VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

VAROVANJE VOJAŠKIH BAZ V OKVIRU ZVEZE NATO

Kandidat: Aljoša Medved

Vrsta študija: študent izrednega študija

Študijski program: varovanje

Mentor predavatelj: mag. Srečko Jarc

Mentor v podjetju: Marko Kotnik, dipl. obr.

Lektorica: Maja Glaser Bedenik, prof. slov.

Maribor, 2026

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani sem avtor diplomskega dela z naslovom »Varovanje vojaških baz v okviru zveze NATO«, ki sem ga napisal pod mentorstvom mag. Srečka Jarca.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel/a, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, avgust 2026 Podpis študenta:

ZAHVALA

Zahvaljujem se vsem strokovnim delavcem Višje strokovne šole Academia za pomoč in podporo skozi celoten študij.

Posebna zahvala mentorju mag. Srečku Jarcu za strokovno usmerjanje, nasvete in pomoč pri izdelavi diplomskega dela.

Zahvaljujem se tudi prijatelju, nadporočniku Marku Kotniku za podporo, strokovne usmeritve in deljenje praktičnih izkušenj.

Zahvala lektorici Maji Glaser Bedenik za strokovni pregled diplomskega dela.

Iskrena hvala družini, ki me je ves čas študija podpirala in spodbujala pri doseganju zastavljenih ciljev.

POVZETEK

Diplomsko delo obravnava sistem varovanja vojaških baz v okviru zveze NATO in analizira ključne varnostne ukrepe za zaščito osebja, infrastrukture ter vojaške opreme pred sodobnimi varnostnimi grožnjami. Zaradi vse bolj kompleksnega varnostnega okolja so vojaške baze izpostavljene različnim oblikam ogrožanja, kot so teroristični napadi, sabotaže, raketni in minometni napadi, brezpilotni sistemi (UAS) ter kibernetske in hibridne grožnje. Namen diplomskega dela je predstaviti sodoben sistem zaščite vojaških baz, ki temelji na konceptu večplastnega varovanja »Defense in Depth«, in proučiti učinkovitost posameznih varnostnih ukrepov pri zagotavljanju zaščite vojaških objektov.

Raziskava temelji na kvalitativnem raziskovalnem pristopu in vključuje analizo domače ter tuje strokovne literature, NATO doktrin, javno dostopne dokumentacije in študij primerov napadov na vojaške baze v Afganistanu in Iraku. Poseben poudarek je namenjen fizičnim, tehničnim in organizacijskim elementom sistema varovanja, med katere sodijo fizične ovire, kontrola dostopa, sistemi video nadzora, senzorji, radarji, biometrični sistemi, obveščevalna dejavnost in delovanje centrov Base Defense Operations Center (BDOC) ter enot Quick Reaction Force (QRF). Obravnavana je tudi vloga sistema Force Protection in uporaba sodobnih tehnologij za zaznavanje ter nevtralizacijo brezpilotnih sistemov.

Na podlagi analize je bilo ugotovljeno, da učinkovito varovanje vojaških baz temelji predvsem na medsebojni povezanosti fizičnih, tehničnih in organizacijskih ukrepov, kakovostni obveščevalni dejavnosti, zgodnjem zaznavanju groženj ter hitrem in usklajenem odzivanju varnostnih sil. Analiza študij primerov je pokazala, da sodobne grožnje zahtevajo stalno prilagajanje varnostnih sistemov, razvoj novih zaščitnih zmogljivosti in vključevanje naprednih tehnologij. Diplomsko delo ugotavlja, da bo prihodnji razvoj varovanja vojaških baz vse bolj temeljil na uporabi umetne inteligence, avtomatiziranih nadzornih sistemov, integriranih komunikacijskih rešitev ter učinkoviti zaščiti pred brezpilotnimi in kibernetskimi grožnjami. Ključnega pomena ostajata tudi stalno usposabljanje varnostnega osebja in mednarodno sodelovanje znotraj zavezništva NATO, saj omogočata učinkovitejše preprečevanje, zaznavanje in obvladovanje sodobnih varnostnih tveganj.

