktuara. Megjithatë, përballimi i ndërprerjeve që tejkalojnë kufijtë sektorialë kërkon edhe mekanizma efektivë koordinimi ndërinstytucional. Në rastin shqiptar, kjo nënvizon rëndësinë e forcimit të bashkëpunimit ndërmjet institucioneve për të siguruar një reagim të integruar ndaj krizave komplekse.

Kontributi i kësaj analize qëndron në një mënyrë të re të konceptimit të rreziqeve ekzistuese dhe të mënyrës se si ato duhet të menaxhohen në një mjedis të karakterizuar nga ndërvarësia. Rëndësia e këtij rikonceptimi nuk lidhet vetëm me aspektin teorik, por veçanërisht me pasojat që sjell për qeverisjen e sigurisë, përfshirë FA-të, koordinimin institucional dhe ndërtimin e qëndrueshmërisë kombëtare, çështje që trajtohen në pjesën vijuese.

## **V. Implikimet për politikat: Ndërtimi i qëndrueshmërisë në një mjedis të paqëndrueshmërisë së vazhdueshme**

Rikonceptimi i paraqitur më sipër ka implikime të drejtpërdrejta për mënyrën se si Shqipëria duhet të ndërtojë dhe të zbatojë qëndrueshmërinë kombëtare. Nëse krizat bashkëkohore përhapen përmes ndërvarësive ndërmjet energjisë, teknologjisë, infrastrukturës dhe sigurisë, atëherë edhe mekanizmat e reagimit duhet të mbështeten në një logjikë të ngjashme të integruar. Kjo nënkupton një zhvendosje nga ndërhyrjet e veçuara institucionale drejt një qasjeje më të koordinuar, në të cilën FA-të, institucionet civile dhe operatorët e infrastrukturës kritike mund të veprojnë në mënyrë të bashkërenduar në kushtet e stresit sistemik.

### **1. Implikimet strategjike**

Trajtimi i qëndrueshmërisë si funksion i integruar ndryshon mënyrën se si organizohen siguria dhe qeverisja: sfida zhvendoset nga mbrojtja e sektorëve individualë drejt menaxhimit të ndërveprimeve. Kjo nënkupton një riorientim nga forcimi i kapaciteteve të veçuara drejt harmonizimit dhe koordinimit ndërinstytucional. Sfidat në koordinim lidhen shpesh me dallimet në përgjegjësi dhe kompetenca, çka evidenton nevojën për mekanizma më të

qartë bashkëpunimi dhe aktivizimi institucional.

Në fushën e sigurisë, kjo nënkupton kalimin nga kontrolli i kërcënimeve drejt menaxhimit të ndërprerjeve, pasi kërcënimet bashkëkohore synojnë ndërvarësitë që lidhin sistemet – logjikë që vlen njësoj për Portin e Durrësit, kabllot e Adriatikut dhe varësinë hidroenergetike, të cilat FA-të dhe institucionet civile duhet t'i trajtojnë si nyje të një rrjeti të vetëm. Siç theksojnë Farrell dhe Newman<sup>31</sup>, ndërvarësia krijon njëkohësisht avantazh strategjik dhe ekspozim sistemik. Kriticiteti i infrastrukturës duhet kuptuar si funksion i pozicionit të saj brenda sistemeve më të gjera – ashtu si Kanali i Panamasë, edhe kriticiteti i Portit të Durrësit nuk buron nga volumi tregtar, por nga roli i tij i dyfishtë civil-ushtarak brenda Korridorit VIII.

## 2. Orientimi i politikave

Nga analiza evidentohen tri drejtime kryesore orientimi:

*Së pari*, kërkohet që sistemet e paralajmërimit të hershëm të lidhen drejtpërdrejt me mekanizmat e zbatimit dhe reagimit institucional. Hendeku i evidentuar gjatë gjithë këtij punimi është i natyrës operacionale: sinjalet e rrezikut ekzistojnë, por ato jo gjithmonë arrijnë të aktivizojnë reagime të koordinuara. Në terma konkretë, kjo nënkupton integrimin e sistemeve të paralajmërimit të hershëm në proceset vendimmarrëse, në mënyrë që ato të mund të aktivizojnë paraprakisht reagime të përcaktuara ndërsektoriale përpara se një ndërprerje të përshkallëzohet në krizë më të gjerë. Mekanizmi i Integruar i Reagimit Politik ndaj Krizave i Bashkimit Evropian (*EU Integrated Political Crisis Response – IPCR*) përfaqëson një përpyqje për krijimin e një arkitekture të tillë aktivizimi, duke lidhur sinjalet e rrezikut me koordinimin politik ndërmjet shteteve anëtare. Kufizimet e tij, përfshirë varësinë nga harmonizimi vullnetar i veprimeve dhe ndryshimet në kapacitetet kombëtare, tregojnë pikërisht elementet që duhet të adresojë një version më i fuqishëm operacional i këtij mekanizmi.<sup>32</sup>

Për Shqipërinë, ky parim nënkupton nevojën që sistemet e monitorimit dhe vlerësimit të rreziqeve të lidhen më qartë me procedurat e aktivizimit institucional, duke përfshirë edhe rolin e FA-ve në skenarë ku një kërcënim prek njëkohësisht fusha të ndryshme si mbrojtja, infrastruktura kritike, energjia, komunikimet dhe siguria kibernetike.

*Së dyti*, kërkohet kalimi nga shkëmbimi i informacionit drejt harmonizimit

<sup>31</sup> Farrell, H., & Newman, A. L. (2019). *Weaponized interdependence: How global economic networks shape state coercion*. *International Security*, 44(1), 42–79. <https://doi.org/10.1162/isec-a-00351>

<sup>32</sup> Council of the European Union. (2024). *The integrated political crisis response (IPCR)*. <https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/>

operacional të veprimeve. Njohja se një ndërprerje ka natyrë ndërsektoriale nuk është e njëjtë me aftësinë për t'iu përgjigjur asaj në mënyrë kolektive. Harmonizimi operacional kërkon protokolle të ndërveprueshme për menaxhimin e krizave, pragje të përbashkëta për aktivizimin e veprimeve dhe struktura koordinimi që funksionojnë në kushtet e stresit, në vend që të krijohen vetëm në mënyrë ad-hoc gjatë krizës. Kërkesat bazë të NATO-s për qëndrueshmërinë kombëtare (*Baseline Requirements for National Resilience*) përcaktojnë pritshmëri të përbashkëta për fusha si energjia, transporti, telekomunikacioni dhe vazhdimësia e qeverisjes, duke treguar njëkohësisht vlerën e standardeve të përbashkëta dhe sfidën e vazhdueshme të zbatimit të pabarabartë të tyre ndërmjet vendeve anëtare.

Për Shqipërinë, kjo nënkupton se sfida nuk qëndron vetëm në shkëmbimin e informacionit ndërmjet institucioneve përgjegjëse, por në krijimin e mekanizmave që mundësojnë veprim të sinkronizuar në kohë krize. Përfshirja e FA-ve në këtë arkitekturë kërkon procedura të qarta koordinimi civil-ushtarak, ushtrime të përbashkëta dhe skenarë operacionalë ku kërcënimet hibride, ndërprerjet e infrastrukturës kritike dhe emergjencat komplekse trajtohen si fenomene të ndërlidhura.

*Së treti*, kërkohet riorganizimi i strukturave institucionale mbi bazën e ndërvarësive dhe jo vetëm sipas kufijve tradicionalë sektorialë. Kjo nuk nënkupton centralizimin e kontrollit, por organizimin e kapaciteteve të reagimit rreth marrëdhënieve dhe ndërveprimeve ndërmjet sistemeve, në vend që ato të trajtohen të izoluar brenda sektorëve të veçantë.

Kjo mund të realizohet përmes ushtrimeve të përbashkëta, të cilat analizojnë mënyrën se si një ndërprerje përhapet përmes infrastrukturave të ndërlidhura; përmes planifikimit të integruar të masave të emergjencës, ku përfshihen njëkohësisht aktorë nga energjia, logjistika, teknologjia digjitale dhe sistemet financiare; si dhe përmes mekanizmave të qeverisjes që bëjnë të dukshme varësitë e përbashkëta, në vend që të supozojnë se çdo sektor mund të menaxhojë rreziqet e veta në mënyrë të pavarur.

Direktiva e Bashkimit Evropian për Qëndrueshmërinë e Subjekteve Kritike (*Critical Entities Resilience Directive*) e vitit 2022 përfaqëson një hap në këtë drejtim, duke vendosur detyrime ndërsektoriale për operatorët e infrastrukturës kritike në shtetet anëtare. Megjithatë, përvoja e zbatimit të saj tregon gjithashtu vështirësinë e përkthimit të kërkesave strukturore në kapacitete të koordinuara operationale, veçanërisht kur objektivat, afatet dhe interesat e aktorëve të ndryshëm nuk përputhen plotësisht.

Në rastin e Shqipërisë, kjo qasje nënkupton nevojën për të kaluar nga një menaxhim kryesisht sektorial i rreziqeve drejt një vlerësimi të ndërvarësive kritike kombëtare. Një hartë kombëtare e lidhjeve ndërmjet energjisë,

transportit, komunikimeve, sistemeve digjitale dhe mbrojtjes do të mundësonte identifikimin e pikave ku një ndërprerje mund të prodhojë efekte zinxhir.

## Përfundime

Analiza e zhvilluar në këtë punim tregon se sfida kryesore e qëndrueshmërisë kombëtare nuk qëndron më në mungesën e aftësisë për të identifikuar dhe parashikuar rreziqet, por në pamundësinë për ta shndërruar këtë njohuri në veprim të shpejtë, të integruar dhe të koordinuar. Rastet e analizuara, nga nyjet kritike detare dhe infrastruktura nënujore, te sistemet energjetike dhe infrastruktura digjitale, dëshmojnë se ndërprerjet nuk respektojnë kufijtë sektorialë dhe institucionalë brenda të cilëve janë organizuar mekanizmat tradicionalë të qëndrueshmërisë. Një goditje e kufizuar në një nyje kritike mund të gjenerojë efekte zinxhir në sisteme të tjera, duke e shndërruar një incident sektorial në një problem të funksionimit të të gjithë sistemit kombëtar. Për këtë arsye, cenueshmëria nuk duhet kuptuar vetëm si ekspozim ndaj një kërcënimi, por si rezultat i mënyrës se si janë konfiguruar dhe ndërveprojnë sistemet, institucionet dhe infrastruktura kritike.

Në këtë kuadër, punimi argumenton se “arkitektura e cenueshmërisë” përbën një mënyrë më të përshtatshme për të kuptuar se si rreziku përhapet dhe amplifikohet në sisteme të ndërlidhura. Kjo qasje e zhvendos analizën nga pyetja se *ku dhe nga vjen kërcënimi* drejt pyetjes se *përmes cilave ndërvarësi ai përhapet dhe cilat struktura e amplifikojnë ndikimin e tij*. Për Shqipërinë, kjo është veçanërisht e rëndësishme, pasi varësia e lartë energjetike nga hidroenergja, pozicioni strategjik i Portit të Durrësit, lidhjet nënujore të komunikimit dhe varësia nga infrastruktura digjitale krijojnë pika ku një ndërprerje mund të tejkalojë shpejt kufijtë e sektorit fillestar. Në këtë perspektivë, qëndrueshmëria nuk mund të vlerësohet vetëm mbi bazën e forcës së institucioneve apo sektorëve individualë, por mbi aftësinë e sistemit për të ruajtur funksionet kritike ndërsa goditjet përhapen përmes ndërvarësive.

Një përfundim i dytë lidhet me hendekun midis parashikimit dhe veprimit. Analiza tregon se ekzistenca e sistemeve të paralajmërimit të hershëm, vlerësimeve të rrezikut dhe institucioneve të specializuara nuk garanton vetvetiu gatishmëri reale. Ajo që përcakton efektivitetin e qëndrueshmërisë është aftësia për ta lidhur informacionin e hershëm me vendimmarrjen, aktivizimin dhe veprimin operacional. Në kushtet e stresit sistematik, ky hendek zgjerohet nga pasiguria, presioni kohor dhe fragmentimi i përgjegjësisë. Prandaj, problemi i qëndrueshmërisë nuk është thjesht një problem informacioni, por një problem i qeverisjes së veprimit.

Për Shqipërinë, analiza eidenton se sfida kryesore nuk lidhet domosdoshmërisht me mungesën e institucioneve apo kapaciteteve sektoriale, por me nevojën për një arkitekturë më të integruar koordinimi për krizat që

tejkalojnë kufijtë e një sektori. Sulmi kibernetik i vitit 2022, ndërvarësia energjetike dhe rëndësia e infrastrukturës detare e nënujore tregojnë se krizat e ardhshme mund të kërkojnë reagim të koordinuar në disa fusha njëkohësisht. Prandaj, forcimi i kapaciteteve institucionale duhet të shoqërohet me procedura të qarta për aktivizimin dhe koordinimin e tyre në një situatë të përbashkët krize.

Një implikim i rëndësishëm i kësaj gjetjeje lidhet me rolin e Forcave të Armatosura të Republikës së Shqipërisë në arkitekturën kombëtare të qëndrueshmërisë. Në një mjedis sigurie ku kërcënimet hibride dhe ndërprerjet e infrastrukturës kritike mund të prekin njëkohësisht dimensionet civile dhe të sigurisë, roli i FA-ve duhet të integrohet më qartë në mekanizmat kombëtarë të reagimit. Kjo nënkupton forcimin e koordinimit civil-ushtarak, qartësimin e procedurave të aktivizimit dhe zhvillimin e ushtrimeve të përbashkëta, me synim rritjen e ndërveprueshmërisë dhe efektivitetit të reagimit kombëtar.

Kontributi kryesor i punimit është rikonceptimi i qëndrueshmërisë nga një karakteristikë e sektorëve individualë në një funksion sistemik të marrëdhënieve ndërmjet tyre. Një sistem nuk është i qëndrueshëm vetëm sepse institucionet e tij janë të forta veçmas; ai është i qëndrueshëm kur këto institucione mund të veprojnë së bashku, me shpejtësinë dhe shkallën e kërkuar, kur një ndërprerje përhapet përtej kufijve të tyre funksionalë. Kjo e zhvendos vëmendjen nga mbrojtja e pjesëve drejt qeverisjes së ndërvarësive dhe nga parashikimi i rrezikut drejt aktivizimit të veprimit.

Prandaj, për Shqipërinë, kalimi nga parashikimi drejt veprimit kërkon një ndryshim në mënyrën se si konceptohet dhe ndërtohet qëndrueshmëria kombëtare: nga menaxhimi i krizave sipas sektorëve drejt një arkitekture të integruar që identifikon ndërvarësitë kritike, përcakton pragjet e aktivizimit, harmonizon përgjegjësitë dhe mundëson veprim të sinkronizuar ndërmjet institucioneve civile, operatorëve të infrastrukturës kritike dhe FA-ve. Nëse krizat e së ardhmes do të përhapen përmes lidhjeve që bashkojnë sistemet, atëherë edhe qëndrueshmëria duhet të ndërtohet pikërisht mbi këto lidhje. Në fund të fundit, sfida strategjike për Shqipërinë nuk është më vetëm të dijë se çfarë mund të ndodhë, por të sigurojë që, kur ajo të ndodhë, institucionet të dinë kur të aktivizohen, kush duhet të veprojë, me kë duhet të koordinohet dhe si të ruhet funksionimi i shtetit përtej kufijve sektorialë.

## Bibliografia

1. AKSK. (2025). Strategjia Kombëtare për Sigurinë Kibernetike 2025–2030 dhe Plani i Veprimit 2025–2027.
2. Autoridad del Canal de Panamá. (2023). *De los llenados cruzados a las soluciones de largo plazo: Cómo administra el Canal de Panamá la escasez del agua*. <https://pancanal.com/como-administra-el-canal-de-panama-la-escasez-del-agua/>
3. Biddle, S. (2026, March 20). Data centers are military targets now. *The Intercept*. <https://theintercept.com/2026/03/20/ai-data-centers-military-targets-iran-war/>
4. Boin, A., & 't Hart, P. (2010). Organising for effective emergency management: Lessons from research. *Australian Journal of Public Administration*, 69(4), 357–371. <https://doi.org/10.1111/j.1467-8500.2010.00694.x>
5. Brad, N. (2026, March 23). Cognitive pre-fracture: Early indicators of domestic instability in hybrid conflict. *LinkedIn*. <https://www.linkedin.com/pulse/cognitive-pre-fracture-early-indicators-domestic-lyxpf/>
6. Carrière-Swallow, Y., Deb, P., Furceri, D., Jiménez, D., & Ostry, J. D. (2022). *Shipping costs and inflation* (IMF Working Paper No. WP/22/61). International Monetary Fund. <https://www.imf.org/-/media/files/publications/wp/2022/english/wpica2022061-print.pdf.pdf>
7. Council of the European Union. (2024). *The integrated political crisis response (IPCR)*. <https://www.consilium.europa.eu/en/policies/ipcr-response-to-crises/>
8. Enhanced Analytic Resilience Index (EARI). (2025). *EARI 2025*. Centrul Euro-Atlantic pentru Reziliență (E-ARC). <https://e-arc.ro/wp-content/uploads/2025/10/EARI2025.pdf>
9. European Commission. (2022). *Directive (EU) 2022/2557 on the resilience of critical entities*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557>
10. Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. [https://doi.org/10.1162/isec\\_a\\_00351](https://doi.org/10.1162/isec_a_00351)
11. Fisher, M. K., & Gamper, C. (2017). *Policy evaluation framework on the governance of critical infrastructure resilience in Latin America*. Inter-American Development Bank. <https://doi.org/10.18235/0000819>
12. Ghosal, A., & Olingo, A. (2026, March 30). The war in Iran sparks a global fertilizer shortage and threatens food prices. *AP News*. <https://>

- apnews.com/article/iran-war-fertilizer-exports-farming
13. Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, 497, 51–59. <https://doi.org/10.1038/nature12047>
  14. International Energy Agency. (2024). *World energy outlook 2024*. <https://www.iea.org/reports/world-energy-outlook-2024>
  15. International Energy Agency. (2026). *Oil market report: May 2026*. <https://www.iea.org/reports/oil-market-report-may-2026>
  16. International Maritime Organization. (2025). *Reports on acts of piracy and armed robbery against ships: Annual report 2024* (MSC.4/Circ.269). [https://www.wcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.4-Circ.269\\_Annual%202024.pdf](https://www.wcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.4-Circ.269_Annual%202024.pdf)
  17. Ligji nr. 25/2024, “Për sigurinë kibernetike”.
  18. Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.
  19. Ministria e Infrastrukturës dhe Energjisë. (2022). *Sfidat e sigurisë kibernetike në Shqipëri*.
  20. Organisation for Economic Co-operation and Development. (2020). *Anticipatory innovation governance: Shaping the future through proactive policy making*. OECD Observatory of Public Sector Innovation.
  21. Organization of American States, Inter-American Committee against Terrorism (CICTE). (2018). *Critical infrastructure protection in Latin America and the Caribbean 2018*.
  22. Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1), 99–118. <https://doi.org/10.2307/1884852>
  23. Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge University Press.
  24. Tooze, A. (2022). *Shutdown: How Covid shook the world's economy*. Allen Lane.
  25. United Nations Conference on Trade and Development. (2023). *Trade and development report 2023: Growth, debt and climate*. [https://unctad.org/system/files/official-document/tdr2023\\_en.pdf](https://unctad.org/system/files/official-document/tdr2023_en.pdf)
  26. United Nations Conference on Trade and Development. (2024). *Navigating troubled waters: Impact to global trade of disruption of shipping routes in the Red Sea, Black Sea and Panama Canal*. [https://unctad.org/system/files/official-document/osginf2024d2\\_en.pdf](https://unctad.org/system/files/official-document/osginf2024d2_en.pdf)
  27. United Nations Office for Disaster Risk Reduction. (2022). *Global assessment report on disaster risk reduction 2022: Our world at risk*. [https://digitallibrary.un.org/record/3969846/files/GAR2022\\_EN.pdf](https://digitallibrary.un.org/record/3969846/files/GAR2022_EN.pdf)

28. van Soest, H., Black, J., Fine, H., & Retter, L. (2025). *Evolving threats to critical undersea infrastructure: Implications for European security and resilience*. RAND Europe. <https://www.rand.org/pubs/perspectives/PEA3800-1.html>
29. VKM nr. 364, datë 30.06.2025, për miratimin e listës së infrastrukturave kritike dhe të rëndësishme të informacionit.
30. Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society*, 9(2), 5. <https://www.ecologyandsociety.org/vol9/iss2/art5/>
31. Wilbur, C. (2026, April 2). Dragging anchor, dodging jurisdiction: Rethinking deterrence for hybrid maritime threats. *Small Wars Journal*. <https://smallwarsjournal.com/2026/04/02/dragging-anchor-dodging-jurisdiction>

## **RUBRIKA E DYTË**

### **INDUSTRIA E MBROJTJES DHE KAPACITETET OPERACIONALE**



# Parandalimi dhe mbrojtja në epokën digjitale: transformimi i FARSH nga burimet e mbrojtjes te kapacitetet operacionale

---

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

## Trajtesë e shkurtuar

*Mjedisi bashkëkohor i sigurisë po ndryshon nën ndikimin e konkurrencës strategjike, rikthimit të konflikteve me intensitet të lartë, kërcënimeve hibride e kibernetike dhe zhvillimit të shpejtë teknologjik. Inteligjenca artificiale, sistemet pa pilot dhe autonome, përpunimi i të dhënave dhe komunikimet e avancuara po ndryshojnë mënyrën se si forcat zbulojnë kërcënimin, marrin vendime, veprojnë dhe mbështeten. Për rrjedhojë, parandalimi dhe mbrojtja varen gjithnjë e më shumë nga integrimi i njerëzve, proceseve dhe teknologjisë në një sistem të gatshëm dhe të qëndrueshëm.*

*Studimi analizon implikimet e këtij transformimi për Forcat e Armatosura të Republikës së Shqipërisë, duke u përqendruar në katër shtylla të ndërruar: personelin, gatishmërinë, zhvillimin e kapaciteteve dhe qëndrueshmërinë e mbrojtjes.<sup>1</sup> Analiza mbështetet në dokumentet strategjike kombëtare, konceptet dhe drejtimit e NATO-s, si dhe në mësimet e konflikteve bashkëkohore.*

*Teza kryesore është se financimi, modernizimi dhe teknologjitë e reja prodhojnë efekt strategjik vetëm kur shndërrohen në personel të përgatitur, njësi të gatshme, kapacitete të integruara dhe aftësi për të vijuar operacionet. Për FARSH, sfida nuk është vetëm gjenerimi i burimeve, por kthimi dhe mbajtja e tyre në kapacitete reale për parandalim, mbrojtje dhe reagim, si dhe në kontribut të besueshëm për mbrojtjen kolektive.*

**Fjalë kyçe:** parandalim, mbrojtje, FARSH, personel, gatishmëri, zhvillim kapacitetesh, qëndrueshmëri, transformim digjital, inovacion.

---

<sup>1</sup> Vizioni i Shefit të Shtabit të Përgjithshëm të FARSH për periudhën 2026-2028.

## Hyrje

Mjedisi ku veprojnë sot forcat e armatosura është më kompleks, i ndërlikur dhe dinamik. Konflikti me intensitet të lartë është rikthyer si mundësi reale në hapësirën euroatlantike, ndërsa konkurrenca strategjike zhvillohet në dimensionin ushtarak, ekonomik, teknologjik, informativ dhe kibernetik. *Konfliktet nuk kufizohen më në një vijë fronti, por mund të përfshijnë infrastrukturën kritike, rrjetet e komunikimit, spektrin elektromagnetik, hapësirën kibernetike, zinxhirët e furnizimit dhe mjedisin informativ.*<sup>2</sup>

Paralelisht po ndryshojnë mjetet dhe mënyrat e përdorimit të fuqisë ushtarake. Inteligjenca artificiale, sistemet pa pilot e autonome, sensorët, komunikimet e avancuara dhe përpunimi i të dhënave po shkurtojnë ciklin nga zbulimi i kërcënimit të vendimi dhe efekti. Por digjitalizimi krijon edhe varësi: sa më e ndërlikur forca, aq më e rëndësishme bëhen mbrojtja e rrjeteve, siguria e të dhënave dhe aftësia për të vepruar në mjedis elektronik ose kibernetik të degraduar.<sup>3</sup>

Në këto kushte, parandalimi duhet kuptuar më gjerë se zotërimi i fuqisë për mbrojtje dhe reagim. Ai bëhet i besueshëm kur kundërshtari vlerëson se agresioni nuk do t'i arrijë objektivat ose se kostot do të tejkalojnë përfitimin. Kjo kërkon aftësi për të zbuluar në kohë, vendosur shpejt, mbrojtur sistemet, ruajtur komandim-kontrollin dhe vijuar operacionin nën presion. Gatishmëria dhe qëndrueshmëria bëhen kështu pjesë e vetë besueshmërisë së parandalimit. Ky ndryshim reflektohet në zhvillimet e NATO-s. Planet e mbrojtjes, Procesi i Planifikimit të Mbrojtjes, objektivat e kapaciteteve dhe kërkesat për gatishmëri po e zhvendosin fokusin nga ekzistenca formale e një kapaciteti të aftësia për ta gjeneruar dhe përdorur realisht. Njëkohësisht, *investimet në teknologji, industri, logjistikë dhe qëndrueshmëri po marrin peshë më të madhe në realizimin e planeve të mbrojtjes kolektive.*<sup>4</sup>

Për Shqipërinë, kjo qasje lidhet drejtpërdrejt me zhvillimin e FARSH. *Plani Afatgjatë i Zhvillimit të FARSH 2024–2033 e lidh zhvillimin e kapaciteteve me misionin kushtetues, detyrat kombëtare dhe detyrimet ndaj NATO-s, si dhe harmonizon planifikimin kombëtar me Procesin e Planifikimit të Mbrojtjes së*

<sup>2</sup> North Atlantic Treaty Organization, *NATO 2022 Strategic Concept* (Brussels: NATO, 2022), paras. 6–16.

<sup>3</sup> North Atlantic Treaty Organization, “Innovation and Technology Adoption,” updated July 8, 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies>.

<sup>4</sup> NATO “Deterrence and Defence,” updated June 25, 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence>; North Atlantic Treaty Organization, “NATO’s Role in Capability Development,” updated July 6, 2026

Aleancës.<sup>5</sup> Në këtë kuptim, modernizimi nuk është seri prokurimesh të veçuara. Një sistem i ri rrit potencialin, por bëhet kapacitet operacional vetëm kur lidhet me personelin, konceptin e përdorimit, doktrinën, stërvitjen, komandim-kontrollin, infrastrukturën, mirëmbajtjen dhe logjistikën. Integrimi i këtyre elementeve përcakton nëse investimi mbetet modernizim teknik apo prodhon rritje të qëndrueshme të fuqisë ushtarake.

Qëllimi i studimit është të analizojë si ndikojnë mjedisi i siguri, transformimi teknologjik dhe kërkesat e mbrojtjes kolektive në zhvillimin e FARSH, me fokus te personeli, gatishmëria, zhvillimi i kapaciteteve dhe qëndrueshmëria.

Teza është se sfida themelore e FARSH në epokën digjitale nuk qëndron vetëm në sigurimin e teknologjive dhe burimeve të reja, por në aftësinë për t'i shndërruar ato në kapacitete reale operacionale. Burimet janë kusht për fuqinë ushtarake, por fitojnë vlerë strategjike vetëm kur kthehen në personel të përgatitur, njësi të gatshme, sisteme të integruara dhe aftësi të qëndrueshme për parandalim, mbrojtje dhe reagim.

## **I. Parandalimi dhe mbrojtja në një mjedis sigurie të transformuar**

Ndryshimet teknologjike nuk e kanë ndryshuar natyrën e luftës si përplasje interesash dhe vullnetesh, por kanë ndryshuar shpejt karakterin e saj. Operacionet në tokë, ajër e det ndërthuren me hapësirën kibernetike, spektrin elektromagnetik, hapësirën kozmike dhe mjedisin informativ. Kjo e bën lidhjen ndërmjet informacionit, vendimmarrjes dhe veprimit një element qendror të fuqisë luftarake.

Në këtë mjedis, informacioni dhe koha marrin vlerë të drejtpërdrejtë operacionale. Forca që zbulon më herët, ndërton pamje më të saktë, vendos më shpejt dhe e përcjell vendimin në mënyrë të sigurt mund të krijojë avantazh edhe ndaj një kundërshtari me epërsi numerike. Vlera e platformës individuale varet gjithnjë e më shumë nga integrimi i saj në rrjetin e sensorëve, strukturave të komandimit dhe kapaciteteve të veprimit.

Sistemet pa pilot e ilustrjnë këtë ndryshim. Ato mund të përdoren për zbulim, mbikëqyrje, identifikim objektivash, korrigjim zjarri, vlerësim efekti dhe, sipas sistemit, goditje. Vlera e tyre përcaktohet nga lidhja e informacionit që prodhojnë me inteligjencën, komandim-kontrollin, sistemet e zjarrit dhe vendimmarrjen. Pa këtë lidhje, teknologjia mbetet kapacitet i pjesshëm, jo pjesë e një sistemi të integruar luftarak.

---

<sup>5</sup> Ministria e Mbrojtjes e Republikës së Shqipërisë, *Plani Afatgjatë i Zhvillimit të Forcave të Armatosura*

E njëjta logjikë vlen për inteligjencën artificiale. Ajo mund të ndihmojë në përpunimin e të dhënave, identifikimin e modeleve, analizën e situatës dhe optimizimin e logjistikës, por nuk zëvendëson gjykimin profesional. Sa më e lartë shpejtësia e përpunimit, aq më e rëndësishme bëhet aftësia e personelit për të vlerësuar besueshmërinë e të dhënave, kufizimet e algoritmeve dhe pasojat e vendimit. NATO e ka vendosur këtë transformim në qendër të ruajtjes së avantazhit teknologjik dhe ushtarak. Qasja ndaj inovacionit vlerëson se IA, dronët dhe sistemet autonome po riformojnë konfliktin dhe kapacitetet e nevojshme për parandalim e mbrojtje. Për këtë arsye, *teknologjia duhet identifikuar, testuar, siguruar dhe integruar me shpejtësinë që kërkon mjedisi operacional*.<sup>6</sup>

Për një forcë të përmasave të FARSH, teknologjia mund të rrisë ndërgjegjësimin për situatën, të shkurtojë reagimin, të përmirësojë mbrojtjen e forcës dhe të shtojë efektin e kapaciteteve ekzistuese. Megjithatë, ajo duhet përzgjedhur sipas nevojës operationale, jo vetëm risisë. Ndjekja e çdo zhvillimi të ri rrezikon të shpërndajë burimet dhe të krijojë sisteme pa koncept të qartë përdorimi.

Pika e nisjes duhet të jetë problemi operacional. Planifikimi duhet të përcaktojë fillimisht efektin e kërkuar, mjedisin e përdorimit, ndërveprimin me sistemet e tjera dhe kërkesat për personel, infrastrukturë e mbështetje. Kjo e zhvendos zhvillimin nga platforma te kapaciteti dhe e lidh modernizimin me gatishmërinë.

Kapaciteti ushtarak krijohet nga bashkëveprimi i elementeve: pajisja ofron mundësinë teknike; personeli e përdor; doktrina dhe procedurat përcaktojnë përdorimin; komandim-kontrolli e lidh me forcën; stërvitja ndërton aftësinë kolektive; mirëmbajtja dhe logjistika sigurojnë vijimësinë. Dobësia e një elementi ul vlerën e të gjithë kapacitetit. Në këtë kontekst, transformimi digjital duhet kuptuar si transformim i forcës, jo si projekt teknik. *Strategjia e Zbatimit të Transformimit Digjital të NATO-s e përkufizon atë si ndryshim të koordinuar të njerëzve, proceseve dhe teknologjisë, me synim infrastrukturë digjitale të sigurt, personel të përgatitur, procese të përshtatura, siguri kibernetike dhe ndërveprueshmëri*.<sup>7</sup>

Për FARSH, vlera e këtij koncepti qëndron te logjika e integritetit. Një sistem modern komandim-kontrolli nuk prodhon vetvetiu komandim më të mirë nëse proceset e shtabit nuk përshtaten; një sistem pa pilot nuk krijon avantazh nëse të dhënat nuk arrijnë në kohë; dhe teknologjia nuk rrit efektivitetin pa personel

<sup>6</sup> North Atlantic Treaty Organization, "Innovation and Technology Adoption," updated July 8, 2026.

<sup>7</sup> North Atlantic Treaty Organization, "NATO's Digital Transformation Implementation Strategy 2.0," May 26, 2026, paras. 6–24, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>.

të trajnuar për përdorim e mirëmbajtje. Transformimi bëhet real kur njerëzit, proceset dhe teknologjia zhvillohen së bashku.

Shpejtësia e përshtatjes po bëhet gjithashtu faktor i konkurrencës ushtarake. Në softuer, IA, sisteme pa pilot dhe teknologji kibernetike, cikli i inovacionit është më i shkurtër se ai tradicional i prokurimit. Për këtë arsye, *NATO synon të shkurtojë kohën nga identifikimi i nevojës te integrimi i zgjidhjes, përmes eksperimentimit, procedurave fleksibël dhe bashkëpunimit me furnizues tradicionalë e jo-traditionalë*.<sup>8</sup>

Në nivel kombëtar, ky parim kërkon lidhje më të drejtpërdrejtë ndërmjet njësisve operacionale, planifikimit, akademisë, kërkimit shkencor, inovacionit dhe industrisë. Problemi identifikohet nga përdoruesi; zgjidhja provohet në kushte të përafërta me operacionin; adoptimi vijon vetëm kur teknologjia demonstroi përmirësim të efektit, gatishmërisë ose mbrojtjes së forcës. Megjithatë, teknologjia dhe shpejtësia e përshtatjes nuk mjaftojnë. Një forcë më e digjitalizuar bëhet edhe më e varur nga energjia, rrjetet, navigimi, të dhënat dhe infrastruktura. Prandaj, transformimi teknologjik duhet të zhvillohet bashkë me mbrojtjen e këtyre elementeve dhe aftësinë për të vepruar kur ato degradohen.

Kjo marrëdhënie ndërmjet teknologjisë, gatishmërisë dhe qëndrueshmërisë lidh transformimin e karakterit të luftës me kërkesat që NATO u vendos forcave aleate.

## **II. Nga transformimi i NATO-s te kërkesat për zhvillimin e FARSH**

Transformimi i NATO-s e ka rikthyer mbrojtjen kolektive në qendër të planifikimit dhe ka rritur kërkesën për kapacitete të përdorshme në kohën që kërkojnë planet e Aleancës. Forcat kombëtare duhet të jenë jo vetëm të deklaruar, por të disponueshme, të ndërveprueshme dhe të përgatitura për misionin. *NDPP harmonizon planifikimin kombëtar me nevojat e Aleancës dhe i shpërndan ato te aleatët përmes objektivave të kapaciteteve*.<sup>9</sup>

Kjo e zhvendos vlerësimin nga ekzistenca e kapacitetit te përdorshmëria. Një njësi që kërkon kohë të gjatë për t'u plotësuar, pajisur ose stërvitur ka vlerë tjetër nga një njësi që gjenerohet sipas afateve të planeve. Po kështu, një sistem modern pa personel, municione, mirëmbajtje ose lidhje me strukturën e komandimit ka potencial teknik, por gatishmëri të kufizuar.

<sup>8</sup> North Atlantic Treaty Organization, "Summary of NATO's Rapid Adoption Action Plan," June 25, 2025, <https://www.nato.int/en/about-us/official-texts-of-natos-rapid-adoption-action-plan>.

<sup>9</sup> North Atlantic Treaty Organization, "NATO Defence Planning Process," updated April 16, 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/nato-defence-planning-process>; North Atlantic Treaty Organization, "NATO Force Model," updated April 2, 2025.

Në këtë kontekst duhet parë edhe rritja e investimeve në mbrojtje. Angazhimi i Hagës e lidh financimin me forcat, kapacitetet, infrastrukturën, gatishmërinë dhe qëndrueshmërinë, duke përfshirë edhe mbrojtjen e infrastrukturës kritike e rrjeteve, përgatitjen civile, inovacionin dhe industrinë.<sup>10</sup> Kështu, investimi në mbrojtje lidhet me të gjithë sistemin që gjeneron dhe mbështet forcën.

Samiti i Ankarasë vijoi këtë drejtim, me theks te realizimi i angazhimeve, kapaciteti industrial, teknologjitë e reja, ndërveprueshmëria digjitale dhe përdorimi i IA-së.<sup>11</sup> Mesazhi është i qartë: rritja e buxheteve duhet të shoqërohet me mekanizma që e kthejnë më shpejt financimin në kapacitet ushtarak.

Për FARSH, rëndësia e këtyre vendimeve qëndron te drejtimi. Zhvillimi i forcës duhet të ruajë lidhjen me objektivat e kapaciteteve dhe planet e mbrojtjes kolektive; gatishmëria duhet të jetë kriter kryesor për vlerësimin e investimeve; logjistika, infrastruktura dhe *Host Nation Support* duhet të mundësojnë pritjen, lëvizjen, furnizimin dhe mbështetjen e forcave; ndërsa industria dhe inovacioni duhet të ndihmojnë ruajtjen e kapaciteteve.

Sfida nuk është vetëm sigurimi i fondeve, por aftësia për t'i përthithur ato. Investimet prodhojnë rezultat kur ecin paralelisht me personelin, infrastrukturën, procedurat, mirëmbajtjen dhe logjistikën. Një platformë pa operatorë të përgatitur, rezerva të mjaftueshme ose integrim në rrjetet e komandimit mbetet kapacitet në tranzicion. Prandaj, planifikimi duhet të fokusohet te konvertimi i burimeve. Financimi fiton vlerë ushtarake kur prodhon personel të përgatitur, pajisje të integruara, stërvitje, komandim-kontroll, mirëmbajtje, rezerva dhe gatishmëri. Sa më koherent ky proces, aq më i madh efekti operacional i investimeve.

*PAZH 2024–2033 përbën bazën kombëtare të kësaj qasjeje, duke e vendosur zhvillimin e kapaciteteve në funksion të objektivave strategjikë dhe harmonizimit me National Defence Planning Process.*<sup>12</sup> Zbatimi kërkon që personeli, gatishmëria, modernizimi, infrastruktura dhe qëndrueshmëria të planifikohen si pjesë e së njëjtës logjikë të gjenerimit të forcës. Brenda kësaj logjike, personeli merr rëndësi të veçantë. Pajisjet mund të sigurohen përmes financimit; kompetenca profesionale duhet ndërtuar dhe ruajtur në kohë. Prandaj, transformimi i forcës nis nga burimet njerëzore.

<sup>10</sup> The Hague Summit Declaration,” June 25, 2025, paras. 2–4, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration>.

<sup>11</sup> North Atlantic Treaty Organization, “The Ankara Summit Declaration,” July 8, 2026, paras. 1–5; North Atlantic Treaty Organization, “Overview – 2026 NATO Summit in Ankara,” July 2026.

<sup>12</sup> Ministria e Mbrojtjes e Republikës së Shqipërisë, *Plani Afatgjatë i Zhvillimit të Forcave të Armatosura 2024–2033*.

### III. Personeli si themel i transformimit të forcës

Diskursi mbi transformimin ushtarak dominohet nga IA, dronët, sistemet autonome dhe rrjetet digjitale, por zhvillimi teknologjik nuk e ul rëndësinë e faktorit njerëzor. Përkundrazi, rrit kërkesën për personel më të arsimuar, të specializuar dhe të aftë për t'u përshtatur.

Teknologjia mund të sigurohet relativisht shpejt; kompetenca ushtarake kërkon kohë. Formimi i një oficeri shtabi, operatori sistemi kompleks, specialisti kibernetik, tekniku i mirëmbajtjes ose instruktori është proces shumëvjeçar. Humbja e një specialisti, sipas funksionit, mund të ulë drejtpërdrejt gatishmërinë e kapacitetit.

Burimet njerëzore duhet të trajtohen si cikël i vetëm i gjenerimit të forcës: rekrutim, arsimim, trajnim, kualifikim, stërvitje, zhvillim profesional, menaxhim karriere dhe mbajtje në shërbim. Kur këto procese shpëputen, mund të plotësohet numri por jo specialiteti, të krijohet ekspertizë pa u ruajtur, ose të futet një sistem në përdorim përpara përgatitjes së personelit.

Rekrutimi duhet të orientohet nga struktura e ardhshme e kapaciteteve. Aftësitë në kibernetikë, CIS, ISR, UAS/C-UAS, sisteme elektronike, automatizim dhe logjistikë të avancuar kërkojnë profile të ndryshme nga sistemet tradicionale. Për këto specialitete FARSH konkurron me tregun civil; prandaj menaxhimi i personelit duhet të adresojë si rekrutimin, ashtu edhe arsyet për të vazhduar karrierën ushtarake.

Mbajtja në shërbim nuk lidhet vetëm me kompensimin. Ajo ndikohet nga perspektiva e karrierës, kualifikimi, përdorimi real i specialitetit, cilësia e drejtimit, kushtet e punës dhe njohja e ekspertizës. Për specialitetet me kosto e kohë të lartë formimi, politikat e mbajtjes janë pjesë e menaxhimit të riskut të kapaciteteve.

Arsimimi ushtarak merr kështu rol strategjik. *Akademia e Forcave të Armatosura ka si mision arsimimin, kualifikimin, kërkimin shkencor dhe trajnimin e personelit ushtarak e civil në fushën e mbrojtjes dhe sigurisë kombëtare.*<sup>13</sup> Sfidë është që përmbajtja, metodat dhe kërkimi të përshtaten me mjedisin operacional.

Oficeri i së ardhmes duhet të kuptojë ndikimin e IA-së, kibernetikës, sistemeve pa pilot, luftës elektronike dhe të dhënave në planëzimin e operacioneve, pa qenë domosdoshmërisht specialist teknik. Nënoficeri duhet të jetë drejtues i trupës dhe bartës i standardit profesional; specialistët të rikualifikohen gjatë karrierës; instruktorët të kthejnë mësimet e operacioneve,

<sup>13</sup> Ministria e Mbrojtjes e Republikës së Shqipërisë, "Akademia e Forcave të Armatosura," <https://www.mod.gov.al/organizimi-fa/7008-akademia-e-forcave-te-armatosura>.

stërvitjeve dhe teknologjiave të reja në përmbajtje konkrete për forcën aktive dhe rezervën.

Kërkesa duhet të lidhet me funksionin: komandanti kupton efektet dhe kufizimet; operatori përdor sistemin; mirëmbajtësi e mban funksional; shtabi e integron në plan; strukturat e kapaciteteve kuptojnë ciklin jetësor. *Ky është edhe thelbi i konceptit të NATO-s për personel të përgatitur për mjedisin digjital, ku kompetencat, përshtatja, të mësuarit e vazhdueshëm dhe kultura organizative zhvillohen bashkë me teknologjinë.*<sup>14</sup>

Ruajtja e kompetencës duhet të shtrihet edhe përtej shërbimit aktiv. Forca rezervë krijon lidhje funksionale me komponentin aktiv kur rezervisti lidhet me një repart, funksion dhe specialitet të përcaktuar, njeh detyrën e pajisjet dhe përfshihet në cikël stërvitjeje që ruan kompetencën.<sup>15</sup> Në fushat si: kibernetika, IT, mjekësia, inxhinieria, transporti dhe teknologjia, rezervistët mund të sjellin edhe përvojë civile të vlefshme. Në këtë mënyrë, rezerva nuk është vetëm rezervë numerike; ajo është edhe rezervë kompetence, mekanizëm për rigjenerimin e forcës dhe urë ndërmjet ekspertizës ushtarake e civile. Prandaj, performanca e politikave të personelit nuk matet vetëm me plotësimin e organikës. Pyetja është nëse forca ka personelin e duhur, me specialitetin dhe nivelin e përgatitjes së kërkuar, në kohën kur nevojitet për gjenerimin e kapacitetit. Vetëm atëherë personeli shndërrohet nga input administrativ në element të fuqisë operacionale.

Kompetenca e personelit, megjithatë, nuk është vetvetiu gatishmëri. Ajo duhet të bashkohet me pajisjet, stërvitjen, komandim-kontrollin, municionet dhe logjistikën në nivel njësie. Gatishmëria është prova nëse investimi te njerëzit dhe sistemet ka krijuar aftësi për mision.

#### **IV. Gatishmëria si masë e kapacitetit operacional**

Gatishmëria është tregues i fuqisë reale të një force, por humbet kuptimin nëse reduktohet në përqindje personeli ose pajisjesh. Një njësi mund të jetë e plotësuar dhe e pajisur, por të mos e kryejë misionin brenda kohës së kërkuar. Prandaj, gatishmëria duhet kuptuar si aftësi e integruar, jo vetëm si kompletim apo inventar. Në këtë kuptim, gatishmëria duhet të vlerësohet në raport me misionin. Ajo krijohet kur personeli i përgatitur, pajisjet funksionale, stërvitja, komandim-kontrolli, logjistika, mirëmbajtja dhe mbështetja me shërbime funksionojnë së bashku në kohën dhe nivelin e kërkuar. Pyetja vendimtare nuk

<sup>14</sup> North Atlantic Treaty Organization, "NATO's Digital Transformation Implementation Strategy 2.0," paras. 23–24, "Digital-Ready Workforce."

<sup>15</sup> Shërbimi Ushtarak Rezervist, "https://www.mod.gov.al/rezervistet/7489-sherbimi-ushtarak-rezervist; Ministria e Mbrojtjes e Republikës së Shqipërisë, "Rikthim në Forcat e Armatosura të Republikës së Shqipërisë."

është vetëm nëse njësia ekziston dhe është e pajisur, por nëse ajo mund të gjenerohet, dislokohet, të veprojë dhe të mbështetet për aq kohë sa kërkon misioni.

Ajo krijohet kur personeli i trajnuar, pajisjet funksionale, stërvitja, municionet, mirëmbajtja, logjistika, komandim-kontrolli dhe procedurat funksionojnë së bashku sipas kërkesave të misionit. Për këtë arsye, gatishmëria është një nga matësit më të mirë të konvertimit të burimeve në efekt operacional.

Vlerësimi duhet të fokusohet te ajo që njësia mund të bëjë: çfarë misioni përmbush, sa shpejt gjenerohet e dislokohet, në çfarë kushtesh vepron, sa gjatë mbështetet dhe çfarë kapacitetesh i nevojiten. Këto pyetje e lidhin gatishmërinë me skenarin operacional dhe e bëjnë atë të dobishme për komandimin e planifikimin.

Stërvitja është mekanizmi kryesor për ndërtimin dhe provën e këtij integrimi. Ajo teston jo vetëm aftësinë individuale, por edhe shtabet, komunikimin, furnizimin, mirëmbajtjen, mbështetjen shëndetësore dhe vendimmarrjen. Prandaj, stërvitja është instrument për gjenerimin e gatishmërisë, jo thjesht aktivitet kalendarik. Sa më kompleks mjedisi, aq më reale duhet të jenë kushtet e stërvitjes. Njësitë duhet të veprojnë edhe me rrjete të kufizuara, furnizim të ndërprerë, informacion të paplotë dhe vendimmarrje nën presion. Vetëm kështu stërvitja zbulon dobësitë që në operacion do të kishin pasoja reale.

Vlerësimet dhe certifikimet e NATO-s e matin njësinë kundrejt një standardi të përbashkët dhe kërkesë operationale. Vlera e tyre rritet kur standardi orienton gjithë ciklin e përgatitjes, në mënyrë që certifikimi të jetë rezultat i natyrshëm i integritetit të personelit, pajisjeve dhe mbështetjes.

Digjitalizimi mundëson matje më dinamike të gatishmërisë. Integrimi i të dhënave për personelin, pajisjet, mirëmbajtjen, stërvitjen, municionet dhe logjistikën i jep komandantit pamje më të saktë; qëllimi nuk është më shumë raportim, por informacion më i mirë për vendimmarrjen.

Një pamje e integruar ndihmon edhe në identifikimin e shkakut të kufizimit. Mungesa e operatorëve kërkon trajnim; disponueshmëria e ulët teknike kërkon pjesë, teknikë ose riparim; mungesa e rezervave kërkon ndërhyrje logjistike. Kështu, të dhënat mbi gatishmërinë ndihmojnë prioritarizimin e investimeve. Kjo është veçanërisht e rëndësishme gjatë modernizimit. Çdo sistem i ri sjell kërkesa për personel, mirëmbajtje, infrastrukturë, municione, stërvitje dhe rrjete komandimi. Nëse nuk planifikohen paralelisht, teknologjia mund ta rrisë kompleksitetin më shpejt se gatishmërinë.

Gatishmëria nuk duhet të jetë gjendje e përkohshme para një stërvitjeje, certifikimi ose dislokimi. Synimi është një cikël ku personeli, mirëmbajtja dhe stërvitja ruajnë aftësinë për mision. Kalimi nga “gatishmëria për aktivitetin” te

“gatishmëria për misionin” është thelbësor për transformimin.

Gatishmëria tregon çfarë mund të bëjë forca sot; zhvillimi i kapaciteteve përcakton çfarë duhet të bëjë nesër. Prandaj, modernizimi duhet të ndërtohet mbi boshllëqe të identifikuara operacionale, jo thjesht mbi zëvendësimin e pajisjeve.

## **V. Zhvillimi i kapaciteteve: nga platforma te pajisja/sistemi i integruar**

Zhvillimi i kapaciteteve duhet të nisë nga misioni dhe efekti operacional. Teknologjia ofron shumë alternativa, ndërsa burimet mbeten të kufizuara; për këtë arsye, prioritetet duhet të udhëhiqen nga rëndësia e boshllëkut dhe efekti që mbyllja e tij krijon për misionin.

Për këtë arsye, PAZH e lidh zhvillimin e kapaciteteve me misionin kombëtar dhe detyrimet ndaj Aleancës. Projektet e modernizimit duhet të vlerësohen jo vetëm për karakteristikat teknike, por për kontributin në një aftësi të kërkuar.<sup>16</sup> Një platformë me performancë të lartë nuk përbën vetvetiu kapacitet të plotë.

Përpara sigurimit të një sistemi duhet të qartësohen efekti i pritshëm, njësia ku integrohet, personeli, sistemet me të cilat komunikon, infrastruktura dhe mënyra e stërvitjes. Kjo redukton rrezikun e “*ishujve*” teknologjikë: pajisje të avancuara që funksionojnë mirë veçmas, por lidhen dobët me forcën.

Integrimi duhet të jetë kriter qendror i modernizimit. Sensorët ajrorë, detarë e tokësorë duhet të lidhen me komandim-kontrollin dhe vendimmarrjen; vendimmarrja me mjetet e angazhimit; veprimi me logjistikën, mbrojtjen dhe rrjetet e sigurta. Në operacionet aleate, kjo lidhje duhet të shtrihet edhe te sistemet e partnerëve, duke e bërë ndërveprueshmërinë pjesë të kapacitetit.

*DTIS 2.0 e vendos këtë logjikë në konceptin e një “Digital Backbone” të sigurt, të shkallëzueshëm dhe të qëndrueshëm, që lidh sensorët, vendimmarrësit dhe ndarjen e të dhënave në funksion të misionit.*<sup>17</sup> Për FARSH, parimi praktik është që sistemet e reja të projektohen që në fillim për integrim dhe ndërveprim.

Zhvillimi i kapaciteteve duhet të përfshijë të gjithë ciklin jetësor. Kostoja fillestare është vetëm pjesë e investimit; personeli, trajnimi, infrastruktura, municionet, pjesët e këmbimit, licencat, përditësimet dhe riparimet përcaktojnë gatishmërinë gjatë përdorimit. Një sistem i përballueshëm për t’u blerë, por i vështirë për t’u mbështetur, mund të krijojë barrë afatgjatë. Prandaj, menaxhimi

<sup>16</sup> Ministria e Mbrojtjes e Republikës së Shqipërisë, *Plani Afatgjatë i Zhvillimit të Forcave të Armatosura 2024–2033*; North Atlantic Treaty Organization, “NATO Defence Planning Process.”

<sup>17</sup> NATO’s Digital Transformation Implementation Strategy 2.0, para. 24, “Digital Backbone” and “Alliance Data Sharing Ecosystem.”

i ciklit jetësor është pjesë e planifikimit të kapacitetit. Vendimi për një sistem duhet të përfshijë mënyrën se si do të gjenerohet dhe ruhet gatishmëria e tij gjatë viteve.

Konfliktet bashkëkohore kanë evidentuar edhe raportin midis sofistikimit dhe masës. Sistemet e avancuara krijojnë avantazh, por operacionet e zgjatura kërkojnë municione, pajisje, pjesë këmbimi dhe kapacitet zëvendësimi. Një forcë moderne mund të jetë e brishtë nëse aftësitë kritike varen nga pak sisteme pa rezerva.

Për një vend me burime të kufizuara, kjo kërkon balancë mes cilësisë, sasisë dhe qëndrueshmërisë. Objektivi është një grup kapacitetesh që plotësojnë njëri-tjetrin, integrohen me NATO-n dhe mund të mbështeten realisht në kohë.

Inovacioni duhet të plotësojë, jo të zëvendësojë planifikimin afatgjatë. Poligonet dhe stërvitjet mund të përdoren për të testuar teknologji, procedura dhe forma të reja organizimi, veçanërisht për sistemet me cikël të shpejtë teknologjik ku performanca laboratorike nuk provon përdorshmërinë në terren.

Një mekanizëm eksperimentimi duhet të lidhë njësitë operacionale, planifikimin, institucionet akademike dhe industrinë. Njësia identifikon problemin; ekspertiza analizon alternativat; industria ose partnerët ofrojnë zgjidhje; operatori e provon. Zgjidhjet efektive kalojnë drejt integritit; dështimet identifikohen herët dhe me kosto më të ulët.

Kjo qasje i lejon FARSH të shfrytëzojë një avantazh të forcës së vogël: përshtatjen e shpejtë. Por shpejtësia ka vlerë vetëm nëse kapaciteti ruhet në kohë. Kështu, qëndrueshmëria bëhet vazhdim logjik i zhvillimit të kapaciteteve.

## **VI. Qëndrueshmëria e mbrojtjes: aftësia për të vijuar misionin**

Gatishmëria dhe qëndrueshmëria janë të lidhura, por përfaqësojnë momente të ndryshme. Gatishmëria tregon nëse forca mund ta nisë dhe përmbushë misionin; qëndrueshmëria, nëse mund ta ruajë aftësinë kur rritet konsumi, dëmtohen pajisjet, ndërpritet furnizimi ose degradohen sistemet.

Ky dallim është thelbësor kur kundërshtari synon jo vetëm njësitë luftarake, por edhe rrjetet, depot, komunikimet, energjinë dhe infrastrukturën mbështetëse. Një forcë e gatshme në fillim, por që humbet shpejt efektivitetin, ka vlerë parandaluese më të ulët se një forcë që absorbon goditjen dhe vijon operacionin.

NATO e konsideron qëndrueshmërinë individuale dhe kolektive bazë të parandalimit dhe mbrojtjes. Ajo përfshin përgatitjen, rezistencën ndaj goditjes, reagimin dhe rikuperimin duke ruajtur funksionet kritike. Përgatitja civile është mundësues i mbrojtjes kolektive, sepse forcat varen nga transporti,

komunikimet, energjia dhe shërbimet civile.<sup>18</sup>

Për FARSH, qëndrueshmëria përfshin municionet, rezervat materiale, mirëmbajtjen, pjesët e këmbimit, transportin, energjinë, mbështetjen shëndetësore, komunikimet, mbrojtjen kibernetike dhe rezervën njerëzore. Vlera e tyre qëndron në aftësinë për t'u aktivizuar në kohën e nevojshme.

Redundanca është element kryesor. Sistemet kritike nuk duhet të varen nga një pikë e vetme dështimi: komandim-kontrolli kërkon procedura alternative; të dhënat, mbrojtje dhe rikuperim; logjistika, alternativa furnizimi; njësitë, stërvitje për të vepruar me informacion e komunikim të degraduar.

Digjitalizimi e rrit këtë kërkesë. Sistemet e ndërlidhura sjellin shpejtësi dhe ndërveprueshmëri, por zgjerojnë sipërfaqen që duhet mbrojtur. Prandaj, siguria kibernetike dhe qëndrueshmëria duhet të projektohen brenda kapacitetit që në fillim.

Qëndrueshmëria lidhet edhe me rigjenerimin: personeli zëvendësohet, pajisjet riparohen ose zëvendësohen dhe rezervat rimbushen. Kjo lidh rezervën njerëzore, rezervat materiale dhe industrinë me aftësinë për të vijuar operacionin përtej ciklit fillestar të gatishmërisë.

Një dimension tjetër është *Host Nation Support*. Mbrojtja kolektive kërkon që forcat aleate të mund të lëvizin, priten, dislokohen, furnizohen dhe mbështeten. Për Shqipërinë, pozicioni gjeografik dhe infrastruktura portuale, ajrore e tokësore krijojnë mundësi që HNS të japë kontribut real në lëvizshmërinë dhe përforsimin aleat.

HNS nuk është vetëm bazë ose korridor. Ai përfshin transportin, magazinimin, karburantin, sigurinë, komunikimet, shërbimet dhe bashkëpunimin ushtarak-civil. Kur këto elemente planifikohen e stërviten paraprakisht, infrastruktura kombëtare bëhet pjesë e fuqisë së mbrojtjes. Këtu qëndrueshmëria shtrihet përtej FARSH. Forcat varen nga energjia, transporti, telekomunikacioni, shëndetësia, industria dhe administrata civile; ndaj bashkëpunimi ushtarak-civil dhe përgatitja institucionale janë elemente të mbrojtjes kombëtare dhe kolektive.

Edhe industria duhet parë përtej dimensionit ekonomik. Aftësia për të mirëmbajtur, riparuar, prodhuar ose rigjeneruar pajisje e materiale ndikon drejtpërdrejt në kohën e ruajtjes së efektivitetit. Prandaj, industria dhe inovacioni duhen vlerësuar edhe nga kontributi në kapacitetet operacionale dhe qëndrueshmërinë.

---

<sup>18</sup> Resilience, Civil Preparedness and Article 3, updated November 13, 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.

## **VII. Inovacioni dhe industria në mbështetje të transformimit dhe qëndrueshmërisë**

Rikthimi i konflikteve me intensitet të lartë e ka rikthyer industrinë e mbrojtjes në rol qendror për gjenerimin dhe qëndrueshmërinë e fuqisë ushtarake. Burimet dhe objektivat e kapaciteteve nuk prodhojnë efekt nëse industria nuk i shndërron në kohë në pajisje, municione, sisteme, mirëmbajtje dhe mbështetje. Për këtë arsye, NATO po e lidh më ngushtë industrinë me zhvillimin e kapaciteteve, ndërveprueshmërinë dhe adoptimin e teknologjisë.

Për Shqipërinë, zhvillimi i industrisë së mbrojtjes duhet vlerësuar nga vlera që i shton gatishmërisë dhe qëndrueshmërisë. Objektivi nuk është prodhimi i gjithë spektrit të sistemeve ushtarake, por identifikimi i fushave ku kapacitetet vendase dhe partneritetet me industrinë aleate plotësojnë nevojat reale, sjellin standarde e ekspertizë dhe zvogëlojnë varësitë kritike.

Kjo mund të përfshijë prodhim, integrim teknologjik, mirëmbajtje, riparim, softuer, komponentë ose shërbime teknike. Veçanërisht e rëndësishme është aftësia për të rikthyer sistemet në gatishmëri brenda vendit, sepse në krizë koha e riparimit dhe siguria e zinxhirit të furnizimit bëhen faktorë operacionalë.

Kjo lidhje shtrihet edhe te kapitali njerëzor. Industria dhe FARSH kanë nevojë për kompetenca të përbashkëta në inxhinieri, elektronikë, teknologji informacioni, softuer dhe mirëmbajtje. Bashkëpunimi me arsimin profesional, akademitë dhe universitetet mund të zgjerojë bazën e specialistëve dhe të lidhë kërkimin e inovacionin me kapacitetet ushtarake.

Po aq e rëndësishme është lidhja e industrisë me përdoruesin operacional. Problemet e evidentuara në stërvitje, mirëmbajtje ose përdorim duhet të kthehen në kërkesa për testim dhe zgjidhje të reja, të provuara para integritetit më të gjerë. Kjo shkurton distancën ndërmjet nevojës operationale dhe zgjidhjes teknologjike dhe ul rrezikun e investimeve të papërshtatshme.

Kështu, industria dhe inovacioni bëhen pjesë e ciklit të gjenerimit, mbështetjes dhe rigjenerimit të kapaciteteve. Vlera e tyre matet me rritjen e gatishmërisë, forcimin e qëndrueshmërisë, zvogëlimin e varësive kritike dhe përshtatjen më të shpejtë të FARSH.

## **VIII. Nga burimet e mbrojtjes te kapaciteti operacional**

Personeli, gatishmëria, zhvillimi i kapaciteteve dhe qëndrueshmëria nuk janë prioritet të pavarura, por pjesë të një procesi të vetëm. Personeli krijon kompetencën; arsimimi dhe stërvitja e kthejnë në aftësi; pajisjet e sistemet e integruara prodhojnë efekt; logjistika, rezervat, infrastruktura dhe rigjenerimi e ruajnë atë në kohë. Ndërveprimi i këtyre elementeve krijon kapacitetin operacional dhe fuqinë ushtarake.

Kjo duhet të ndryshojë edhe mënyrën e matjes së transformimit. Treguesit e inputeve duhen plotësuar me tregues rezultati: jo vetëm sa personel rekrutohet, por sa kualifikohet e ruhet; jo vetëm sa sisteme blihen, por sa janë të integruara e të gatshme; jo vetëm sa rezervistë regjistrohen, por sa shpejt integrohen; jo vetëm sa stërvitje zhvillohen, por çfarë mangësish mbyllen dhe sa rritet gatishmëria.

E njëjta logjikë vlen për investimet. Rritja e financimit krijon mundësi për modernizim, por fuqia mbrojtëse rritet vetëm kur financimi kthehet në personel, pajisje, stërvitje, integrim, logjistikë dhe qëndrueshmëri. Një hallkë e ngadaltë frenon gjithë ciklin e kapacitetit. Prandaj, krahas financimit duhet të rritet kapaciteti institucional për planifikim dhe realizim. Projekte më të mëdha e teknologji më komplekse kërkojnë ekspertizë për kërkesat, prokurimin, menaxhimin e kontratave, integrimin dhe mirëmbajtjen. Transformimi përfshin edhe proceset që mbështesin strukturën luftarake.

Transformimi digjital mund të përmirësojë edhe proceset e personelit, logjistikës, mirëmbajtjes dhe planifikimit, duke rritur cilësinë e të dhënave dhe shpejtësinë e vendimmarrjes. Por teknologjia duhet të shoqërohet me ndryshim procesesh; automatizimi i një procedure joefikase nuk e bën vetvetiu sistemin më efektiv.

Në fund, duhet matur rruga nga burimi te kapaciteti operacional: sa shpejt investimi krijon efekt, sa integrohet, sa kushton për t'u mbajtur, sa gjatë ruhet gatishmëria dhe sa shpejt rigjenerohet. Këto pyetje e lidhin planifikimin afatgjatë me përdorimin real.

Ky parim vlen edhe për kontributin e Shqipërisë në NATO. Një aleat vlerësohet jo vetëm nga madhësia e forcës ose buxhetit, por nga kapacitetet që ofron kur kërkohen. Repartet e deklaruara, kontributet në operacione, kapacitetet e veçanta, HNS, infrastruktura, logjistika, kibernetika, trajnimi dhe potenciali industrial krijojnë vlerë kur janë të gatshme, të ndërveprueshme dhe të qëndrueshme.

Kjo e bën lidhjen ndërmjet sigurisë kombëtare dhe mbrojtjes kolektive më të drejtpërdrejtë. Shqipëria përfiton nga fuqia e Aleancës dhe njëkohësisht e forcon atë përmes kapaciteteve që zhvillon e kontribuon. Pyetja strategjike nuk është vetëm çfarë siguron NATO për Shqipërinë, por çfarë vlere të gatshme dhe të përdorshme i ofron Shqipëria NATO-s.

Përgjigjja nuk kërkon që FARSH të ketë çdo kapacitet, por që kapacitetet e marra përsipër të jenë reale, të integruara, të gatshme dhe të qëndrueshme. Këtu bashkohen vizioni kombëtar i zhvillimit të forcës dhe besueshmëria e mbrojtjes kolektive.

## Rekomandime

Transformimi duhet të nisë dhe të përfundojë te aftësia për mision. Çdo kapacitet duhet të planifikohet së bashku me personelin, kualifikimin dhe ruajtjen e ekspertizës së nevojshme.

Arsimimi dhe stërvitja duhet të përgatisin forcën për kërkesat e së ardhmes, duke integruar IA, kibernetikën, UAS, luftën elektronike, të dhënat dhe operacionet shumëdomainëshe. Kualifikimi duhet të jetë proces i vazhdueshëm gjatë karrierës.

Forca rezervë duhet të zhvillohet si pjesë funksionale e forcës aktive, e lidhur me njësinë, detyrën dhe specialitetin. Stërvitja dhe aktivizimi periodik duhet ta kthejnë nga potencial numerik në kapacitet real.

Gatishmëria duhet të matet mbi aftësinë për të kryer dhe mbështetur misionin. Personeli, pajisjet, stërvitja, mirëmbajtja, municionet dhe logjistika duhet të japin një pamje të përbashkët për vendimmarrjen.

Zhvillimi i kapaciteteve duhet të ndjekë ciklin jetësor. Pajisja, personeli, doktrina, stërvitja, infrastruktura, komandim-kontrolli, mirëmbajtja dhe rezervat duhet të planifikohen si një tërësi, nga siguri te gatishmëria e plotë.

Për teknologjitë me zhvillim të shpejtë duhet proces i vazhdueshëm eksperimentimi, testimi dhe integrimi. Nevojat duhet të vijnë nga njësitë operacionale dhe zgjidhjet efektive të kalojnë shpejt në përdorim.

Qëndrueshmëria duhet të trajtohet si kapacitet operacional. Rezervat, HNS, mbrojtja kibernetike, komunikimet alternative, energjia dhe logjistika duhet të testohen edhe në kushte degradimi, ndërprerjeje dhe presioni operacional.

Industria e mbrojtjes duhet të lidhet me nevojat e FARSH dhe zvogëlimin e varësive kritike, veçanërisht në mirëmbajtje, riparim, rezerva, integrim teknologjik dhe rigjenerim të forcës.

Rritja e investimeve duhet të sjellë rritje të matshme të kapaciteteve operacionale. Çdo projekt madhor duhet të adresojë një nevojë të qartë, të ketë afat gatishmërie dhe të kontribuojë drejtpërdrejt në misionet kombëtare dhe të Aleancës.

## Përfundime

Epoka digjitale nuk e zvogëlon rëndësinë e fuqisë ushtarake; ajo ndryshon mënyrën si ndërtohet dhe përdoret. IA, sistemet pa pilot, kibernetika, sensorët, të dhënat dhe komunikimet krijojnë avantazh vetëm kur integrohen me personelin, komandim-kontrollin, stërvitjen, sigurinë dhe logjistikën.

Për këtë arsye, transformimi digjital nuk është thjesht pajisje apo teknologji e re. Ai kërkon ndryshim në mënyrën si forca arsimon, stërvitet, vendos, operon dhe mbështet kapacitetet.

Personeli mbetet themeli i transformimit, ndërsa gatishmëria është prova e tij. Rekrutimi, arsimimi, kualifikimi dhe rezerva duhet të prodhojnë njësi të afta të kryejnë dhe mbështesin misionin në kohën e kërkuar.

Modernizimi duhet të matet me kapacitete të integruara, jo me numrin e platformave. Personeli, pajisjet, doktrina, komandim-kontrolli, stërvitja, infrastruktura, mirëmbajtja dhe logjistika duhet të funksionojnë si sistem i vetëm, i ndërveprueshëm dhe i qëndrueshëm.

Qëndrueshmëria, inovacioni dhe industria e mbrojtjes duhet ta ndihmojnë forcën të përballojë konsumimin dhe ndërprerjet, të zvogëlojë varësitë kritike dhe të rigjenerojë kapacitetet.

Në thelb, sfida për FARSH është shndërrimi i burimeve në fuqi ushtarake reale: personel të përgatitur, njësi të gatshme, kapacitete të integruara dhe aftësi për të vijuar misionin.

Ky duhet të jetë rezultati i transformimit: aftësi të besueshme për mbrojtjen kombëtare dhe kontribut operacional real, të qëndrueshëm e të gatshëm për Aleancën.

## **Bibliografia**

1. The Hague Summit Declaration. The Hague, June 25, 2025.
2. The Ankara Summit Declaration. Ankara, July 8, 2026.
3. Vizioni i Shefit të Shtabit të Përgjithshëm të FARSH për periudhën 2026-2028.
4. NATO 2022 Strategic Concept. Brussels: NATO, 2022.
5. Resilience, Civil Preparedness and Article 3. Updated November 13, 2024.
6. Ministria e Mbrojtjes e Republikës së Shqipërisë. Akademia e Forcave të Armatosura.
7. Strategy for Industry-NATO Cooperation. July 8, 2026.
8. Plan i Afatgjatë i Zhvillimit të Forcave të Armatosura 2024–2033.
9. Ministria e Mbrojtjes e Republikës së Shqipërisë. Shërbimi Ushtarak Rezervist.
10. Deterrence and Defence. Updated June 25, 2026.
11. Innovation and Technology Adoption. Updated July 8, 2026.
12. NATO Defence Planning Process. Updated April 16, 2025. <https://www.nato.int/en/what-ww-do/introduction-to-nato/nato-defence-planning-process>.
13. North Atlantic Treaty Organization. “NATO Force Model.” Updated April 2, 2025.
14. NATO’s Digital Transformation Implementation Strategy 2.0. May 26, 2026.
15. Summary of NATO’s Rapid Adoption Action Plan. June 25, 2025.

# Industria ushtarake përballë sfidave dhe mundësive të epokës digjitale

---

Kolonel (R) Hysni GJERGJI  
Agjencia e Industrisë së Mbrojtjes

## Trajtesë e shkurtuar

*Transformimi digjital po ndryshon strukturën, organizimin dhe logjikën strategjike të industrisë ushtarake. Inteligjenca artificiale, sistemet autonome, robotika, prodhimi aditiv, mikroelektronika, sensorët e avancuar, analizimi i të dhënave dhe rrjetet moderne të komunikimit po krijojnë një mjedis në të cilin avantazhi ushtarak nuk përcaktohet vetëm nga zotërimi i platformave të avancuara, por gjithnjë e më shumë nga aftësia për të zhvilluar, integruar, përditësuar, prodhuar në shkallë dhe mbrojtur teknologjinë me ritëm të lartë. Ky transformim krijon një paradoks strategjik: sa më e digjitalizuar bëhet industria e mbrojtjes, aq më produktive dhe fleksibël mund të jetë, por njëkohësisht zgjerohet sipërfaqja e ekspozimit ndaj spiunazhit industrial, operacioneve kibernetike, sabotimit teknik, komprometimit të zinxhirit të furnizimit dhe kërcënimeve të brendshme.*

*Studimi përdor analizë cilësore dokumentare, krahasuese dhe raste studimore nga zhvillimet euroatlantike dhe lufta në Ukrainë. Argumenti qendror është se avantazhi industrial ushtarak në epokën digjitale buron nga kombinimi i inovacionit, sigurisë së teknologjisë, kapacitetit për shkallëzim të prodhimit dhe shpejtësisë së përshtatjes. Në përfundim propozohen implikime dhe rekomandime për zhvillimin e industrisë së mbrojtjes në Shqipëri, me fokus te specializimi inteligjent, teknologjitë dual-use, interoperabiliteti NATO dhe parimi security by design.*

**Fjalë kyçe:** industri ushtarake; transformim digjital; inteligjencë artificiale; teknologji dual-use; siguri kibernetike; TECHINT; zinxhir furnizimi; inovacion ushtarak; NATO; Shqipëri.

## Hyrje

**H**istoria e fuqisë ushtarake është e lidhur ngushtë me aftësinë e shpërndarjes për të shpërndarur progresin shkencor në kapacitete operative. Revolucioni industrial mundësoi prodhimin masiv; mekanizimi ndryshoi manovrën; aviacioni zgjeroi hapësirën e operacioneve; elektronika dhe radarët transformuan zbulimin; ndërsa teknologjia bërthamore ndryshoi vetë logjikën e parandalimit. Epoka digjitale përfaqëson një transformim të krahasueshëm, por me një veçori: ajo nuk ndryshon vetëm armën përfundimtare, por të gjithë ciklin e jetës së kapacitetit ushtarak, nga kërkimi dhe projektimi deri te prodhimi, mirëmbajtja, modernizimi dhe përdorimi operacional.

NATO e ka vendosur inovacionin teknologjik dhe transformimin digjital në qendër të përshtatjes së Aleancës. Koncepti Strategjik i vitit 2022 e trajton inovacionin teknologjik dhe reziliencën si çështje ndërsektoriale të rëndësishme për detyrat kryesore të Aleancës (NATO, 2022). Strategjia e NATO-s për teknologjitë emergjente dhe disruptive mbështetet te parimi “foster and protect”: zhvillimi dhe adoptimi i teknologjive dual-use duhet të ecë paralelisht me mbrojtjen e tyre nga ndërhyrja, manipulimi dhe shfrytëzimi nga aktorë kundërshtarë (NATO, 2026a).

Ndryshimi është gjithashtu industrial. Rapid Adoption Action Plan i NATO-s synon që adoptimi i shumicës së produkteve të reja teknologjike të realizohet brenda një periudhe maksimale prej 24 muajsh, duke reflektuar hende kun ndërmjet ciklit tradicional të prokurimit ushtarak dhe ritmit të inovacionit komercial (NATO, 2025a). Në korrik 2026, Strategy for Industry–NATO Cooperation (SYNC) e formalizoi më tej këtë logjikë duke vendosur tri prioritetë: bashkëpunim më të thellë me industrinë; përsheptim të inovacionit dhe interoperabilitetit; dhe forcim, shkallëzim e qëndrueshmëri të prodhimit (NATO, 2026b).

Në nivel evropian, European Defence Industrial Strategy dhe White Paper for European Defence – Readiness 2030, e lidhin gatishmërinë ushtarake me kapacitetin industrial, investimet, prokurimin bashkëpunues, sigurinë e furnizimit dhe aftësinë për të rritur prodhimin në krizë (European Commission & High Representative, 2024; European Commission & High Representative, 2025). Për rrjedhojë, industria e mbrojtjes nuk është thjesht një sektor ekonomik që furnizon forcat e armatosura; ajo është pjesë përbërëse e fuqisë kombëtare dhe e parandalimit.

## I. Problemi kërkimor

Problemi kryesor i studimit buron nga paradoksi i digjitalizimit. Automatizimi, softuerët, inteligjenca artificiale dhe lidhja në rrjet mund të rrisin produktivitetin, cilësinë, ndërveprueshmërinë dhe ritmin e inovacionit

teknologjik ushtarak. Por të njëjtat elemente krijojnë varësi nga të dhënat, mikro-elektronika, rrjetet, furnitorët dhe personeli me akses të lartë. Një industri më “inteligjente” mund të jetë njëkohësisht më e ekspozuar ndaj ndërhyrjes kibernetike, komprometimit të zinxhirit të furnizimit dhe spiunazhit teknologjik.

Pyetja qendrore është: Si mund të shfrytëzohen avantazhet e transformimit digjital për rritjen e kapacitetit industrial ushtarak, duke kontrolluar njëkohësisht rreziqet strategjike që ky transformim ka krijuar?

### ***Pyetjet kërkimore***

- Cilat teknologji dhe modele organizative po ushtrojnë ndikimin më të madh mbi transformimin e industrisë së mbrojtjes, në rajon, NATO apo tek aktorët e huaj?
- Si e ndryshon digjitalizimi natyrën e kërcënimeve ndaj industrisë ushtarake?
- Çfarë mësimesh japin lufta në Ukrainë dhe politikat e reja NATO/BE për marrëdhënien ndërmjet inovacionit, prodhimit dhe përshtatjes?
- Çfarë mundësish krijohen për shtetet me bazë industrial ushtarake të vogël dhe çfarë implikimesh lindin për Shqipërinë?

### ***Teza e studimit***

Studimi mbështet tezën se në epokën digjitale epërsia industriale ushtarake nuk përcaktohet vetëm nga aftësia për të projektuar sistemin më të avancuar, por nga aftësia për ta inovuar, mbrojtur, prodhuar në shkallë dhe përshtatur atë më shpejt se kundërshtari. Në këtë kuptim, inovacioni pa kapacitet prodhues mbetet prototip, ndërsa prodhimi pa siguri krijon cenueshmëri, sikurse ndërsa teknologjia pa aftësi për përditësim dhe zëvendësim rrezikon të vjetrohet shpejt.

### ***Metodologjia dhe kufizimet***

Studimi kombinon analizën dokumentare, analizën krahasuese dhe metodën e rasteve studimore. Burimet primare përfshijnë dokumente zyrtare të NATO-s, Bashkimit Evropian, Departamentit Amerikan të Mbrojtjes, NIST-it, GAO-s, Ministrisë së Mbrojtjes së Ukrainës dhe Brave1. Burimet dytësore përfshijnë publikime të SIPRI, RAND dhe CSIS mbi autonominë, transformimin digjital, arkitekturat e hapura dhe inovacionin ushtarak.

Përzgjedhja e rasteve është e qëllimshme dhe jo statistikisht përfaqësuese. Studimi synon të identifikojë mekanizma dhe tendenca strategjike, jo të provojë marrëdhënie shkakësore. Një kufizim tjetër është natyra dinamike e teknologjisë së mbrojtjes dhe e konfliktit në Ukrainë. Disa tregues mund të ndryshojnë shpejt dhe një pjesë e të dhënave operative mbetet e klasifikuar. Për këtë arsye përdoren vetëm të dhëna publike, ndërsa pretendimet operative trajtohen me kujdes.

## **II. Transformimi digjital dhe ndryshimi i modelit të industrisë ushtarake**

### ***Nga platformat fizike te sisteme e përcaktuara nga softueri***

Në industrinë tradicionale, vlera e një platforme lidhej kryesisht me karakteristikat fizike, me motorin, mbrojtjen, rrezen, armatimin dhe qëndrueshmërinë mekanike. Në sistemet moderne, performanca varet gjithnjë e më shumë nga softueri, sensorët, përpunimi i të dhënave, komunikimet dhe aftësia për integrim me sisteme të tjera. Kjo prire përshkruhet si kalim drejt “software-defined warfare”, ku modernizimi i kapacitetit mund të realizohet përmes ndryshimeve të shpejta në kod, algoritme dhe arkitekturë digjitale dhe jo vetëm përmes zëvendësimit të platformës.

Ky model e ndryshon ekonominë e ciklit të jetës. Një platformë mund të qëndrojë në shërbim për dekada, ndërsa komponentët digjitalë mund të vjetrohen brenda pak vitesh. Për rrjedhojë, modulariteti, ndërfaqet e standardizuara dhe arkitekturat e hapura bëhen parakushte për modernizim të vazhdueshëm. NATO e ka përfshirë shprehimisht modularitetin, arkitekturat e hapura dhe standardet digjitale në SYNC 2026 (NATO, 2026b). Analizat mbi Modular Open Systems Approaches në sektorin amerikan tregojnë se standardet e hapura mund të rrisin konkurrencën dhe të lehtësojnë integrimin e teknologjive të reja, por kërkojnë koordinim institucional dhe industrial (Sanders & Holderness, 2021).

### ***Inteligjenca artificiale, të dhënat dhe autonomia***

Inteligjenca artificiale është teknologji horizontale. Vlera e saj rritet kur kombinohet me të dhëna, sensorë, fuqi llogaritëse dhe sisteme autonome. NATO e ka trajtuar IA-në si një nga teknologjitë prioritare dual-use dhe që prej vitit 2021 ka zhvilluar një qasje që kombinon adoptimin me përdorimin e përgjegjshëm dhe mbrojtjen kundër përdorimit kundërshtar (NATO, 2021). Raporti Science & Technology Macro Trends 2025–2045 parashikon se gara për IA dhe teknologji kuantike, integrimi teknologjik dhe varësitë, do të jenë ndër tendencat qendrore të dy dekadave të ardhshme (NATO Science & Technology Organization, 2025).

Autonomia ushtarake nuk është një teknologji e vetme, por rezultat i kombinimit të sensorëve, softuerit, algoritmeve dhe sistemit të kontrollit. SIPRI ka treguar se inovacioni në autonomi vjen nga një ekosistem i përzier civil-ushtarak dhe se shumë teknologji bazë janë dual-use (Boulain, 2016; Boulain & Verbruggen, 2017). Kjo e bën bashkëpunimin me startup-et, universitetet dhe kompanitë teknologjike një element strukturor të industrisë së mbrojtjes moderne.

## ***Rasti studimor: Ukraina dhe cikli i shpejtë i inovacionit***

Lufta në Ukrainë është një rast me rëndësi të veçantë, sepse e ka vendosur teknologjinë në një cikël shumë të shpejtë reagimi. Zgjidhja teknologjike në terrenin luftarak prodhon kundërmasë, e cila nga ana tjetër kërkon përshtatje të re. Kjo është veçanërisht e dukshme në ekosistemin e UAV, luftën elektronike dhe teknologjitë e navigimit. Brave1, është institucioni shtetëror ukrainas për teknologjitë e mbrojtjes, i cili raportonte në vitin 2026 rreth 2,500 kompani dhe mbi 5,000 produkte/zhvillime në ekosistemin e tij, përfshirë mbi 500 prodhues UAV, mbi 300 prodhues EW/SIGINT dhe mbi 200 zhvillues të produkteve AI (Brave1, 2026a).

Më i rëndësishëm se numri i kompanive është modeli institucional. Brave1 përpiqet të lidhë kërkesën e forcave të armatosura me zhvilluesit, financimin, testimin dhe kalimin drejt produktit të ri. Në korrik 2026, programi i ri i granteve identifikoi 53 prioritete teknologjike në nëntë fusha dhe financim të diferencuar sipas nivelit të pjekurisë teknologjike, nga vlerësimi i konceptit deri te testimi i produktit përfundimtar (Ministry of Defence of Ukraine, 2026). Ky model tregon se inovacioni ushtarak kërkon jo vetëm fonde R&D, por një rrugë institucionale nga problemi operacional te përdorimi real.