Ključne besede: *varovanje vojaških baz, NATO, Defense in Depth, Force Protection, brezpilotni sistemi, BDOC, QRF.*

ZUSAMMENFASSUNG

Sicherung von Militärbasen im Rahmen der NATO

Die Diplomarbeit behandelt das Sicherungssystem von Militärbasen im Rahmen der NATO und analysiert zentrale Sicherheitsmaßnahmen zum Schutz von Personal, Infrastruktur und Ausrüstung vor modernen Bedrohungen wie Terroranschlägen, unbemannten Systemen, Sabotage sowie Cyber- und hybriden Bedrohungen. Ziel der Untersuchung war es, das mehrschichtige Schutzsystem „Defense in Depth“ darzustellen und die Wirksamkeit moderner Sicherheitsmaßnahmen zu analysieren.

Die Forschung basiert auf der Analyse von Fachliteratur, NATO-Doktrinen, öffentlich zugänglichen Dokumenten und Fallstudien von Angriffen auf Militärbasen in Afghanistan und im Irak. In der Arbeit werden physische, technische und organisatorische Elemente des Schutzsystems vorgestellt, darunter Videoüberwachungssysteme, Zugangskontrollen, Bedrohungserkennung sowie die Tätigkeit der Zentren BDOC und der Einheiten QRF.

Die Ergebnisse zeigen, dass der wirksame Schutz von Militärbasen auf der Integration verschiedener Sicherheitssysteme, der frühzeitigen Erkennung von Bedrohungen, einer qualitativ hochwertigen Aufklärungstätigkeit sowie der schnellen Reaktion der Sicherheitskräfte beruht. Die Diplomarbeit kommt zu dem Schluss, dass zukünftige Schutzsysteme zunehmend auf künstlicher Intelligenz, automatisierten Überwachungssystemen sowie dem Schutz vor unbemannten und Cyber-Bedrohungen basieren werden.

Schlüsselwörter: Sicherung von Militärbasen, NATO, Defense in Depth, Force Protection, unbemannte Systeme, BDOC, QRF.

SEZNAM KRATIC

Slovenski pomen	Angleški pomen	Kratica
Organizacija Severnoatlantske pogodbe	North Atlantic Treaty Organization	NATO
Zaščita sil	Force Protection	FP
Center za obrambno delovanje baze	Base Defense Operations Center	BDOC
Sile za hitro posredovanje	Quick Reaction Force	QRF
Sistemi brezpilotnih zrakoplovov	Unmanned Aerial Systems	UAS
Brezpilotno letalo	Unmanned Aerial Vehicle	UAV
Sistem za zaščito pred brezpilotnimi sistemi	Counter-Unmanned Aerial Systems	C-UAS
Sistem za zaščito pred raketnimi, artilerijskimi in minometnimi napadi	Counter Rocket, Artillery and Mortar	C-RAM
Sistem video nadzora	Closed-Circuit Television	CCTV
Stopnja zaščite sil	Force Protection Condition	FPCON
Improvizirano eksplozivno sredstvo	Improvised Explosive Device	IED
Obveščevalni podatki iz javno dostopnih virov	Open Source Intelligence	OSINT
Standardni operativni postopki	Standard Operating Procedures	SOP
NATO center odličnosti za kibernetsko obrambo	Cooperative Cyber Defence Centre of Excellence	CCDCOE

Vir: NATO doktrine in strokovna literatura

KAZALO VSEBINE

1 UVOD 10

1.1 Opredelitev problema 10
1.2 Namen in cilji 11
1.3 Raziskovalna vprašanja in hipoteze 12
1.4 Metodologija 13

2 TEORETIČNA IZHODIŠČA 14

2.1 Vojaške baze in njihov pomen 14
2.2 NATO in koncept kolektivne varnosti 15
2.3 Večplastno varovanje (Defense in Depth) 15
2.4 Vojaške baze kot kritična infrastruktura 16
2.5 Struktura vojaške baze in varnostne cone 17
2.5.1 Zunanja varnostna cona 17
2.5.2 Srednja varnostna cona 17
2.5.3 Notranja varnostna cona 17

3 VARNOSTNE GROŽNJE VOJAŠKIM BAZAM 19

3.1 Terorizem in sabotaža 19
3.2 Raketni in minometni napadi 21
3.3 Brezpilotni sistemi (UAS) 22
3.4 Kibernetske in hibridne grožnje 24