## ***Prodhimi aditiv dhe logjistika digjitale***

Prodhimi aditiv (additive manufacturing) krijon mundësi për prototipizim të shpejtë, prodhim të disa pjesëve këmbimi dhe decentralizim të kufizuar të logjistikës. Departamenti Amerikan i Mbrojtjes e ka institucionalizuar përdorimin e prodhimit aditiv dhe ka përfshirë sigurinë kibernetike të workflow dhe zinxhirit të furnizimit ndër objektivat kryesore (U.S. Department of Defense, 2021). Ky aspekt është thelbësor, pasi nëse një komponent prodhohet nga një model digjital, integriteti i skedarit dhe i procesit të prodhimit bëhet pjesë e integritetit fizik të komponentit.

Ky aspekt sjell një ndryshim konceptual nga inventari vetëm fizik, drejt kombinimit të inventarit fizik me inventarin digjital të certifikuar. Megjithatë, përdorimi ushtarak kërkon kontroll të rreptë të konfigurimit, materialeve, certifikimit dhe sigurisë. Për rrjedhojë, prodhimi aditiv duhet parë si mjet për qëndrueshmëri dhe shpejtësi dhe jo si zëvendësim universal i zinxhirit tradicional të prodhimit.

## ***Digital twin<sup>1</sup> dhe mirëmbajtja parashikuese***

Digital twin është përfaqësimi virtual i një platforme, komponenti ose procesi, i cili mund të bashkojë të dhënat e projektimit, prodhimit, përdorimit

<sup>1</sup> [https://www.google.com/goto?url=CAESYgHrOzAVImjD1B\\_1jOE9PQkejwrLcWBLOFSJgGBmVro6iEGDRqgM\\_](https://www.google.com/goto?url=CAESYgHrOzAVImjD1B_1jOE9PQkejwrLcWBLOFSJgGBmVro6iEGDRqgM_)

dhe mirëmbajtjes. Në një model të pjekur, kjo lejon simulim të ndryshimeve, identifikim të hershëm të defekteve dhe mirëmbajtje parashikuese. Në terma strategjikë, vlera e tij qëndron në uljen e kohës ndërmjet identifikimit të një problemi dhe modifikimit të produktit. Por përqendrimi i të dhënave teknike e bën gjithashtu digital twin një aset me vlerë të lartë për spiunazhin industrial dhe cyber intelligence.

### **III. Kërcënimet dhe cenueshmëritë e industrisë së digjitalizuar**

#### ***Zgjerimi i perimetrit të sigurisë***

Në fabrikën tradicionale të industrisë ushtarake perimetri i sigurisë identifikohet kryesisht me territorin, gardhin rrethues dhe objektin. Në fabrikën digjitale, perimetri real përfshin serverët, cloud-in, pajisjet mobile, furnitorët, softuerin e palëve të treta, sistemet industriale të kontrollit dhe personelin me akses të privilegjuar. Kjo risi kërkon kalim nga koncepti “facility security” drejt “defence-industrial ecosystem security”.

#### ***Cyber-physical sabotage dhe siguria OT/TCS***

Integrimi i Information Technology (IT) me Operational Technology (OT) krijon efikasitet, por edhe mundësi që një komprometim kibernetik të prodhojë sabotazh fizik. Për një ndërmarrje të industrisë së mbrojtjes, objektivi nuk është vetëm databaza. Objektivi mund të jenë parametrat e një makinerie CNC, sensorët e procesit, PLC-të, sistemet e testimit ose të kontrollit të cilësisë. Rreziku më i avancuar është manipulimi, i cili nuk ndal prodhimin, por degradon produktin në mënyrë të vështirë për t’u zbuluar.

Rasti Stuxnet mbetet referencë konceptuale sepse demonstroi se si një malware-i mund të projektohet për të manipuluar procese industriale dhe për të prodhuar shkatërrim fizik. Për industrinë ushtarake, mësimi është nevoja për segmentim IT/OT, monitorim të integritetit të parametrave, kontroll të aksesit dhe verifikim të pavarur të cilësisë.

#### ***Siguria e zinxhirit të furnizimit***

Një platformë moderne varet nga një rrjet i gjerë furnitorësh dhe nënkontraktorësh. NIST<sup>2</sup> e trajton Cybersecurity Supply Chain Risk Management si disiplinë të integruar të menaxhimit të rrezikut, për shkak se produktet dhe shërbimet mund të përmbajnë funksionalitete keqdashëse, komponentë të falsifikuar ose cenueshmëri të krijuara këto nga praktika të dobëta zhvillimi dhe prodhimi (Boyens et al., 2024).

<sup>2</sup> [https://www.google.com/goto?url=CAESTQHrOzAVCqSfKw4PtqgYcze0mRA8zH7LSBYTa-lGxVXdFbaAMNes3\\_gEysCsoNZj6j9dmmhcV1YwxISgiqL0a40nteC3eyQ\\_xjhoDmD](https://www.google.com/goto?url=CAESTQHrOzAVCqSfKw4PtqgYcze0mRA8zH7LSBYTa-lGxVXdFbaAMNes3_gEysCsoNZj6j9dmmhcV1YwxISgiqL0a40nteC3eyQ_xjhoDmD)

Në sektorin e mbrojtjes, kompleksiteti është edhe më i lartë. GAO raportoi në vitin 2025 se Departamenti Amerikan i Mbrojtjes mbështetet në një rrjet global me mbi 200,000 furnitorë dhe se varësia nga disa burime të huaja mund të krijojë rrezik për sigurinë kombëtare (U.S. Government Accountability Office, 2025). Kjo e zhvendos sigurinë nga kontrolli i kontraktorit kryesor te njohja e niveleve të thella të zinxhirit, origjinës së komponentëve, varësive dhe alternativave.

### ***Mikro-elektronika dhe varësitë kritike***

Mikro-elektronika është një shembull tipik i teknologjisë me rëndësi disproporcionale. Radarët, komunikimet, UAV-të, raketat, lufta elektronike dhe sistemet e komandim-kontrollit varen nga gjysmëpërçuesit. Globalizimi dhe përqendrimi i kapaciteteve të prodhimit kanë krijuar shqetësime afatgjata për aksesin e besueshëm në mikro-elektronikë të avancuar (U.S. Government Accountability Office, 2015). Në një krizë, një komponent me vlerë të ulët monetare mund të bllokojë prodhimin e një sistemi me vlerë shumë më të lartë strategjike.

### ***Spiunazhi industrial, TECHINT dhe Reverse Engineering***

Në industrinë ushtarake, dokumentacioni teknik, source code, algoritmet, parametrat e sensorëve, materialet dhe rezultatet e testimeve mund të jenë objektiv inteligjence. Vjedhja e tyre mund të shkurtojë ciklin R&D të kundërshtarit, të lehtësojë zhvillimin e kundërmasave ose të zbulojë dobësi operative. Për këtë arsye, mbrojtja e pronësisë intelektuale në sektorin e mbrojtjes nuk është vetëm interes ekonomik; ajo është çështje e ruajtjes së avantazhit ushtarak.

TECHINT dhe *Reverse Engineering* krijojnë një problem tjetër: çdo pajisje që eksportohet ose përdoret në operacione duhet të konsiderohet potencialisht e ekspozuar ndaj analizës kundërshtare. Kjo kërkon technology protection by design: minimizim të ekspozimit të panevojshëm, arkitekturë modulare, kontroll të aksesit diagnostik, menaxhim të çelësave kriptografikë dhe ndarje të teknologjive kritike sipas nevojës për njohje.

### ***Insider threat dhe inxhinieria sociale e fuqizuar nga AI***

Digjitalizimi rrit fuqinë e përdoruesit të autorizuar. Një inxhinier, administrator sistemi ose teknik mund të ketë akses në volume të mëdha informacioni teknik. Kërcënimi i brendshëm mund të lidhet me motivim financiar, shantazh, pakënaqësi, rekrutim, ideologji ose neglizhencë. Për pozicionet kritike, verifikimi vetëm në momentin e punësimit është i pamjaftueshëm; kërkohet vlerësim periodik, ndarje detyrash dhe zbatim rigoroz i parimit least privilege. Inteligjenca artificiale e rrit cilësinë e

inxhinierisë sociale duke mundësuar personalizim të shpejtë, klonim zanor, deepfake dhe komunikime bindëse. Kjo dobëson besueshmërinë e sinjaleve tradicionale të autenticitetit. Në mjedisin e mbrojtjes, kërkesat sensitive duhet të verifikohen përmes kanaleve të pavarura dhe procedurave të paracaktuara, pavarësisht se sa autentik duket komunikimi.

#### **IV. Mundësitë strategjike dhe modeli i industrisë të së ardhmes**

##### ***Demokratizimi i inovacionit dhe teknologjitë dual-use***

Një pjesë e inovacionit me rëndësi ushtarake zhvillohet jashtë kontraktorëve tradicionalë të mbrojtjes. Software-i, robotika, mikro-elektronika, teknologjitë hapësinore dhe AI janë sektorë ku industria civile ka ritëm të lartë inovacioni. NATO e ka institucionalizuar këtë realitet përmes DIANA-s, e cila lidh kompani dual-use me financim, accelerator sites, mbi 200 qendra testimi dhe mundësi validimi në mjedise relevante (NATO DIANA, 2026). Kjo krijon mundësi të veçanta për shtetet e vogla si Shqipëria. Ato nuk kanë nevojë të konkurrojnë në të gjithë spektrin e industrisë së rëndë. Mund të specializohen në segmente ku kapitali njerëzor, integrimi i software-it dhe shpejtësia e inovacionit kanë peshë më të madhe se madhësia e fabrikës.

##### ***Nga prototipi te prodhimi***

Një nga dobësitë klasike të inovacionit ushtarak është hendeku ndërmjet demonstruesit teknologjik dhe kapacitetit të prokuruar. Rapid Adoption Action Plan synon ta reduktojë këtë hendek, ndërsa SYNC 2026 e lidh inovacionin drejtpërdrejt me procedura më të shkathëta prokurimi dhe me rrugë të qarta nga testimi drejt blerjes (NATO, 2025a; NATO, 2026b). Strategjia e re parashikon gjithashtu NATO Engine, një rrjet që synon të lidhë kompani inovative që kanë nevojë të rrisin prodhimin me prodhues dhe fabrika që disponojnë kapacitet fleksibël, përfshirë modelin *factory-for-hire* (NATO, 2026b). Ky koncept e ndan pjesërisht funksionin e projektimit nga pronësia e kapacitetit prodhues dhe mund të shkurtojë rrugën nga prototipi te prodhimi masiv.

##### ***Gatishmëria industriale si pjesë e gatishmërisë ushtarake***

Konflikti me intensitet të lartë rikthen rëndësinë e sasisë, rezervave, municioneve dhe pjesëve këmbimi. Një sistem shumë i avancuar por i pamundur për t'u zëvendësuar në kohë mund të krijojë avantazh të përkohshëm, jo domosdoshmërisht qëndrueshmëri. SYNC 2026 kërkon kapacitete prodhuese fleksibël, mundësi për *surge production*, rezerva dhe ushtrime table-top për të testuar reagimin industrial në skenarë me kërkesë të lartë (NATO, 2026b). Kjo formalizon idenë se gatishmëria industriale është pjesë e gatishmërisë së mbrojtjes.

## ***Perspektiva e Bashkimit Evropian***

European Defence Industrial Strategy vendosi objektiva të matshëm për një bazë industriale më të integruar. Të paktën 40% të pajisjeve do të prokurohen në mënyrë bashkëpunuese deri në vitin 2030, tregtia brenda BE-së do të arrijë të paktën 35% të vlerës së tregut të mbrojtjes dhe do të rritet gradualisht pjesa e buxheteve të prokurimit e shpenzuar brenda BE-së (European Commission & High Representative, 2024). White Paper 2025 dhe Readiness Roadmap 2030, e shtyjnë më tej qasjen drejt mbylljes së boshllëqeve të kapaciteteve dhe forcimit të EDTIB (European Commission & High Representative, 2025; European Commission, 2025).

Për vendet evropiane më të vogla, rëndësia e këtyre politikave është se integrimi në zinxhirë shumëkombësh mund të jetë më realist sesa ndërtimi kombëtar i sistemeve të plota. Prodhimi i komponentëve të certifikuar, mirëmbajtja, software-i dhe nën-sistemet mund të krijojnë vlerë industriale dhe rol strategjik në aleancë.

## **V. Implikimet për Shqipërinë**

### ***Nevojitet specializim inteligjent, jo imitimi i fuqive të mëdha***

Për Shqipërinë, një strategji realiste duhet të shmangë objektivin e prodhimit të plotë në çdo kategori dhe të fokusohet te segmentet ku kombinimi i kërkesës, kapitalit njerëzor dhe interoperabilitetit krijon avantazh. Modeli më i përshtatshëm është specializimi inteligjent në fusha të zgjedhura, me objektiv integrimin në zinxhirët industrialë NATO/BE. Industria moderne nuk zhvillohet vetëm përmes fabrikave. Ajo kërkon një ekosistem ku Ministria e Mbrojtjes dhe Forcat e Armatosura shpallin nevojën operative dhe strukturat përgjegjëse për industrinë krijojnë kuadrin e licencimit, standardizimit dhe koordinimit. Më pas kompanitë zhvillojnë produktin, universitetet dhe qendrat kërkimore si IKSHU QISMI sigurojnë dije dhe kapital njerëzor ndërsa partnerët NATO/BE ofrojnë standarde, testim, financim dhe tregje. Cikli ideal duhet të jetë; Kërkesë operationale, kërkesë teknike, prototip, feedback i operatorit, certifikim dhe në fund prodhim. Për Shqipërinë, institucionalizimi i këtij cikli do të ishte më me vlerë sesa financimi i projekteve të izoluar pa rrugë të qartë drejt përdorimit.

### ***Security by design dhe siguria industriale***

Rritja e industrisë së mbrojtjes rrit gjithashtu vlerën e saj si objektiv inteligjence i aktorëve dhe i influencës së huaj. Për këtë arsye, siguria duhet të integrohet që në projektim dhe licencim, jo të shtohet pas ndërtimit të kapaciteteve. Modeli duhet të përfshijë sigurinë fizike, të personelit, informacionit, kibernetike, OT/ICS, të zinxhirit të furnizimit, mbrojtjen e

pronësisë intelektuale, *business continuity* dhe *technology protection*.

Në të njëjtën kohë nevojitet kulturë e spiunazhit industrial dhe njohje e ekspozimit të personelit kritik, kontroll i aksesit sipas *need-to-know*, menaxhim i vizitorëve dhe kontraktorëve, vlerësim i furnitorëve, mbrojtje e projekteve teknike dhe mekanizma raportimi për tentativa rekrutimi, inxhinieri sociale ose interesa të pazakonta ndaj teknologjive kritike.

Anëtarësimi në NATO dhe procesi i integritetit evropian krijojnë një avantazh institucional. Standardet NATO, mekanizmat DIANA<sup>3</sup>, politikat e reja industriale dhe nevoja për diversifikim të furnizimit krijojnë hapësirë për furnitorë jotradicionalë. Për një ekonomi të vogël, objektivi “të prodhojmë një komponent kritik dhe të certifikuar të një sistemi shumëkombësh” mund të jetë më realist dhe më i qëndrueshëm se objektivi “të prodhojmë të gjithë sistemin”.

## Përfundime

*Së pari*, shpejtësia e përshtatjes teknologjike dhe luftarake po bëhet atribut i fuqisë ushtarake. Një teknologji që nuk mund të përditësohet shpejt humbet vlerën përballë kundërmasave. *Së dyti*, konflikti me intensitet të lartë rikthen rëndësinë e masës dhe të kapacitetit për zëvendësim. High-tech dhe mass nuk janë alternativa, por dimensione që duhet të balancohen. *Së treti*, industria civile e teknologjisë është tashmë pjesë e ekosistemit të fuqisë ushtarake, sidomos në IA, software, mikroelektronikë dhe robotikë.

*Së katërti*, siguria dhe inovacioni nuk mund të trajtohen si politika të ndara. Sa më e vlefshme teknologjia, aq më e lartë vlera e saj si objektivi për spiunazh, manipulim, ndërhyrje ose sabotim. Së pesti, kapaciteti industrial ka funksion parandalues. Një kundërshtar duhet të llogarisë jo vetëm stokun ekzistues të një aleance, por edhe aftësinë e saj për të zëvendësuar humbjet, rritur prodhimin dhe zhvilluar kundërmasa.

Kjo sugjeron një ndryshim në mënyrën e matjes së fuqisë industriale. Treguesit klasikë, si numri i fabrikave, punonjësve dhe kapaciteti nominal, duhet të plotësohen me kohën e prototipizimit, shpejtësinë e certifikimit, kohën e *scale-up*, diversifikimit të furnizimit, sigurinë kibernetike, aftësinë për *update software* dhe kapacitetin për të ruajtur pronësinë intelektuale.

Transformimi digjital po ndryshon në mënyrë strukturore industrinë ushtarake. Në modelin e shekullit XX, fuqia industriale lidhej kryesisht me fabrikat, makineritë, lëndët e para dhe fuqinë punëtore. Në modelin e shekullit XXI, këtyre u shtohen software-i, të dhënat, algoritmet, mikro-elektronika,

<sup>3</sup> <https://www.google.com/goto?url=CAESUwHrOzAVQBqSILI64x5oFjDT7quzTcO1ufNFriZUyC3eXbhfQv5eyhxV-wAz2Fepqke88BsVwHQa1ZV9seuWHZhvgc5GBGWTG9yINPb02cqECAJ>

pronësia intelektuale, arkitekturat e hapura, siguria kibernetike dhe ritmi i inovacionit. Rastet e analizuara tregojnë se avantazhi teknologjik është gjithnjë e më pak statik. Ai konsumohet nga kundërmasat dhe duhet rigjeneruar përmes cikleve të shpejta të testimit, feedback-ut dhe modifikimit. Në të njëjtën kohë, inovacioni nuk shndërrohet automatikisht në fuqi ushtarake: ai duhet të jetë i certifikueshëm, i prokurueshëm, i prodhueshëm në shkallë dhe i mbrojtur nga komprometimi.

Në këtë kuptim, teza e studimit konfirmohet në nivel analitik: avantazhi industrial ushtarak në epokën digjitale është funksion i ndërveprimit ndërmjet inovacionit, sigurisë, shkallëzimit të prodhimit dhe shpejtësisë së përshtatjes. Dobësia serioze e njërit prej këtyre elementeve mund të kufizojë vlerën e të tjerëve.

Për Shqipërinë, transformimi krijon një dritare mundësie, por kërkon realizëm strategjik. Një bazë industriale e vogël nuk duhet të konkurrojë në çdo segment. Ajo duhet të ndërtojë kompetenca të specializuara, të certifikueshme dhe të eksportueshme, të integrohet në zinxhirët euroatlantikë dhe të përdorë kapitalin njerëzor në fushat ku teknologjitë dual-use ulin barrierat tradicionale të hyrjes.

Përfundimisht, industria ushtarake e epokës digjitale nuk mund të ndahet nga siguria e ekosistemit të saj. Fabrika, software-i, furnitori, laborator, të dhënat dhe personeli janë pjesë e të njëjtës sisteme. Për këtë arsye, zhvillimi industrial dhe security by design duhet të ecin paralelisht që nga faza e parë e politikës, investimit dhe projektimit.

## **Rekomandime për Industrinë Ushtarake në Shqipëri**

1. Hartimi i një Strategjie Kombëtare për Industrinë dhe Teknologjinë e Mbrojtjes, të ndërlidhur me planifikimin e kapaciteteve të vetëfurnizimit dhe objektivat e NATO/BE.
2. Identifikimi i teknologjive, materialeve dhe komponentëve kritikë ku ekziston varësi e jashtme dhe hartimi i alternativave ose rezervave dhe krijimi i një mekanizmi të përhershëm “problem operacional – prototip – testim – feedback – certifikim – prokurim”.
3. Integrimi i standardeve të sigurisë kibernetike dhe OT/ICS si kërkesë licencimi dhe auditimi për subjektet e industrisë së mbrojtjes .
4. Zbatimi i *security by design* dhe *technology protection by design* në projektet që përmbajnë pronësi intelektuale ose teknologji sensitive.
5. Zhvillimi i kapaciteteve të industrial counterintelligence dhe procedurave të raportimit për tentativa rekrutimi, spiunazh ose inxhinieri sociale.
6. Vlerësimi periodik i sigurisë për personelin në pozicione kritike, sipas

proporcionalitetit, ligjit dhe nevojës për njohje.

7. Vendosja e kërkesave të sigurisë ndaj nënkontraktorëve dhe furnitorëve dhe krijimi i një sistemi të vlerësimit të *supply-chain* risk.
8. Zhvillimi i kapaciteteve fleksibël prodhuese për produktet e identifikuara si kritike.
9. Krijimi i kapaciteteve kombëtare për testim, kontroll cilësie dhe certifikim, me njohje sa më të gjerë të standardeve NATO/BE.
10. Mbrojtja e pronësisë intelektuale shqiptare dhe kontraktimi i qartë i të drejtave mbi të dhënat, software-in dhe rezultatet e R&D.

## Bibliografia

1. Boulanin, <https://www.sipri.org/publications/2016/working-paper/mapping-innovation-ecosystem-driving-advance-autonomy-weapon-systems>
2. Boulanin, V., & Verbruggen, M. (2017). <https://www.sipri.org/publications/2017/policy-reports/mapping-development-autonomy-weapon-systems>
3. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1, Update 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>
4. Brave1. (2026a). <https://www.brave1.gov.ua/en/>
5. Brave1. (2026b). <https://www.brave1.gov.ua/en/about>
6. European Commission. (2025). Readiness Roadmap 2030. [https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030\\_en](https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en) European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2024). A new European defence industrial strategy: Achieving EU readiness through a responsive and resilient European defence industry. European Union.
7. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025). Joint White Paper for European Defence Readiness 2030 (JOIN(2025) 120 final). European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0120>
8. Ministry of Defence of Ukraine. (2026, July 13). <https://mod.gov.ua/en/news/brave1-launches-new-grants-for-defense-technology-projects-to-strengthen-the-defence-forces-of-ukraine-s-technological-advantage-on-the-battlefield>
9. Mulchandani, N., & Shanahan, J. N. T. (2022). <https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age>

10. NATO. (2021, October 22). <https://www.nato.int/en/news-and-events/articles/news/2021/10/22/nato-releases-first-ever-strategy-for-artificial-intelligence>
11. NATO. (2022). NATO 2022 Strategic Concept. <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>
12. NATO. (2025a). Summary of NATO's Rapid Adoption Action Plan. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/summary-of-natos-rapid-adoption-action-plan>
13. NATO. (2026a). Innovation and technology adoption: Emerging and disruptive technologies. <https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies>
14. NATO. (2026b). Strategy for Industry–NATO Cooperation. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/08/strategy-for-industry-nato-cooperation>
15. NATO DIANA. (2026). Defence Innovation Accelerator for the North Atlantic. <https://www.diana.nato.int/>
16. NATO Science & Technology Organization. (2025). Science & Technology Macro Trends 2025–2045. North Atlantic Treaty Organization.
17. Sanders, G., & Holderness, A. (2021). <https://www.csis.org/analysis/readiness-open-systems-hoë-prepared-are-pentagon-and-defense-industry-coordinate>
18. U.S. Department of Defense. (2021, July 29). <https://www.defense.gov/News/News-Stories/Article/Article/2712969/dod-promotes-additive-manufacturing-expansion-standardization-training-through/>
19. U.S. Government Accountability Office. (2015). (GAO-16-185T). <https://www.gao.gov/products/gao-16-185t>
20. U.S. Government Accountability Office. (2025). (GAO-25-107283). <https://www.gao.gov/products/gao-25-107283>



## **RUBRIKA E TRETË**

**ARSIMIMI USHTARAK,  
LIDERSHIPI DHE  
ZHVILLIMI PROFESIONAL**



# Mësimdhënia e terminologjisë ushtarake përmes materialeve autentike operacionale: një qasje e bazuar në Anglishten për Qëllime Specifike

---

Dr. Manjola LIKAJ

Dr. Alma VLADI

*Departamenti i Shkencave të Komunikimit  
dhe Gjuhëve të Huaja,  
Fakulteti i Mbrojtjes dhe i Sigurisë, AFA*

## Trajtesë e shkurtuar

Rëndësia në rritje e gjuhës angleze në bashkëpunimin ushtarak shumëkombësh ka transformuar ndjeshëm fushën e mësimdhënies së Anglishtes Ushtarake. Pjesëmarrja e personelit ushtarak të Forcave të Armatosura të Shqipërisë në operacione dhe stërvitje të përbashkëta ushtarake të NATO-s, misione paqeruajtëse, si dhe në programe ndërkombëtare trajnimi, e ka bërë komunikimin efektiv përmes gjuhës angleze një domosdoshmëri strategjike. Megjithatë, qasjet tradicionale ndaj mësimdhënies së terminologjisë në disa raste nuk funksionojnë në përgatitjen e studentëve për realitetet gjuhësore të mjediseve operacionale. Ky artikull shqyrton rolin e materialeve autentike operacionale në mësimdhënien e terminologjisë ushtarake brenda kornizës së Anglishtes për Qëllime Specifike (AQS). Studimi analizon se si dokumentet autentike ushtarake, raportet taktike, udhëzimet e operacioneve, transkriptet e komunikimeve me radio dhe materialet e bazuara në strukturat e NATO-s kontribuojnë në përvetësimin e fjalorit, motivimin e studentëve ushtarakë, kuptimin kontekstual dhe kompetencën komunikuese.

Artikulli përdor një model kërkimi me metoda të përziera që përfshin një grup studentësh ushtarakë që ndjekin në kurset e Anglishtes Ushtarake në Fakultetin e Mbrojtjes dhe Sigurisë (FMS), në Akademinë e Forcave të Armatosura (AFA), Tiranë. Të dhënat sasiore u mblodhën përmes testeve paraprake para fillimit të kursit dhe testeve pasuese në përfundim të tij,

*që matnin përvetësimin e terminologjisë, ndërsa të dhënat cilësore u morën përmes vëzhgimit në klasë. Gjetjet tregojnë se materialet autentike operacionale përmirësojnë ndjeshëm përvetësimin e terminologjisë, kuptimin kontekstual dhe aftësitë gjuhësore të studentëve në komunikimin operacional. Studimi gjithashtu nxjerr në pah disa sfida, duke përfshirë mbingarkesën njohëse, kompleksitetin e zhargonit ushtarak dhe kufizimet e aksesueshmërisë që lidhen me materialet e klasifikuara. Artikulli arrin në përfundimin se materialet autentike operacionale ofrojnë një urë efektive midis të mësuarit në klasë dhe komunikimit ushtarak në botën reale dhe për këtë arsye, këtë lloj materialesh, duhet të bëhen një komponent kryesor i mësimdhënies së Anglishtes Ushtarake.*

**Fjalë kyçe:** Anglishtja Ushtarake, Anglishtja për Qëllime Specifike, materialet autentike, terminologjia ushtarake, komunikimi operacional i NATO-s, STANAG 6001, përvetësimi i terminologjisë.

## Hyrje

Gjuha angleze është bërë gjuha dominuese e komunikimit ushtarak ndërkombëtar. Në aleancat shumëkombëshe si NATO-ja, gjuha angleze funksionon si gjuhë e përbashkët operacionale e përdorur në stërvitjet e përbashkëta, ndarjen e informacioneve të inteligjencës, udhëzimet e strukturave komanduese, operacionet paqeruajtëse dhe bashkëpunimin ushtarak ndërkombëtar. Si rrjedhim, nga personeli ushtarak pritet jo vetëm të zotërojnë aftësi të përgjithshme të gjuhës angleze, por edhe të zotërojnë terminologjinë e specializuar ushtarake dhe diskursin operacional.

Kërkesa në rritje për mësimdhënien efektive të Anglishtes Ushtarake i ka nxitur studiuesit dhe personelin akademik të rishqyrtojnë metodat tradicionale të mësimdhënies së terminologjisë. Qasjet konvencionale të mësimdhënies shpesh mbështeten në memorizimin, listat e izoluara të terminologjisë dhe ushtrimet gramatikore pa kontekst të përcaktuar. Edhe pse këto metoda mund të mbështesin memorizimin afatshkurtër, ato shpesh nuk funksionojnë në zhvillimin e kompetencës praktike komunikuese të kërkuar në mjedise autentike operacionale.

Anglishtja për Qëllime Specifike thekson rëndësinë e mësimdhënies gjuhësore të kontekstualizuar dhe të orientuar drejt profesionit. Brenda këtij kuadri, Anglishtja Ushtarake shihet si një degë e specializuar e AQS-së e fokusuar në komunikimin operacional, terminologjinë ushtarake, ndërveprimin taktik dhe diskursin profesional. Një nga strategjitë më efektive në mësimdhënien e AQS-së është integrimi i materialeve autentike.

Materialet autentike operacionale i referohen teksteve ushtarake të botës reale dhe burimeve të komunikimit të krijuara fillimisht për qëllime

operacionale dhe jo për përdorim edukativ. Këto materiale mund të përfshijnë dokumente informuese të NATO-s, manuale në terren, urdhra operationale, raporte ushtarake, udhëzime taktike, transkripte të komunikimeve me radio dhe buletine lajmesh ushtarake. Përdorimi i tyre në klasë u lejon studentëve të njihen me terminologjinë në kontekste reale dhe të zhvillojnë aftësi gjuhësore të lidhura ngushtë me detyrat ushtarake profesionale.

Përdorimi i materialeve autentike ka fituar vëmendje gjithnjë e më të madhe në mësimdhënien e gjuhëve, sepse nxit të nxënit kontekstual, motivimin e studentëve, kompetencën komunikuese dhe ruajtjen e fjalorit. Në mjediset ushtarake, materialet autentike janë veçanërisht të vlefshme sepse i ekspozojnë studentët ndaj kompleksitetit gjuhësor dhe gjuhës procedurale të përdorur në operatione reale.

Ky artikull studion efektivitetin e mësimdhënies së terminologjisë ushtarake përmes materialeve autentike operationale në klasat e Anglishtes Ushtarake. Studimi shqyrton se si ndikojnë këto në përvetësimin e terminologjisë, motivimin, kuptimin kontekstual dhe aftësitë e komunikimit operacional të studentëve.

Objektivat e studimit janë:

1. Të eksplorohet roli i materialeve autentike operationale në mësimdhënien e Anglishtes Ushtarake.
2. Të shqyrtohet efektiviteti i tyre në mësimdhënien e terminologjisë ushtarake.
3. Të identifikohen përfitimet dhe sfidat e përdorimit të materialeve autentike në klasat e Anglishtes Ushtarake.
4. Të propozohen rekomandime metodologjike për lektorët e Anglishtes Ushtarake.

Artikulli argumenton se materialet autentike operationale e përmirësojnë ndjeshëm të nxënit e Anglishtes Ushtarake duke e lidhur mësimdhënien në klasë me komunikimin e vërtetë operacional.

## **I. Rishikimi i literaturës**

### ***Anglishtja për Qëllime Specifike***

Anglishtja për Qëllime Specifike është një degë e mësimdhënies së gjuhëve të huaja e hartuar për të përmbushur nevojat profesionale dhe akademike të studentëve në fusha të specializuara. Sipas Hutchinson dhe Waters (1987), AQS-ja përqendrohet në kërkesat specifike komunikuese të studentëve dhe jo në kompetencën e përgjithshme gjuhësore. Në mësimdhënien e AQS-së, të mësuarit e gjuhëve të huaja është i lidhur ngushtë me detyrat profesionale dhe diskursin profesional.

Anglishtja Ushtarake përfaqëson një formë të specializuar të AQS-së sepse përfshin terminologjinë, procedurat e komunikimit dhe modelet e diskursit specifik për kontekstet ushtarake. Ndryshe nga mësimdhënia e përgjithshme e gjuhës angleze, mësimdhënia e Anglishtes Ushtarake synon t'i përgatisë studentët për detyra operacionale, të tilla si informacionet për misionet, koordinimin taktik, komunikimin në raste emergjente, raportimin e inteligjencës dhe bashkëpunimin shumëkombësh.

Metodologjia e AQS-së thekson origjinalitetin e materialeve mësimore, analizën e nevojave të studentëve dhe kompetencën komunikuese. Dudley-Evans dhe St John (1998) argumentojnë se materialet autentike janë thelbësore në AQS sepse i ekspozojnë studentët ndaj gjuhës aktuale të përdorur në mjediset profesionale.

Në mjediset ushtarake, mësimdhënia e Anglishtes Ushtarake duhet të marrë në konsideratë edhe saktësinë dhe qartësinë operacionale. Komunikimi në formë të gabuar në kontekste ushtarake mund të çojë në dështimin e operacioneve ose edhe në humbje jete. Si rrjedhim, mësimdhënia e Anglishtes Ushtarake kërkon trajnim gjuhësor shumë të specializuar dhe realist.

### ***Anglishtja Ushtarake si komunikim i specializuar***

Anglishtja Ushtarake ndryshon ndjeshëm nga Anglishtja e Përgjithshme sepse funksionon brenda mjediseve profesionale dhe operacionale shumë të specializuara. Ajo karakterizohet nga terminologji specifike, shprehje procedurale, shkurtesa, akronime, struktura komanduese dhe modele diskursi të hartuara për të siguruar komunikim efikas dhe të saktë gjatë operacioneve ushtarake. Ndryshe nga komunikimi i përditshëm, diskursi ushtarak i jep përparësi saktësisë, qartësisë dhe standardizimit, pasi keqkuptimet në kontekstet operacionale mund të çojnë në dështim të misionit ose rrezik operacional (Hutchinson & Waters, 1987).

Komunikimi ushtarak është i lidhur ngushtë me detyrat operacionale, të tilla si planifikimi i misionit, raportimi i informacioneve të inteligjencës, koordinimi taktik, reagimi ndaj emergjencave, operacionet paqeruajtëse dhe bashkëpunimi shumëkombësh. Si rezultat, Anglishtja Ushtarake përfshin një gamë të gjerë fjalori teknik dhe formash gjuhësore institucionale që rrallë hasen në mësimdhënien e Anglishtes së Përgjithshme (Dudley-Evans & St John, 1998).

Një nga tiparet përcaktuese të Anglishtes Ushtarake është përdorimi i gjerë i akronimeve dhe shkurtesave. Personeli ushtarak shpesh mbështetet në forma të shkurtuara për të komunikuar shpejt dhe me efikasitet në kushte kritike. Shembuj të zakonshëm përfshijnë:

- SOP (Procedurat Standarde të Veprimit).

- ROE (Rregullat e Angazhimit).
- CASEVAC (Evakuimi i Viktimave).
- IED (Pajisjet Shpërthyesë të Improvizuar).
- SITREP (Raporti për Situatën).
- AO (Zona e Operacioneve).
- MEDEVAC (Evakuimi Mjekësor).

Këto shkurtime formojnë një komponent thelbësor të komunikimit operacional dhe pasqyrojnë preferencën ushtarake për shkëmbim informacioni konciz dhe të shpejtë. Sipas Smith (2017), diskursi ushtarak mbështetet shumë në terminologjinë standarde dhe format e shkurtuara në mënyrë që të sigurojë qartësi dhe ndërveprim gjatë operacioneve shumëkombëshe.

Anglishtja Ushtarake përmban gjithashtu gjuhë procedurale dhe shprehje formale të përdorura në komunikimin që zhvillohet në linjën e komandimit. Komandat, njoftimet, paralajmërimet dhe transmetimet me radio shpesh ndjekin struktura gjuhësore standarde të hartuara për të zvogëluar paqartësinë dhe për të përmirësuar koordinimin operacional. Shprehje të tilla si “hold position” (ruaj pozicionin), “maintain radion silence” (mos transmeto në radio) ose “request immediate support” (kërko mbështetje të menjëhershme) mbartin kuptime operationale shumë specifike që kërkojnë kuptim kontekstual (Walker, 2015).

Një tjetër karakteristikë e rëndësishme e Anglishtes Ushtarake është struktura e diskursit të saj operacional. Komunikimi ushtarak është shpesh hierarkik dhe i orientuar drejt misionit, duke theksuar drejtpërdrejtshmërinë dhe efikasitetin në vend të përpunimit. Në shumë situata operationale, komunikimi duhet të ndodhë shpejt dhe në kushte me shumë presion psikologjik. Si pasojë, personeli ushtarak pritet ta përpunojë dhe ta prodhojë gjuhën e synuar shpejt dhe saktë. Sipas standardeve të komunikimit të NATO-s, efektiviteti operacional varet shumë nga procedurat e standardizuara të komunikimit dhe saktësia gjuhësore (NATO STANAG 6001, 2010). Sipas Seidlhofer (2011), personeli ushtarak nga prejardhje të ndryshme gjuhësore dhe kulturore duhet të komunikojë në mënyrë efektive duke përdorur terminologjinë operationale standarde, në mënyrë që të koordinohen sipas standardeve të përcaktuara.

Korniza e STANAG 6001 e NATO-s thekson rëndësinë e aftësisë gjuhësore në kontekste ushtarake. STANAG 6001 përcakton nivele të standardizuara të aftësisë gjuhësore për personelin ushtarak që merr pjesë në operacione shumëkombëshe dhe misione ndërkombëtare. Korniza thekson kompetencën komunikuese në aftësitë e të dëgjuarit, të folurit, leximit dhe shkrimit, veçanërisht në situata të rëndësishme operationale (NATO STANAG 6001, 2010).

Aftësitë e të dëgjuarit dhe të folurit janë veçanërisht të rëndësishme sepse komunikimi ushtarak ndodh shpesh përmes transmetimeve me radio, udhëzimeve, koordinimit të emergjencave dhe ndërveprimit operacional në kohë reale. Ky lloj komunikimi shpesh zhvillohet në mjedise stresuese, të zhurmshme dhe të ndjeshme ndaj kohës, ku keqkuptimi mund të ketë pasoja serioze. Si rrjedhim, personeli ushtarak duhet të jetë i aftë të kuptojë të folurit në mënyrë të shpejtë, udhëzimet procedurale dhe terminologjinë e specializuar nën presion (Smith, 2017).

Studiuesit e Anglishtes Ushtarake dhe AQS-së kanë argumentuar se metodat tradicionale të mësimdhënies së gjuhëve të huaja shpesh janë të pamjaftueshme për përgatitjen e studentëve për komunikim autentik ushtarak. Qasjet konvencionale të bazuara në tekstet shkollore zakonisht thjeshtojnë gjuhën dhe e paraqesin fjalorin në mënyrë të izoluar, gjë që mund të mos pasqyrojë kompleksitetin e diskursit të vërtetë operacional. Mësimi përmendësh i listave të terminologjisë nuk siguron kompetencë komunikuese në mjediset ushtarake (Gilmore, 2007).

Për këtë arsye, shumë studiues mbështesin përdorimin e diskursit operacional realist dhe materialeve ushtarake autentike në mësimdhënien gjuhësore. Ekspozimi ndaj udhëzimeve të misionit, raporteve taktike, manualeve në terren, transkripteve të komunikimit me radio dhe skenarëve operacionalë u mundëson studentëve të zhvillojnë kompetencën gjuhësore dhe aftësitë e komunikimit profesional (Dudley-Evans & St John, 1998).

Si rrjedhim, mësimdhënia e Anglishtes Ushtarake duhet të shkojë përtej qasjeve tradicionale të fokusuara në gramatikë dhe të përvetësojë metodologji komunikuese, të bazuara në detyra dhe të orientuara drejt kontekstit. Këto lloj qasjesh i përgatitin më mirë studentët për realitetet gjuhësore të operacioneve ushtarake moderne dhe bashkëpunimit ndërkombëtar.

### ***Materialet autentike në mësimdhënien e Anglishtes Ushtarake***

Materialet autentike në përgjithësi përcaktohen si tekste, regjistrime audio, materiale vizuale ose burime komunikimi të krijuara për qëllime të jetës reale dhe jo posaçërisht për mësimdhënie në klasë. Në edukimin gjuhësor, materialet autentike i ekspozojnë studentët ndaj gjuhës që shfaqet natyrshëm dhe përdoret nga folësit vendas ose profesionistë në kontekste reale komunikuese. Ndryshe nga materialet e thjeshtuara të teksteve shkollore, burimet autentike pasqyrojnë modele të vërteta diskursi, përdorim të fjalorit, variacion stilistik dhe kuptim kontekstual (Nunan, 1999).

Studiuesit në përvetësimin e gjuhës së dytë dhe mësimdhënien e AQS-së kanë theksuar vazhdimisht vlerën pedagogjike të autenticitetit në të nxënit e gjuhës. Sipas Gilmore (2007), materialet autentike u ofrojnë studentëve

njohjen me “gjuhën e vërtetë” dhe kapërcejnë mangësitë që ekzistojnë midis mësimdhënies në klasë dhe komunikimit në botën reale. Ato gjithashtu rrisin motivimin e studentëve sepse studentët i perceptojnë materialet si të rëndësishme për nevojat e tyre të ardhshme profesionale.

Në kontekstet e AQS-së, autenticiteti është veçanërisht i rëndësishëm sepse mësimdhënia e gjuhës duhet të pasqyrojë kërkesat aktuale komunikuese të një profesioni ose disipline specifike. Dudley-Evans dhe St John (1998) argumentojnë se mësimdhënia e AQS-së duhet të jetë e lidhur ngushtë me nevojat profesionale të studentëve dhe duhet të përfshijnë diskursin profesional dhe detyrat e specializuara të komunikimit. Anglishtja Ushtarake, si një degë e specializuar e AQS-së, kërkon që studentët të kuptojnë terminologjinë shumë specifike, komunikimin procedural, diskursin operacional dhe konventat gjuhësore institucionale. Për këtë arsye, integrimi i materialeve autentike operacionale është veçanërisht i vlefshëm në mësimdhënien e Anglishtes Ushtarake.

Materialet autentike operacionale në mësimdhënien e Anglishtes Ushtarake mund të përfshijnë:

- urdhrat operacionalë,
- udhëzimet e strukturave të NATO-s,
- manualët në terren,
- raportet taktike,
- transkriptet e komunikimeve me radio,
- artikujt e lajmeve ushtarake,
- dokumentet e planifikimit të misionit,
- raportet pas veprimit,
- përmbledhjet e inteligjencës,
- procedurat standarde të operimit (SOP),
- raportet e misionëve paqeruajtëse,
- hartat dhe diagramet ushtarake,
- komunikimin e reagimit ndaj emergjencave,
- raportet e vlerësimit të rrezikut,
- planet e dislokimit ushtarak,
- raportet e zbulimit dhe vëzhgimit,
- komunikimet gjatë stërvitjeve ushtarake,
- procedurat e evakuimit mjekësor (MEDEVAC),
- dokumentet e koordinimit operacional ,

- raportet e incidenteve ushtarake,
- udhëzimet për menaxhimin e krizave,
- komunikimet në qendrat komanduese,
- brifingjet para misionit dhe pas misionit,
- dokumentet e logjistikës ushtarake,
- raportet e patrullimit,
- komunikimet e operacioneve paqeruajtëse,
- raportet e sigurisë dhe mbrojtjes,
- komunikimet e emergjencës në terren,
- dokumentet e bashkëpunimit shumëkombësh,
- raportet e inteligjencës operacionale,
- protokollet e komunikimit taktik,
- udhëzimet për rregullat e angazhimit (ROE),
- skenarët e simulimeve ushtarake.

Këto materiale i ekspozojnë studentët ndaj realiteteve gjuhësore të komunikimit ushtarak. Ndryshe nga dialogët artificialë të teksteve shkollore, tekstet autentike ushtarake përmbajnë terminologji, shkurtesa, shprehje procedurale dhe struktura operacionale të vërteta të përdorura nga profesionistët ushtarakë (Smith, 2017).

Një nga avantazhet kryesore të materialeve autentike është promovimi i të mësuarit të fjalorit kontekstual. Përvetësimi i fjalorit bëhet më efektiv kur studentët hasin terminologjinë brenda situatave kuptimplote komunikuese sesa përmes memorizimit të izoluar. Nation (2001) thekson se ekspozimi ndaj fjalorit kontekstual mbështet një përpunim më të thellë leksikor dhe një kujtesë më të fortë. Për shembull, termat ushtarakë si “reconnaissance” (zbulim), “deployment” (dislokim), “engagement” (angazhim) ose “rules of engagement” (rregullat e angazhimit) fitojnë kuptim më të qartë kur paraqiten në raportet taktike ose në udhëzimet e misionit.

Mësimi kontekstual gjithashtu mbështet memorizimin në terma afatgjatë. Teoritë konjitive të të mësuarit të gjuhës sugjerojnë që fjalori i të mësuarit brenda konteksteve kuptimplote ka më shumë gjasa të mbahet mend dhe të transferohet në detyra reale komunikimi (Ellis, 2003). Në mësimdhënien e Anglishtes Ushtarake, kjo është veçanërisht e rëndësishme sepse komunikimi operacional kërkon kuptim të menjëhershëm dhe përdorim të saktë të terminologjisë në situata operacionale.

Një tjetër avantazh i materialeve autentike është rritja e motivimit të studentëve. Studentët dhe personeli ushtarakë janë më të angazhuar kur

materialet mësimore lidhen drejtpërdrejt me përgjegjësitë e tyre profesionale dhe detyrat e ardhshme operacionale. Gilmore (2007) vëren se materialet autentike krijojnë një ndjenjë realizmi që rrit perceptimin e studentëve për rëndësinë dhe dobinë e detyrave.

Motivimi është veçanërisht i rëndësishëm në mjediset e AQS-së, sepse studentët shpesh e vlerësojnë mësimdhënien e gjuhës sipas vlerës së saj praktike. Studentët ushtarakë kanë tendencë t'u përgjigjen pozitivisht detyrave të rëndësishme operacionale, siç janë analiza e misionit, ushtrimet për komunikimet me radio, udhëzimet taktike dhe raportet e situatës (Hutchinson & Waters, 1987).

Materialet autentike kontribuojnë gjithashtu ndjeshëm në zhvillimin e kompetencës komunikuese. Sipas parimeve të mësimdhënies së gjuhës në mënyrë komunikative të propozuara nga Canale dhe Swain (1980), studentët duhet të zhvillojnë aftësinë për të përdorur gjuhën në mënyrë efektive në situata reale komunikuese. Dokumentet autentike ushtarake i vendosin studentët në kontekstet e mëposhtme:

- komunikime procedurale,
- udhëzime operacionale,
- strukturat e komandës,
- modelet e ndërveprimit profesional,
- konventat e diskursit ushtarak,
- shkëmbimin e shpejtë të informacionit,
- koordinimin e misioneve shumëkombëshe,
- raportimin e incidenteve dhe situatave operative,
- planifikimin taktik dhe strategjik,
- komunikimin gjatë emergjencave,
- procedurat e sigurisë dhe mbrojtjes,
- analizën e inteligjencës ushtarake,
- komunikimin në qendrat komanduese,
- operacionet paqeruajtëse dhe humanitare,
- procedurat e evakuimit dhe mbështetjes logjistike,
- brifingjet operacionale,
- komunikimet me radio në terren,
- menaxhimin e krizave operacionale.

Përmes ekspozimit të përsëritur, studentët njihen me strukturat e diskursit dhe strategjitë e komunikimit që përdoren zakonisht në mjediset ushtarake. Për më tepër, materialet autentike i ndihmojnë studentët të zhvillojnë

kompetencën pragmatike. Komunikimi ushtarak shpesh kërkon gjuhë koncize, të drejtpërdrejtë dhe shumë të strukturuar. Studentët duhet të kuptojnë jo vetëm kuptimet e fjalorit, por edhe se si funksionon gjuha brenda konteksteve operacionale. Tekstet autentike zbulojnë se si personeli ushtarak jep komanda, raporton incidente, koordinon veprimet dhe shkëmben informacionet taktike (Walker, 2015).

Një përfitim tjetër i rëndësishëm është zhvillimi i kompetencës komunikuese ndërkulturore. Operacionet moderne ushtarake shpesh përfshijnë bashkëpunim shumëkombësh brenda organizatave të tilla si NATO ose misionet paqeruajtëse të Kombeve të Bashkuara. Byram (1997) argumenton se materialet autentike i ekspozojnë studentët ndaj stileve të ndryshme të komunikimit dhe modeleve të ndërveprimit ndërkulturore. Në kontekstet ushtarake, një ekspozim i tillë është thelbësor për bashkëpunimin operacional shumëkombësh.

Pavarësisht këtyre avantazheve pedagogjike, materialet autentike paraqesin edhe disa sfida. Një sfidë e rëndësishme është kompleksiteti gjuhësor. Dokumentet autentike ushtarake shpesh përmbajnë terminologji të dendur, shkurtesa, akronime, shprehje teknike dhe struktura komplekse fjalish që mund t'i mbingarkojnë studentët, veçanërisht ata që kanë nivele më të ulëta të aftësisë gjuhësore të Anglishtes Ushtarake (Gilmore, 2007). Për shembull, raportet operative mund të përfshijnë shkurtesa shumë të specializuara, të tilla si:

- MIA (I Zhdukur në Aksion).
- POW (I Burgosur Luftë).
- QRF (Forca e Reagimit të Shpejtë).
- ISR (Zbulim, Mbikëqyrje dhe Vëzhgim).
- TOC (Qendra Operacionale Taktike).
- ETA (Koha e Parashikuar e Mbërritjes).
- KIA (I Vrarë në Aksion).
- COMMS (Komunikime).
- LZ (Zona e Uljes).
- RTO (Operator Radioje).
- UAV (Mjet Ajror pa Pilot).
- NBC (Bërthamor, Biologjik dhe Kimik).
- FOB (Baza Operacionale e Përparuar).

Një sfidë tjetër përfshin shpejtësinë dhe qartësinë e komunikimit autentik të folur. Transmetimet me radio dhe regjistrimet operacionale shpesh përmbajnë zhurmë në sfond, të folur në mënyrë të shpejtë, fjali të paplota dhe shkurtime procedurale. Edhe pse këto karakteristika pasqyrojnë komunikim ushtarak real, ato mund të krijojnë vështirësi në të kuptuar për studentët (Field, 2008).

Specifikat kulturore dhe institucionale gjithashtu mund ta ndërlikojnë të kuptuarit. Komunikimi ushtarak formësohet nga traditat institucionale, strukturat e komandës dhe procedurat operacionale që mund të ndryshojnë në vende dhe organizata ushtarake (Seidlhofer, 2011).

Për më tepër, lektorët përballen me vështirësi praktike kur zgjedhin materiale autentike. Disa dokumente ushtarake mund të jenë të klasifikuara, të kufizuara ose të paarrtshme për përdorim në mësimdhënie. Si rrjedhim, lektorët duhet të zgjedhin me kujdes burimet e deklasifikuara dhe të përshtatshme nga ana pedagogjike.

Një çështje tjetër e rëndësishme është përshtatja për mësimdhënie. Materialet autentike nuk janë hartuar për studentët që mësojnë një gjuhë të huaj. Si rrjedhim, lind nevoja që lektorët shpesh duhet të thjeshtojnë detyrat, të mësojnë terminologjinë paraprakisht dhe të ofrojnë mbështetje kontekstuale për të siguruar të kuptuarit nga ana e studentëve (Tomlinson, 2013).

Pavarësisht këtyre sfidave, shumica e studiuesve të AQS-së dhe Anglishtes Ushtarake mbështesin fort përdorimin e materialeve autentike sepse ato mundësojnë zhvillimin e aftësive dhe përgatitjen e studentëve për komunikim në botën reale. Studiuesit argumentojnë se materialet autentike operacionale krijojnë një lidhje të drejtpërdrejtë midis të mësuarit të gjuhës dhe praktikës ushtarake profesionale (Smith, 2017).

Në mësimdhënien e Anglishtes Ushtarake, autenticiteti nuk është thjesht një preferencë metodologjike, por një domosdoshmëri profesionale. Meqenëse personeli ushtarak operon në mjedise komunikimi me rreziqe të larta ku saktësia dhe qartësia janë thelbësore, ekspozimi ndaj diskursit autentik operacional është kritik për përgatitjen efektive gjuhësore.

## **II. Metodologjia**

Ky studim përdori një model kërkimor me metoda të përziera që kombinonin qasje sasiore dhe cilësore për të shqyrtuar efektivitetin e materialeve autentike operacionale në përvetësimin e terminologjisë së Anglishtes Ushtarake. Komponenti sasior mati progresin e studentëve përmes testeve paraprake para fillimit të periudhës së eksperimentit dhe pas përfundimit të saj, ndërsa komponenti cilësor eksplori perceptimet, motivimin dhe qëndrimet e studentëve ndaj materialeve mësimore.

### ***Pjesëmarrësit***

Pjesëmarrësit ishin 30 studentë ushtarakë të FMS-së, AFA, Tiranë, që ndiqnin kurset e gjuhës angleze. Aftësitë e tyre në gjuhën angleze korrespondonin afërsisht me nivelin 2 sipas STANAG 6001. Studentët u ndanë në dy grupe me madhësi të barabartë. Grupi eksperimental me 15 studentë ndoqi mësimdhënien përmes materialeve autentike operacionale, ndërsa grupi

i kontrollit po me 15 studentë ndoqi mësimdhënien tradicionale të bazuar në tekstet shkollore.

### ***Instrumentet kërkimore***

Të dhënat u mbledhën duke përdorur teste dhe vëzhgimet në klasë. Testet para fillimit të periudhës eksperimentale dhe testet pasuese në përfundim të kësaj periudhe iu dhanë të dy grupeve para dhe pas periudhës mësimore për të matur njohjen e fjalorit ushtarak, kuptimin e akronimeve, kuptimin kontekstual dhe përdorimin e terminologjisë operacionale. Testet përfshinin pyetje me alternativa, ushtrime me lidhje për fjalorin, ushtrime me plotësim të hapësirave bosh dhe skenarë të shkurtër operacionale.

Vëzhgimi në klasë u krye gjatë gjithë periudhës mësimore për të monitoruar pjesëmarrjen e studentëve ushtarakë, modelet e ndërveprimit, përdorimin e terminologjisë, angazhimin dhe performancën komunikuese.

### ***Materiale mësimore***

Grupi eksperimental përdori materiale autentike operacionale, duke përfshirë udhëzime të NATO-s, urdhra operacionesh, manuale në terren, raporte taktike, transkripte të komunikimeve me radio, lista të akronimeve ushtarake, dokumente të planifikimit të misioneve etj.

Nga ana tjetër, grupi i kontrollit përdori tekstet tradicionale të Anglishtes Ushtarake që përmbanin tekste të thjeshtuara të synuara për mësimdhënie dhe ushtrime të izoluara terminologjike.

### ***Procedura***

Studimi u krye gjatë tetë javëve. Gjatë javës së parë, pjesëmarrësit plotësuan testin paraprak. Nga java e dytë deri në javën e shtatë, të dy grupet morën pjesë në seancat e mësimdhënies së terminologjisë dhe aktiviteteve me qasje komunikative. Grupi eksperimental u angazhua në detyra të kontekstualizuara duke përdorur materiale autentike operacionale, duke përfshirë lojëra me role, punë në çift, punë në grup dhe ushtrime analize terminologjike, ndërsa grupi i kontrollit ndoqi aktivitete konvencionale të bazuara në tekstet shkollore. Javën e fundit, pjesëmarrësit zhvilluan testin përfundimtar.

## **III. Analiza e rezultateve**

Analiza e të dhënave tregon se të dy grupet përmirësuan njohuritë e tyre të terminologjisë së Anglishtes Ushtarake gjatë periudhës mësimore; megjithatë, përmirësimi i arritur nga grupi eksperimental ishte dukshëm më i lartë.

Në fillim të studimit, të dy grupet demonstuan një nivel të ngjashëm performance. Grupi eksperimental mori një rezultat mesatar para testit prej 52.3, ndërsa grupi i kontrollit shënoi 51.8. Diferenca midis dy grupeve në fazën fillestare ishte minimale, duke treguar njohuri bazë të krahasueshme.

Pas periudhës eksperimentale të mësimdhënies së synuar drejt terminologjisë me materiale autentike operacionale, grupi eksperimental arriti një rezultat mesatar pas testit prej 85.6, që përfaqëson një rritje prej 63.7% në performancë. Në krahasim me grupin eksperimental, grupi i kontrollit arriti një rezultat mesatar pas testit prej 68.4, që korrespondon me një rritje prej 32.0%. Këto rezultate tregojnë se grupi i ekspozuar ndaj materialeve autentike operacionale u përmirësua afërsisht dy herë më shumë sesa grupi që mësoi përmes mësimdhënies tradicionale të bazuar në tekstet shkollore.

Analiza e elementëve të tjerë zbuloi gjithashtu ndryshime të rëndësishme midis grupeve. Njohja e fjalorit në grupin eksperimental u përmirësua me 34%, krahasuar me 17% në grupin e kontrollit. Grupi eksperimental gjithashtu tregoi dukshëm performancë më të mirë në kuptimin e akronimeve dhe përdorimin e terminologjisë operacionale.

Në bazë të vëzhgime të kryera në klasë, përmirësimi më i madh u vu re në të kuptuarit kontekstual. Studentët e ekspozuar ndaj materialeve autentike operacionale treguan aftësi më të fortë për të interpretuar terminologjinë në situata reale operacionale, ndërsa grupi i kontrollit tregoi kryesisht përmirësim në nivelin e njohjes.

Pavarësisht rezultateve pozitive, u identifikuan disa sfida. Përafërsisht 42% e studentëve fillimisht përjetuan vështirësi në kuptimin e terminologjisë së specializuar dhe shkurtesave ose akronimeve ushtarake. Megjithatë, këto vështirësi u ulën gradualisht ndërkohë që studentët u njohën më shumë me gjuhën autentike operacionale.

Në përgjithësi, analiza tregon se materialet autentike operacionale patën një ndikim të fortë pozitiv në përvetësimin e terminologjisë së Anglishtes Ushtarake, angazhimin e studentëve dhe kuptimin e gjuhës kontekstuale. Gjetjet sugjerojnë se materialet autentike janë dukshëm më efikase sesa mësimdhënia tradicionale e bazuar në tekstet shkollore në zhvillimin e kompetencës gjuhësore operacionale.

#### **IV. Përfundime**

Ky artikull shqyrtoi rolin e materialeve autentike operacionale në mësimdhënien e terminologjisë ushtarake në kuadër të Anglishtes Ushtarake si një degë e AQS-së. Studimi u përqendrua në analizimin e ndikimit të materialeve autentike në përvetësimin e terminologjisë ushtarake, zhvillimin e kompetencës komunikuese dhe rritjen e angazhimit të studentëve gjatë procesit mësimor. Rezultatet e studimit treguan se përdorimi i dokumenteve autentike operacionale ndihmon studentët të kuptojnë terminologjinë ushtarake jo vetëm në nivel teorik, por edhe në kontekste reale komunikimi dhe përdorimi profesional.

Gjetjet e studimit tregojnë se integrimi i materialeve autentike operacionale rrit ndjeshëm përvetësimin e terminologjisë ushtarake, kuptimin kontekstual, motivimin dhe angazhimin e studentëve. Duke i ekspozuar studentët ndaj diskursit real operacional, materialet autentike krijojnë një lidhje të drejtpërdrejtë midis mësimdhënies në klasë dhe komunikimit real ushtarak. Studentët e ekspozuar ndaj këtyre materialeve demonstruan rezultate më të larta në përdorimin e terminologjisë, në interpretimin e situatave operative dhe në aftësinë për të komunikuar në mënyrë më të saktë dhe profesionale.

Studimi tregoi gjithashtu se përdorimi i aktiviteteve ndërvepruese, si lojërat me role, puna në çift dhe në grup, detyrat e analizës së terminologjisë, ushtrimet e aftësisë së dëgjimit dhe simulimet operacionale, kontribuon ndjeshëm në zhvillimin e aftësive komunikuese dhe profesionale të studentëve. Këto aktivitete krijojnë një mjedis më dinamik dhe praktik të të nxënit, duke i ndihmuar studentët të përdorin terminologjinë ushtarake në situata që pasqyrojnë realitetin operacional. Për më tepër, materialet autentike rrisin ndërgjegjësimin e studentëve për strukturat e komunikimit ushtarak, procedurat standarde dhe format profesionale të ndërveprimit.

Megjithatë, studimi evidentoi edhe disa sfida që lidhen me përdorimin e materialeve autentike. Kompleksiteti i terminologjisë ushtarake, përdorimi i shpeshtë i akronimeve dhe shkurtesave, si dhe vështirësia e disa dokumenteve autentike mund të krijojnë pengesa për studentët me nivele më të ulëta të gjuhës. Gjithashtu, aksesueshmëria e kufizuar e disa materialeve operative dhe nevoja për përshtatje pedagogjike mbeten sfida të rëndësishme për instruktorët e Anglishtes Ushtarake. Megjithatë, përfitimet e përgjithshme të materialeve autentike rezultuan dukshëm më të mëdha sesa vështirësitë që shfaqen gjatë përdorimit të tyre në klasë.

Pavarësisht rezultateve pozitive, studimi kishte disa kufizime. Madhësia relativisht e vogël e kampionëve dhe kohëzgjatja e kufizuar e eksperimentit nuk lejojnë përgjithësime absolute për të gjitha kontekstet e mësimdhënies së Anglishtes Ushtarake. Për këtë arsye, studimet e ardhshme mund të përfshijnë grupe më të mëdha pjesëmarrësish, periudha më të gjata eksperimentale dhe analiza krahasuese ndërmjet niveleve të ndryshme të kompetencës gjuhësore.

Në përfundim, studimi konfirmon se materialet autentike operacionale përbëjnë një mjet të rëndësishëm dhe efektiv në mësimdhënien e terminologjisë ushtarake. Në një kohë kur bashkëpunimi ushtarak ndërkombëtar po zgjerohet vazhdimisht, zhvillimi i kompetencës profesionale në Anglishten Ushtarake mbetet thelbësor për komunikimin operacional, ndërveprimin shumëkombësh dhe suksesin e misioneve ushtarake. Për këtë arsye, integrimi sistematik i materialeve autentike duhet të konsiderohet një komponent kyç i programeve mësimore të Anglishtes Ushtarake.

## Bibliografia

1. Byram, M., (1997), *Teaching and Assessing Intercultural Communicative Competence*, Multilingual Matters, fq. 34–36.
2. Canale, M. & Swain, M., (1980), “Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing,” *Applied Linguistics* 1, nr., fq. 1–47.
3. Dudley-Evans, Tony & Jo St. J. M., (1998), *Developments in English for Specific Purposes: A Multi-Disciplinary Approach*, Cambridge University Press, fq. 4–10, 171.
4. Ellis, R. (2003) *Task-Based Language Learning and Teaching*, Oxford University Press, fq. 28–29.
5. Field, J., (2008), *Listening in the Language Classroom*, Cambridge University Press, fq. 137–140.
6. Gilmore, A., (2007), “Authentic Materials and Authenticity in Foreign Language Learning,” *Language Teaching* 40, nr. 2, fq. 97–118.
7. Hutchinson, T., & Waters, A., (1987), *English for Specific Purposes: A Learning-Centered Approach*, Cambridge University Press, fq. 53–54.
8. Nation, I. S. P., (2001), *Learning Vocabulary in Another Language*, Cambridge University Press, fq. 84–85.
9. NATO Standardization Agency, (2010), *STANAG 6001: Language Proficiency Levels*, NATO Standardization Agency, 1–3, B-1.
10. NATO Standardization Office. (various publications). *Standardization Agreements (STANAGs)*.
11. Nunan, D., (1999), *Second Language Teaching and Learning*, Heinle & Heinle, fq. 27–28.
12. Seidlhofer, B., (2011), *Understanding English as a Lingua Franca*, Oxford University Press, fq. 7–9, 84–86.
13. Smith, M., (2017). *On the Applications of Computer-Assisted Language Learning in a Military English Context*, University of Bath, fq. 5–10.
14. Tomlinson, B., (2013), *Developing Materials for Language Teaching*, 2nd ed., Bloomsbury, fq. 5–7.
15. Walker, P., (2015), *Effective Communication in Military Operations*, Routledge, fq. 40–43.



# Koncepti Platonian mbi edukimin ushtarak dhe integrimi në strukturat ushtarake moderne

---

**Dr. Blerina KUQI**

**Msc. Marsida MINGA**

*Fakulteti i Mbrojtjes dhe i Sigurisë, AFA*

## **Trajtesë e shkurtuar**

*Ky artikull synon të bëjë një analizë të ushtrisë moderne sipas pikëpamjes së Platonit, të shprehur në veprën e tij “Republika”, në të cilën ai flet për edukimin ushtarak dhe klasën e “rojtarëve”. Kohët moderne kërkojnë që ushtria të ketë më tepër ekspertizë dhe profesionalizëm. Në teorinë e Platonit edukimi nuk reduktohet thjesht tek ekspertiza apo teknika, por themeli i tij është morali. Ai evidenton dy virtyte të rëndësishme “vetëpërmbytjen” dhe “drejtësinë” që i përgjigjen arsyes, të cilat janë aktuale dhe të domosdoshme në formësimin e ushtarakëve të sotëm.*

*Artikulli synon një qasje teorike dhe analitike, duke u nisur nga këto dy virtyte për t'i integruar në modelin modern të trajnimeve ushtarake dhe se si mund të implementohen ato sot. Pyetjet kërkimore që ngrihen janë: së pari, si ndikojnë këto virtyte në formimin e karakterit dhe të vlerave të brendshme të ushtarakut në mënyrë që njësitë të jenë të mirëorientuara? Së dyti, si rikonceptohet ushtria moderne nga pikëpamja e edukimit të Platonit nëpërmjet mekanizmave racionalë?*

*Ky punim ka si qëllim që, nëpërmjet një analize historiko-analitike, të argumentojë se njësitë ushtarake mund të jenë më eficiente nëpërmjet edukimit moral dhe racionalizimit të forcës. Një njësi ushtarake e udhëhequr nga arsyeja respekton më mirë hierarkinë dhe i shërben më mirë sigurisë kombëtare. Ne mbështetemi te modeli Platonian për të treguar se si edukimi i shërben kapërcimit të logjikës militariste, duke krijuar një dialog ndërmjet periudhës antike dhe debatit bashkëkohor mbi ushtrinë moderne.*

**Fjalët kyçe:** Platoni, edukim ushtarak, virtyt, racionalizim, siguri kombëtare.

## Metodologjia

Ky artikull mbështetet në një metodologji cilësore të një natyre interpretuese, qasja mbetet filozofike dhe konsiston në analizën e veprës “Republika” të Platonit, një vepër me ndikim në rrafshin etik dhe politik. Në të argumentohet mbi edukimin ushtarak dhe frymën morale të një shteti të drejtë. Ky punim ka për qëllim të analizojë, së pari, edukimin ushtarak nga pikëpamja e lexuar në veprën e Platonit dhe orientimin e këtij edukimi përkundrejt vlerave si kuraja dhe virtyti, disiplina dhe bindja. Së dyti, do të realizohet një analizë krahasuese e këtij themeli teorik, të cilin e gjejmë në mendimin e Platonit, me kontekstin e edukimit ushtarak në ditët e sotme.

Analiza krahasuese nuk do të orientohet drejt të dhënave sasiore apo empirike, por do të mbetet në rrafshin teorik, duke konsideruar konceptet filozofike të gjetura në këtë vepër për t’i integruar në kontekstin bashkëkohor të debateve ndërmjet studiuesve të fushës. Analiza cilësore do të jetë në mbështetje të pyetjeve kërkimore të ngritura në këtë punim.

## Hyrje

**K**y punim përbën një kontribut teorik përsa i përket edukimit në kontekstin ushtarak. Edukimi përbën një ndër shtyllat e rëndësishme të ushtrisë, e cila në vetvete është pjesë e pandarë e çdo shteti. Ndër mendimtarët e antikitetit ne gjejmë në mendimin e Platonit lidhjen ndërmjet edukimit ushtarak, shtetit dhe virtytit si komponentë që kanë një lidhje organike në emër të shtetit të së drejtës. Në filozofinë e Platonit merr kuptim formimi i forcave ushtarake jo vetëm në edukimin fizik, por mbi të gjitha në kultivimin e disa vlerave në emër të së mirës së përgjithshme. Këto vlera janë guximi, disiplina, drejtësia. Siç shprehet dhe studiuesja e Platonit, Annas: “drejtësia është virtyt i qytetit si bashkësi, ku secili qytetar jep kontributin për të mirën e përbashkët”<sup>1</sup>.

Në vizionin e tij për “polisin” të cilin ne e lexojmë në veprën “Republika”, por edhe të “Ligjet”, sepse këto janë vepra të cilat duhen lexuar së bashku, Platoni flet për edukimin e klasës së “gardianëve”, edukimi i të cilëve konsistonte me një frymë morale që kontribuon në aktet e mbrojtjes së vendit. Sipas tij, ushtaraku ngrihet në nivelin e gjykimit moral si një subjekt i disiplinuar, por edhe me vetë-kontroll.

Sigurisht që këto ide janë të lidhura me kontekstin historik të shkrimit të veprës dhe të situatave publike të asaj periudhe, por mjaft parime filozofike kanë ndikim edhe në aktualitetin tonë sot. Ky punim hedh tezën se edukimi

<sup>1</sup> Julia Annas, *An Introduction to Plato's Republic*, (New York: Oxford University Press, 1981), f.119.

ushtarak modern kërkon jo vetëm kompetenca operacionale, por në ushtrimin e lidhshimit kanë vlerë edhe gjykimi etik si orientues i një vendimmarrjeje të drejtë.

Perspektiva e këtij punimi është cilësore nisur nga shfrytëzimi i parimeve filozofike në kontekstin e objektivave të edukimit ushtarak modern. Analiza e parimeve filozofike të Platonit hedh dritë mbi modele të edukimit ushtarak dhe të lidhshimit, duke argumentuar se integrimi i vlerave është një kontribut në filozofinë e edukimit ushtarak.

## **I. Koncepti i Platonit mbi edukimin**

Në veprën e tij “Republika” Platoni na paraqet konceptin e edukimit si një vizion të gjerë që lidhet me jetën e mirë në “polis”. Sipas tij vetëm nëpërmjet edukimit mund të përmbushet e mira për qytetarin.

Për këtë arsye kjo vepër shërben si pikë referimi për analizën cilësore në nivel interpretues që ne do t’i bëjmë edukimit ushtarak nga pikëpamja e një mendimtari antik. Sigurisht që mendimi modern dhe postmodern e kanë kapërcyer qasjen Platoniane, duke i shërbyer më së shumti kërkesave të kohës, duke e lidhur edukimin më tepër me studimin e subjektit nga pikëpamja psikologjike se sa nga ajo filozofike. Mendimi antik ishte i lidhur ngushtë me moralin dhe etikën. Dilemat e kohës sonë bëjnë që ne të kthejmë edhe njëherë vëmendjen tek mendimtarët antikë për t’u fokusuar te mësimet e moralit. Po ashtu edhe te “Ligjet” një vepër tjetër me rëndësi e Platonit ku trajtohet shteti dhe principet mbi të cilat duhet të ndërtohet një shtet i mirë, sërish edukimi zë një vend parësor për jetën e qytetarëve.

Këto vepra na bëjnë të mendojmë se shqetësimi për çështjet e edukimit është i hershëm. Në qoftë se do të bënim një vlerësim racional të idesë së shtetit ideal dhe personifikimit që Platoni bën në nivelet e shpirtit do të përfitonim një hierarki me disa nivele të çmontuara më pas në nivelin individual të qytetarit brenda shtetit. Në këtë mënyrë evidentojmë shpirtin dëshirues i personifikuar me fshatarët dhe artizanët, shpirtin guximtar me luftëtarët dhe shpirti i arsyeshëm që lidhet me urtësinë dhe mendimin.

Në qasjen Platoniane ne gjejmë konceptin e rëndësishëm të drejtësisë, të barasvlershëm me “harmoninë” pasi për të “drejtësi do të thotë harmoni”. Drejtësia bëhet kështu një ndër virtytet dhe burimet më të rëndësishme të një shteti. “Harmonia është drejtësia, në kuptimin që gjithçka është në vendin që i takon në një hierarki të drejtë”<sup>2</sup>. Kjo frazë na bën të kuptojmë se çdo hierarki është e drejtë kur secili nga nivelet përmbush qëllimet dhe arrin të ruajë harmoninë nëpërmjet vetëpërmbytjes. Drejtësia mund të konsiderohet e

---

<sup>2</sup> Zhanë Hersh, *Habia Filozofike* shqipëroi Artan Fuga, (Tiranë: Dituria, 1993), f. 31.

përmbushur në një shtet në momentin që hierarkia i bindet arsyes.

Kështu çështjet e edukimit janë të lidhura ngushtë me shtetin dhe me qytetarin. Një shtet bëhet i drejtë kur ka qytetarë të mirë edukuar dhe të vetëpërmbytur. Qytetarë të cilët udhëhiqen nga arsyeja dhe nga virtyti e bëjnë një shtet më të drejtë pasi në mendimin platonian jeta publike është e lidhur me moralin dhe për pasojë qytetarë të tillë do të kenë aftësinë për të jetuar të vërtetën dhe për ta identifikuar atë.

## II. Edukimi ushtarak nga pikëpamja e Platonit

Platoni analizon ata të cilët do të mbronin shtetin duke i cilësuar si rojtarë ose “gardianët”, të cilët zotëronin guximin, por njëkohësisht duhet të kishin edhe vetëpërmbytje. Analiza e tij lidhet me çështjen se si duheshin edukuar ata. “Zhvillimi moral i njeriut shkon krahas ngritjes së tij intelektuale, sepse rritja e shkallës së njohjes shton dashurinë për të vërtetën, bukurinë dhe mirësinë”<sup>3</sup>. Sipas studiuesit Shtumph, Platoni e konsideron moralin dhe disiplinën në radhët e ushtrisë si jetike për fatet e saj “me pa evitueshmërinë e luftës, tani do të jetë e nevojshme të kesh një ushtri të tërë për të shkuar në betejë me një pushtues dhe do të ruajnë rregullin e brendshëm”<sup>4</sup>.

Në analizën e përgjithshme të edukimit evidentohet dhe një virtyt tjetër që është ai i “vetëpërmbytjes”. Platoni e parashtron këtë si një ndër virtytet me të cilat duhet të edukohen “rojtaret”. Në shpirtin e tyre dallohen tre nivele, niveli i guximit, niveli i urtësisë si një ndër cilësitë e mendimit filozofik, por edhe vetëpërmbytja, e cila i shërben edhe edukimit të karakterit moral. Këtë ide e gjejmë edhe tek Aristoteli, në mendimin etik të të cilit gjëja e duhur gjendet tek “e mesmja e artë”. “Ashtu si virtyti ngrihet ndërmjet teprisë dhe mungesës ashtu edhe guximi ngrihet ndërmjet nxitimit dhe frikës, ndërsa vetëpërmbytja qëndron ndërmjet kënaqësisë dhe mungesës së ndjeshmërisë”<sup>5</sup>. Në këtë mënyrë një ushtarak kryen funksionin e tij duke qenë një ushtarak i denjë. “Edukimi të cilin ai promovon ndihmon shpirtin të kuptojë natyrën e tij të vërtetë”<sup>6</sup>.

Edukimi i “rojtareve” kërkon edhe një formim në art, (muzikë) krahas edukimit fizik dhe të dyja këto i shërbejnë guximit dhe vetëpërmbytjes, pasi forcojnë mendjen, shpirtin, por edhe trupin. Në librin e dytë të Republikës

<sup>3</sup> Samuel Enoch Stumpf, *Filozofia, Historia & Problemet* shqipëroi Kastriot Myftiu, Paqësor Shehu, (Tiranë: Botimet Toena), f. 65.

<sup>4</sup> *Po aty*, f. 68.

<sup>5</sup> Aristotle, *Nicomachean Ethics* VI, (1140a24–1140b30).

<sup>6</sup> Bompas Smith, *Plato and modern education*. (Oxford University Press. The Monist, vol.33, No2 April 1923), f. 161-183; f.169 [https:// www.jstor.org/stable/27900943](https://www.jstor.org/stable/27900943) Accessed on 15 April 09:24:47 UTC

ngrihet pyetja “Cili do të jetë ky edukim? Ky edukim mos vallë do të jetë e vështirë të gjendet një më i mirë nga ai që është gjetur tashmë prej kohësh? Ky edukim përbëhet nga gjimnastika për trupin dhe nga muzika për shpirtin”<sup>7</sup>. Në mendimin politik të Platonit edukimi ushtarak përbën një ndër çështjet më me rëndësi duke përfaqësuar kështu një hapësirë nëpërmjet së cilës qytetarët do të përmbushin detyrat e tyre në polis. Ideja e tij për këtë formë edukimi nuk i përgjigjet vetëm aspektit teknik të përgatitjes ushtarake, por ky konceptim shkon deri tek formimi moral, intelektual dhe qytetar. Në thelb qëllimi mbetet formimi individual i qytetarëve ku forca fizike të orientohej nga arsyeja dhe kuraja për të luftuar në emër të drejtësisë dhe të mirës publike.

Ashtu sikurse te “Ligjet”, por edhe te “Republika” lexohet se edukimi është mekanizmi i parë nëpërmjet të cilit mund të arrihet drejtësia në një shtet. Edukimi ushtarak i takon kryesisht klasës së rojtarëve, e cila ka për detyrë të ruajë rregullin e brendshëm, por edhe ta mbrojë atë nga kundërshtarët e jashtëm. Platoni thekson se edukimi ushtarak duhet të shkojë njëkohësisht me urtësinë filozofike, me moralin dhe nxitja për të ushtruar forcën duhet t’i përgjigjet arsyes. Sipas këtij modeli ushtaraku përfaqëson një subjekt veprimet e të cilit udhëhiqen nga virtyti dhe jo nga pasionet apo interesat personale.

Edukimi i rojtarëve përfshin dy fusha sipas tij, edukimin fizik që forcon trupin dhe zhvillon disiplinën dhe qëndrueshmërinë. Nga ana tjetër është muzika që nënkupton, artet duke kontribuar në formimin e karakterit të ushtarakut, duke i dhënë më shumë kontroll mbi veten dhe ndjeshmëri për të drejtën. Këto dy fusha edukimi do të ndikonin në ruajtjen e ekuilibrave ndërmjet trupit dhe shpirtit.

Në themel të teorisë së Platonit qëndron bindja se guximi përbën një virtyt racional që merr rëndësi kur udhëhiqet nga arsyeja dhe ushtrohet në përputhje me drejtësinë. Vetëpërmbytja nuk përbën frikë në këtë rast, por një sens për të mirën. Për këtë arsye disiplina nënkupton bindje ndaj një gjykimi të arsyeshëm, ku forca përdoret vetëm për qëllime të drejta politike dhe kjo përbën shprehjen praktike të virtytit.

Platoni e konsideron sigurinë e “polisit” si të pandashëm nga thelbi moral i atyre që kanë përgjegjësinë për ta mbrojtur atë. Kjo qasje i jep karakter politik veprimit të orientuar drejt të mirës së përgjithshme, ku veprimet nuk udhëhiqen nga ambicia personale, por nga e mira e përbashkët. Edukimi ushtarak me themel formimin e karakterit të virtytshëm dhe të vetëpërmbytjes i shërben ruajtjes së pushtetit politik dhe ushtarak.

Madje te vepra “Ligjet”<sup>8</sup> edukimi ushtarak është zgjatim i formimit të çdo

<sup>7</sup> Platoni, *Republika* shqipëroi Artur Zheji, (CEU & Shtëpia e Librit, 1999), f. 80.

<sup>8</sup> Platon, *Ligjet* shqipëroi Robert Kosova, (Tiranë: Plejad, 2018), Libri I.

qytetari ku përgatitja nënkuptohet si përgjegjësi duke e ngritur atë në nivelin e një subjekti racional në mbrojtje të drejtësisë së shtetit ideal. Mbrojtja e polisit merr kështu karakter etik.

### **III. Përfshirja e konceptit Platonian në praktikën bashkëkohore ushtarake**

Edukimi ushtarak sot është mjaft i lidhur me termat si teknologji, mjedis, ekonomi, por asnjëherë nuk duhet harruar lidhja me termat e etikës dhe të përgjegjësisë. Ashtu siç shprehet dhe autori Hartle përgjegjësia dhe gatishmëria janë arsyeja e vetë ekzistencës së ushtrisë, gjithmonë në mbrojtje të sigurisë kombëtare<sup>9</sup>. Një lidhje e tillë merr përgjigje në veprën e Platonit dhe shtrihet deri në kohët që jetojmë, pasi themeli moral dhe teorik mbeten aktual. Mjedisi ushtarak sot vepron në një asimetri të raportit forcë-gatishmëri-përgjigje. Ajo çfarë kërkon ky punim të arrijë është pikërisht implikimi moral në këtë raport dhe ngritja e hipotezës se oficerët duhet të jenë të edukuar me gjykim moral dhe të njohin vlerat të cilat pretendojnë se mbrojnë. Kjo hipotezë nuk synon të provojë se oficeri duhet të jetë subjekt i moralit, por se figura e tij nuk mund të jetë e përjashtuar nga botëkuptimi moral dhe nga koncepti i drejtësisë.

Platoni përcaktonte në edukim koncepte si guxim, vetëpërmbytje, drejtësi. “Nëse i mbahemi pastaj parimit të parë të vendosur bashkërisht sipas të cilit rojtarët tanë, të çliruar nga çdo detyrë tjetër, duhet të jenë vetëm mbrojtës të zot të lirisë së shtetit, duke e bërë të vetmen detyrë të tyre dhe duke mos u marrë me asnjë punë tjetër që nuk lidhet me këtë qëllim, ose nëse do të imitojnë ndonjë send në rini të tyre, kjo ka për të qenë diçka nga karakteret që i përshtaten profesionit të tyre si guximi, vetëpërmbytja, mëshira, shpirtmadhësia dhe virtyte të tjera si këto por ata nuk do të imitojnë asgjë që është e ulët dhe e turpshme”<sup>10</sup>. Këto koncepte kanë shënuar profesionin e ushtarakut në shumë ushtri ndërkombëtare. Sfidat e lidërshipt që has forca e armatosur kryqëzohen me interesa me natyrë etike. Ushtritë moderne përballen sot me terma si kontrolli civil, të drejtat e njeriut, transparenca, intelijenca artificiale etj.

Në qoftë se ne do të përfshinim teorinë e Platonit në ushtrinë e sotme, do të arrinim në përfundimin se virtyti nënkupton më tepër vlera ushtarake të cilat mundësojnë krijimin e traditës ushtarake. Guximi sot do të nënkuptonte më tepër operacionalitet, dija do të ishte e barasvlershme me lidërshiptin strategjik dhe vendimmarrjen strategjike. Drejtësia do të nënkuptonte krijimin e një mjedisi operacional që mbron më tepër të drejtat e njeriut. Disiplina nënkupton sot njësi të organizuara mirë dhe respektim i hierarkisë ushtarake.