4 SISTEM VAROVANJA VOJAŠKIH BAZ 26

4.1 Fizično varovanje 26
4.2 Tehnično varovanje (video nadzor, senzorji, kontrola dostopa) 28
4.2.1 Varovanje pomorskih vojaških baz in zaščita pred brezpilotnimi plovili 29
4.3 Organizacijski ukrepi (QRF, BDOC, obveščevalna dejavnost) 30
4.3.1 BDOC (Base Defense Operations Center) 31
4.3.2 QRF (Quick Reaction Force) 32
4.3.3 Obveščevalna dejavnost 34
4.4 Večplastni sistem zaščite 35
4.5 Varnostne stopnje in protokoli (FPCON) 35
4.6 Integracija varnostnih sistemov 36

5 ANALIZA PRIMEROV IN INCIDENTOV 39

5.1 Izbrane vojaške baze 39
5.1.1 Camp Bastion – Afganistan 39
5.1.2 Al Asad Airbase – Irak 41
5.1.3 Balad Air Base – Irak 42

5.2 Primerjava sistemov varovanja 43
5.3 Analiza napadov na vojaške baze 43
5.4 Ključne ugotovitve (Lessons Learned) 44
6 RAZPRAVA IN PRIPOROČILA 46
6.1 Interpretacija rezultatov 46
6.2 Predlogi za izboljšanje varovanja 47
6.3 Omejitve raziskave 49
6.4 Preverjanje hipotez 50
7 SKLEP 52
8 VIRI IN LITERATURA 55

KAZALO SLIK

Slika 1: Posledice napada na Camp Bastion v Afganistanu leta 2012 20
Slika 2: Sistem C-RAM za zaščito vojaških baz pred raketnimi in minometnimi napadi 21
Slika 3: Counter-UAS sistem za zaznavanje in nevtralizacijo dronov 23
Slika 4: Kibernetska zaščita vojaških sistemov 25
Slika 5: Fizično varovanje vojaške baze z zaščitnimi ovirami in nadzornimi točkami 27
Slika 6: Sistem video nadzora in termovizijskih kamer v vojaški bazi 28
Slika 7: Base Defense Operations Center (BDOC) 32
Slika 8: Enota QRF pri hitrem posredovanju v vojaški bazi 33
Slika 9: FPCON varnostne stopnje v okviru zaščite sil NATO 36
Slika 10: Vojaška baza Camp Bastion v Afganistanu 40
Slika 11: Al Asad Airbase v Iraku 41
Slika 12: Balad Air Base v Iraku 42
Slika 13: Sodobni integrirani sistemi varovanja vojaških baz 48
Slika 14: Prihodnost varovanja vojaških baz v okviru NATO 54

KAZALO TABEL

TABELA 1: GLAVNE VARNOSTNE GROŽNJE VOJAŠKIM BAZAM.....19
TABELA 2: ELEMENTI SISTEMA VAROVANJA VOJAŠKIH BAZ.....26
TABELA 3: FPCON VARNOSTNE STOPNJE V OKVIRU NATO FORCE PROTECTION SISTEMA 35
TABELA 4: PRIMERJAVA SISTEMOV VAROVANJA IZBRANIH VOJAŠKIH BAZ 43
TABELA 5: KLJUČNE UGOTOVITVE SODOBNIH NAPADOV NA VOJAŠKE BAZE 45
TABELA 6: PREDLOGI ZA IZBOLJŠANJE SISTEMA VAROVANJA VOJAŠKIH BAZ 47
TABELA 7: HIPOTEZE IN UGOTOVITVE 51

1 UVOD

Sodobni oboroženi konflikti so pokazali, da vojaške baze predstavljajo pomembne tarče sodobnega vojskovanja. Napadi v Afganistanu, Iraku in Ukrajini so razkrili ranljivost vojaške infrastrukture pred asimetričnimi grožnjami, brezpilotnimi sistemi, raketnimi napadi in kibernetskim delovanjem. Zato države članice NATO razvijajo napredne sisteme zaščite sil (Force Protection), ki temeljijo na povezovanju fizičnih, tehničnih in organizacijskih ukrepov.