<sup>9</sup> Anthony E Hartle, *Moral Issues in Military Decision Making*, 2nd edition, (Lawrence, KA: University Press of Kansas, 2004), f. 37-38.

<sup>10</sup> Platoni, *Republika...*, f. 108.

“Përveç kurrikulës me fokus tek parimet morale, studimet e rasteve dhe virtytet e bazuara në individ, personelit duhet ti mësohet natyra dhe vlera e drejtësisë dhe e vetëpërmbytjes dhe të inkurajohet t’i promovojë ato”<sup>11</sup>. Duke u mbështetur në një qasje të tillë vlerësojmë si mjaft të dobishëm kontributin teorik të veprës së Platonit në organizimin e strukturave ushtarake në ditët e sotme.

## Përfundime

Filozofia e edukimit ushtarak përbën rrafshin etik dhe moral të ndërtimit të subjektivit ushtarak dhe të mënyrës se si duhet të ndërtohen dhe organizohen nga pikëpamja hierarkike njësitë ushtarake. Boshti i mendimit Platonian thekson se në këtë kontekst nuk ka vetëm rëndësi ekspertiza teknike, por njohja si element konjitiv të të ushtruarit të detyrës së ushtarakut, e cila është sfiduese dhe ndonjëherë e paparashikueshme, Kjo tezë na bën që të rikthehemi tek teori antike si Platoni në formën e një dialogu me të tashmen, për të krijuar lidhjet e edukimit racional të ushtarakut sot. Kjo është edhe hipoteza që u ngrit dhe u analizua në mënyrë teorike dhe interpretative në këtë punim.

Sigurisht nuk kërkohet implementimi praktik i këtyre koncepteve ashtu siç ne i gjejmë në antikitet, sepse çdo implikim praktik nuk është thjesht një lidhje cilësore me teorinë së cilës i përgjigjet, por duhen marrë parasysh rrethanat dhe sistemi organizativ në kohën që organizohet një strukturë ushtarake.

Rekomandimi i këtij punimi lidhet me konkluzionin se, vlerat morale mund të shërbejnë në çdo rrethanë dhe formësojnë edukimin ushtarak në çdo kohë. Në një botë ku teknologjia ka ndikim të fuqishëm edhe në mënyrën se si ne perceptojmë sot mbrojtjen, kompleksiteti i dilemave morale që parashtrihen e bën teorinë e Platonit relevante dhe mjaft të dobishme edhe në ditët e sotme. Evidentimi se fuqia ushtarake duhet të orientohet nga arsyeja filozofike shfaqet shumë eficient. Kjo teori ofron një kornizë konceptuale për të kuptuar më mirë lidhjen ndërmjet ekspertizës ushtarake dhe përgjegjësisë etike në rrafshin e drejtësisë dhe sigurisë kombëtare.

## Bibliografia

1. Annas, Julia, *An Introduction to Plato's Republic* (New York: Oxford University Press, 1981).
2. Aristotle, *Nicomachean ethics* (T. Irwin, Trans., 2nd ed. Hackett Publishing, 1999).

---

<sup>11</sup> Jim Robinson, *Plato and the Virtues of Military Units*, *Journal of Military Ethics*, (2014 13:2, 190-202, DOI: 10.1080/15027570.2014.944359), f.199.

3. Hartle, Anthony E, *Moral Issues in Military Decision Making*, 2nd edition, (Lawrence, KA: University Press of Kansas, 2004).
4. Hersh, Zhanë, *Habia Filozofike shqipëroi Artan Fuga*, (Tiranë: Shtëpia Botuese Dituria, 1993).
5. Platoni, *Ligjet shqipëroi Robert Kosova*, ( Tiranë: Plejad, 2018).
6. Platoni, *Republika shqipëroi Artur Zheji*, (CEU & Shtëpia e Librit,1999).
7. Robinson Jim, *Plato and the Virtues of Military Units*, *Journal of Military Ethics*, (2014 13:2, 190-202, DOI: 10.1080/15027570.2014.944359).
8. Smith, Bompas, *Plato and modern education*. (Oxford University Press. The Monist, vol.33, No2 April 1923). Pp. 161-183. Pp.169 [https:// www.jstor.org/stable/27900943](https://www.jstor.org/stable/27900943)
9. Stumpf, Samuel Enoch, *Filozofia, Historia & Problemet shqipëroi Kastriot Myftiu*, Paqësor Shehu, (Tiranë: Botimet Toena).

# Transformimi i edukimit ushtarak bashkëkohor përmes integritit të inteligjencës artificiale

---

**Msc. Edgen MURATI**

*Akademia e Forcave të Armatosura*

## **Trajtesë e shkurtuar**

*Transformimi i arsimit të lartë ushtarak në kushtet e një mjedisi sigurie gjithnjë e më kompleks kërkon adoptimin e qasjeve inovative që ndërthurin teknologjinë me pedagogjinë bashkëkohore. Ky punim shqyrton rolin e inteligjencës artificiale dhe sistemeve inteligjente të mësimdhënies në përmirësimin e procesit të edukimit ushtarak, me fokus në zhvillimin e aftësive menaxhuese në kuadër të zhvillimit të teknologjisë dhe atë të mbrojtjes, vendimmarrjes në kohë reale dhe përgatitjes për skenarë kompleksë operativë.*

*Nëpërmjet një analize të literaturës dhe praktikave bashkëkohore në institucionet e arsimit ushtarak, studimi identifikon potencialin e teknologjive, si: mësimi i personalizuar përmes inteligjencës artificiale (AI), simulimet virtuale dhe sistemet adaptive të trajnimit për të rritur efektivitetin dhe fleksibilitetin e procesit mësimor. Gjithashtu, trajtohen sfidat që lidhen me integrimin e këtyre teknologjive, përfshirë aspektet etike, teknike dhe organizative.*

*Punimi synon të kontribuojë në krijimin e një kornize konceptuale për transformimin e edukimit ushtarak në përputhje me standardet bashkëkohore të sigurisë dhe kërkesat e ndërveprueshmërisë ndërkombëtare në kuadër të partneritetit me vendet e NATO-s.*

**Fjalë kyçe:** Inteligjenca artificiale, edukimi ushtarak, transformimi digjital, sisteme inteligjente të mësimdhënies, simulim virtual, vendimmarrje, siguri kibernetike, NATO, mësimi i personalizuar, modernizimi i mbrojtjes.

## Hyrje

Transformimi i arsimit ushtarak në epokën digjitale po ndikohet ndjeshëm nga zhvillimi dhe integrimi i inteligjencës artificiale (IA), e cila po shndërrohet në një nga teknologjitë më të rëndësishme për sigurinë dhe mbrojtjen moderne. Në nivel ndërkombëtar, organizata si NATO e konsiderojnë IA si një teknologji kyçe që ndikon në të gjitha dimensionet e operacioneve ushtarake, duke përfshirë mbrojtjen kolektive, menaxhimin e krizave dhe sigurinë bashkëpunuese. (Christie & Ertan, 2021; Clement, 2024)

Në këtë kontekst, përdorimi i IA nuk kufizohet vetëm në operacione luftarake, por shtrihet gjithnjë e më shumë edhe në edukimin ushtarak, përmes integritit të sistemeve inteligjente të mësimdhënies, simulimeve virtuale dhe analizës së të dhënave në kohë reale. Institucionet ushtarake të vendeve anëtare të NATO-s po investojnë në transformimin e metodave tradicionale të trajnimit drejt modeleve të bazuara në teknologji, me qëllim rritjen e efikasitetit dhe përgatitjes së personelit për skenarë kompleksë operativë. (Szabadföldi, 2021)

Një element thelbësor në këtë proces është zhvillimi i një kuadri të përgjegjshëm për përdorimin e inteligjencës artificiale. Sipas studimeve mbi implikimet e IA në kontekstet ushtarake, përdorimi i saj kërkon një qasje të strukturuar që merr në konsideratë aspektet etike, ligjore dhe strategjike, duke përfshirë kontrollin njerëzor dhe përgjegjshmërinë në vendimmarrje. (Ertan, 2022)

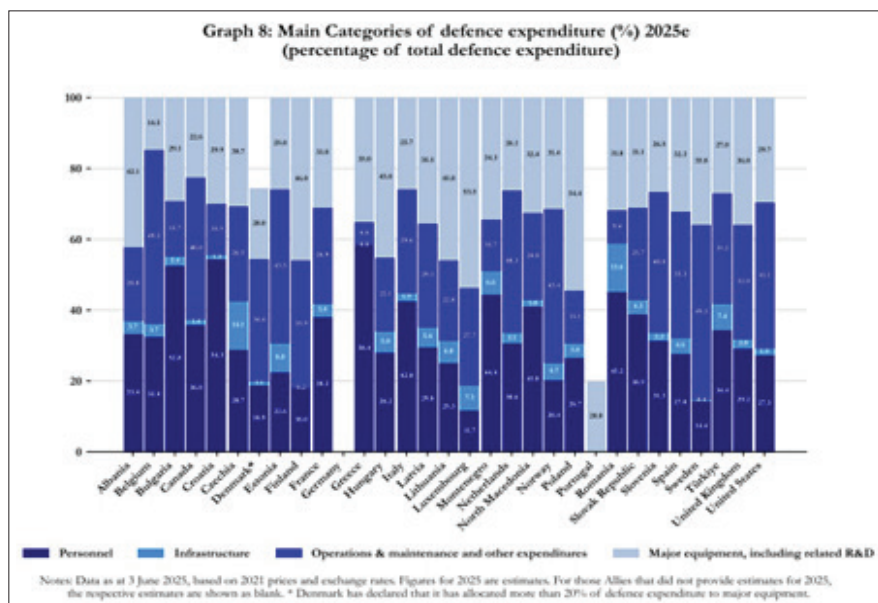


Figura 1. Shpërndarja e shpenzimeve të mbrojtjes sipas kategorive kryesore për vendet anëtare të NATO-s.

*Vihet re një pjesë e konsiderueshme e buxhetit e dedikuar për pajisje kryesore dhe kërkim-zhvillim (R&D), duke reflektuar orientimin drejt modernizimit dhe adoptimit të teknologjive të avancuara, përfshirë inteligjencën artificiale.*

*Burimi: <https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2025-en.pdf>*

Në rastin e Shqipërisë, si vend anëtar i NATO-s, këto zhvillime reflektohen në përpjekjet për modernizimin e Forcave të Armatosura dhe përshtatjen e sistemit të edukimit ushtarak me standardet e Aleancës. Megjithatë integrimi i IA-së është ende në faza zhvillimi, orientimi drejt transformimit digjital dhe adoptimit të teknologjive të avancuara përbën një prioritet strategjik në kuadër të rritjes së kapaciteteve profesionale dhe ndërveprueshmërisë ndërkombëtare. (Alex, 2022)

Në këtë kuadër, analiza e përdorimit aktual të inteligjencës artificiale në edukimin ushtarak, si në nivel ndërkombëtar ashtu edhe në kontekstin shqiptar, paraqet një rëndësi të veçantë për të kuptuar drejtimin e zhvillimeve të ardhshme dhe sfidat që shoqërojnë këtë transformim.

## **I. Kuadri teorik dhe literatura**

Zhvillimi i inteligjencës artificiale (IA) ka sjellë transformime të thella në mënyrën se si krijohet dhe transmetohet dija, duke ndikuar ndjeshëm në sistemet arsimore dhe në sektorin e mbrojtjes. Në literaturën bashkëkohore, IA përkufizohet si një sistem teknologjik që simulon procese njohëse njerëzore, përfshirë të mësuarit, arsyetimin dhe vendimmarrjen, përmes analizës së të dhënave dhe përdorimit të algoritmeve të avancuara. (Russell & Norvig, 2016). Në kontekstin ushtarak, këto aftësi janë thelbësore për përpunimin e shpejtë të informacionit dhe reagimin në situata komplekse operacionale. (Szabadföldi, 2021)

Një nga konceptet më të rëndësishme të lidhura me IA në arsim është mësimi i personalizuar (adaptive learning), i cili bazohet në përdorimin e sistemeve inteligjente për të përshtatur përmbajtjen mësimore sipas nevojave individuale të nxënësve. Sipas studimeve të Holmes dhe Luckin (2016), sistemet adaptive mund të përmirësojnë ndjeshëm rezultatet e të nxënit dhe të rrisin angazhimin e studentëve, duke krijuar përvoja më efektive dhe të personalizuar të mësimit. Në edukimin ushtarak, kjo qasje është veçanërisht e rëndësishme për zhvillimin e aftësive specifike dhe përgatitjen për skenarë të ndryshëm operative. (Christie & Ertan, 2021)

Një dimension tjetër kyç është përdorimi i simulimeve virtuale dhe teknologjive imersive, si realiteti virtual (VR) dhe realiteti i shtuar (AR). Këto teknologji mundësojnë krijimin e mjediseve të kontrolluara dhe të sigurta për zhvillimin e trajnimeve komplekse, duke reduktuar kostot dhe rreziqet

e trajnimeve tradicionale. Sipas OECD (2021), përdorimi i teknologjive digjitale në arsim dhe trajnim është rritur ndjeshëm në dekadën e fundit, duke reflektuar një zhvendosje drejt modeleve të mësimi të bazuara në teknologji. Në kontekstin ushtarak, këto zhvillime përkthehen në rritjen e efektivitetit të trajnimit dhe përgatitjes operacionale. (Ertan, 2022)

Në aspektin e vendimmarrjes, IA përdoret gjerësisht në sistemet e mbështetjes së vendimmarrjes (Decision Support Systems), të cilat analizojnë sasi të mëdha të dhënash dhe ofrojnë rekomandime në kohë reale. Sipas Russell dhe Norvig (2021), këto sisteme përmirësojnë cilësinë dhe shpejtësinë e vendimmarrjes, duke qenë veçanërisht të rëndësishme në kontekste me pasiguri të lartë. Në edukimin ushtarak, kjo kontribuon në zhvillimin e aftësive kritike të analizës dhe reagimit në situata kompleks. (Alex, 2022)

Megjithatë, literatura thekson se integrimi i IA-së në edukim dhe në sektorin ushtarak shoqërohet me sfida të rëndësishme, përfshirë transparencën e algoritmeve, etikën e përdorimit dhe nevojën për kontroll njerëzor. Sipas NATO Science and Technology Organization, përdorimi i IA-së në kontekstin ushtarak duhet të mbështetet në parime të qarta si përgjegjshmëria, besueshmëria dhe ndërveprueshmëria, duke siguruar përputhjen me normat ndërkombëtare dhe standardet etike (Reding et al., 2026). Clement (2024) thekson se zhvillimi i kornizave rregullatore dhe etike është një nga sfidat kryesore për adoptimin e IA-së në nivel institucional.

Në kontekstin shqiptar, adoptimi i këtyre koncepteve është ende në faza zhvillimi, por integrimi në strukturat e NATO-s dhe orientimi drejt modernizimit të Forcave të Armatosura krijojnë kushte të favorshme për implementimin e teknologjive inteligjente në edukimin ushtarak. Investimet në digjitalizim dhe përmirësimin e infrastrukturës teknologjike përbëjnë hapa të rëndësishëm drejt përputhjes me standardet ndërkombëtare dhe rritjes së kapaciteteve profesionale. (Alex, 2022)

## **II. Transformimi i edukimit ushtarak në kontekstin e sigurisë**

Transformimi i edukimit ushtarak duhet të analizohet në kontekstin e ndryshimeve të thella në mjedisin global të sigurisë, i cili karakterizohet nga kërcënime hibride, sulme kibernetike dhe zhvillimi i shpejtë i teknologjive të avancuara. Sipas analizave strategjike të NATO-s, këto zhvillime kërkojnë një rishikim të mënyrës se si trajnohet dhe përgatitet personeli ushtarak, duke kaluar nga modele tradicionale në qasje më fleksibël dhe të bazuara në teknologji (Christie & Ertan, 2021; Clement, 2024)

Një nga treguesit kryesorë të këtij transformimi është rritja e investimeve në sektorin e mbrojtjes, veçanërisht në teknologji dhe kërkim-zhvillim

(R&D). Të dhënat e NATO-s tregojnë se një pjesë e konsiderueshme e buxhetit të mbrojtjes në vendet anëtare i dedikohet modernizimit dhe zhvillimit të kapaciteteve teknologjike, me disa vende që investojnë mbi 20% të shpenzimeve të tyre në pajisje dhe inovacion. Ky trend reflekton rëndësinë në rritje të teknologjive si inteligjenca artificiale në përballimin e sfidave të sigurisë moderne. (Nunes et al., 2025)

Ky orientim ka ndikim të drejtpërdrejtë në edukimin ushtarak, duke kërkuar përfshirjen e aftësive të reja në kurrikula, si analiza e të dhënave, operacionet kibernetike dhe përdorimi i sistemeve autonome. Sipas OECD (2021), zhvillimi i aftësive digjitale është një nga prioritetet kryesore për sistemet arsimore në nivel global, ndërsa në kontekstin ushtarak kjo përkthet në nevojën për trajnime më të avancuara dhe të specializuara. (Szabadföldi, 2021)

Në rastin e Shqipërisë, ky transformim lidhet ngushtë me procesin e integritimit në NATO dhe përshtatjen me standardet e Aleancës. Përpjekjet për modernizimin e sistemit të edukimit ushtarak përfshijnë përmirësimin e kurrikulave, rritjen e bashkëpunimit ndërkombëtar dhe adoptimin gradual të teknologjive të reja. Megjithatë niveli i investimeve është më i kufizuar krahasuar me vendet më të zhvilluara, Shqipëria përfiton nga transferimi i njohurive dhe përvojave përmes bashkëpunimit me vendet aleate. (Alex, 2022)

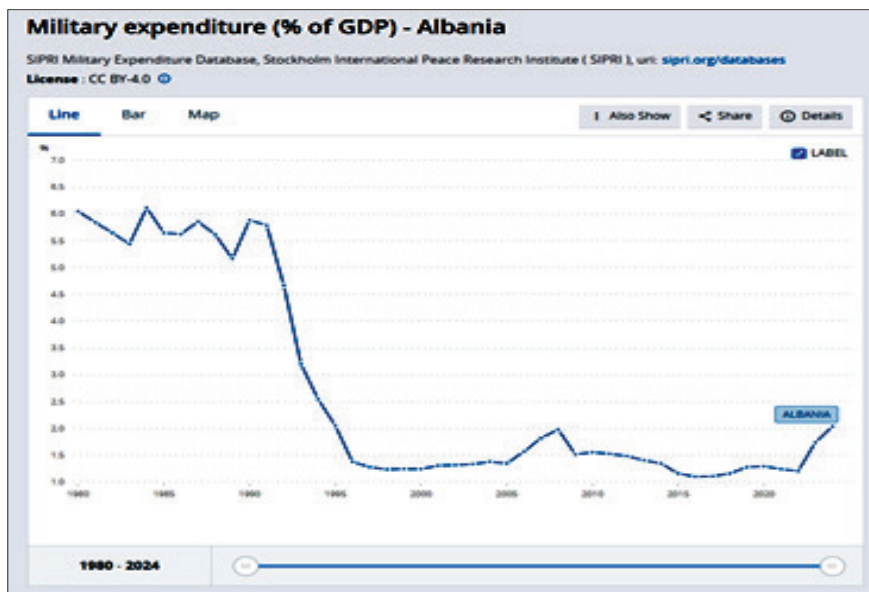


Figura 2. Të dhënat tregojnë se Shqipëria ka rritur gradualisht shpenzimet e mbrojtjes në përputhje me objektivat e NATO-s, duke reflektuar angazhimin për modernizimin e kapaciteteve ushtarake. Burimi: <https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=AL>

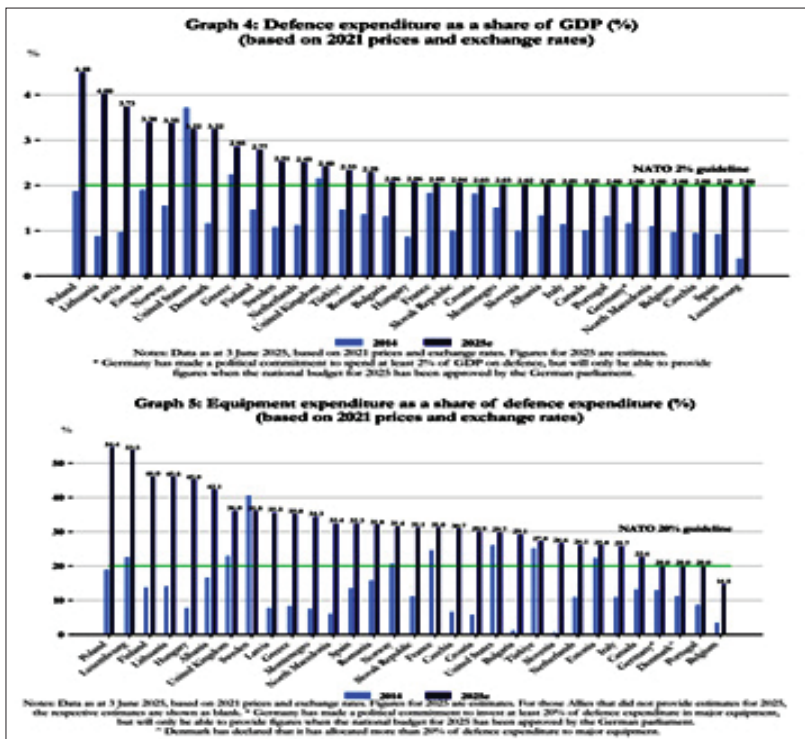


Figura 3. Shpenzimet e mbrojtjes si përqindje e PBB-së për vendet e NATO-s (Graph4) dhe shpenzimet për pajisje ushtarake (% e buxhetit të mbrojtjes) (Graph5). Burimi: <https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2025-en.pdf>

Një aspekt thelbësor i këtij transformimi është zhvillimi i kapitalit njerëzor, i cili konsiderohet një element kyç për sigurinë moderne. Edukimi ushtarak duhet të fokusohet në zhvillimin e aftësive të lidershit, fleksibilitetit dhe adaptimit ndaj ndryshimeve të shpejta teknologjike. Përdorimi i IA-së në edukim kontribuon në krijimin e një mjedisi më dinamik dhe interaktiv të të nxënit, duke rritur efektivitetin e trajnimit dhe përgatitjes së personelit. (Ertan, 2022)

Megjithatë, transformimi i edukimit ushtarak përballet edhe me sfida të rëndësishme, përfshirë mungesën e infrastrukturës teknologjike, nevojën për trajnimin e stafit akademik dhe rreziqet që lidhen me sigurinë e të dhënave. Sipas Clement (2024), adresimi i këtyre sfidave kërkon një qasje të koordinuar ndërmjet institucioneve ushtarake, akademike dhe teknologjike, si dhe zhvillimin e politikave të qarta për përdorimin e teknologjive të avancuara.

### III. Roli i inteligjencës artificiale në edukimin ushtarak

Roli i inteligjencës artificiale në edukimin ushtarak po bëhet gjithnjë e më i rëndësishëm në kontekstin e transformimit digjital të sektorit të mbrojtjes. Në institucionet ushtarake të vendeve anëtare të NATO-s, IA po përdoret për të përmirësuar cilësinë e mësimdhënies, për të rritur efektivitetin e trajnimit dhe për të përgatitur personelin për sfidat komplekse të sigurisë moderne. Kjo përfshin integrimin e teknologjive si sistemet inteligjente të mësimdhënies, simulimet virtuale dhe analizën e avancuar të të dhënave. (Christie & Ertan, 2021; Clement, 2024; Reding et al., 2026)

Një nga aplikimet më të rëndësishme të IA në edukimin ushtarak është mësimi i personalizuar (adaptive learning). Përmes përdorimit të algoritmeve të avancuara, sistemet inteligjente mund të analizojnë performancën e studentëve dhe të përshtatin përmbajtjen mësimore në kohë reale. Sipas Holmes dhe Luckin (2016), përdorimi i IA-së në arsim mund të rrisë ndjeshëm angazhimin dhe rezultatet e të nxënit. Po ashtu, studime të tjera tregojnë se sistemet adaptive mund të përmirësojnë performancën e studentëve deri në 20–30%, duke krijuar një përvojë më efikase dhe të personalizuar të të nxënit. (Luckin et al., 2018; Szabadföldi, 2021)



Figura 4. Simulim i një skenari të sulmit multi-domain me sisteme autonome (swarm) Burimi: <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-229/MP-MSG-229-21.pdf>

Përdorimi i simulimeve virtuale dhe teknologjive imersive, si realiteti virtual (VR) dhe realiteti i shtuar (AR), përbën një tjetër komponent kyç të integritetit të AI në edukimin ushtarak. Këto teknologji mundësojnë krijimin e mjediseve të kontrolluara dhe të sigurta për zhvillimin e trajnimeve komplekse. Sipas Singer (2009), teknologjitë e simulimit kanë transformuar mënyrën e zhvillimit të trajnimeve ushtarake, duke mundësuar skenarë realistë dhe duke rritur përgatitjen operacionale të personelit. Në këtë drejtim, përdorimi i IA-së rrit më tej efektivitetin e këtyre sistemeve duke i bërë ato më dinamike dhe adaptive. (Ertan, 2022; Singer, 2010)

Në aspektin e vendimmarrjes, inteligjenca artificiale luan një rol kyç përmes sistemeve të mbështetjes së vendimmarrjes, të cilat analizojnë të dhëna në kohë reale dhe ofrojnë rekomandime strategjike. Russell dhe Norvig (2021) theksojnë se sistemet inteligjente kanë aftësinë të përpunojnë sasi të mëdha informacioni dhe të identifikojnë modele që nuk janë lehtësisht të dallueshme nga njerëzit. Në kontekstin ushtarak, kjo përkthehet në përmirësimin e cilësisë së vendimmarrjes dhe rritjen e shpejtësisë së reagimit ndaj situatave kritike (Alex, 2022; Russell & Norvig, 2016)

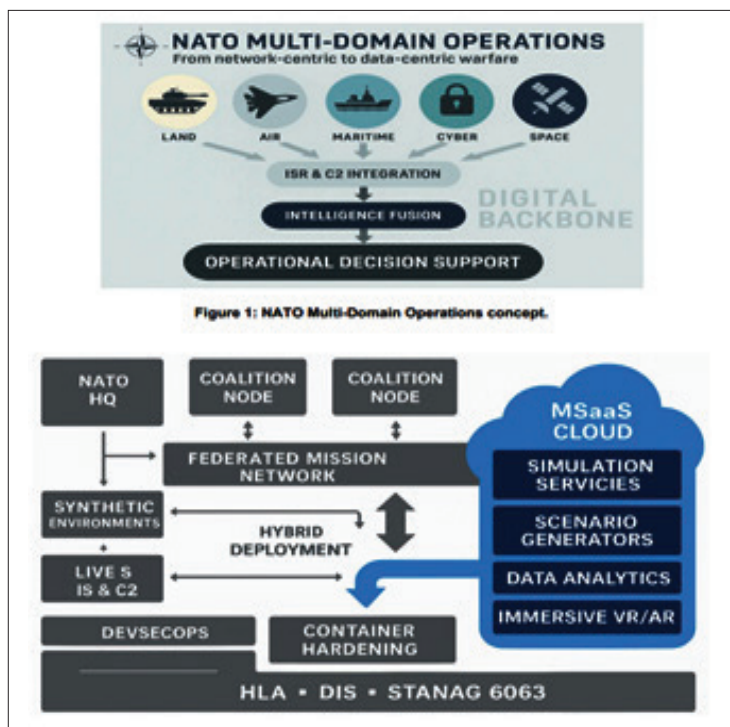


Figura 5. Arkitektura e simulimit dhe trajnimit ushtarak në NATO (MSaaS)  
Burimi: <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-229/MP-MSG-229-21.pdf>

Një dimension tjetër i rëndësishëm është përdorimi i AI për analizën e performancës dhe vlerësimin e progresit të studentëve. Sipas OECD (2021), përdorimi i teknologjive digjitale në arsim mundëson monitorimin e vazhdueshëm të performancës dhe ofrimin e feedback-ut të personalizuar, duke rritur efektivitetin e të nxëniet dhe përmirësimin e rezultateve akademike.

Në kontekstin shqiptar, përdorimi i IA-së në edukimin ushtarak është ende në fazat fillestare, por potenciali për zhvillim është i konsiderueshëm. Integrimi në strukturat e NATO-s dhe proceset e modernizimit të Forcave të Armatosura krijojnë kushte të favorshme për adoptimin e teknologjive inteligjente. Përfshirja graduale e sistemeve digjitale në proceset edukative dhe trajnimin ushtarak përbën një hap të rëndësishëm drejt përputhjes me standardet ndërkombëtare dhe rritjes së kapaciteteve profesionale. (Alex, 2022; Clement, 2024)

Megjithatë, përdorimi i IA-së në edukimin ushtarak shoqërohet edhe me sfida të rëndësishme, përfshirë çështjet etike, transparencën e algoritmeve dhe nevojën për ruajtjen e kontrollit njerëzor. Sipas Floridi et al. (2018), zhvillimi i sistemeve të inteligjencës artificiale duhet të mbështetet në parime etike që garantojnë përdorim të përgjegjshëm dhe të besueshëm. Në këtë kuadër, edhe NATO Science and Technology Organization thekson rëndësinë e zhvillimit të standardeve dhe politikave për përdorimin e IA-së në sektorin ushtarak. (Floridi et al., 2018; Reding et al., 2026)

#### **IV. Sfidat dhe kufizimet e IA në edukimin ushtarak**

Integrimi i inteligjencës artificiale në edukimin ushtarak paraqet një transformim të rëndësishëm teknologjik, por gjithashtu shoqërohet me një sërë sfidash komplekse që lidhen me aspektet etike, teknologjike dhe organizative. Literatura bashkëkohore thekson se përdorimi i AI në sektorin e mbrojtjes kërkon një balancë të kujdesshme midis inovacionit dhe kontrollit institucional, në mënyrë që të shmangen rreziqet e përdorimit të pakontrolluar të teknologjisë. (Clement, 2024; Reding et al., 2026; Tsamados et al., 2022)

Një nga sfidat kryesore lidhet me aspektet etike dhe transparencën e algoritmeve. Sistemet e inteligjencës artificiale, veçanërisht ato të bazuara në mësim të thellë (deep learning), shpesh funksionojnë si “black box”, duke e bërë të vështirë kuptimin e mënyrës se si arrihen vendimet. Sipas Bostrom (2014), zhvillimi i sistemeve inteligjente duhet të shoqërohet me mekanizma të fortë kontrolli për të garantuar që vendimet të jenë të përgjegjshme dhe të përputhshme me normat etike dhe ligjore. Në kontekstin ushtarak, kjo është veçanërisht kritike për shkak të ndikimit të drejtpërdrejtë në vendimmarrje strategjike dhe operacionale. (Bostrom, 2014; Floridi et al., 2018)

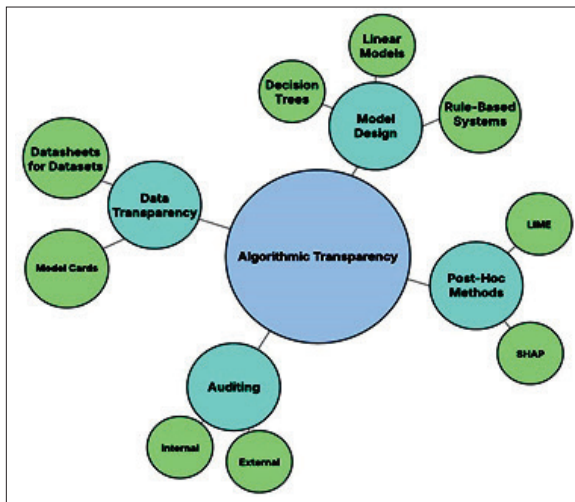


Figura 6. Problemi i transparencës (“black box”) në sistemet e inteligjencës artificiale. Burimi: <https://www.tenable.com/blog/cybersecurity-snapshot-memory-bugs-pervasive-in-open-source-sw-while-car-dealership-chaos>

Një tjetër kufizim i rëndësishëm është kompleksiteti teknologjik dhe nevoja për infrastrukturë të avancuar. Implementimi i AI kërkon investime të konsiderueshme në sisteme kompjuterike, rrjete të sigurta dhe kapacitete të përpunimit të të dhënave. Sipas Brynjolfsson dhe McAfee (2017), organizatat që nuk investojnë në mënyrë të mjaftueshme në teknologji dhe në kapital njerëzor rrezikojnë të mbeten pas në procesin e transformimit digjital. Në rastin e Shqipërisë, këto kufizime janë më të theksuara për shkak të burimeve të kufizuara dhe nivelit ende në zhvillim të infrastrukturës teknologjike. (Alex, 2022)

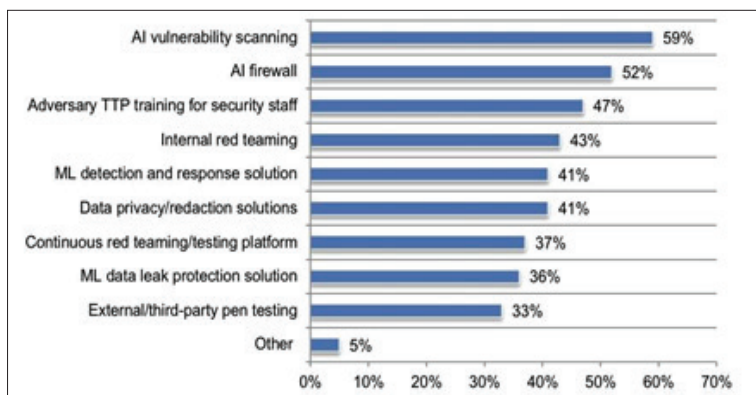


Figura 7. Barrierat kryesore në implementimin e inteligjencës artificiale. Burimi: <https://www.tenable.com/blog/cybersecurity-snapshot-memory-bugs-pervasive-in-open-source-sw-while-car-dealership-chaos>

Siguria e të dhënave dhe kërcënimet kibernetike përbëjnë një sfidë tjetër kritike. Sistemet e IA-së mbështeten në sasi të mëdha të dhënash, të cilat mund të jenë objekt sulmesh ose manipulimi. Sipas Goodfellow et al. (2016), sistemet e bazuara në IA mund të jenë të ndjeshme ndaj sulmeve të tipit adversarial, të cilat mund të ndikojnë në rezultatet dhe vendimet e tyre. Në sektorin ushtarak, kjo përbën një rrezik serioz për sigurinë dhe kërkon zhvillimin e mekanizmave të avancuar të mbrojtjes. (Christie & Ertan, 2021; Kurakin et al., 2016)

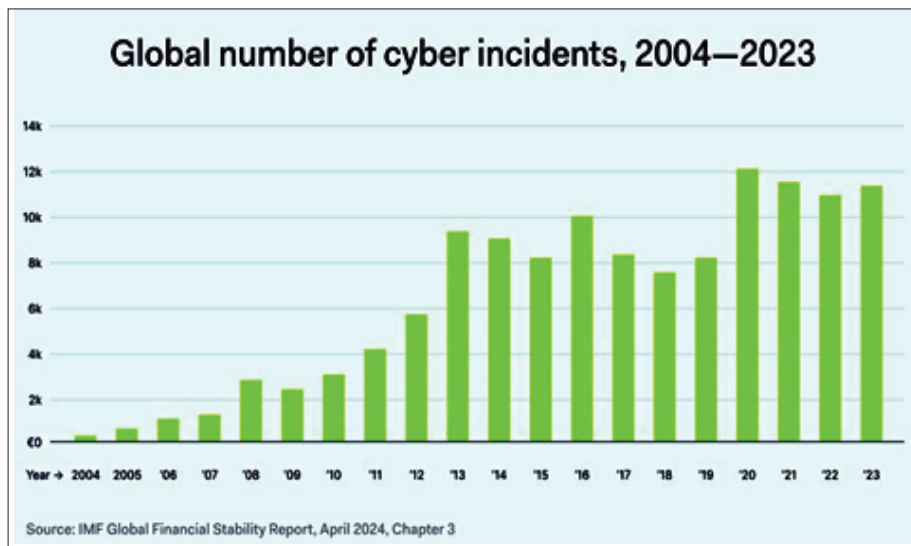


*Figura 8. Rritja e kërcënimeve kibernetike në nivel global*  
*Burimi: <https://nordlayer.com/blog/cybersecurity-statistics-of-2024>*

Nga ana organizative, integrimi i IA-së kërkon një transformim të thellë të strukturave dhe proceseve institucionale. Rezistenca ndaj ndryshimit, mungesa e aftësive digjitale dhe nevoja për trajnimin e stafit përbëjnë pengesa të rëndësishme në implementimin e teknologjive të reja. Sipas Davenport dhe Ronanki (2018), sukses i implementimit të IA-së varet jo vetëm nga teknologjia, por edhe nga gatishmëria organizative dhe kultura institucionale. Në këtë kontekst, edukimi ushtarak duhet të fokusohet në zhvillimin e aftësive të reja dhe në adaptimin ndaj ndryshimeve teknologjike. (Thakur & Mittal, n.d.)

Në kontekstin shqiptar, këto sfida përforcohen nga nevoja për investime në infrastrukturë dhe zhvillimin e kapaciteteve njerëzore. Megjithatë, pjesëmarrja në strukturat e NATO-s ofron mundësi për transferimin e njohurive dhe për adoptimin e praktikave më të mira ndërkombëtare. Bashkëpunimi me vendet aleate dhe përfshirja në programe të përbashkëta trajnimi mund të kontribuojnë në kapërcimin e këtyre kufizimeve dhe në përshpejtimin e transformimit

digjital. (Alex, 2022; Clement, 2024)

Një sfidë shtesë lidhet me varësinë nga teknologjia dhe rrezikun e reduktimit të rolit të faktorëve njerëzorë në vendimmarrje. Sipas Russell dhe Norvig (2021), megjithëse IA mund të përmirësojë efikasitetin dhe analizën, mbajtja e kontrollit njerëzor mbetet thelbësore për garantimin e vendimeve të sigurta dhe të përgjegjshme në kontekstin ushtarak.

## V. Model konceptual i integrit të IA në edukimin ushtarak

Bazuar në analizën teorike dhe empirike të paraqitur në seksionet e mëparshme, mund të propozohet një model konceptual për integrimin e inteligjencës artificiale në edukimin ushtarak, i cili synon të ndërthurë dimensionin teknologjik, pedagogjik dhe atë të sigurisë. Ky model mbështetet në qasjet bashkëkohore të sistemeve inteligjente dhe transformimit digjital, duke reflektuar nevojën për një integrim të qëndrueshëm dhe të strukturuar të teknologjive të avancuara në proceset edukative ushtarake. (Luckin et al., 2018; Russell & Norvig, 2016)

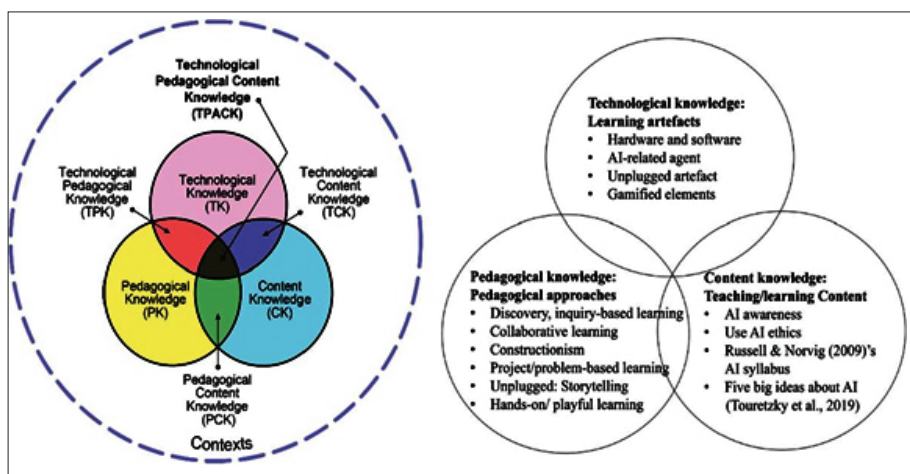


Figura 9. Model konceptual i integrit të inteligjencës artificiale në edukimin ushtarak. Burimi: <https://militaryembedded.com/ai/big-data/ai-and-the-ooda-loop-how-ai-enhances-strategic-decisions-for-todays-warfighters>

Komponenti i parë i modelit lidhet me dimensionin teknologjik, i cili përfshin përdorimin e sistemeve të inteligjencës artificiale si mësimi i personalizuar (adaptive learning), simulimet imersive (VR/AR) dhe sistemet e mbështetjes së vendimmarrjes. Sipas Topol (2019), integrimi i AI në sistemet e trajnimit mundëson një transformim të thellë të mënyrës së të nxënies, duke e bërë atë më të personalizuar, interaktiv dhe të bazuar në të dhëna. Në kontekstin

ushtarak, këto teknologji kontribuojnë në zhvillimin e aftësive operacionale dhe vendimmarrëse në mjedise komplekse. (Ertan, 2022; Szabadföldi, 2021)

Transformimi i edukimit ushtarak në epokën digjitale përfaqëson një nga zhvillimet më të rëndësishme në fushën e sigurisë dhe mbrojtjes moderne. Integrimi i inteligjencës artificiale ka potencialin të përmirësojë ndjeshëm cilësinë e trajnimit, të rrisë efikasitetin e proceseve edukative dhe të përgatisë personelin për sfidat komplekse të mjedisit të sigurisë bashkëkohore.