NATO pri varovanju vojaških baz uporablja koncept večplastnega varovanja »Defense in Depth«, namen katerega je zgodnje zaznavanje, preprečevanje in omejevanje sodobnih groženj. Sistem temelji na povezovanju fizičnega varovanja, tehničnih sistemov, obveščevalne dejavnosti in organizacijskih ukrepov.

Sodobni konflikti na Bližnjem vzhodu in v Ukrajini so pokazali potrebo po stalnem prilagajanju sistemov varovanja novim oblikam ogrožanja. Vojaške baze so danes izpostavljene terorističnim napadom, raketnemu obstreljevanju, brezpilotnim sistemom in kibernetskemu ter hibridnemu delovanju.

Diplomsko delo obravnava sistem varovanja vojaških baz v okviru zveze NATO in analizira ključne varnostne ukrepe, sodobne grožnje in primere napadov na vojaške baze. Na podlagi strokovne literature, NATO doktrin in študija primerov bodo predstavljene ključne ugotovitve ter priporočila za izboljšanje varovanja vojaških objektov.

1.1 Opredelitev problema

Varovanje vojaških baz predstavlja pomemben del sodobnega varnostnega sistema, saj baze omogočajo izvajanje obrambnih, logističnih in operativnih nalog zveze NATO. Zaradi svoje strateške vrednosti so pogosto tarča različnih varnostnih groženj, ki lahko vplivajo na operativno sposobnost vojaških sil in varnost osebja ter infrastrukture.

Sodobno varnostno okolje zaznamujejo asimetrične, hibridne in tehnološko napredne grožnje, kot so terorizem, raketni napadi, kibernetski napadi in uporaba brezpilotnih sistemov (UAS). Konflikti v Afganistanu, Iraku in Ukrajini so pokazali, da tradicionalni sistemi varovanja pogosto niso več dovolj učinkoviti za zaščito vojaških objektov.

Ključni problem raziskave je vprašanje, kako so sistemi varovanja vojaških baz v okviru zveze NATO prilagojeni sodobnim varnostnim grožnjam in kateri ukrepi imajo največji pomen pri zaščiti vojaških objektov.

Raziskava obravnava koncept »Defense in Depth«, ki temelji na večplastnem sistemu zaščite za zgodnje zaznavanje in preprečevanje groženj. Poseben poudarek je namenjen nadzoru dostopa, usklajenemu poveljevanju, delovanju centra BDOC in vlogi enot QRF pri zaščiti vojaških baz.

Poseben izziv sodobnega varovanja predstavlja uporaba komercialno dostopnih brezpilotnih sistemov, ki omogočajo izvajanje napadov z nizkimi stroški in visoko stopnjo mobilnosti. Takšne grožnje zahtevajo prilagajanje obstoječih sistemov varovanja in razvoj novih zaščitnih rešitev.

1.2 Namen in cilji

Namen diplomskega dela je proučiti sistem varovanja vojaških baz v okviru zveze NATO in analizirati ključne ukrepe za zaščito osebja, infrastrukture ter vojaške opreme pred sodobnimi varnostnimi grožnjami. Poseben poudarek je namenjen večplastnemu sistemu varovanja in povezovanju fizičnih, tehničnih ter organizacijskih ukrepov zaščite.

Raziskava obravnava vpliv sodobnih groženj, kot so brezpilotni sistemi, hibridno delovanje, terorizem in kibernetske grožnje, na razvoj sistemov varovanja vojaških baz. Na podlagi strokovne literature, NATO doktrin in študij primerov bodo predstavljene ključne ugotovitve in priporočila za izboljšanje zaščite vojaških objektov.

Cilji diplomskega dela so:

- predstaviti pomen vojaških baz za obrambni sistem NATO,
- opredeliti koncept večplastnega varovanja (»Defense in Depth«),
- analizirati glavne varnostne grožnje vojaškim bazam,
- proučiti fizične, tehnične in organizacijske ukrepe varovanja,
- predstaviti delovanje sistema BDOC in enot QRF
- analizirati uporabo sodobnih tehnologij pri varovanju vojaških baz,
- proučiti primere napadov na vojaške baze,
- oblikovati priporočila za izboljšanje sistema varovanja.

Diplomsko delo temelji na analizi javno dostopnih virov, strokovne literature, NATO doktrin in študij primerov s področja varovanja vojaških baz v okviru sistema kolektivne varnosti NATO.

1.3 Raziskovalna vprašanja in hipoteze

Osrednje raziskovalno vprašanje diplomskega dela je:

Kako je zasnovan sistem varovanja vojaških baz in kako učinkovito odgovarja na sodobne varnostne grožnje?

Na podlagi osrednjega raziskovalnega vprašanja bodo obravnavana tudi naslednja podvprašanja:

- kateri so ključni elementi sistema varovanja vojaških baz,
- katere sodobne grožnje najbolj ogrožajo vojaške baze,
- kakšna je vloga tehničnih sistemov, centra BDOC in enot QRF pri zaščiti baze,
- kako učinkoviti so obstoječi sistemi zaščite pred brezpilotnimi in hibridnimi grožnjami,
- katere izboljšave bi lahko povečale učinkovitost varovanja.

V diplomskem delu bodo preverjene naslednje hipoteze:

Hipoteza 1 (H1)

Varovanje vojaških baz temelji na integraciji fizičnih, tehničnih in organizacijskih ukrepov.

Hipoteza temelji na predpostavki, da učinkovito varovanje zahteva povezovanje različnih varnostnih ukrepov in sistemov.

Hipoteza 2 (H2)

Ključni dejavniki učinkovitega varovanja so zgodnje zaznavanje groženj, nadzor dostopa in usklajeno poveljevanje.

Hipoteza temelji na pomenu pravočasnega zaznavanja groženj, učinkovitega nadzora dostopa in hitrega odzivanja varnostnih sil.

Hipoteza 3 (H3)

Sodobne grožnje, zlasti brezpilotni sistemi, zahtevajo uvedbo večplastnih in tehnološko naprednih zaščitnih ukrepov.

Hipoteza temelji na ugotovitvah sodobnih konfliktov, kjer brezpilotni sistemi in hibridne grožnje zahtevajo uporabo sodobnih zaščitnih rešitev.

Preverjanje hipotez bo izvedeno s pomočjo analize strokovne literature, NATO doktrin in študij primerov napadov na vojaške baze v sodobnih konfliktih.

1.4 Metodologija

Diplomsko delo temelji na kvalitativnem raziskovalnem pristopu, katerega namen je analiza sistema varovanja vojaških baz in učinkovitosti varnostnih ukrepov pri zaščiti vojaških objektov pred sodobnimi grožnjami.

Pri izdelavi diplomskega dela bodo uporabljene naslednje raziskovalne metode:

Metoda analize literature

Uporabljena bo domača in tuja strokovna literatura s področja varovanja, vojaške varnosti in kritične infrastrukture. Poseben poudarek bo namenjen NATO doktrinam, strokovnim člankom in raziskavam s področja zaščite vojaških objektov.

Metoda analize dokumentov

Analizirani bodo javno dostopni dokumenti, NATO doktrine, varnostni standardi in vojaški priročniki s področja zaščite sil (Force Protection). Namen analize je proučiti organizacijo in delovanje sistemov varovanja v sodobnih vojaških operacijah.

Študija primerov (case study)

Analizirani bodo primeri napadov na vojaške baze v sodobnih konfliktih. Poudarek bo na uporabljenih varnostnih ukrepih, odzivu varnostnih sil in ugotavljanju ključnih ranljivosti ter pridobljenih izkušnjah (»lessons learned«).

Primerjalna metoda

Primerjalna metoda bo uporabljena za primerjavo različnih sistemov varovanja in njihove učinkovitosti pri odzivanju na sodobne grožnje.

Raziskava temelji na javno dostopnih virih (OSINT) in ne vključuje zaupnih ali operativnih podatkov o konkretnih sistemih varovanja. Obravnavani bodo predvsem splošni koncepti zaščite sil, organizacijski modeli in kategorije varnostnih ukrepov.

Pri raziskavi bosta uporabljena deskriptivni in analitični pristop za interpretacijo ugotovitev ter preverjanje postavljenih hipotez.