Analiza e literaturës dhe e praktikave ndërkombëtare tregon se vendet anëtare të NATO po investojnë gjithnjë e më shumë në teknologji të avancuara, duke përfshirë inteligjencën artificiale, për të modernizuar sistemet e tyre të edukimit dhe trajnimit ushtarak. Kjo tendencë reflekton një ndryshim të thellë në mënyrën se si përgatitet personeli ushtarak, duke kaluar nga modele tradicionale në qasje të bazuara në teknologji dhe të dhëna. (Clement, 2024)

Megjithatë, integrimi i IA-së nuk është pa sfida. Çështjet etike, siguria e të dhënave, mungesa e infrastrukturës dhe nevoja për zhvillimin e kapaciteteve njerëzore përbëjnë pengesa të rëndësishme që duhet të adresohen në mënyrë të koordinuar. Në këtë drejtim, bashkëpunimi ndërkombëtar dhe zhvillimi i politikave të qarta për përdorimin e IA-së janë thelbësore për garantimin e një transformimi të suksesshëm. (Floridi et al., 2018; Reding et al., 2026)

Në kontekstin shqiptar, përpjekjet për modernizimin e edukimit ushtarak dhe përfshirjen e teknologjive të avancuara përbëjnë një hap të rëndësishëm drejt përputhjes me standardet e NATO-s. Megjithëse sfidat mbeten, veçanërisht në aspektin e burimeve dhe infrastrukturës, potenciali për zhvillim është i konsiderueshëm përmes bashkëpunimit ndërkombëtar dhe investimeve strategjike. (Alex, 2022)

Sa i përket perspektivave të ardhshme, pritet që inteligjenca artificiale të luajë një rol gjithnjë e më të rëndësishëm në edukimin ushtarak, duke mundësuar zhvillimin e sistemeve të avancuara të trajnimit, përdorimin e simulimeve më realiste dhe përmirësimin e proceseve të vendimmarrjes. Teknologji të tilla si mësimi përforcues (reinforcement learning), sistemet autonome dhe analiza e avancuar e të dhënave do të kontribuojnë në krijimin e një mjedisi më dinamik dhe të adaptueshëm të të nxënit. (Russell & Norvig, 2016)

Në përfundim, integrimi i inteligjencës artificiale në edukimin ushtarak përfaqëson një domosdoshmëri strategjike për përballimin e sfidave të sigurisë moderne. Një qasje e balancuar që kombinon inovacionin teknologjik me parimet etike dhe zhvillimin e kapaciteteve njerëzore do të jetë çelësi për suksesin e këtij transformimi në të ardhmen.

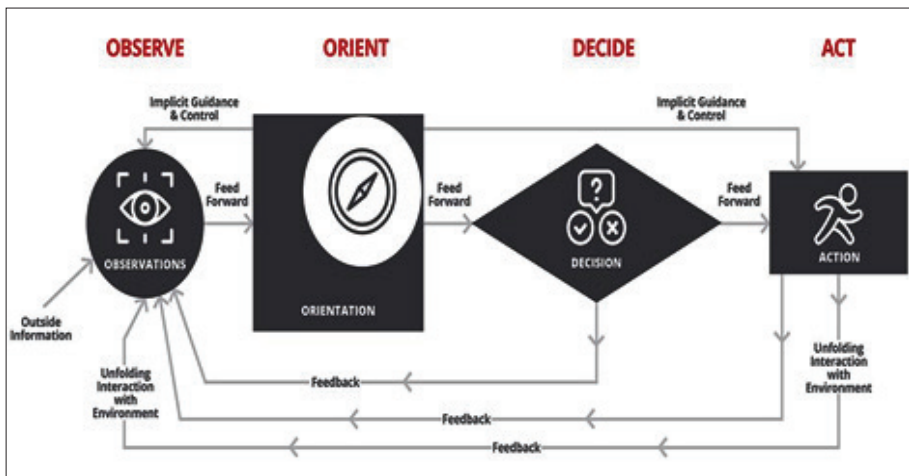


Figura 10. Cikli i vendimmarrjes dhe mësimit në sistemet e inteligjencës artificiale.  
Burimi: <https://militaryembedded.com/ai/big-data/ai-and-the-ooda-loop-how-ai-enhances-strategic-decisions-for-todays-warfighters>

Komponenti i dytë lidhet me dimensionin pedagogjik, i cili fokusohet në zhvillimin e kurrikulave të bazuara në kompetenca digjitale dhe në përdorimin e metodave inovative të mësimdhënies. Sipas OECD (2021), sistemet arsimore moderne duhet të integrojnë aftësi si mendimi kritik, analiza e të dhënave dhe zgjidhja e problemeve komplekse. Në këtë drejtim, përdorimi i IA-së në edukim krijon mundësi për zhvillimin e modeleve të reja pedagogjike që janë më fleksibile dhe të orientuara drejt studentit. (Luckin et al., 2018; Luckin & Holmes, 2016)

Komponenti i tretë përfshin dimensionin e sigurisë dhe qeverisjes së teknologjisë, i cili lidhet me përdorimin e përgjegjshëm të inteligjencës artificiale dhe me zhvillimin e mekanizmave për mbrojtjen e të dhënave dhe garantimin e transparencës. Sipas Taddeo dhe Floridi (2018), qeverisja e IA-së në kontekstin e sigurisë kërkon zhvillimin e politikave të qarta dhe standardeve etike që garantojnë përdorimin e kontrolluar dhe të besueshëm të teknologjisë. Në këtë kuadër, politikat dhe udhëzimet e NATO-s dhe *NATO Science and Technology Organization* luajnë një rol kyç në orientimin e përdorimit të IA-së në sektorin ushtarak. (Clement, 2024; Reding et al., 2026)

Një element shtesë i këtij modeli është ndërveprimi midis këtyre tre dimensioneve, i cili krijon një sistem të integruar dhe dinamik të edukimit ushtarak. Sipas Brynjolfsson dhe McAfee (2017), transformimi digjital nuk është vetëm një proces teknologjik, por një ndryshim sistematik që kërkon integrimin e teknologjisë me proceset organizative dhe njerëzore. Në këtë drejtim, modeli i propozuar synon të krijojë një ekuilibër midis inovacionit

teknologjik dhe zhvillimit të kapaciteteve njerëzore. (McAfee & Brynjolfsson, 2019)

Në kontekstin shqiptar, ky model mund të shërbejë si një kornizë strategjike për modernizimin e edukimit ushtarak, duke ndihmuar në harmonizimin me standardet e NATO-s dhe në përmirësimin e ndërveprueshmërisë ndërkombëtare. Megjithatë sfidat që lidhen me burimet dhe infrastrukturën mbeten, implementimi gradual i këtij modeli mund të kontribuojë në rritjen e cilësisë së trajnimit dhe në zhvillimin e kapaciteteve profesionale të Forcave të Armatosura të Shqipërisë. (Alex, 2022)

## **VI. Përfundime dhe parashikime për të ardhmen**

Transformimi i edukimit ushtarak në epokën digjitale përfaqëson një nga zhvillimet më të rëndësishme në fushën e sigurisë dhe mbrojtjes moderne. Integrimi i inteligjencës artificiale ka potencialin të përmirësojë ndjeshëm cilësinë e trajnimit, të rrisë efikasitetin e proceseve edukative dhe të përgatisë personelin për sfidat komplekse të mjedisit të sigurisë bashkëkohore.

Analiza e literaturës dhe e praktikave ndërkombëtare tregon se vendet anëtare të NATO-s po investojnë gjithnjë e më shumë në teknologji të avancuara, duke përfshirë inteligjencën artificiale, për të modernizuar sistemet e tyre të edukimit dhe trajnimit ushtarak. Kjo tendencë reflekton një ndryshim të thellë në mënyrën se si përgatitet personeli ushtarak, duke kaluar nga modele tradicionale në qasje të bazuara në teknologji dhe të dhëna. (Clement, 2024)

Megjithatë, integrimi i IA-së nuk është pa sfida. Çështjet etike, siguria e të dhënave, mungesa e infrastrukturës dhe nevoja për zhvillimin e kapaciteteve njerëzore përbëjnë pengesa të rëndësishme që duhet të adresohen në mënyrë të koordinuar. Në këtë drejtim, bashkëpunimi ndërkombëtar dhe zhvillimi i politikave të qarta për përdorimin e IA-së janë thelbësore për garantimin e një transformimi të suksesshëm. (Floridi et al., 2018; Reding et al., 2026)

Në kontekstin shqiptar, përpjekjet për modernizimin e edukimit ushtarak dhe përfshirjen e teknologjive të avancuara përbëjnë një hap të rëndësishëm drejt përputhjes me standardet e NATO-s. Megjithatë sfidat mbeten, veçanërisht në aspektin e burimeve dhe infrastrukturës, potenciali për zhvillim është i konsiderueshëm përmes bashkëpunimit ndërkombëtar dhe investimeve strategjike. (Alex, 2022)

Sa i përket perspektivave të ardhshme, pritet që inteligjenca artificiale të luajë një rol gjithnjë e më të rëndësishëm në edukimin ushtarak, duke mundësuar zhvillimin e sistemeve të avancuara të trajnimit, përdorimin e simulimeve më realiste dhe përmirësimin e proceseve të vendimmarrjes. Teknologji të tilla si mësimi përforcues (reinforcement learning), sistemet autonome dhe analiza e avancuar e të dhënave do të kontribuojnë në krijimin e një mjedisi më dinamik

dhe të adaptueshëm të të nxënit. (Russell & Norvig, 2016)

Në përfundim, integrimi i inteligjencës artificiale në edukimin ushtarak përfaqëson një domosdoshmëri strategjike për përballimin e sfidave të sigurisë moderne. Një qasje e balancuar që kombinon inovacionin teknologjik me parimet etike dhe zhvillimin e kapaciteteve njerëzore do të jetë çelësi për suksesin e këtij transformimi në të ardhmen.

## **Bibliografia**

1. Alex, E. T. L. (2022). The impact of ai on nato member states' strategic thinking. Proceedings of the international scientific conference strategies XXI. Volume XVIII, 493–505.
2. Bostrom, N. S. (2014). Paths, dangers, strategies. *Strategies*.
3. Christie, E., & Ertan, A. (2021). NATO and artificial intelligence. Christie, Edward Hunter and Amy Ertan, NATO and Artificial Intelligence (June 10, 2022). In Romaniuk, SN, and Manjikian. M.(Eds). Routledge Companion to Artificial Intelligence and National Security Policy. Routledge. Forthcoming.
4. Clement, S. (2024). NATO and Artificial Intelligence: Navigating the challenges and opportunities. Science and Technology Committee (STC), 58, 1–17.
5. Ertan, A. (2022). Exploring the security implications of artificial intelligence in military contexts. Royal Holloway, University of London London.
6. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., & Rossi, F. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707.
7. Kurakin, A., Goodfellow, I., & Bengio, S. (2016). Adversarial machine learning at scale. ArXiv Preprint ArXiv:1611.01236.
8. Luckin, R., & Holmes, W. (2016). Intelligence unleashed: An argument for AI in education.
9. Luckin, R., Holmes, W., & Forcier, L. B. (2018). An argument for AI in education. UCL Knowledge Lab.[Google Scholar].
10. McAfee, A., & Brynjolfsson, E. (2019). Machine, platform, crowd. How to Tame Our Digital Future. Kyiv: Nash Format.
11. Nunes, I. F., Daehnhardt, P., Seabra, P., Rizzi, A., Csernaton, R., & Eugénio, A. (2025). The Hague NATO Summit 2025.
12. Reding, D. F., Wells, B., & Nguyen, P. B. U. (2026). International Defense

- Innovation as a Complex Sociotechnical System: A Case Study of the NATO Science and Technology Organization. In *Advanced Topics in Defense Project Management* (pp. 203–255). Bentham Science Publishers.
13. Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Malaysia. Pearson Education Limited London, UK:
  14. Singer, M. J. (2010). Evaluation of a game-based simulation during distributed exercises. US Army Research Institute for the Behavioral and Social Sciences.
  15. Szabadföldi, I. (2021). Artificial intelligence in military application—opportunities and challenges. *Land Forces Academy Review*, 26(2), 157–165.
  16. Thakur, B., & Mittal, N. (n.d.). Role of the United Nations Educational, Scientific and Cultural Organization (UNESCO), the Organization for Economic Cooperation and Development (OECD) and Global EdTech Standards in Shaping Artificial Intelligence and Cyber Law Curriculum Policies: A Comparative Study of Finland, Singapore and India. *International Annals of Criminology*, 1–14.
  17. Tsamados, A., Aggarwal, N., Cows, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: key problems and solutions. *AI & Society*, 37(1), 215–230.



## **RUBRIKA E KATËRT**

**ZHVILLIMI I TEKNOLOGJISË  
DHE INOVACIONIT  
NË FUSHËN E MBROJTJES**



# Platformat parandaluese “proaktive” të sigurisë dhe mbrojtjes kibernetike

---

Kolonel Inxh. Gjergji VASILI

Departamenti i Inovacionit dhe Teknologjisë, IKSHU

## Trajtesa e shkurtuar

*Sistemi i sigurisë kibernetike ka pësuar një transformim rrënjësor gjatë viteve të fundit, duke lëvizur nga një model mbrojtës “reaktiv” drejt një qasjeje parandaluese dhe “proaktive”. Kjo “zhvendosje” nuk është thjesht një preferencë teknologjike, por një domosdoshmëri ekzistenciale në një mjedis dixhital ku kërcënimet elektronike zhvillohen me një shpejtësi marramendëse dhe sofistikim tepër të lartë. Siguria kibernetike “reaktive” fokusohet në zgjidhjen e problemeve të sigurisë pasi ato kanë ndodhur, një metodologji gjithnjë e më shumë e pamjaftueshme përballë sulmuesve kibernetike që arrijnë kohë rekord të depërtimit në rrjetet e sistemeve TIK. Sipas të dhënave të vitit 2025, koha mesatare e “shpërthimit” të sulmeve kibernetike është zvogëluar në mënyrë drastike, shpesh në minuta e jo më në ditë, duke e kthyer mbrojtjen e bazuar në “reagim” një strategji të dështuar. Mbrojtja kibernetike “proaktive”, në anën tjetër, përfshin identifikimin e dobësive dhe kërcënimeve përpara se ato të shndërrohen në incidente reale. Në epokën e Inteligjencës Artificiale (IA) dhe të sulmeve kibernetike të automatizuara, qasjet tradicionale të bazuara në detektim dhe përgjigje-reagim për mbrojtje po tregohen plotësisht të pamjaftueshme.*

*Ky shkrim analizon platformat parandaluese “proaktive” si paradigmë e re për mbrojtjen dhe sigurinë kibernetike të sistemeve TIK apo çdo sistemi teknologjik për vitin 2026. Ai shqyrton “evoluimin” nga mbrojtja reaktive drejt parandalimit të kërcënimeve para materializimit të tyre, komponentët teknologjikë kryesorë (“Predictive Artificial Intelligence (AI)/Machine*

*Learning<sup>1</sup> (ML)”, “Continuous Threat Exposure Management” (CTEM)<sup>2</sup>, “Integrated XDR”<sup>3</sup>, “deception technologies”, “Zero Trust” dhe “agentic AI”<sup>4</sup>), trendet e tregut teknologjik, si dhe implikimet për kontekstin e teknologjisë ushtarake dhe ndër aleatëve. Gjetjet tregojnë se platformat “proaktive” pritet të përbëjnë rreth 50% të shpenzimeve të sigurisë të sistemeve TIK deri në vitin 2030, duke zëvendësuar gradualisht modelet klasike të detektimit<sup>5</sup>. Shkrimi ofron rekomandime për adoptimin e tyre në mjedise civile, administratën shtetërore dhe strukturat ushtarake të FARSH, përgjegjëse për sigurinë kibernetike të sistemeve TIK dhe sistemeve teknologjike.*

**Fjalët kyçe:** mbrojtje kibernetike proaktive, preemptive cybersecurity, continuous threat exposure management (CTEM), XDR, agentic AI, Zero Trust, deception technology.

## Hyrje

Pëizazhi i kërcënimeve kibernetike në vitin 2026 karakterizohet nga shpejtësia e sulmeve të orkestruara nga Inteligjenca Artificiale, rritja eksponenciale e sipërfaqes së sulmit dhe kompresimi i kohës nga kompromisi deri te dëmi. Modelet tradicionale që mbështeten te detektimi pas faktit dhe te përgjigjia njerëzore nuk arrijnë të përballojnë këtë ritëm. Si pasojë, industria, administrata shtetërore dhe institucionet e mbrojtjes po orientohen drejt platformave parandaluese “proactive”, të cilat synojnë të parashikojnë paraprakisht, të neutralizojnë dhe të ndërpresin kërcënimet para se ato të arrijnë objektivat kritike<sup>6</sup>. Qëllimi i këtij shkrimi është të ofrojë një analizë të strukturuar dhe të detajuar të koncepteve, teknologjive, trendeve dhe sfidave

<sup>1</sup> Teknologji që përdor algoritme të AI dhe ML për parashikimin e rezultateve të ardhshme bazuar në të dhëna historike.

<sup>2</sup> CTEM: është një qasje e vazhdueshme e sigurisë kibernetike që identifikon, vlerëson, prioritetizon dhe zbut në mënyrë sistematike ekspozimet ndaj kërcënimeve në të gjithë sipërfaqen e sulmit të organizatës.

<sup>3</sup> Integrated XDR (Extended Detection and Response): një platformë e integruar sigurie që shtrin detektimin dhe përgjigjen përtej “endpoint”-eve, duke mbuluar rrjetin, cloud-in, email-in, dhe identitetet, për të ofruar vizibilitet të plotë, detektim më të saktë, dhe përgjigje të automatizuar ndaj kërcënimeve të avancuara kibernetike; NIST SP 800-207, “Zero Trust Architecture” (referencë indirekte), Microsoft Security, “What is XDR?”.

<sup>4</sup> Inteligjencë Artificiale me agjentë: sisteme të IA-së që nuk kufizohen vetëm në dhënien e një përgjigjeje, por mund të planifikojnë, marrin vendime dhe kryejnë në mënyrë të pavarur (autonom) një seri veprimesh për të arritur një objektiv.

<sup>5</sup> <https://www.cybersecuritydive.com/news/preemptive-security-predicted-half-it-security-2030/760642/>

<sup>6</sup> <https://www.threater.com/blog/what-is-preemptive-cybersecurity-gartner-named-it-the-future-here-is-what-it-actually-means/>

të këtyre platformave, me fokus të veçantë në zhvillimet e vitit 2026, në interes edhe të strukturave ushtarake të sigurisë kibernetike brenda FARSH-së.

## I. Siguria kibernetike nga mbrojtja “reaktive” drejt qasjeve parandaluese dhe “proaktive”

Evoluimi i sigurisë kibernetike përfaqëson një transformim themelor të paradigmes së mbrojtjes të sistemeve digjitale. Në fazat e hershme të sigurisë kibernetike, mbrojtja bazohej kryesisht në mekanizma statikë, si “firewall”-et, antiviruset, sistemet IDS (Intrusion Detection Systems) dhe rregullat e bazuara në nënshkrime. Këto teknologji ishin efektive ndaj kërcënimeve të njohura, por kishin kufizime të konsiderueshme përballë sulmeve të reja, të sofistikuar dhe të personalizuar. Modeli “reaktiv” funksiononte kryesisht sipas logjikës: “sulm → zbulim → analizë → reagim → rikuperim”. Me rritjen e kompleksitetit të infrastrukturave të sistemeve TIK, si “cloud computing, IoT/IoE” dhe përdorimit të Inteligjencës Artificiale, kjo qasje u bë gjithnjë e më e pamjaftueshme. Për këtë arsye, siguria kibernetike filloi të zhvendosej drejt “threat intelligence, threat hunting, behavioral analytics, XDR, Zero Trust” dhe automatizimit të reagimit.

Në këtë paradigmë të re, objektivi nuk është vetëm të zbulohet sulmi pasi ka ndodhur, por të identifikohen **indikatorët, modelet e sjelljes dhe dobësitë që mund të paralajmërojnë një sulm të ardhshëm**. Ndryshimi më i rëndësishëm konceptual është kalimi nga platforma “si reagojmë ndaj sulmit?” në platformën: **“si e zbulojmë, parashikojmë dhe parandalojmë sulmin përpara se të shkaktojë dëme?”**. Në modelin “proaktiv”, analistët kërkojnë në mënyrë të vazhdueshme shenja të aktivitetit keqdashës. Kjo realizohet përmes “threat hunting”, ku ekipet e sigurisë nuk presin që një sistem automatik të raportojë një incident, por formulojnë hipoteza dhe kërkojnë në të dhënat e rrjetit, “endpoint”-eve dhe sistemeve të tjera për sjellje anormale.

Sipas Gartner<sup>7</sup>, “preemptive cybersecurity” përfshin teknologji që parashikojnë dhe neutralizojnë kërcënimet para se ato të materializohen, duke u bazuar në tre parime kryesore (**3 D’s**):

- “Deny”- “prapësimi” i hyrjes (exposure management, blocking malicious infrastructure).
- “Deceive” – “mashtrimi” i sulmuesit përmes teknologjive të deception.
- “Disrupt” – “ndërprerja” e zinxhirit të sulmit para se ai të përparojë.

<sup>7</sup> Gartner. (2026). Don’t Delay in Building Preemptive Cybersecurity Solutions. By Carl Manion, 15 January 2026. <https://www.gartner.com/en/articles/preemptive-cybersecurity-solutions?> (January 15, 2026).

Një tjetër evolucion i rëndësishëm është kalimi nga rregullat statike drejt sistemeve adaptive. Në një sistem tradicional kemi: **rregull → ngjarje → alarm**; kurse në një sistem modern kemi: **të dhëna → analizë kontekstuale → identifikim anomalie → vlerësim rreziku → vendim → veprim automatik**. Këtu IA dhe “Machine Learning” mund të analizojnë sasi shumë të mëdha të të dhënave dhe të identifikojnë modele që mund të jenë të vështira për t’u evidentuar nga operatorët njerëzorë. IA duhet të konsiderohet si komponent i një arkitekture të integruar sigurie dhe jo si zëvendësim i plotë i ekspertizës njerëzore. Faza më e avancuar është kalimi drejt sigurisë kibernetike “parashikuese”.

Në këtë model përdoren: “machine learning + threat intelligence + analitikë e sjelljes + attack surface management + automatizim” për të vlerësuar probabilitetin e një incidenti të ardhshëm. Procesi konceptual mund të paraqitet si: mbledhja e të dhënave → analiza e sjelljes → identifikimi i anomalive → korelacioni me “threat intelligence” → vlerësimi i rrezikut → parashikimi i skenarit të mundshëm → masa parandaluese → monitorim i vazhdueshëm. Kjo krijon një cikël të mbyllur të sigurisë sipas: **“predict → prevent → detect → respond → recover → learn”**. Në sistemet ushtarake, ky evolucion ka rëndësi edhe më të madhe për shkak të natyrës “multi-domain” të konflikteve moderne.

Një sulm kibernetik mund të synojë: - komandën dhe kontrollin (C2); - sistemet e komunikimit dhe të informacionit; - sistemet e radarëve dhe sensorët; - UAV/UCAV; - avionët dhe sistemet avionike; - sistemet e navigimit; - platformat detare; - sistemet e logjistikës dhe të furnizimit; - infrastrukturën kritike; - zinxhirin e furnizimit të teknologjisë.

Në këtë kontekst, objektivi nuk është vetëm mbrojtja e rrjeteve teknologjike, por siguri i vijueshmërisë së misionit. Një arkitekturë teknologjike moderne mund të funksionojë sipas platformës: sensorë → telemetri → SIEM<sup>8</sup>/XDR → IA/ML → inteligjencë mbi kërcënimet kibernetike (threat intelligence) → vlerësim i rrezikut → automatizim → masat bllokuese → kundërveprim.

Kjo mundëson një mbrojtje të vazhdueshme dhe adaptive të sistemeve ushtarake. Siguria kibernetike e së ardhmes nuk do të matet vetëm nga aftësia për të reaguar shpejt ndaj një sulmi, por nga aftësia për ta parashikuar, parandaluar dhe neutralizuar atë përpara se të ndikojë në mision.

---

<sup>8</sup> SIEM = Security Information and Event Management: një platformë që mbledh, analizon dhe ndërlidh të dhëna nga burime të ndryshme sigurie (si firewall, antivirus, serverë, rrjete) për të zbuluar kërcënimet, dhe aktivitetet e dyshimta në kohë reale.

## II. Komponentët dhe teknologjitë kryesore të platformave parandaluese “proaktive”

Platformat parandaluese “proaktive” integrojnë disa komponentë dhe shtresa teknologjike, si:

- **Kërkim aktiv për kërcënime (threat hunting):** metodologji e drejtuar nga analistët që përdorin kornizën “MITRE ATT&CK<sup>9</sup>” për të paramenduar dhe kërkuar praninë e kundërshtarëve brenda rrjetit, pa prituri alarme automatike. Korniza teknologjike “MITRE ATT&CK” shërben si platformë standarde dhe hartë sjelljeje që transformon “threat hunting” nga një kërkim i rëndomtë i treguesve statikë të kompromentimit në një analizë dinamike të “taktikave, teknikave dhe procedurave” (TTPs) të sulmuesit, sipas radhës së veprimeve të komponentëve “TTP”:

- Taktikat “pse”: përfaqësojnë qëllimin taktik të kundërshtarit gjatë një faze të caktuar të sulmit (p.sh.: “initial access, persistence, privilege escalation, defense evasion”).
- Teknikat “si”: përshkruajnë metodën specifike me anë të së cilës sulmuesi arrin objektivin taktik (p.sh. teknikën “T1059” - Command and Scripting Interpreter<sup>10</sup>).
- Procedurat/nën-teknikat “më saktësisht”: ekzekutimi konkret operativ ose komandues nga një grup i caktuar komponentësh (p.sh. përdorimi i parametrave: - “EncodedCommand, - NoProfile” në PowerShell nga grupi APT29<sup>11</sup>).

“Gjuetari” (*hunter*) i kërcënimeve nuk pret alarme, ai ndërton një hipotezë pune duke u bazuar tek matrix-i i “ATT&CK” dhe intelijenca e kërcënimeve (CTI). Çdo teknikë në “ATT&CK” lidhet me burime specifike të të dhënave. “Gjuetari” përcakton se cilat “log”-e duhet të analizohen për të zbuluar teknikën. Kërkimi ndërtohet mbi sjelljen anormale në vend të adresave “IP” apo “hash<sup>12</sup>”-eve statike, duke targetuar linjat e komandave, modifikimet e regjistrimit ose thirrjet API<sup>13</sup>.

<sup>9</sup> MITRE Adversarial Tactics, Techniques, and Common Knowledge: MITRE është një organizatë kërkimore dhe zhvillimore jo-fitimprurëse në SHBA, e cila krijoi këtë kornizë; <https://www.mitre.org>; <https://attack.mitre.org>

<sup>10</sup> <https://attack.mitre.org/techniques/T1059/>

<sup>11</sup> <https://attack.mitre.org/groups/G0016/>; <https://attack.mitre.org/techniques/T1059/001/>; <https://www.cisa.gov/news-events/>

<sup>12</sup> Hash: rezultati i një funksioni kriptografik (si SHA-256, MD5) që transformon të dhënat në një varg fiks të gjatësisë (p.sh., 64 karaktere heksadecimale për SHA-256) - National Institute of Standards and Technology, Special Publication 800-63B.

<sup>13</sup> API: Application Programming Interface (Ndërfaqja e Programimit të Aplikacioneve) - është një grup rregullash, protokollesh dhe mjetesh që lejon dy ose më shumë aplikacione softuerike të komunikojnë me njëra-tjetrën.

Përdoren korniza si “Atomic Red Team” për të ekzekutuar në mënyrë të kontrolluar procedurën e zgjedhur.

- **Inteligjenca e kërcënimeve kibernetike (cyber threat intelligence - CTI):** përpunimi i të dhënave strategjike mbi taktikat, teknikat dhe procedurat (TTPs) të aktorëve keqdashës për të parashikuar dhe bllokuar “vektoret” e ardhshëm të sulmit kibernetik. CTI mbledh dhe analizon informacion mbi: - aktorët kërcënues; - infrastrukturën e sulmuesve; - indikatorët e komprometimit (IoCs); - dobësitë e shfrytëzueshme; - objektivat potencialë; - modelet historike të sulmeve. Në këtë mënyrë, organizata nuk fokusohet vetëm tek pyetja: “A po sulmohemi?” por edhe: “Kush mund të na sulmojë, si mund të na sulmojë dhe cilat janë shenjat paralajmëruese?”. Ky informacion ushqen sistemet SIEM<sup>14</sup>, EDR/XDR<sup>15</sup>, mekanizmat e zbulimit dhe platformat e automatizimit të sigurisë kibernetike.

- **Arkitektura “zero besim” dhe siguria e identitetit (Zero Trust Architecture (ZTA) and identity security):** përfaqëson një tjetër ndryshim paradigmatic – zbatimin e parimit: «kurrë mos beso, gjithmonë verifiko» (*never trust, always verify*), pra verifikim i vazhdueshëm i përdoruesve, pajisjeve teknologjike dhe “agjentëve” të IA (non-human identities) duke përdorur mikrosegmentimin dhe identifikimin e vazhdueshëm për të parandaluar lëvizjet “anësore” (*lateral movement*). Çdo kërkesë për akses vlerësohet në bazë të: - identitetit; - pajisjes; - kontekstit; - privilegjeve; - sjelljes; - nivelit të rrezikut; - burimit dhe destinacionit të komunikimit. Kjo është veçanërisht e rëndësishme në infrastrukturën teknologjike moderne, ku kufiri midis “brenda” dhe “jashtë” rrjetit është bërë gjithnjë dhe më i paqartë.

- **Platformat e menaxhimit të ekspozimit të vazhdueshëm ndaj kërcënimeve / vlerësimit të ekspozimit** (Continuous Threat Exposure Management (CTEM)/Exposure Assessment Platforms (EAP): identifikim i vazhdueshëm i ekspozimeve (vulnerabilitete, keqkonfigurime, privilegje të tepërta, rrugë sulmi) dhe renditja prioritare sipas ndikimit në funksionimin e sistemeve. Kjo platform kalon nga skanime “periodike” në monitorime “real-time”.

<sup>14</sup> Security Information and Event Management (menaxhimi i informacionit dhe ngjarjeve të sigurisë) - është një platformë e integruar sigurie që kryen dy funksione kryesore: - Security Information Management (SIM) – mbledh, ruan dhe analizon të dhënat e “logs” nga burime të ndryshme (serverë, firewall, antivirus, rrjete, etj.) për qëllime raportimi dhe pajtueshmëri; - Security Event Management (SEM) – monitoron në kohë reale ngjarjet e sigurisë, analizon dhe lidh ngjarje-alarme, dhe zbulon aktivitetet e dyshimta ose sulmet kibernetike.

<sup>15</sup> EDR = Endpoint Detection and Response (detektimi dhe përgjigja në pajisjet fundore); XDR = Extended Detection and Response (detektimi dhe përgjigja e zgjeruar): Gartner, “Market Guide for Endpoint Detection and Response Solutions”.

- **Continuous Threat Exposure Management (CTEM)<sup>16</sup>**: është një kuadër procedure për menaxhimin e vazhdueshëm dhe sistematik të ekspozimeve kibernetike. Ai nuk është një produkt i vetëm, por një qasje operationale që synon të identifikojë, të rendisë sipas rëndësisë, konfirmojë ose të verifikojë saktësinë dhe reduktojë rreziqet reale që mund të shfrytëzohen nga sulmuesit, në vend që të fokusohet vetëm te listat e vulnerabiliteteve.

- **Exposure Assessment Platforms (EAP)**: janë platformat teknologjike që mbështesin programet CTEM. Ato ofrojnë aftësi për zbulim të vazhdueshëm, analizë kontekstuale, dhënie prioriteti të bazuar në rrezik dhe udhëzime specifike për riparimin e sistemit të komprometuar, të ekspozimeve në mjedise hibride (on-premises, cloud, SaaS, identitet, etj.).

Pesë fazat kryesore të funksionimit të “CTEM”, të cilat veprojnë si një cikël i vazhdueshëm teknik dhe që përsëriten vazhdimisht janë:

1. **“Scoping” (përcaktimi i fushëveprimit)**. Kjo fazë përcakton se çfarë duhet të mbrohet dhe si do të matet suksesi: - identifikohen asetet kritike (“crown jewels”) dhe shërbimet e organizatës që kanë ndikim të lartë; - përcaktohet kufiri i sipërfaqes së sulmit (attack surface); - vendosen objektivat dhe treguesit e matshëm të suksesit. Qëllimi është të shmanget “vulnerabilitet-menaxhimin për gjithçka” dhe të fokusohet përpjekja tek ajo që ka rëndësi reale për organizatën.

2. **Discovery (zbulimi)**. Në këtë fazë bëhet zbulimi i vazhdueshëm i aseteve dhe ekspozimeve brenda fushëveprimit të përcaktuar: - përfshin jo vetëm dobësitë ose pikat e dobëta në sisteme, por edhe keqkonfigurime, dobësi të identitetit, privilegje të tepërta, ekspozime “SaaS”, “shadow IT”, lidhje me palë të treta dhe rrugë të mundshme sulmi. Zbulimi duhet të jetë i vazhdueshëm (continuous), sepse sipërfaqja e sulmit ndryshon vazhdimisht.

3. **Prioritization (renditja sipas rëndësisë dhe urgjencës)**. Jo çdo ekspozim dobësie në sistem ka të njëjtën rëndësi. Kjo “renditje” kombinohet me: - probabilitetet e shfrytëzimit (exploitability – EPSS<sup>17</sup>, KEV<sup>18</sup>, threat intelligence); - ndikimet në organizatë; - kushtet e ekspozimit; - arritshmërinë;

<sup>16</sup> Programet CTEM = iniciativa të strukturuar për menaxhimin e vazhdueshëm të rreziqeve kibernetike, për të prioritarizuar dobësitë që janë më të shfrytëzueshme dhe me ndikim më të madh. <https://ctem.org/docs/stages/>

<sup>17</sup> EPSS = Exploit Prediction Scoring System (sistemi i parashikimit të shfrytëzueshmërisë): është një sistem i hapur dhe i bazuar në të dhëna, i cili parashikon probabilitetin që një dobësi (vulnerability) specifike të shfrytëzohet duke ndihmuar ekipet e sigurisë të prioritarizojnë neutralizimin e një kërcënimi bazuar në rrezikun real, jo vetëm në rrezikshmërinë teknike.

<sup>18</sup> KEV = Known Exploited Vulnerabilities (dobësi të njohura të shfrytëzuara): është një listë zyrtare e mirëmbajtur nga CISA (Cybersecurity and Infrastructure Security Agency – SHBA), e cila përmban dobësi (vulnerabilities) për të cilat ka prova të qarta se po shfrytëzohen aktivisht në natyrë nga sulmuesit; <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

- kushte paraprake; - kontrollët kompensuese ekzistuese. Rezultati është një renditje për mbrojtje sipas prioriteteve me SLA<sup>19</sup>- të përkatëse, që ekipet e infrastrukturës teknologjike dhe zhvillimit të mbrojtjes mund t'i përmbushin realisht detyrimet e sigurisë.

**4. Validation (validimi & konfirmim të vlefshmërisë).** Kjo fazë e dallon CTEM nga menaxhimi tradicional i vulnerabiliteteve: - verifikohet nëse ekspozimi është vërtet i shfrytëzueshëm në mjedisin konkret; - analizohen rrugët e sulmit (attack path analysis); - testohen kontrollët ekzistuese përmes simulimeve, “breach and attack simulation” (BAS) ose “adversarial exposure validation”. Validimi shmang gjetjet që nuk paraqesin rrezik real.

**5. Mobilization (mobilizimi).** Faza e fundit fokusohet tek veprimet, si: - koordinimi i ekipeve të sigurisë (“security, IT, cloud, development, business owners”); - automatizimi i “veprimeve” korrigjuese, riparuese, ose për eliminim probleme, dobësi, ose kërcënime të identifikuara (pa ndërhyrje manual) ku është e mundur; - gjenerimi i udhëzimeve të qarta për fiksimit të problemit; - matja e progresit dhe e reduktimit të rrezikut të sulmit kibernetik. “Mobilizimi” e mbyll ciklin dhe “ushqen” fazën e re të “scoping”-ut, duke e bërë procesin të vazhdueshëm.

**Platformat “EAP”** mbështesin veçanërisht fazat e “zbulimit, prioritizimit” dhe pjesërisht “mobilizimin”. Ato ofrojnë: - zbulim të unifikuar të aseteve në mjedise hibride; - analizë të rrugëve të sulmit; - vlerësim kontekstual të rrezikut (jo vetëm CVSS); - integrim me “threat intelligence”; - vizualizime dhe rekomandime për neutralizim të një kërcënimi; - lidhje me sistemet e “ticketing” dhe automatizimit (SOAR<sup>20</sup>, ITSM). Organizatat i përdorin EAP-të si “motor” operacional të programit CTEM.

“CTEM” është kuadri metodologjik (procesi), ndërsa “EAP” janë platformat që e bëjnë këtë proces të zbatueshëm në shkallë. Përdorimi i suksesshëm kërkon jo vetëm teknologji, por edhe disiplinë në “scoping”, validim të rregullt dhe mobilizim të qartë të ekipeve. Në kontekstin teknologjik dhe të sigurisë kibernetike për vitin 2026, CTEM/EAP përbëjnë një nga shtyllat kryesore të kalimit nga platformat e mbrojtjes “reactive” drejt qasjeve parandaluese “proaktive”.

<sup>19</sup> SLA = Service Level Agreement (marrëveshja e niveli të shërbimit): është një kontratë zyrtare midis një ofruesi të shërbimit (p.sh., cloud provider, ISP, software-i) dhe një klienti, e cila përcakton standardet e pritshme të performancës, disponueshmërisë, dhe përgjegjësisë për shërbimin e ofruar; ISO/IEC 20000-1, “IT Service Management Standard”

<sup>20</sup> SOAR = Security Orchestration, Automation, and Response: është një platformë ose grup mjetesh të sigurisë kibernetike të rrisë efikasitetin, të ulë ngarkesën e analistëve, dhe të përmirësojë kohën e përgjigjes ndaj kërcënimeve.

- **Parashikimi i IA/ML dhe analitikat e sjelljes (Artificial Intelligence /Machine Learning prediktiv and Behavioral Analytics (UEBA):** Modele që ndërtojnë “linjat bazë” të sjelljes normale dhe parashikojnë sjellje anormale ose lëvizje të ardhshme të sulmuesit dixhital. “UEBA” është një qasje e avancuar e analizës së sjelljes që përdor Inteligjencën Artificiale (IA) dhe Machine Learning (ML) për të ndërtuar profile dinamike të sjelljes “normale” të përdoruesve dhe të entiteteve (pajisje, aplikacione, IP, llogari shërbimi, etj.), dhe më pas për të zbuluar devijime anormale që mund të tregojnë kërcënime. Kur kombinohet me “AI/ML prediktiv”, ajo kalon nga detektimi i anomalive drejt parashikimit të sjelljeve të ardhshme të rrezikshme.

### **1. Procesi bazë i funksionimit të “UEBA”:**

**Hapi 1: Mbledhja e të dhënave.** Platforma grumbullon të dhëna nga burime të shumta: - log-et e autentifikimit (IAM<sup>21</sup>, active directory, SSO<sup>22</sup>); - aktiviteti i “endpoint”-eve dhe rrjetit; - aksesit në skedarë, “cloud” dhe “SaaS”; - ngjarjet e privilegjeve; - të dhëna nga SIEM, EDR, XDR, etj.

**Hapi 2: Ndërtimi i “baseline”-ve të sjelljes.** Gjatë një periudhe “mësimore” (zakonisht 2–4 javë ose më shumë), sistemi përdor modele statistikore dhe “ML” për të krijuar profile individuale dhe grupe, si: - orët tipike të punës; - sistemet dhe aplikacionet që aksesohen zakonisht; - vëllimi i skedarëve ose i të dhënave; - vendndodhjet gjeografike; - sekuencat tipike të veprimeve. Modelet përditësohen vazhdimisht për të pasqyruar ndryshimet legjitime.

**Hapi 3: Analiza e anomalive dhe “risk scoring”.** Çdo ngjarje e re krahasohet me “linjën bazë”. Sistemi vlerëson: - devijimin individual (sa i rrallë është veprimi për atë përdorues); - krahasimin me “peer group”; - modelet kohore (time-series); - sekuencat e veprimeve (p.sh. login → mbledhje informacioni nga AD → akses “share” i ndjeshëm → “upload” në “cloud personal”). Rezultati është një “risk score” që grumbullohet me kalimin e kohës. Një veprim i vetëm mund të jetë me risk të ulët, por kombinimi i disa anomalive ngre rezultatin total dhe shkakton alarm.

**Hapi 4: Konteksti dhe “storytelling”.** Platformat moderne ndërtojnë “timeline” të aktivitetit të entiteteve, lidhin ngjarjet midis burimeve të ndryshme

<sup>21</sup> IAM = Identity and Access Management (menaxhimi i identitetit dhe aksesit): sistemi që menaxhon kush ka akses, në çfarë burimesh, dhe nën çfarë kushtesh. Është shtylla kryesore e sigurisë moderne, duke siguruar që vetëm përdoruesit e autorizuar të kenë akses të kontrolluar të të dhënave dhe sistemet kritike; NIST SP 800-63B, “Digital Identity Guidelines”.

<sup>22</sup> SSO = Single Sign-On (hyrje e vetme/identifikim i njëhershëm): një sistem që lejon përdoruesit të hyjnë në shumë aplikacione me një identifikim të vetëm, duke përmirësuar produktivitetin, eksperiencën e përdoruesit, dhe menaxhimin e sigurisë nëpërmjet reduktimit të fjalëkalimeve të shumta; NIST SP 800-63B, “Digital Identity Guidelines”.

dhe ofrojnë shpjegime të kuptueshme për analistët (shpesh me ndihmën e “Generative AI”).

**2. Roli i “AI/ML prediktiv”:** Përtej detektimit të anomalive, modelet prediktive synojnë të parashikojnë: - lëvizjet e ardhshme të sulmuesit (p.sh. parashikimi i hapave të ardhshëm në “zinxhirin” e sulmit); - rrezikun e komprometimit të një llogarie ose pajisjeje teknologjike; - rrugët e mundshme të sulmit (attack path prediction); - probabilitetin që një sjellje e caktuar të çojë në incident. Teknikat e përdorura përfshijnë: - modele statistikore dhe “unsupervised learning” (për anomali të panjohura), - “supervised learning”; - “deep learning” për sequenca komplekse dhe marrëdhënie midis entiteteve; - “ensemble methods” për saktësi më të lartë.

**3. Si përdoret në praktikë:** “Use case”-e kryesore: - zbulimi i llogarive të kompromentuara; - kërcënimet e brendshme (qëllimore ose nga pakujdesia); - lëvizja laterale; - eksfiltrimi<sup>23</sup> i të dhënave; - abuzimi i privilegjeve; - sjellje anomale e agjentëve IA ose llogarive të shërbimit; - “phishing and business email compromise” (BEC) përmes ndryshimeve të sjelljes komunikuese. Integrimi me platforma të tjera: - “SIEM/XDR – UEBA” pasuron alarmet me kontekst sjelljeje dhe “risk score”, “SOAR – risk score” i lartë mund të shkaktojë automatizim (bllokim sesioni, “MFA step-up”, izolim); - “CTEM/ Exposure Management”: sjellja anomale ndihmon në verifikim i ekspozimeve; - “Identity platforms” – vendimmarrje “adaptive access” (Zero Trust).

**4. Përfitimet kryesore:** - zbulon kërcënime që nuk kanë “firma” të njohura; - redukton false positives përmes kontekstualizimit dhe “peer analysis”; - zbulon kërcënime të brendshme që mbrojtja perimetrale nuk i sheh; - mbështet qasjen proaktive duke identifikuar sjellje të dyshimta herët; - ofron renditje sipas prioritetit të bazuar në risk, jo vetëm mbi rregullat statike.

**5. Kufizimet dhe sfidat:** - kërkon të dhëna cilësore; - ndryshimet legjitime të sjelljes mund të shkaktojnë alarme të rreme nëse modelet nuk përshtaten mirë; - “explainability” & disa modele “deep learning” janë të vështira për t’u shpjeguar; - mbulimi i plotë kërkon integrim të gjerë të burimeve të të dhënave; - nevojitet “human-in-the-loop” për vendime kritike.

**“UEBA” with “AI/ML prediktiv”** ndryshon logjikën e detektimit: në vend që të kërkojë “a përputhet me një “model” të njohur keqdashës?”, ajo pyet “a është kjo sjellje e qëndrueshme me atë që kemi vëzhguar më parë për këtë entitet dhe për grupin e tij?”. Në kontekstin teknologjik për vitin 2026, kjo “aftësi” është bërë shtyllë e platformave moderne të sigurisë kibernetike

<sup>23</sup>Procesi i transferimit të të dhënave sensitive nga një sistem i brendshëm në një vend të kontrolluar. Përdoren metoda të ndryshme për të nxjerrë të dhënat si: Email, Cloud storage, FTP/SFTP, DNS tunneling, HTTPS/SSL.

(veçanërisht “XDR” dhe “Autonomous SOC”), duke mundësuar zbulimin e hershëm të kërcënimeve të sofistikuara dhe mbështetjen e qasjeve parandaluese proaktive.

- **Zbulim dhe reagimi i zgjeruar ndaj incidenteve të sigurisë dhe “SIEM/XSIAM”<sup>24</sup> të integruar** (Extended Detection and Response (XDR)<sup>25</sup> and integrated SIEM/XSIAM). Unifikim i të dhënave nga “endpoint”, rrjet, “cloud”, identitet dhe email, me aftësi automatizimi.

**Extended Detection and Response (XDR)** është një arkitekturë e unifikuar e sigurisë kibernetike që grumbullon, normalizon, vendos lidhje të të dhënave ose ngjarjeve dhe analizon ato nga “shtresa” të shumta të mjedisit (“endpoint”, rrjet, “cloud”, identitet, email, “SaaS”) për të ofruar detektim, investigim dhe përgjigje të automatizuar ndaj kërcënimeve. Ajo evoluoi nga “Endpoint Detection and Response” (EDR) duke e zgjeruar mbulimin përtej pajisjeve fundore.

**XSIAM (Extended Security Intelligence and Automation Management)** është termi i Palo Alto Networks<sup>26</sup> për një platformë më të gjerë, të drejtuar nga IA, që unifikon “XDR”, funksionalitetet e “SIEM, SOAR<sup>27</sup>, Attack Surface Management, Threat Intelligence” dhe “UEBA” në një zgjidhje të vetme “cloud-native”. Qëllimi i saj është të zëvendësojë ose të reduktojë ndjeshëm nevojën për “SIEM” tradicionale në operacionet e përditshme digjitale.

**1. Si funksionon “XDR” – arkitektura dhe procesi.** “XDR” operon në tre faza kryesore:

- **Mbledhja, importimi dhe transferimi i të dhënave nga burime të ndryshme në një sistem qendror dhe “normalizimi” i të dhënave.** Platforma mbledh të dhëna nga: - agjentë “endpoint” (EDR/XDR agents); - firewall-e, NDR, DNS; - identitet (IAM, Active Directory, Entra ID); - Cloud (AWS, GCP, SaaS); - Email dhe “collaboration tools”; - burime “third-party”. Të dhënat “normalizohen” në një model të përbashkët “data” që lejon korrelacionin e lehtë midis tyre.

---

<sup>24</sup> XSIAM = Extended Security Intelligence, Automation, and Management (inteligjencë e zgjeruar e sigurisë, automatizim dhe menaxhim): një platformë e drejtuar nga AI që automatizon të gjithë operacionet e sigurisë, duke shkruar përtej detektimit dhe përgjigjes (XDR) drejt një SOC autonom, parashikues, dhe të plotësisht të integruar. Është e ardhmja e menaxhimit të sigurisë kibernetike, duke reduktuar varësinë nga ndërhyrja njerëzore dhe duke rritur shpejtësinë dhe saktësinë e përgjigjes ndaj kërcënimeve; <https://www.paloaltonetworks.com/cortex/xsiams>; Palo Alto Networks, “What is XSIAM?”

<sup>25</sup> Sqarimi teknik për termin XDR te “referenca 1”.

<sup>26</sup> Palo Alto Networks — kompania krijuese të platformës XSIAM, si dhe të teknologjiave të tjera të sigurisë kibernetike, <https://www.paloaltonetworks.com>; <https://www.paloaltonetworks.com/resources/datasheets/cortex-xsiams-datasheet>

<sup>27</sup> Shiko sqarimin teknik te “20”.

- **Analiza, korrelacioni dhe detektimi.** Në vend që të gjenerojë alarme të izoluar, “XDR”: - aplikon rregulla, “machine learning and behavioral analytics”; - lidh automatikisht ngjarjet midis “shtresave” (p.sh. login i dyshimtë + proces i dyshimtë në “endpoint” + lidhje e dyshimtë në rrjet); - ndërton “timeline” të sulmit dhe “root-cause analysis”; - grupon alarme të lidhura në incidente. Kjo redukton ndjeshëm volumën e alarmeve dhe ofron kontekst të plotë për analistët.

- **Përgjigje e automatizuar dhe e orkestruar.** Nga një “console” e vetme, “XDR” mund të: - izolojë “endpoint”-in; - bllokojë IP-të ose “domain” në “firewall”; - aktivizojë llogarinë e përdoruesit; - karantinojë email-in; - ekzekutojë “playbook”-e SOAR.

**2. Si përdoret në praktikë:** - platforma grumbullon të dhëna në kohë reale; - AI/ML dhe rregullat identifikojnë aktivitet të dyshimtë, - ngjarjet lidhen automatikisht në incidente me prioritet; - analisti sheh një “timeline” të plotë të sulmit (kush, çfarë, kur, si); - përgjigja mund të jetë automatike (për raste me besueshmëri të lartë) ose e asistuar; - “threat hunting” bëhet mbi të dhëna të unifikuar.

**Aftësi kyçe të platformave “XDR/XSIAM”:** - lidh “cross-domain” dhe “incident grouping”; - “Root-cause analysis” dhe “attack chain reconstruction”; - UEBA i integruar; - “Threat intelligence” e shkrirë me të dhënat; - automatizim i përgjigjes; - “Threat hunting” i avancuar; - tek XSIAM: edhe “log management, compliance reporting” dhe “Attack Surface Management”.

**3. Përfitimet kryesore:** - reduktim dramatik i alarmeve (pak incidente të kuptueshme); - shpejtësi më e madhe e detektimit dhe e përgjigjes (minuta në vend të orëve/ditëve); - vizibilitet i unifikuar mbi të gjithë sipërfaqen e sulmit; - më pak “console” dhe më pak kompleksitet operacional; - mbështetje e qasjes “proactive” përmes “behavioral analytics” dhe automatizimit.

**4. Kufizimet dhe konsideratat:** - “XDR native” funksionon më mirë me ekosistemin e vetë vendorit; “open XDR” lejon integrim më të gjerë “third-party”; - për pajtueshmëri që kërkon ruajtje shumëvjeçar të log-eve, shumë organizata mbajnë ende një “SIEM” paralelisht; - cilësia e detektimit varet shumë nga thellësia e telemetrisë së “endpoint”-it (“EDR” i fortë mbetet themeli i procesit); - kërkon integrim të mirë dhe “akordim” fillestar të proceseve.

**XDR** përfaqëson evolutimin e detektimit dhe përgjigjes nga “bunker” të izoluar (EDR, NDR, etj.) drejt një platforme të unifikuar “cross-domain”.

**XSIAM** shkon edhe më larg duke synuar të bëhet “qendra e operacioneve”, duke thithur funksionalitetet e “SIEM, SOAR” dhe të tjera në një arkitekturë

të drejtuar nga IA<sup>28</sup>. Në praktikën e vitit 2026, këto platforma janë bërë shtylla e operacioneve moderne të sigurisë, duke mundësuar korrelacion automatik, reduktim të aktiviteteve dëmtuese dhe përgjigje më të shpejtë, elemente thelbësore për kalimin nga mbrojtja reaktive drejt qasjeve parandaluese “proactive”<sup>29</sup>.

- **Orkestrimi, automatizimi dhe reagimi ndaj incidenteve të sigurisë si dhe agjenti IA** (Security Orchestration, Automation and Response (SOAR) and Agentic AI<sup>30</sup>). Përdorim i algoritmeve të të “mësuarit automatik” për identifikimin e anomalive në kohë reale dhe ekzekutimin e skenarëve të përgjigjes automatike (*playbooks*). Agjentë autonomë të IA kryejnë përzgjedhje, investigim dhe reagimi i zgjeruar ndaj incidenteve të sigurisë me ndërhyrje minimale njerëzore (“autonomous SOC”).

1. **Çfarë është “SOAR”**. SOAR është një platformë që kombinon tre funksione kryesore: - **“orchestration”**: koordinimi i veprimeve midis mjeteve të ndryshme të sigurisë përmes API-ve dhe integritimeve; - **“automation”**: ekzekutimi automatik i detyrave të përsëritura dhe të paracaktuara; - **“response”**: menaxhimi i rastit (case management) dhe ekzekutimi i veprimeve të përgjigjes ndaj incidenteve. SOAR nuk zbulon kërcënime vetë; ai merr alarme nga “SIEM, XDR, EDR, email”, etj., dhe orkestron hetimin si dhe reagimin sipas logjikës së paracaktuar.

2. **Arkitektura teknike e “SOAR”**. Një platformë SOAR moderne përbëhet nga këto komponentë kryesorë: - **“Trigger/Ingestion”** (merr alarme, ngjarje ose ticket-e nga burime të jashtme (SIEM, XDR, mailbox, etj.); - **“Integrations/Connectors”** (“wrapper API” që lejojnë thirrjen e veprimeve në mjete të treta (EDR, firewall, IAM, TI, ticketing); - **“Playbook Engine”** (motori i ekzekutimit të workflow-eve (me hapa, kushte, degëzime); - **“Case/Incident Management”**; - **“Scripting/Code Layer”** (mbështetje për aplikacionet “Python, JavaScript” ose gjuhë të ngjashme për logjikë komplekse); - **“Human-in-the-Loop Gates”** (pika aprovimi për veprime me ndikim të lartë); - **“Audit&Reporting”** (“log” i plotë, “input”-i dhe “output”-i).

3. **Si funksionon një “Playbook SOAR”**. “Playbook”-u është zemra e “SOAR”-it. Ai është një “workflow” i paracaktuar që ekzekutohet gjithmonë në të njëjtën mënyrë kur plotësohen kushtet e “trigger”-it. Struktura tipike e një playbook-u:

<sup>28</sup> <https://deep-layer-security.io/insights/siem-vs-xdr-vs-soar>

<sup>29</sup> <https://blog.it-learn.io/posts/2026-04-24-xdr-explained-cortex-vs-crowdstrike-vs-sentinel/>

<sup>30</sup> Agentic AI = Inteligjencë Artificiale që vepron si “agjent” autonom, duke marrë vendime, duke planifikuar veprime, dhe duke ekzekutuar detyra komplekse në botën reale pa ndërhyrje të vazhdueshme njerëzore. Është e ardhmja e IA-së, duke shkuar përtej thjesht “të menduarit” drejt “të vepruarit” autonom.

- a) **Trigger:** kushti që nisin p.sh. “Alert severity  $\geq$  High XDR”; email i raportuar si “phishing”.
- b) **Enrichment:** mbledhja e kontekstit (“query SIEM”, kërkim “IOC” në “threat intelligence”, “lookup” i përdoruesit në “IAM”, detonim i skedarit në “sandbox”).
- c) **Decision Logic:** degëzime “if-then-else” (p.sh. nëse “hash” është “known-malicious” → vazhdo me “containment”; përndryshe → “escalate”).
- d) **Actions:** veprime konkrete (izolim “endpoint, disable account, block IP, quarantine email”, hap “ticket” në “Jira/ServiceNow”, njoftim në “Slack”).
- e) **Human Approval** (opsionale): pika ku analisti duhet të aprovjë veprime kritike.
- f) **Closure & Documentation:** mbyllja e rastit dhe gjenerimi i raportit.

“Playbook”-et janë të shkëlqyera për skenarë të parashikueshëm dhe të përsëritur, por dështojnë kur sulmi del jashtë kushteve të parashikuara nga autori i “playbook”-ut.

**4. “Agentic AI” – evolucioni përtej “SOAR”.** “Agjenti” i IA përfaqëson një ndryshim paradigme. Ndryshe nga SOAR (që ekzekuton logjikë të shkruar paraprakisht), agjentët IA: - vendosin vetë se cili hap të ndërmerret më pas, bazuar në evidencën e mbledhur; - formojnë hipoteza, testojnë ato dhe përshtatin planin e hetimit në kohë reale; - arsyetojnë mbi të dhëna të paparashikuara; - operojnë me autonomi të kufizuar brenda “guardrail”-eve të përcaktuara.

**5. Bashkëpunimi “SOAR” dhe “Agentic AI”.** Në vitin 2026 modelet kombinohen: - “Agentic AI” merret me arsyetimin, hetimin dhe vendimmarrjen dinamike; - “SOAR” mbetet “shtresa” e ekzekutimit të besueshëm të veprimeve përcaktuese (izolim, bllokim, njoftim). Agjenti IA “vendos” çfarë duhet bërë; SOAR “e bën” atë në mënyrë të kontrolluar dhe të përsëritshme.

SOAR ofron automatizim të besueshëm dhe të audituar të proceseve përmes “playbook”-eve përcaktuese. “Agentic AI” sjell aftësinë e arsyetimit dinamik dhe të përshtatjes në kohë reale, duke kapërcyer kufizimet e “playbook”-eve statike. Në arkitekturat e konsoliduara të viti 2026, ato nuk zëvendësojnë njëra-tjetrën, por plotësojnë: “Agentic AI” heton dhe vendos, ndërsa “SOAR” ekzekuton me disiplinë dhe kontroll. Kjo kombinim është themeli teknik i “Agentic SOC”<sup>31</sup> dhe i kalimit drejt operacioneve të sigurisë me autonomi të plotë dhe të menaxhim të kufizuar.

<sup>31</sup> Agentic SOC = Security Operations Center edrejtuar nga inteligenca artificiale agjentike, ku agjentët autonomë të IA-së kryejnë detektimin, investigimin, dhe përgjigjen ndaj kërcënimeve me ndërhyrje minimale njerëzore. Është e ardhmja e operacioneve të sigurisë, duke shkuar përtej automatizimit (SOAR) drejt autonomisë së plotë dhe mësimi të vazhdueshëm.

- **Teknologjitë e mashtrimit dhe mbrojtje me objektiv të lëvizshëm** (Deception Technologies and Moving Target Defense). **“Deception Technologies”** (teknologjitë e mashtrimit) janë një “shtresë” e mbrojtjes aktive që vendos asete false (decoys), “lures” (karremë) dhe “honeytokens” (shenja joshëse) brenda mjedisit real digjital. Qëllimi është të tërheqë, të zbulojë dhe të ngadalësojë sulmuesin, duke gjeneruar alarme me besueshmëri shumë të lartë (pothuajse “zero false positives”), sepse përdoruesit legjitimë nuk kanë arsye të ndërveprojnë me këto asete.

### *1. Si funksionon në praktikë:*

- **“Deployment”**: platforma (shpesh me IA) vendos automatikisht “decoys” dhe “lures” në rrjet, “endpoint, cloud, identity layer”, duke i bërë ato të duken sa më realiste; - **“Interaction Detection”**: çdo ndërveprim me një “decoy/lure/honeytoken (login attempt, file open, API call, credential use)” gjeneron menjëherë alarm me kontekst të plotë (IP, user, commands, timeline); - **“Engagement & Intelligence Gathering”**: “Decoy”-t e avancuara mund të “luajnë” me sulmuesin (përgjigje dinamike, AI-generated responses) për të mbledhur “tactics, techniques, procedures”; - **“Response Integration”**: alarmi dërgohet në SIEM/XDR/SOAR për korrelacion, investigim dhe përgjigje të automatizuar (izolim, bllokim).

2. **Avantazhi kryesor**: ndryshe nga detektimi tradicional (që duhet të dallojë “të mirën” nga “të keqen”), çdo ndërveprim me “mjete mashtrimi” është me përkufizim keqdashës → sinjal me “besnikëri” ekstremisht të lartë.

- **“Moving Target Defense” (MTD)** është një strategji mbrojtëse që ndryshon dinamikisht konfigurimin, sipërfaqen e sulmit ose karakteristikat e sistemit për ta bërë atë të paparashikueshëm dhe më të vështirë për t’u shfrytëzuar nga sulmuesi. Në vend që sistemi të mbetet statik (duke i dhënë sulmuesit kohë për zbulim), MTD e “lëviz” sistemin vazhdimisht. Kategoritë kryesore të teknikave MTD (sipas shtresave): - **“Dynamic Network”**: “IP shuffling, port randomization, virtual IP rotation, DNS shuffling, traffic obfuscation”; - **“Dynamic Platform/Runtime”**: “address space layout randomization (ASLR), instruction set randomization, container/VM migration”; - **“Dynamic Software”**: “code diversification, software diversity” (“binary”-ies të ndryshme që bëjnë të njëjtën gjë); - **“Dynamic Data”**: ndryshimi i formatit, “encoding”-ut ose strukturës së të dhënave; - **“Dynamic Configuration”**: ndryshimi i parametrave, privilegjeve, shërbimeve të ekspozuara.

3. **Si përdoren së bashku “Deception + MTD”**. Platformat integrojnë dy qasje: - **“Deception”** krijon “kurthe” statike ose gjysmë-dinamike që tërheqin dhe zbulojnë; - **“MTD”** e bën mjedisin real të “lëvizshëm”, duke rritur koston dhe kompleksitetin e sulmit; - **Kombinimi**: sulmuesi që lëviz ndesh në “lures/decoys”, ndërsa asetet reale ndryshojnë vazhdimisht (IP, porte, konfigurime).

Shembull i avancuar: Platforma vendos “decoys” që “lëvizin” ose përdor MTD për të “qarkulluar” asetet reale ndërsa “decoys” mbeten si pika tërheqëse.

**4. Përfitimet:** - sinjale me false positive ekstremisht të ulët; - zbulim i sulmeve që mjetet tradicionale i humbasin; - intelligence e pasur mbi sjelljen e sulmuesit; - efekt psikologjik dhe operacional; - mbështetje e fortë për qasjen “preemptive” (“deny – deceive – disrupt”).

**5. Kufizimet:** - kërkon planifikim të mirë për të mos u zbuluar lehtë nga sulmuesit e sofistikuar; - “decoy”-t e dobëta mund të injorohen ose të identifikohen; - MTD mund të sjellë “overhead” (performancë, kompleksitet menaxhimi) nëse nuk implementohet me kujdes; - nuk zëvendëson kontrollët parandaluese; është shtresë plotësuese.

“**Deception Technologies**” krijojnë një “fushë minash” të kontrolluar brenda mjedisit, ku çdo hap i gabuar i sulmuesit gjeneron alarm të pastër dhe zbulim.

“**Moving Target Defense**” e bën sipërfaqen e sulmit të lëvizshme dhe të paparashikueshme. Së bashku, ato formojnë një nga shtyllat më të fuqishme të mbrojtjes proaktive dhe parandaluese. Në arkitekturat e 2026 ato integrohen thellësisht me XDR, SOAR dhe “Agentic AI” për detektim të hershëm dhe përgjigje të automatizuar.

### III. Trendet kryesore për vitin 2026

- **Kalimi drejt “autonomous/Agentic SOC”:** – agjenti IA merr përsipër punën e nivelit L2 (partial autonomy-njeriu aprovon veprime) dhe pjesërisht të nivelit L3 (conditional autonomy– njeriu ndërhyr vetëm në raste kritike). Shumica e platformave të 2026 operojnë midis L2 dhe L3.

- **Rritja e rëndësisë së “identitetit” dhe “Cloud”:** si sipërfaqe detektimi në platformat “XDR”.

- **Integrimi i “exposure management” me detektimin dhe përgjigjen** në platforma të unifikuara (p.sh. Cortex XSIAM<sup>32</sup>, Falcon<sup>33</sup>, etj.). Të dyja janë liderë në fushën e sigurisë kibernetike, por “Cortex XSIAM” shkon më larg drejt autonomisë së plotë, ndërsa “Falcon” është më i fokusuar në mbrojtjen e “endpoint”-eve dhe “XDR”.

**Parashikim i lartë**– parashikon lëvizjet e ardhshme të sulmuesit me besueshmëri shumë të lartë.

<sup>32</sup> Cortex XSIAM: platformë e avancuar sigurie e drejtuar nga agjentë IA, që automatizon të gjithë ciklin e operacioneve të sigurisë me ndërhyrje minimale njerëzore; <https://www.paloaltonetworks.com/cortex/xsiams>.

<sup>33</sup> Falcon (CrowdStrike): platformë e integruar sigurie në cloud, e fokusuar fillimisht në EDR/XDR, që ofron mbrojtje të avancuar të “endpoint”-eve, detektim të kërcënimeve, dhe përgjigje të automatizuar; <https://www.crowdstrike.com/products/falcon-platform/>

- **Siguria e vetë IA-së** (AI-SPM<sup>34</sup>, mbrojtja e modeleve dhe e “pipeline”-ve të të dhënave).

- **Konsolidimi i platformave** – organizatat preferojnë më pak “console” dhe më shumë integrim.

#### **IV. Aplikime në kontekstin ushtarak, aleat dhe NATO**

NATO ka zhvendosur gradualisht fokusin e mbrojtjes kibernetike nga modeli kryesisht reaktiv drejt qasjeve parandaluese “proaktive”. Kjo reflektohet në: - Alliance Digital Strategy (2026); - Digital Transformation Implementation Strategy; - NATO Principles of Responsible Use of AI; - aktivitetet e NATO STO (Science & Technology Organization) dhe CCDCOE (Cooperative Cyber Defence Centre of Excellence) që zhvillojnë koncepte, ushtrime dhe arkitektura referuese.

##### ***Aplikimet kryesore të platformave parandaluese “proactive”:***

**a) “Autonomous/Agentic Cyber Defence Agents”:** NATO STO ka publikuar punime mbi zhvillimin e A/ACD Agents për mjedise “tactical edge”. Arkitekturat e propozuara kombinojnë “Multi-Agent Reinforcement Learning (MARL), Large Language Models” dhe sisteme “rule-based” për monitorim, detektim dhe “mitigim autonom”. Agjentët IA trajnohen në “Automated Cyber Operations (ACO) gym” që simulohen rrjetet e mbrojtura të NATO-s.

**b) “Zero Trust Architecture”:** “Zero Trust” është bërë parim bazë për infrastrukturën digjitale të Aleancës. Ajo aplikohet në “federated platforms, cloud hibrid, tactical edge and mission-critical services” për të siguruar “continuous verification, least privilege and data-centric security”.

**c) “Continuous Threat Exposure Management (CTEM) dhe Exposure Assessment”:** në kontekst ushtarak, “CTEM” përdoret për vlerësim të vazhdueshëm të ekspozimeve në rrjete statike, mobile dhe të kontestuar, duke renditur me prioritet asetet kritike për sigurimin e misionit.

**d) “XDR/SIEM të integruara dhe platforma “AI-native”:** Platforma si “CrowdStrike Falcon” janë përdorur me sukses në ushtrimin Locked Shields 2025 (organizuar nga CCDCOE), ku ekipi Gjermani-Singapor arriti rezultatin më të lartë. Këto platforma ofrojnë detektim “cross-domain”, korrelacion automatik dhe përgjigje të shpejtë në skenarë kompleksë të mbrojtjes kibernetike.

---

<sup>34</sup> AI Security Posture Management: platformë ose grup mjetesh që mbrojnë sistemet e IA duke identifikuar asetet, vlerësuar rreziqet, dhe zbatuar politika sigurie për të parandaluar sulmet specifike ndaj AI-së; Wiz, “AI SPM” (2024)

e) **“Deception Technologies”**: përdoren si “shtresë” parandaluese për zbulimin e hershëm të “lëvizjeve anësore” dhe për mbledhjen e zbulimeve mbi TTP-të e kundërshtarit dhe alarmeve me besueshmëri të lartë.

f) **“SOAR + Agentic AI”**: orkestrimi i përgjigjes së automatizuar dhe hetimeve autonome po testohet për të reduktuar kohën e reagimit në operacione “multi-domain”, duke ruajtur “human-in-the-loop” për vendime kritike.

**Iniciativa mbështetëse**: - **NATO DIANA** (Defence Innovation Accelerator for the North Atlantic): përshpejton adoptimin e teknologjive “dual-use”, përfshirë zgjidhje proaktive dhe IA për “decision superiority”; - **NCIA Technology Strategy**; - **CWIX&Locked Shields**: testohen kapacitetet e IA për “Cyber Indications & Warning” dhe mbrojtje parandaluese “proaktive”.

Në kontekstin ushtarak dhe të NATO-s, platformat parandaluese “proaktive” po integrohen gradualisht për të kaluar nga detektimi reaktiv drejt parashikimit, parandalimit dhe neutralizimit të kërcënimeve para se ato të ndikojnë sigurinë e misionit. Prioriteti është ndërveprueshmëria, autonomia e kontrolluar dhe rezistenca në mjedise të degraduara.

## V. Integrimi i platformave parandaluese “proaktive” të sigurisë kibernetike në FARSH

Forcat e Armatosura të Republikës së Shqipërisë kanë ndërmarrë hapa të rëndësishëm në ndërtimin e kapaciteteve kibernetike, si: - ngritjen e Komandës Kibernetike dhe Ndërlidhjes (KKN); - Strategjia e Mbrojtjes Kibernetike 2024–2028; - Strategjia Kombëtare e Sigurisë Kibernetike 2025–2030 (miratuar në 2025); - anëtarësimi në NATO CCDCOE (2026) dhe pjesëmarrja në ushtrime me aleatët & NATO. Për shkak të burimeve të kufizuara, integrimi duhet të jetë gradual, sipas prioriteteve dhe i përputhur plotësisht me standardet e NATO-s.

Rekomandohen këto faza “logjike” ndërveprimi teknologjik në sistemet TIK:

**Faza 1 – Themelimi i mbrojtjes “proactive” (afatshkurtër)**: - Zero Trust Architecture si parim bazë për rrjetet e SKI të FARSH; - “Continuous Threat Exposure Management (CTEM)/Exposure Assessment: për identifikimin e vazhdueshëm të ekspozimeve në asetet kritike ushtarake; - përforcimi i kapaciteteve ekzistuese të detektimit drejt qasjes “predictive”.

**Faza 2 – Unifikimi i detektimit dhe reagimit ndaj kërcënimeve**: - adoptimi gradual i platformave “XDR” (ose platformave “AI-native” si Falcon/Cortex) për korrelacion “cross-domain” (endpoint, network, identity, cloud); - integrimi i “SOAR” për automatizimin e proceseve të përsëritura të reagimit ndaj incidenteve; - fillimi i përdorimit të “UEBA/Behavioral Analytics” për zbulimin e sjelljeve anomale (veçanërisht “insider threats dhe credential abuse”).

**Faza 3 – Kapacitete parandaluese të avancuara (afatmesëm):** - “Deception Technologies” për zbulim të hershëm të “lëvizjeve anësore” (lateral movement) me alarme me besnikëri të lartë; - experimentim i kontrolluar me “Agentic AI/Autonomous Cyber Defence Agents” në mjedise të izoluar ose të simuluar, në përputhje me “Principles of Responsible Use” të NATO-s; - përgatitja për “post-quantum cryptography” në komunikimet kritike me NATO-n.

**Parime udhëzuese për integrim të suksesshëm:**

- Përputhshmëria me standartet e NATO-s: – “Zero Trust, Federated Mission Networking”, ndërveprueshmëri dhe siguri realizimi të misionit;
- Qasje me faza dhe e matshme – fillim me asetet më kritike (komandim-kontroll, sisteme të komunikimit).
- “Human-in-the-loop” - autonomi e kufizuar, me kontroll të qartë njerëzor.
- Trajnim dhe doctrine: zhvillimi i “Doktrinës Kombëtare të Mbrojtjes Kibernetike” në përputhje me NATO-n dhe investim i vazhdueshëm në burime njerëzore & personel.
- Bashkëpunimi ndërkombëtar (CCDCOE, DIANA), shfrytëzimi i mbështetjes amerikane.
- Integrimi me infrastrukturën ekzistuese – shmangia e “bunkerëve” teknologjik të rinj dhe maksimizimi i investimeve aktuale (“Cyber Operations Center, kit deployable”).

**Sfidat kryesore:** - Burimet njerëzore dhe financiare të kufizuara; - nevoja për ndërveprueshmëri të plotë me sistemet e aleatëve & NATO; - menaxhimi i rrezikut të teknologjive të reja (“AI agentike) në mjedis ushtarak; - mbrojtja e zinxhirit të furnizimit dhe e infrastrukturës kritike kombëtare që mbështet FARSH.

Integrimi i platformave parandaluese “proactive” në FARSH duhet të ndjekë një qasje pragmatike dhe të përputhur me NATO-n: fillimisht implementimin e platformave “Zero Trust + CTEM” + përforcim i detektimit ekzistues, pastaj “XDR/SOAR” dhe gradualisht kapacitete më të avancuara (Deception, Agentic AI). KKN duhet të mbetet qendra e këtij transformimi, duke kombinuar teknologjinë me doktrinën, trajnimin dhe bashkëpunimin me aleatët & NATO-n. Suksesi do të matet me rritjen e sigurimit të misionit dhe të gatishmërisë operationale në hapësirën kibernetike, si në misionet kombëtare ashtu edhe në ato aleate.

## Përfundime

Platformat parandaluese “proaktive” përfaqësojnë ndryshimin më të rëndësishëm të paradigmës në mbrojtjen kibernetike të dekadës. Në vitin 2026, ato po kalojnë nga koncept i avancuar në nevojë operationale. Institucionet, organizatat dhe strukturat e mbrojtjes kibernetike të Forcat e Armatosura që do të arrijnë të zhvendosin qendrën e gravitetit nga “detektimi i shpejtë” drejt “parandalimit inteligjent” do të kenë avantazh të qëndrueshëm përballë kërcënimeve të epokës së Inteligjencës Artificiale. Suksesi kërkon jo vetëm teknologji, por edhe ndryshim kulture, procesesh dhe kapacitetesh njerëzore.

## Bibliografia:

1. Gartner (2025–2026). Raporte mbi Preemptive Cybersecurity dhe Hype Cycle for Security Operations; “How to Implement CTEM in your organization” (2024).
2. Forrester Wave për XDR (2026).
3. Crowd Strike, Palo Alto Networks, Tenable, Cyware etj. mbi AI-driven dhe agentic defense.
4. NATO Alliance Digital Strategy (2026)
5. NATO STO papers mbi Autonomous Cyber Defence Agents (2025–2026)
6. NCIA Technology Strategy
7. NATO Science & Technology Reports.
8. NATO CCDCOE: <https://ccdcoe.org/>.
9. <https://www.sto.nato.int/challenges-for-developing-autonomous-cyber-defense/>.
10. Cyber Security Global Alliance: <https://www.csga-global.org/>.
11. <https://www.sto.nato.int/Pages/default.aspx> (NATO Science&Tech. Org.).
12. <https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/>.
13. <https://www.nsa.gov/Cybersecurity/>.
14. <https://www.cisa.gov/>.
15. <https://ctem.org/docs/what-is-continuous-threat-exposure-management>.
16. <https://www.nec.com/en/global/solutions/cybersecurity/blog/250829/index.html>
17. <https://www.armorcode.com/blog/mastering-the-5-stages-of-the-ctem-framework/>

18. <https://cyberdefenders.org/cybersecurity-glossary/security-orchestration-automation/>
19. <https://d3security.com/blog/best-agentic-soc-platforms/2026/> .
20. <https://www.dropzone.ai/blog/blog-soar-to-agentic-soc-evolution-security-automation>
21. <https://aksk.gov.al/en/the-national-cyber-security-strategy-2025-2030/>
22. <https://mod.gov.al/politikat-e-sigurise/strategji-te-mm>
23. <https://www.nato.int/en/official-texts-and-resources/2026/alliance-digital-strategy>.



# **Aplikimet e inteligjencës artificiale dhe “agjentëve” autonomë të saj në sistemet e mbrojtjes, avantazhet operacionale, rreziqet, sfidat dhe lufta e së ardhmes**

---

**Kolonel (R) Msc. Adi NDONI**

*Departamenti i Inovacionit dhe Teknologjisë, IKSHU*

## **Trajtesë e shkurtuar**

*Ky punim analizon përdorimin e Inteligjencës Artificiale (IA) dhe të sistemeve “Agentic AI” në sistemet moderne të mbrojtjes dhe të mënyrën e zhvillimit të operacioneve ushtarake. Vëmendje e veçantë i kushtohet kalimit nga sistemet tradicionale të automatizuara drejt agjentëve inteligjentë autonomë, të aftë të perceptojnë mjedisin operacional, të përpunojnë të dhëna në kohë reale, të marrin vendime dhe të ndërmarrin veprime të koordinuara me shkallë të ndryshme autonomie.*

*Studimi shqyrton aplikimet e Agentic AI në sistemet autonome ajrore, tokësore, detare, komandim-kontroll, inteligjencën ushtarake, luftën elektronike, mbrojtjen kibernetike dhe operacionet multidomain. Integrimi i IA mundëson përpunimin e sasive të mëdha të informacionit, përshpejtimin e vendimmarrjes, rritjen e ndërveprueshmërisë dhe koordinimin e sistemeve në kohë reale, duke krijuar potencial për rritjen e ndjeshme të efektivitetit dhe superioritetit operacional. Në të njëjtën kohë, punimi evidenton sfidat që shoqërojnë rritjen e autonomisë, veçanërisht rrezikun e gabimeve algoritmike, cenueshmërinë ndaj sulmeve kibernetike, vështirësitë e kontrollit njerëzor dhe çështjet e përgjegjësisë juridike e morale.*

*Për këtë arsye, përdorimi i Agentic AI në mbrojtje kërkon një ekuilibër ndërmjet inovacionit teknologjik, efektivitetit operacional, kontrollit njerëzor dhe respektimit të së drejtës ndërkombëtare humanitare. Në përfundim, punimi argumenton se IA dhe Agentic AI do të jenë ndër faktorët kryesorë të transformimit të forcave të armatosura dhe të luftës moderne, veçanërisht në operacionet multidomain.*

*Megjithatë, përfitimet e tyre strategjike mund të realizohen në mënyrë të qëndrueshme vetëm nëpërmjet zhvillimit të teknologjive të sigurta, standardeve të përshtatshme, mekanizmave efektivë të kontrollit njerëzor dhe respektimit të normave ndërkombëtare.*

**Fjalët kyçe:** Inteligjencë Artificiale; Agentic AI; agjentë autonomë; sisteme autonome; autonomi ushtarake; operacione multidomain; Swarm Warfare, Cognitive Warfare, Human-Machine Teaming, lufta algoritmike.

## **I. Aplikimet e Inteligjencës Artificiale dhe Agentic AI në sistemet e mbrojtjes**

Zhvillimi i Inteligjencës Artificiale (IA) dhe i sistemeve Agentic AI ka transformuar rrënjësisht mënyrën se si konceptohen dhe realizohen operacionet moderne ushtarake. Në dekadat e fundit, teknologjitë inteligjente kanë kaluar nga përdorimi eksperimental në komponentë thelbësorë të strukturave moderne të mbrojtjes. Sot, IA nuk përdoret vetëm për automatizimin e proceseve teknike, por edhe për analizë operative, planifikim strategjik, koordinim multidomain dhe vendimmarrje në kohë reale.

Aplikimet e IA shtrihen pothuajse në çdo dimension të luftës moderne: në ajër, në tokë, në det, në hapësirën kibernetike dhe në sistemet e komandimit strategjik. Përmes autonomisë, përpunimit masiv të informacionit dhe aftësisë për adaptim, Agentic AI po krijon një paradigmë të re të operacioneve ushtarake, ku shpejtësia e analizës dhe reagimit bëhet faktor dominues i superioritetit operacional.

### ***Sistemet autonome ajrore***

Sistemet autonome ajrore përfaqësojnë një nga aplikimet më të avancuara dhe më të përhapura të IA në sektorin e mbrojtjes. Dronët inteligjentë ose UAV-të (Unmanned Aerial Vehicles) kanë ndryshuar mënyrën e realizimit të operacioneve ushtarake, duke rritur ndjeshëm kapacitetet e zbulimit dhe goditjes precize. Fillimisht, dronët përdoreshin kryesisht për misione survejimi dhe zbulimi, sot është zgjeruar ndjeshëm funksionaliteti i tyre. Sistemet moderne janë të afta të analizojnë mjedisin operacional, të identifikojnë objektiva, të ndjekin automatikisht lëvizjet e kundërshtarit dhe të përshtatin misionin në kohë reale.

Një nga funksionet kryesore të dronëve inteligjentë është zbulimi dhe survejimi strategjik. Përmes kamerave elektro-optike, sensorëve infra të kuq dhe radarëve inteligjentë, dronët mund të monitorojnë zona të gjera operative dhe të transmetojnë informacion në kohë reale drejt qendrave të komandimit. IA analizon automatikisht imazhet dhe identifikon aktivitete ose objekte të

dyshimta, duke reduktuar ngarkesën e operatorëve njerëzorë.<sup>1</sup>

Gjithashtu, IA ka përmirësuar ndjeshëm identifikimin e objektivave. Algoritmet e Machine Learning dhe Deep Learning mund të dallojnë automatikisht mjete të blinduara, sisteme raketore, objekte strategjike ose lëvizje trupash në bazë të karakteristikave vizuale, termike dhe elektromagnetike, duke rritur ndjeshëm saktësinë e operacioneve dhe redukon rrezikun e gabimeve.

Sistemet moderne autonome janë të afta të kryejnë goditje precize me ndërhyrje minimale njerëzore. Dronët mund të analizojnë situatën taktike, të përzgjedhin itinerarin optimal dhe të godasin objektivin me saktësi të lartë.<sup>2</sup> Një zhvillim revolucionar në këtë fushë është koncepti i “Swarm Drones”. Këto sisteme përfshijnë dhjetëra ose qindra dronë që bashkëpunojnë në mënyrë autonome si një organizëm inteligjent kolektiv.