2 TEORETIČNA IZHODIŠČA

Teoretična izhodišča predstavljajo osnovo za razumevanje sistema varovanja vojaških baz in sodobnih varnostnih groženj. Zaradi razvoja asimetričnih in hibridnih oblik ogrožanja postaja zaščita vojaških objektov pomemben del nacionalne in kolektivne varnosti.

NATO pri zaščiti vojaških baz uporablja koncept večplastnega varovanja »Defense in Depth«, katerega cilj je zgodnje zaznavanje groženj, nadzor dostopa in hitro odzivanje na incidente. Sistem temelji na povezovanju fizičnih, tehničnih in organizacijskih ukrepov zaščite.

V poglavju bodo predstavljeni pomen vojaških baz, koncept kolektivne varnosti, večplastni sistem zaščite, vloga vojaških baz kot kritične infrastrukture in osnovni elementi strukture vojaških baz ter varnostnih con.

2.1 Vojaške baze in njihov pomen

Vojaške baze so ključni objekti za delovanje oboroženih sil, saj omogočajo nastanitev osebja, skladiščenje opreme, logistično podporo in izvajanje vojaških operacij. Zagotavljajo pripravljenost vojaških sil in podporo pri domačih ter mednarodnih operacijah.

V zavezništvu imajo pomembno vlogo pri kolektivni obrambi in mednarodnem sodelovanju. Med najpogostejše sodijo kopenske, letalske in pomorske baze, logistični ter obveščevalni centri in začasne operativne baze.

Vojaške baze omogočajo logistično podporo, skladiščenje orožja in opreme, načrtovanje operacij ter usposabljanje vojaškega osebja. Poleg operativne funkcije imajo pomembno vlogo tudi pri skupnih vajah in podpori zavezniškim operacijam. (US Army, 2021)

Zaradi strateške vrednosti so pogosto tarča različnih varnostnih groženj, ki lahko zmanjšajo operativno sposobnost vojaških sil ter ogrozijo osebje in infrastrukturo.

Sodobne baze uporabljajo fizične, tehnične in organizacijske ukrepe zaščite, kot so video nadzor, sistemi kontrole dostopa, senzorji, radarji in obveščevalna dejavnost. (NATO, 2022)

Konflikti v Afganistanu, Iraku in Ukrajini so pokazali, da so vojaške baze izpostavljene tudi asimetričnim in hibridnim grožnjam. Zato morajo biti sistemi varovanja prilagodljivi, tehnološko napredni in sposobni hitrega odzivanja.

2.2 NATO in koncept kolektivne varnosti

NATO je politično-varnostna in obrambna zveza, ustanovljena leta 1949 z namenom zagotavljanja kolektivne obrambe držav članic. Danes predstavlja enega najpomembnejših sistemov kolektivne varnosti na svetu. (NATO, 2022)

Temelj delovanja predstavlja 5. člen Severnoatlantske pogodbe, ki določa, da se napad na eno članico obravnava kot napad na celotno zavezništvo. Namen takšnega sistema je odvračanje agresije in zagotavljanje skupne obrambe držav članic. (NATO, 2022)

Kolektivna varnost temelji na sodelovanju držav članic pri obrambi, izmenjavi informacij, skupnem načrtovanju in vojaških operacijah. Pomembno vlogo imajo tudi vojaške baze, ki zagotavljajo logistično podporo, premik sil in zaščito zavezniških enot.

Po koncu hladne vojne se je delovanje NATO razširilo tudi na krizno upravljanje, boj proti terorizmu, zaščito kritične infrastrukture in odzivanje na sodobne grožnje, kot so kibernetski napadi, hibridno delovanje in brezpilotni sistemi. Zato zavezništvo razvija nove koncepte zaščite sil ter posodablja sisteme varovanja vojaških objektov.

Zaščita vojaških baz predstavlja pomemben del sistema kolektivne varnosti, saj baze omogočajo nastanitev enot, logistično podporo in izvajanje operacij. Pri zaščiti se uporabljajo standardizirane doktrine, večplastno varovanje, obveščevalna dejavnost in sistemi za zgodnje zaznavanje ter hitro odzivanje na incidente.

2.3 Večplastno varovanje (Defense in Depth)

Koncept večplastnega varovanja »Defense in Depth« je osnovni model zaščite vojaških baz v okviru NATO. Temelji na več medsebojno povezanih obrambnih nivojih za zaznavanje, omejevanje in nevtralizacijo groženj. (NATO, 2020)

Sistem običajno vključuje zunanjo, srednjo in notranjo varnostno cono. Zunanja cona omogoča zgodnje zaznavanje groženj in nadzor širšega območja okoli baze. Vključuje patrulje, radarje, nadzorne kamere, senzorje gibanja in druge sisteme za spremljanje širšega območja. (AJP-3.14, 2024)

Srednja varnostna cona vključuje zaščitne ograje, kontrolne točke, ovire in sisteme za kontrolo dostopa. Namenjena je preprečevanju nepooblaščenega vstopa oseb in vozil. (NATO, 2021)

Notranja cona zajema ključne objekte, kot so poveljniški centri, skladišča orožja in komunikacijski sistemi. Zaščita vključuje omejen dostop, dodatne tehnične sisteme in stalno prisotnost varnostnih sil. (US Army, 2021)

Sistem vključuje tudi obveščevalno dejavnost, analizo tveganj, sisteme zgodnjega opozarjanja in usklajeno poveljevanje. Pri odzivanju na incidente imajo pomembno vlogo tudi enote QRF (Quick Reaction Force).

Sodobno večplastno varovanje vključuje tudi zaščito pred brezpilotnimi sistemi, elektronskim motenjem in kibernetskimi napadi. NATO zato uporablja integrirane nadzorne sisteme, avtomatizirane senzorje in sisteme za zaznavanje ter nevtralizacijo dronov.

Sodobni konflikti so pokazali, da učinkovita zaščita vojaških baz zahteva hitro zaznavanje groženj, usklajeno delovanje varnostnih sil in stalno prilagajanje zaščitnih ukrepov novim oblikam ogrožanja.

2.4 Vojaške baze kot kritična infrastruktura

Vojaške baze predstavljajo pomemben del kritične infrastrukture, saj omogočajo delovanje oboroženih sil, logistično podporo in izvajanje vojaških operacij. Njihova poškodba ali uničenje lahko pomembno vpliva na obrambno sposobnost države in delovanje vojske. (NATO, 2021)

V okviru NATO imajo vojaške baze pomembno vlogo pri izvajanju vojaških operacij, logistični podpori in premiku sil. Zaradi strateškega pomena so pogosto tarča različnih varnostnih groženj.

Sodobne vojaške baze vključujejo energetske sisteme, komunikacijska omrežja, transportno infrastrukturo in informacijske sisteme, ki so povezani z drugimi deli kritične infrastrukture države. Napadi na vojaške objekte lahko zato vplivajo tudi na delovanje civilnih sistemov, kot so promet, komunikacije in oskrba z energijo. (CCDCOE, 2022)

Hibridne grožnje vključujejo kombinacijo fizičnih, informacijskih in kibernetskih napadov na vojaške objekte in infrastrukturo. Vojaške baze so lahko tarča sabotaž, kibernetskih napadov, terorističnih aktivnosti ali napadov z brezpilotnimi sistemi.

NATO pri zaščiti kritične infrastrukture uporablja različne varnostne standarde, analizo tveganj, nadzor dostopa, tehnične sisteme zaščite in krizno upravljanje. Pomemben del zaščite predstavlja tudi zagotavljanje neprekinjenega delovanja ključnih sistemov v primeru napadov ali kriznih razmer.

Za zmanjševanje posledic napadov NATO uporablja rezervne komunikacijske sisteme, alternativne vire energije in načrte kriznega odzivanja za ohranjanje operativne sposobnosti vojaških sil.

2.5 Struktura vojaške baze in varnostne cone

Struktura sodobne vojaške baze omogoča izvajanje vojaških nalog, logistično podporo in zaščito osebja ter opreme. Vojaške baze v okviru NATO temeljijo na funkcionalni razdelitvi območij in večplastnem sistemu zaščite.