### ***Sistemet tokësore autonome***

Përveç dimensionit ajror, IA po transformon edhe operacionet tokësore përmes përdorimit të mjeteve autonome robotike. Sistemet tokësore autonome ose UGV-të (Unmanned Ground Vehicles) janë projektuar për të operuar në mjedise me rrezik të lartë dhe për të kryer detyra që tradicionalisht realizoheshin nga personeli ushtarak. Një nga përdorimet më të zakonshme është patrullimi autonom. Robotët tokësorë mund të monitorojnë baza ushtarake, kufij ose zona kritike infrastrukturore pa nevojën e pranisë së vazhdueshme njerëzore. Përmes sensorëve inteligjentë dhe algoritmeve të analizës së sjelljes, këto sisteme mund të identifikojnë lëvizje të dyshimta dhe të raportojnë kërcënime në kohë reale. Në fushën logjistike, sistemet autonome përdoren për transportin e furnizimeve, municioneve dhe pajisjeve në zona të rrezikshme, duke rritur efikasitetin operacional të forcave ushtarake. Një tjetër aplikim shumë i rëndësishëm është neutralizimi i eksplozivëve dhe operacionet EOD (Explosive Ordnance Disposal). Robotët inteligjentë mund të identifikojnë, analizojnë dhe neutralizojnë mjete shpërthyes pa rrezikuar jetën e specialistëve ushtarakë. Në konfliktet moderne urbane, ku mjedisi operacional është kompleks dhe i rrezikshëm, robotët autonomë mund të eksplorojnë ndërtesa, të zbulojnë kërcënime dhe të mbështesin njësitë luftarake me informacione taktike në kohë reale.

### ***Sistemet detare autonome***

Dimensioni detar po përjeton gjithashtu transformim të rëndësishëm përmes integritimit të IA dhe sistemeve autonome. Anijet pa ekuipazh dhe nëndetëset

<sup>1</sup> NATO, Science and Technology Macro Trends 2025–2045, NATO Science & Technology Organization, 2025.

<sup>2</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 12.

autonome po zhvillohen për të kryer operacione zbulimi, mbikëqyrjeje dhe mbështetjeje luftarake në mjedise detare komplekse.<sup>3</sup> Një nga funksionet kryesore të këtyre sistemeve është monitorimi i zonave detare strategjike. Platformat autonome mund të patrullojnë korridore detare, porte ose zona ekonomike ekskluzive për periudha të gjata pa nevojën e ekuipazhit njerëzor. Përmes sensorëve sonarë, radarëve dhe sistemeve të IA, anijet autonome janë të afta të identifikojnë anije të dyshimta, aktivitete ilegale, kërcënime detare, lëvizje nëndetësesh armike. Nëndetëset autonome përbëjnë një nga zhvillimet më strategjike të luftës detare moderne. Ato mund të operojnë në mënyrë të fshehtë për periudha të gjata dhe të kryejnë zbulim, mbledhje inteligjence, identifikim minash, mbështetje për operacione speciale.<sup>4</sup> IA mund të analizojë të dhënat sonarike dhe të identifikojë objekte që përfaqësojnë rrezik për lundrimin ushtarak ose civil. Në të ardhmen, flotat detare autonome pritet të luajnë rol të rëndësishëm në kontrollin e hapësirave detare dhe në operacionet multidomain.

### ***Inteligjenca ushtarake dhe analiza e të dhënave***

Një nga fushat ku IA ka sjellë transformimin më të madh është inteligjenca ushtarake dhe analiza e të dhënave. Operacionet moderne gjenerojnë sasi gjigante informacioni nga satelitët, dronët, komunikimet elektronike, rrjetet sociale dhe burimet e hapura informative. Analiza manuale e këtij informacioni është pothuajse e pamundur në kohë reale. Për këtë arsye, IA përdoret për të analizuar automatikisht të dhënat dhe për të identifikuar informacione me rëndësi operative ose strategjike. Sistemet inteligjente mund të analizojnë imazhe satelitore, interpretojnë komunikime elektronike, monitorojnë rrjetet sociale, analizojnë burime OSINT (Open Sources Intelligence), zbulojnë modele sjelljeje.

Një funksion shumë i rëndësishëm është identifikimi i kërcënimeve dhe analiza parashikuese duke analizuar sjelljen historike të kundërshtarit dhe parashikuar operacione të mundshme. Kjo krijon avantazh strategjik në vendimmarrje, pasi komandantët marrin informacion më të shpejtë, më të saktë dhe më të analizuar sesa në sistemet tradicionale të inteligjencës.

### ***Lufta kibernetike***

Lufta kibernetike është bërë një nga dimensionet më të rëndësishme të sigurisë moderne, dhe Agentic AI po luan rol gjithnjë e më kritik në këtë fushë. Sistemet inteligjente përdoren për mbrojtjen e rrjeteve ushtarake,

---

<sup>3</sup> NATO, Emerging and Disruptive Technologies Report, (Brussels: NATO Headquarters, 2022), 21.

<sup>4</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 18.

zbulimin e sulmeve dhe reagimin automatik ndaj kërcënimeve kibernetike. Një nga funksionet kryesore të IA në mbrojtjen kibernetike është zbulimi i anomalive. Algoritmet mund të identifikojnë sjellje të pazakonta në rrjete dhe të sinjalizojnë tentativa sulmi ose infiltrimi. Gjithashtu, Agentic AI përdoret për analizë malware, izolim automatik të sistemeve të komprometuara, reagim në kohë reale ndaj sulmeve, analizë të trafikut të rrjetit. Në dimensionin ofensiv, IA mund të përdoret për operacione automatike kibernetike, identifikim dobësish në rrjete armike, analiza të mbrojtjes kundërshtare, zhvillim të malware inteligjent. Kjo krijon një mjedis të ri konfliktesh, ku lufta zhvillohet jo vetëm në terrenin fizik, por edhe në hapësirën digjitale.

### ***Komandim-Kontrolli (C2)***

Sistemet e C2 përbëjnë qendrën nervore të operacioneve ushtarake moderne. Integrimi i IA po transformon mënyrën se si realizohet koordinimi operacional dhe vendimmarrja strategjike.<sup>5</sup> IA mundëson analizën e situatës në kohë reale përmes integrit të informacionit nga platforma të shumta operative. Kjo krijon një pamje të integruar të fushës së betejës dhe rrit ndjeshëm ndërgjegjësimin për situatën. Gjithashtu, sistemet inteligjente ofrojnë rekomandime taktike për komandantët duke analizuar pozicionet e forcave, kapacitetet armike, rrezikun operacional, mundësitë taktike. Automatizimi i proceseve redukton kohën e vendimmarrjes dhe lejon reagim më të shpejtë ndaj zhvillimeve operative. Në konfliktet moderne, ku dinamika e luftës ndryshon brenda sekondave, kjo aftësi përbën avantazh kritik.

Një dimension veçanërisht i rëndësishëm është integrimi multidomain. IA koordinon operacionet ndërmjet forcave tokësore, ajrore, detare, hapësinore dhe kibernetike, duke krijuar një strukturë të unifikuar operative.<sup>6</sup> Sistemet C2 të bazuara në Agentic AI pritet të evoluojnë drejt rrjeteve autonome të komandimit, ku analiza, planifikimi dhe koordinimi operacional do të realizohen me ndërhyrje minimale njerëzore, duke transformuar rrënjësisht konceptin tradicional të komandim kontrollit.

## **II. Avantazhet operationale dhe strategjike të IA dhe Agentic AI në sistemet e mbrojtjes**

Në epokën e luftës së informacionit, automatizimit dhe operacioneve multidomain, superioriteti ushtarak nuk përcaktohet më vetëm nga numri i trupave, fuqia e armëve ose kapaciteti industrial, por gjithnjë e më shumë nga aftësia për të përpunuar informacionin, për të marrë vendime të shpejta dhe për të koordinuar sisteme komplekse në kohë reale. IA po krijon një avantazh

<sup>5</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 18.

<sup>6</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 18.

të ri strategjik, ku dominimi operacional arrihet përmes superioritetit algoritmik dhe kontrollit të informacionit. Sistemet inteligjente po rrisin ndjeshëm efikasitetin e operacioneve ushtarake, duke reduktuar kohën e reagimit, duke minimizuar rrezikun për personelin dhe duke përmirësuar koordinimin ndërmjet forcave në të gjitha dimensionet e luftës moderne.

### *Shpejtësia e vendimmarrjes*

Një nga avantazhet më të rëndësishme të IA në sistemet e mbrojtjes është shpejtësia jashtëzakonisht e lartë e analizës dhe vendimmarrjes. Në konfliktet moderne, ku situata operative mund të ndryshojë brenda sekondave, aftësia për të reaguar më shpejt se kundërshtari përbën faktor kritik për suksesin operacional.<sup>7</sup> Tradicionalisht, procesi i vendimmarrjes ushtarake mbështetej në analizën njerëzore të informacionit të mbledhur nga sensorët, inteligjenca operative dhe raportet taktike. Ky proces kërkonte kohë dhe ishte i kufizuar nga kapacitetet njohëse njerëzore.

Në epokën moderne, sasia e informacionit të gjeneruar nga satelitët, radarët, dronët, sensorët elektronikë dhe rrjetet e komunikimit është aq e madhe sa analizimi manual bëhet i pamundur në kohë reale. Sistemet e IA janë të afta të analizojnë miliona të dhëna brenda pak sekondash, të identifikojnë modele operative dhe të ofrojnë rekomandime taktike ose strategjike me shpejtësi shumë më të madhe sesa operatorët njerëzorë. Kjo krijon një avantazh të konsiderueshëm në luftën moderne, ku koha e reagimit mund të përcaktojë rezultatin e një operacioni. Në mbrojtjen ajrore, sistemet IA mund të identifikojnë një raketë ose avion armik, të analizojnë trajektoren, të vlerësojnë nivelin e kërcënimit dhe të aktivizojnë menjëherë sistemin mbrojtës. Shpejtësia e reagimit e tejkalon aftësinë njerëzore për të reaguar në mënyrë efektive.

Një tjetër dimension kritik i cili krkon vendimmarrje të shpejtë është lufta elektronike. Sulmet elektronike dhe ndërhyrjet në komunikime ndodhin me ritme jashtëzakonisht të larta dhe kërkojnë reagim të menjëhershëm. Sistemet Agentic AI mund të identifikojnë automatikisht burimin e ndërhyrjes, të ndryshojnë parametrat e komunikimit dhe të zbatojnë masa mbrojtëse pa ndërhyrje njerëzore. Gjithashtu, IA po transformon ciklin operacional të vendimmarrjes ushtarake, i njohur si OODA Loop (Observe–Orient–Decide–Act). Shtetet ose forcat që arrijnë të përshpejtojnë këtë cikël përmes IA fitojnë avantazh operacional, pasi mund të veprojnë dhe të përshtaten më shpejt sesa kundërshtari. Në këtë kontekst, shpejtësia algoritmike po bëhet një element kyç i superioritetit strategjik në konfliktet e së ardhmes.

---

<sup>7</sup> Kenneth Payne, I, Warbot: The Dawn of Artificially Intelligent Conflict, (London: Hurst Publishers, 2021), 95.

## ***Reduktimi i rrezikut për personelin***

Një nga objektivat kryesore të integritit të sistemeve autonome në mbrojtje është reduktimi i ekspozimit të personelit ushtarak ndaj rreziqeve. IA dhe robotika ushtarake po mundësojnë realizimin e misioneve në mjedise jashtëzakonisht të rrezikshme pa nevojën e pranisë së drejtpërdrejtë njerëzore.<sup>8</sup>

Sistemet autonome përdoren gjithnjë e më shumë në zona të minuara dhe në operacione të neutralizimit të mjeteve shpërthyes. Robotët inteligjentë mund të identifikojnë, analizojnë dhe neutralizojnë eksplozivët me saktësi të lartë, duke shmangur rrezikimin e specialistëve ushtarakë. Gjithashtu, këto sisteme kanë rëndësi të veçantë në mjediset NBC (Nuclear, Biological, Chemical), ku ekspozimi njerëzor mund të ketë pasoja fatale. Dronët, robotët tokësorë dhe platformat autonome mund të operojnë në zona të kontaminuara për të mbledhur informacion, për të monitoruar situatën ose për të realizuar operacione mbështetëse.

Në konfliktet moderne urbane, ku rreziku për trupat është shumë i lartë për shkak të pritave, snajperëve ose mjeteve shpërthyes të improvizuara, sistemet autonome mund të përdoren për zbulim, patrullim, eksplorim ndërtesash, identifikim kërcënimesh, mbështetje taktike. Përdorimi i dronëve inteligjentë për survejim dhe goditje precize ka reduktuar ndjeshëm nevojën për operacione të drejtpërdrejta me trupa në zona të rrezikshme. Operacionet që më parë kërkonin ndërhyrje fizike të forcave speciale mund të realizohen nga platforma autonome me rrezik minimal për personelin. Nga perspektiva strategjike si dhe nga ndjeshmëria e lartë publike ndaj humbjeve ushtarake, reduktimi i humbjeve njerëzore ka ndikim të rëndësishëm politik, social dhe psikologjik.

## **Superioriteti i informacionit**

Në epokën moderne, informacioni është bërë një nga burimet më strategjike të fuqisë ushtarake. Superioriteti i informacionit nënkupton aftësinë për të mbledhur, analizuar, shpërndarë dhe përdorur informacionin më shpejt dhe më efektivisht sesa kundërshtari. IA ka revolucionarizuar këtë dimension të luftës moderne. Përmes analizës së avancuar të inteligjencës, sistemet IA mund të përpunojnë sasi gjigante informacioni nga burime të ndryshme dhe të identifikojnë të dhëna me rëndësi operative ose strategjike. Një nga avantazhet më të rëndësishme të IA është aftësia për të krijuar ndërgjegjësim për situatën në kohë reale. Komandantët ushtarakë mund të kenë një pamje të integruar të fushës së betejës dhe të kuptojnë më shpejt zhvillimet operative.

---

<sup>8</sup> Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (New York: W. W. Norton & Company, 2018), 102.

Dominimi i informacionit nuk lidhet vetëm me mbledhjen e informacionit, por edhe me aftësinë për të kontrolluar dhe manipuluar rrjedhën e informacionit. Në konfliktet moderne, lufta informative dhe operacionet psikologjike po bëhen po aq të rëndësishme sa operacionet kinetike tradicionale. Përmes IA, shtetet mund të analizojnë sjelljen e popullatës, identifikojnë narrativa informative, zbulojnë dezinformimin, realizojnë operacione psikologjike të targetuara.<sup>9</sup>

### ***Operacionet multidomain***

Një nga karakteristikat kryesore të luftës moderne është integrimi i operacioneve në dimensione të ndryshme të konfliktit: tokë, ajër, det, hapësirë dhe mjedis kibernetik. Ky koncept njihet si “multidomain operations” dhe kërkon koordinim shumë të avancuar ndërmjet forcave dhe sistemeve të ndryshme operative.<sup>10</sup> Agentic AI luan rol thelbësor në realizimin e këtij koordinimi kompleks. Përmes analizës së të dhënave në kohë reale dhe rrjeteve inteligjente të komunikimit, IA mund të sinkronizojë veprimet ndërmjet forcave tokësore, ajrore, detare dhe kibernetike. Një operacion modern mund të përfshijë dronë ajrorë për zbulim, satelitë për mbikëqyrje strategjike, sulme kibernetike ndaj sistemeve armike, ndërhyrje elektronike, operacione tokësore të koordinuara. IA mund të analizojë të gjitha këto dimensione njëkohësisht dhe të rekomandojë mënyrën optimale të koordinimit operacional.

Një aspekt shumë i rëndësishëm është integrimi me sistemet hapësinore. Satelitët modernë ofrojnë navigim, komunikim dhe inteligjencë strategjike, dhe IA mund të analizojë të dhënat e tyre në kohë reale për mbështetje operative. Koncepti i “Joint All-Domain Operations” pritet të mbështetet pothuajse plotësisht në sisteme inteligjente autonome që do të koordinojnë operacionet në të gjitha dimensionet e konfliktit.

### ***Optimizimi logjistik***

Logjistika është një nga komponentët më kritikë të suksesit ushtarak. Historikisht, shumë konflikte janë përcaktuar jo vetëm nga fuqia luftarake, por edhe nga aftësia për të furnizuar trupat me municione, karburant, ushqime dhe pajisje. IA po transformon rrënjësisht sistemet logjistike ushtarake përmes analizës parashikuese dhe automatizimit të proceseve. Sistemet inteligjente mund të analizojnë ritmet operationale, konsumin e burimeve dhe lëvizjen e forcave për të parashikuar nevojat logjistike në kohë reale. Kjo mundëson optimizimin e furnizimeve, reduktimin e mungesave operative, shpërndarje

---

<sup>9</sup> Kenneth Payne, I, Warbot: The Dawn of Artificially Intelligent Conflict, (London: Hurst Publishers, 2021), 145.

<sup>10</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 18.

më efikase të burimeve, minimizimin e humbjeve logjistike. Përmes IA-së, zinxhiri logjistik bëhet më fleksibël dhe më rezistent ndaj ndërprerjeve. Sistemet autonome mund të identifikojnë automatikisht rrugët më të sigurta për transport, të analizojnë kërcënimet operative dhe të përshtasin furnizimet sipas zhvillimeve në terren.

Një tjetër avantazh është mirëmbajtja parashikuese. Algoritmet IA mund të monitorojnë gjendjen teknike të mjeteve ushtarake dhe të parashikojnë defektet përpara se ato të ndodhin duke reduktuar kostot operative dhe rritur gatishmërinë luftarake të forcave. Automatizimi logjistik po krijon gjithashtu mundësi për përdorimin e automjeteve autonome të furnizimit, dronëve logjistikë, magazinave inteligjente, sistemeve robotike të transportit.

### **III. Rreziqet dhe sfidat e Agentic AI në sistemet e mbrojtjes**

Megjithëse IA dhe sistemet Agentic AI ofrojnë avantazhe të mëdha operacionale dhe strategjike, integrimi i tyre në strukturat moderne të mbrojtjes shoqërohet gjithashtu me rreziqe dhe sfida komplekse. Sa më i lartë të jetë niveli i autonomisë së sistemeve inteligjente, aq më të mëdha bëhen edhe pasiguritë që lidhen me kontrollin operacional, sigurinë teknologjike, përgjegjësinë juridike dhe stabilitetin ndërkombëtar. Sistemet teknologjike po fitojnë aftësi për të përcaktuar objektiva dhe potencialisht për të përdorur forcë vdekjeprurëse me ndërhyrje minimale njerëzore. Ky transformim krijon jo vetëm avantazhe operative, por edhe dilema etike, juridike dhe strategjike.

#### ***Problemet etike***

Një nga debatet më të rëndësishme që lidhen me përdorimin e Agentic AI në sistemet e mbrojtjes është dimensionet etik të autonomisë ushtarake. Çështja kryesore konsiston në faktin se sistemet inteligjente mund të marrin vendime me pasoja vdekjeprurëse pa ndërhyrje të drejtpërdrejtë njerëzore. Në konfliktet tradicionale, vendimi për përdorimin e forcës ushtarake është marrë nga individë njerëzorë që mbajnë përgjegjësi morale, juridike dhe profesionale për pasojat e veprimeve të tyre. Në rastin e armëve autonome, kjo linjë përgjegjësie bëhet shumë më e paqartë.

Shumë ekspertë dhe organizata ndërkombëtare argumentojnë se vendimet për jetën dhe vdekjen nuk duhet t'i delegohen plotësisht makinave. Për këtë arsye është zhvilluar koncepti i “Meaningful Human Control”, sipas të cilit njeriu duhet të ruajë rol aktiv dhe vendimtar në autorizimin e përdorimit të forcës vdekjeprurëse.<sup>11</sup> Problematik mbetet edhe proporcionaliteti i forcës.

---

<sup>11</sup> United Nations, Report on Lethal Autonomous Weapons Systems, (New York: United Nations, 2023).

E drejta ndërkombëtare humanitare kërkon që përdorimi i forcës të jetë proporcional me objektivin ushtarak dhe të minimizojë dëmet ndaj civilëve. Megjithatë, sistemet inteligjente mund ta kenë të vështirë të interpretojnë situata komplekse njerëzore, emocionale ose sociale që shpesh ndikojnë në vendimet ushtarake.<sup>12</sup> Një algoritëm mund të identifikojë një objektiv si kërcënim legjitim bazuar në modele sjelljeje ose parametra teknikë, por të mos kuptojë kontekstin humanitar ose civil të situatës. Kjo rrit rrezikun e dëmeve anësore dhe të shkeljeve të së drejtës ndërkombëtare.

### ***Rreziku i vendimmarrjes së gabuar***

Kompleksiteti i algoritmeve dhe varësia nga të dhënat operative krijojnë rrezik real për vendimmarrje të gabuar. Një nga problemet kryesore lidhet me interpretimin e pasaktë të të dhënave. Sistemet Agentive AI bazohen në shumë burime informacioni për të kuptuar mjedisin operacional. Nëse këto të dhëna janë të paplota, të deformuara ose të manipuluar, algoritmi mund të arrijë në përfundime të gabuara. Një sistem autonom mund të identifikojë gabimisht një automjet civil si objektiv ushtarak për shkak të ngjashmërisë vizuale ose termike me një mjet luftarak.

Në mjedise komplekse operative, ku dallimi ndërmjet objektivave civilë dhe ushtarakë është i vështirë, ky rrezik bëhet veçanërisht serioz. Një problem tjetër lidhet me “bias-in algoritmik”. Algoritmet e IA mësojnë nga të dhënat me të cilat trajnohen. Nëse këto të dhëna janë të njëanshme, të paplota, sistemi mund të zhvillojë modele të gabuara të analizës dhe vendimmarrjes. Në kontekstin ushtarak, “bias-i operacional” mund të çojë në identifikim të gabuar të kërcënimeve, vlerësim të pasaktë të rrezikut, përdorim disproporcional të forcës. Një sfidë tjetër lidhet me mungesën e transparencës së algoritmeve komplekse të deep learning. Shumë sisteme IA funksionojnë si “black boxes”, ku edhe vetë zhvilluesit nuk mund të shpjegojnë plotësisht mënyrën se si algoritmi arrin në një vendim të caktuar. Kjo krijon vështirësi serioze në verifikimin e vendimeve, auditimin operacional, analizën pas veprimit, përcaktimin e përgjegjësisë.

### ***Cenueshmëria kibernetike***

Sistemet autonome mund të sulmohen përmes malware-ve të sofistikuar, të cilët mund të manipulojnë algoritmet, të ndërpresin funksionimin e sistemeve ose të marrin kontrollin e platformave autonome. Një tjetër kërcënim serioz është spoofing, ku kundërshtari manipulon sinjalet ose informacionin që merr sistemi inteligjent. Për shembull, një dron autonom mund të mashtrohet përmes manipulimit të sinjaleve GPS dhe të devijohet nga objektivi ose të humbasë

---

<sup>12</sup> European Union, Artificial Intelligence Act, (Brussels: European Commission, 2024).

kontrollin operacional.<sup>13</sup> Gjithashtu, jamming elektronik mund të ndërpresë komunikimet ndërmjet sistemeve autonome dhe qendrave të komandimit. Në një mjedis të luftës elektronike intensive, kjo mund të shkaktojë humbje koordinimi dhe degradim të aftësive operative. Manipulimi i sensorëve përbën një tjetër rrezik kritik. Kundërshtari mund të përdorë sinjale false, imazhe mashtruese, interferenca elektromagnetike, teknika të dezinformimit elektronik. Kjo mund të çojë sistemet autonome drejt vendimeve të gabuara operationale.

Një dimension i ri i konfliktit është shfaqja e sulmeve “AI kundër AI”, ku sistemet inteligjente përdoren për të mashtruar, manipuluar ose neutralizuar sisteme të tjera autonome. Në të ardhmen, konfliktet mund të karakterizohen nga përballje ndërmjet algoritmeve rivale që operojnë me shpejtësi shumë më të madhe se proceset njerëzore të vendimmarrjes.<sup>14</sup> Për këtë arsye, siguria kibernetike është bërë komponent thelbësor i zhvillimit të Agentic AI në mbrojtje.

### ***Varësia teknologjike***

Një tjetër sfidë strategjike lidhet me rritjen e varësisë nga IA dhe sistemet autonome. Sa më shumë që operacionet ushtarake mbështeten në IA, aq më i madh bëhet rreziku në rast të dështimit ose komprometimit të këtyre sistemeve. Një nga pasojat e kësaj varësie është reduktimi gradual i aftësive njerëzore. Nëse vendimmarrja, analiza dhe koordinimi operacional delegohen gjithnjë e më shumë tek algoritmet, operatorët njerëzorë mund të humbasin aftësitë tradicionale të analizës taktike dhe strategjike. Kjo krijon rrezik operacional në rast se sistemet inteligjente dështojnë teknikisht, komprometohen kibernetikisht, humbasin komunikimin, japin rezultate të pasakta.

Varësia teknologjike mund të krijojë gjithashtu dobësi strategjike kombëtare. Shtetet që varen nga teknologjitë e avancuara të IA mund të bëhen të cenueshme ndaj ndërprerjes së zinxhirit të furnizimit, embargoeve teknologjike, varësisë nga kompani private, monopolizimit të teknologjive kritike. Në rast konflikti të madh, humbja e infrastrukturës digjitale ose e sistemeve të IA mund të paralizojë operacionet ushtarake moderne. Për këtë arsye, shumë shtete po kërkojnë të ruajnë balancën ndërmjet automatizimit dhe aftësive tradicionale njerëzore në strukturat e mbrojtjes.

### ***Garat teknologjike dhe strategjike***

Zhvillimi i IA ushtarake po shoqërohet me një garë globale teknologjike ndërmjet fuqive kryesore botërore. Shtete si SHBA-të, Kina, Rusia dhe aktorë

<sup>13</sup> NATO, Emerging and Disruptive Technologies Report, (Brussels: NATO Headquarters, 2022), 33.

<sup>14</sup> NATO, NATO Artificial Intelligence Strategy, (Brussels: NATO Headquarters, 2021), 18.

të tjerë strategjikë po investojnë miliarda dollarë në zhvillimin e sistemeve autonome, armëve inteligjente dhe platformave të bazuara në IA.<sup>15</sup> Kjo garë teknologjike krijon potencial për destabilizim strategjik ndërkombëtar. Ashtu si gara bërthamore gjatë Luftës së Ftohtë, edhe gara për dominim në IA mund të çojë në rritje të tensioneve gjeopolitike dhe në zhvillim të pakontrolluar të armëve autonome.

Një nga rreziqet më të mëdha është përshkallëzimi autonom i konflikteve. Sistemet inteligjente operojnë me shpejtësi shumë të larta dhe mund të reagojnë automatikisht ndaj kërcënimeve ose provokimeve. Në situata krize, kjo mund të krijojë zinxhir reagimesh automatike që tejkalojnë kontrollin njerëzor.<sup>16</sup> Për shembull, dy sisteme autonome rivale mund të interpretojnë veprimet e njëri-tjetrit si kërcënim dhe të aktivizojnë kundërmasa ose sulme pa ndërhyrje njerëzore, duke përshkallëzuar konfliktin në mënyrë të pakontrolluar. Gjithashtu, ekziston rreziku që teknologjitë e Agentic AI të përhapen tek aktorë jo-shtetërorë, organizata terroriste ose grupe kriminale, duke rritur pasigurinë globale. Për këtë arsye, shumë ekspertë argumentojnë se zhvillimi i IA ushtarake duhet të shoqërohet me marrëveshje ndërkombëtare, mekanizma kontrolli, standarde etike, transparencë strategjike, masa për ndërtimin e besimit ndërmjet shteteve.<sup>17</sup> Në të kundërt, konkurrenca e pakontrolluar në IA ushtarake mund të krijojë një mjedis ndërkombëtar shumë më të paqëndrueshëm dhe të paparashikueshëm në dekadat e ardhshme.

#### **IV. Agentic AI dhe lufta e së ardhmes**

Lufta e së ardhmes pritet të zhvillohet në një mjedis operacional shumë më kompleks, më të automatizuar dhe më të shpejtë se konfliktet tradicionale. Në këtë realitet të ri, shpejtësia e analizës dhe e reagimit do të jetë po aq e rëndësishme sa fuqia kinetike. IA nuk do të shërbejë vetëm si mjet mbështetës për komandantët ushtarakë, por do të bëhet komponent aktiv i planifikimit, koordinimit dhe ekzekutimit operacional. Lufta do të zhvillohet njëkohësisht në hapësirën tokësore, ajrore, detare, kibernetike, hapësinore dhe informative. Agentic AI do të luajë rol qendror në integrimin dhe koordinimin e këtyre dimensioneve të ndryshme të konfliktit. Ky transformim pritet të ndikojë jo vetëm teknologjinë ushtarake, por edhe vetë konceptin e fuqisë dhe të sigurisë ndërkombëtare.

---

<sup>15</sup> Kenneth Payne, I, Warbot: The Dawn of Artificially Intelligent Conflict, (London: Hurst Publishers, 2021), 145.

<sup>16</sup> Paul Scharre, Army of None: Autonomous Weapons and the Future of War, (New York: W. W. Norton & Company, 2018), 210.

<sup>17</sup> United Nations, Report on Lethal Autonomous Weapons Systems, (New York: United Nations, 2023).

## ***Lufta algoritmike***

Një nga konceptet më të rëndësishme që po shfaqet në doktrinat moderne ushtarake është “lufta algoritmike” (algorithmic warfare).<sup>18</sup> Ky koncept i referohet përdorimit të IA dhe algoritmeve autonome për analizë operative, planifikim taktik dhe realizim të operacioneve në kohë reale.<sup>19</sup> Konfliktet e së ardhmes pritet të karakterizohen nga automatizimi ekstrem i proceseve ushtarake, në të cilin sistemet inteligjente do të jenë të afta të mbledhin informacion, të analizojnë kërcënimet, të identifikojnë objektiva dhe të propozojnë ose ekzekutojnë kundërmasa pothuajse pa ndërhyrje njerëzore.

Një aspekt tjetër thelbësor i luftës algoritmike është dominimi i informacionit, kush kontrollon më mirë informacionin do të ketë avantazh strategjik. IA mundëson përpunimin e të dhënave nga satelitët, dronët, sensorët ISR, komunikimet elektronike, rrjetet kibernetike dhe burimet OSINT. Përmes analizës së integruar të këtyre të dhënave, sistemet inteligjente krijojnë një pamje operationale të përditësuar në kohë reale, duke rritur ndjeshëm ndërgjegjësimin për situatën dhe efikasitetin e vendimmarrjes. Lufta algoritmike do të karakterizohet gjithashtu nga përdorimi i sistemeve autonome bashkëpunuese, që përfshijnë rrjete inteligjente sistemesh të cilat komunikojnë dhe koordinohen në mënyrë automatike.<sup>20</sup>

## ***Swarm Warfare***

Ky koncept bazohet në përdorimin e një numri të madh platformash autonome, kryesisht drone, që operojnë në mënyrë të koordinuar si një inteligjencë kolektive. Ndryshe nga sistemet tradicionale të kontrolluara në mënyrë qendrore, “swarm systems” funksionojnë në mënyrë decentralizuar. Çdo njësi individuale është e aftë të marrë informacion nga mjedisi dhe nga njësitë e tjera të swarm-it, duke përshtatur sjelljen operative në kohë reale. Një nga avantazhet kryesore të swarm systems është aftësia për të mbingarkuar sistemet tradicionale të mbrojtjes, të cilat janë zakonisht të projektuara për të përballuar numër të kufizuar objektivash. Një swarm me dhjetëra ose qindra dronë mund të tejkalojë kapacitetin e reagimit të mbrojtjes dhe të depërtojë në objektivat strategjike. Swarm systems kanë fleksibilitet të lartë operacional. Nëse një pjesë e swarm neutralizohet, pjesa tjetër mund të riorganizohet automatikisht dhe të vazhdojë misionin.

---

<sup>18</sup> Kenneth Payne, I, Warbot: The Dawn of Artificially Intelligent Conflict, (London: Hurst Publishers, 2021), 95.

<sup>19</sup> NATO Science & Technology Organization, Science and Technology Macro Trends 2025–2045, 2025.

<sup>20</sup> James Johnson, “Artificial Intelligence and Future Warfare,” Defense Studies, Vol. 21, No. 2, (2021), 146.

Kjo e bën swarm warfare shumë më rezistente ndaj humbjeve sesa strukturat tradicionale ushtarake. Një karakteristikë tjetër shumë e rëndësishme është përshtatja në kohë reale. Inteligjenca kolektive e swarm-it mund të ndryshojë itineraret operative, identifikojë kërcënime të reja, rishpërndajë objektivat si dhe të modifikojë taktikat gjatë misionit. Në të ardhmen, swarm warfare pritet të përdoret jo vetëm në dimensionin ajror, por edhe në operacionet detare autonome, në sistemet tokësore robotike, në luftën kibernetike dhe në operacionet elektronike. Shumë ekspertë ushtarakë e konsiderojnë swarm warfare si një nga elementët më transformues të luftës së shekullit XXI, pasi ai kombinon IA, autonominë dhe operacionet rrjetore në një model të ri të fuqisë ushtarake.<sup>21</sup>

### ***Human-Machine Teaming***

Megjithëse zhvillimi i Agentic AI po rrit vazhdimisht autonominë e sistemeve ushtarake, shumica e doktrinave moderne nuk synojnë zëvendësimin total të njeriut. Përkundrazi, modeli dominues i së ardhmes pritet të jetë bashkëpunimi ndërmjet njeriut dhe makinës, i njohur si “Human-Machine Teaming”.<sup>22</sup>

Ky koncept bazohet në kombinimin e aftësive njerëzore me kapacitetet analitike dhe operative të IA. Njeriu dhe sistemi inteligjent nuk veprojnë si elementë të ndarë, por si pjesë të një strukture të integruar operative.<sup>23</sup> Në këtë model, njeriu ruan kontrollin mbi aspektet strategjike dhe etike të operacioneve ushtarake. Komandantët njerëzorë përcaktojnë objektivat strategjike, vendosin prioritetet operative, mbikëqyrin sistemet autonome, autorizojnë përdorimin e forcës.<sup>24</sup>

Nga ana tjetër, IA analizon të dhënat operative, realizon planifikim taktik, optimizon përdorimin e burimeve, koordinon sistemet autonome dhe ekzekuton detyra operative me shpejtësi të lartë. Ky bashkëpunim krijon një sinergji ndërmjet intuitës njerëzore dhe efikasitetit algoritmik. Njeriu ofron gjykim etik, kuptim strategjik, interpretim kontekstual, fleksibilitet psikologjik. Ndërsa IA ofron analizë masive të të dhënave, reagim të menjëhershëm, përpunim simultan të informacionit.

Në të ardhmen, Human-Machine Teaming pritet të bëhet modeli standard i operacioneve ushtarake multidomain. Pilotët do të bashkëpunojnë me dronë

---

<sup>21</sup> James Johnson, “Artificial Intelligence and Future Warfare,” *Defense Studies*, Vol. 21, No. 2, (2021), 146.

<sup>22</sup> NATO, *NATO Artificial Intelligence Strategy*, (Brussels: NATO Headquarters, 2021), 18.

<sup>23</sup> NATO, *Summary of NATO’s Revised Artificial Intelligence (AI) Strategy*, Brussels, 10 July 2024.

<sup>24</sup> United Nations, *Report on Lethal Autonomous Weapons Systems*, (New York: United Nations, 2023).

autonomë, komandantët do të mbështeten nga sisteme inteligjente të analizës operative dhe njësitë tokësore do të operojnë së bashku me robotë autonomë. Megjithatë, ky model kërkon zhvillim të avancuar të besimit ndërmjet operatorit dhe sistemit, ndërveprimi intuitiv njeri-makinë, transparencës algoritmike, sigurisë kibernetike, kontrollit operacional.<sup>25</sup> Nëse këto sfida adresohen me sukses, Human-Machine Teaming mund të transformojë rrënjësisht mënyrën e zhvillimit të operacioneve ushtarake në dekadat e ardhshme.

### *Cognitive Warfare*

Një nga dimensionet më të rëndësishme dhe më të ndërlikuara të luftës së së ardhmes është “cognitive warfare” ose lufta njohëse. Ky koncept lidhet me përdorimin e informacionit, teknologjisë dhe IA për të ndikuar perceptimet, mendimin dhe sjelljen e individëve ose shoqërive.<sup>26</sup> Ndryshe nga lufta tradicionale kinetike, lufta konjitive synon mendjen njerëzore si objektiv strategjik. Qëllimi nuk është vetëm shkatërrimi fizik i kundërshtarit, por ndikimi mbi perceptimin publik, moralin, vendimmarrjen politike, sjelljen sociale dhe proceset psikologjike.

Inteligjenca artificiale po bëhet instrument kyç në realizimin e operacioneve njohëse për shkak të aftësisë së saj për të analizuar sasi të mëdha informacioni dhe për të identifikuar modele sjelljeje. IA mund të përdoret për operacione psikologjike, manipulim informacioni, dezinformim, propagandë të personalizuar si dhe analiza të sjelljes sociale. Përmes analizës së rrjeteve sociale, algoritmet mund të identifikojnë preferencat politike, dobësitë psikologjike, polarizimin social dhe grupet e ndikueshme.

Kjo mundëson krijimin e fushatave të targetuara informative dhe psikologjike me ndikim shumë më të madh sesa propaganda tradicionale. Një nga rreziqet më serioze është përdorimi i IA për gjenerimin e përmbajtjeve të manipuluar, si deepfakes, video sintetike, audio të falsifikuara dhe lajme të automatizuara.<sup>27</sup> Këto teknologji mund të përdoren për destabilizim politik, manipulim të opinionit publik ose krijim konfuzioni në periudha krizash dhe konfliktesh.

Në të ardhmen, lufta konjitive pritet të bëhet pjesë integrale e strategjiave ushtarake dhe hibride. Konfliktet nuk do të zhvillohen vetëm në fushën e betejës, por edhe në hapësirën informative dhe psikologjike të shoqërive moderne. Për këtë arsye, shumë ekspertë argumentojnë se mbrojtja kundër luftës konjitive do të kërkojë jo vetëm teknologji të avancuar, por edhe edukim

<sup>25</sup> UK MoD, JSP 936: Dependable Artificial Intelligence (AI) in Defence – Part 1: Directive, London, 13 November 2024.

<sup>26</sup> NATO, Cognitive Warfare, (Brussels: NATO Headquarters, 2021).

<sup>27</sup> European Union, Artificial Intelligence Act, (Brussels: European Commission, 2024).

mediatik, reziliencë sociale, mbrojtje të infrastrukturës informative, strategji kundër dezinformimit si dhe bashkëpunim ndërkombëtar në sigurinë digjitale. Në këtë kontekst, IA nuk po ndryshon vetëm mënyrën se si luftohet, por edhe mënyrën se si perceptohet dhe përjetohet vetë konflikti në shoqëritë moderne.

## Përfundime

IA dhe Agentic AI po transformojnë rrënjësisht sistemet moderne të mbrojtjes dhe mënyrën e zhvillimit të operacioneve ushtarake. Sistemet autonome ofrojnë shpejtësi, precizion dhe efikasitet të lartë operacional, duke krijuar avantazhe strategjike për shtetet që zotërojnë teknologjitë më të avancuara. Megjithatë, përdorimi i tyre sjell sfida serioze etike, juridike dhe të sigurisë. Autonomia e armëve, rreziku i vendimmarrjeve të gabuara dhe cenueshmëria ndaj sulmeve kibernetike kërkojnë një qasje të balancuar ndërmjet inovacionit dhe kontrollit.

Në të ardhmen, Agentic AI do të bëhet pjesë qendrore e luftës moderne, veçanërisht në operacionet multidomain dhe në sistemet e komandimit inteligjent. Suksesi i këtyre teknologjive do të varet nga aftësia për të kombinuar superioritetin teknologjik me kontrollin njerëzor dhe respektimin e normave ndërkombëtare.

## Bibliografia

1. Cummings, Michael. *Human Command and Control of AI-Enabled Systems*. Washington D.C.: Center for Naval Analyses, 2020.
2. Kissinger, Henry; Schmidt, Eric & Huttenlocher, Daniel. *The Age of AI: And Our Human Future*. New York: Little, Brown and Company, 2021.
3. Payne, Kenneth. I. *Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers, 2021.
4. Russell, Stuart & Norvig, Peter. *Artificial Intelligence: A Modern Approach*. New Jersey: Pearson Education, 2021.
5. Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company, 2018.
6. United Nations. *Report of the Group of Governmental Experts on Lethal Autonomous Weapons Systems*. New York: United Nations, 2023.
7. U.S. Department of Defense. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington D.C.: Department of Defense, 2018.
8. Horowitz, Michael. "Artificial Intelligence and the Future of Warfare." *Foreign Affairs*, Vol. 98, No. 3, (2019).

9. Johnson, James. "Artificial Intelligence and Future Warfare." *Defense Studies*, Vol. 21, No. 2, (2021).
10. Payne, Kenneth. "Artificial Intelligence: A Revolution in Strategic Affairs?" *Survival*, Vol. 60, No. 5, (2018).

### **Dokumente strategjike**

1. NATO Artificial Intelligence Strategy. Brussels: NATO Headquarters, 2021.
2. United Nations Reports on Autonomous Weapons Systems.
3. European Union. Artificial Intelligence Act. Brussels: European Commission, 2024.
4. NATO. Emerging and Disruptive Technologies Report, 2022.