Velikost in organizacija baze sta odvisni od njenega namena, lokacije in operativnih nalog. Večina vojaških baz vključuje poveljniške objekte, logistične centre, skladišča orožja, nastanitvene objekte, komunikacijske sisteme in transportna območja. (US Army, 2021)

Pomembni objekti, kot so poveljniški centri, komunikacijski sistemi in skladišča streliva, imajo višjo stopnjo zaščite zaradi njihovega pomena za delovanje vojaških sil. (NATO, 2021)

Za zagotavljanje učinkovite zaščite se vojaške baze delijo na različne varnostne cone. Takšna organizacija omogoča nadzor gibanja oseb in vozil ter omejevanje dostopa do posebej varovanih območij.

2.5.1 Zunanja varnostna cona

Zunanja cona predstavlja prvo obrambno linijo vojaške baze. Namenjena je zgodnjemu zaznavanju groženj in nadzoru okolice baze. Vključuje patrulje, opazovalnice, radarje, senzorje gibanja in nadzorne kamere. (AJP-3.14, 2024)

2.5.2 Srednja varnostna cona

Srednja cona zajema območje okoli baze in predstavlja glavno fizično zaščito objekta. Vključuje zaščitne ograje, zidove, ovire za vozila, kontrolne točke in sisteme za kontrolo dostopa.

Na kontrolnih točkah se izvajajo identifikacija oseb, pregled vozil in preverjanje dovoljenj za vstop. (US Army, 2021)

2.5.3 Notranja varnostna cona

Notranja cona vključuje ključne objekte, kot so poveljniški centri, komunikacijski sistemi in skladišča orožja. Dostop do teh območij je dovoljen le pooblaščenim osebam. (AJP-3.14, 2024)

Za zaščito notranjih območij se uporabljajo biometrični sistemi, elektronska kontrola dostopa, video nadzor, alarmni sistemi in oboroženo varovanje.

Pomembno vlogo pri zaščiti baze imajo tudi centri BDOC (Base Defense Operations Center), ki usklajujejo varnostne aktivnosti in odzivanje ob incidentih, ter enote QRF (Quick Reaction Force), namenjene hitremu posredovanju ob povečani stopnji ogroženosti. (US Department of Defense, 2020)

3 VARNOSTNE GROŽNJE VOJAŠKIM BAZAM

Vojaške baze so zaradi svoje strateške in operativne vrednosti pogosto tarča različnih varnostnih groženj. Poleg klasičnih vojaških napadov sodobno varnostno okolje vključuje tudi asimetrične, hibridne in tehnološko napredne oblike ogrožanja.

Med najpogostejše grožnje sodijo terorizem, sabotaža, raketni in minometni napadi, brezpilotni sistemi ter kibernetske in hibridne grožnje. Takšne nevarnosti zahtevajo visoko stopnjo pripravljenosti, zgodnje zaznavanje groženj ter hitro odzivanje varnostnih sil. (NATO, 2021)

Tabela 1: Glavne varnostne grožnje vojaškim bazam

Vrsta grožnje	Značilnosti	Možne posledice
Terorizem	Napadi na osebje in infrastrukturo	Žrtve, materialna škoda
Sabotaža	Namerno poškodovanje sistemov	Zmanjšana operativna sposobnost
Raketni in minometni napadi	Posredni napadi z razdalje	Poškodbe objektov in opreme
Brezpilotni sistemi (UAS)	Izvidovanje ali napadi z droni	Ogrožanje baze in nadzora
Kibernetski napadi	Napadi na informacijske sisteme	Motnje komunikacije in delovanja
Hibridne grožnje	Kombinacija fizičnih in informacijskih napadov	Destabilizacija delovanja baze

Vir: prirejeno po NATO Force Protection doctrine (Nato, Allied Joint Doctrine for Force Protection (AJP-3.14), Edition B Version 1, 2024)

Izkušnje iz konfliktov v Afganistanu, Iraku in Ukrajini so pokazale, da napadalci pogosto uporabljajo nizkocenovne tehnologije, mobilne sisteme in kombinacijo različnih načinov delovanja. Posebno nevarnost predstavljajo napadi na komunikacijske sisteme, skladišča orožja, letalsko infrastrukturo in poveljniške centre.

Zaradi povezanosti fizičnih, informacijskih in kibernetskih groženj mora biti zaščita vojaških baz zasnovana kot večplasten sistem varovanja, ki omogoča preprečevanje, zaznavanje in hitro odzivanje na incidente. (US Army, 2021)

3.1 Terorizem in sabotaža

Terorizem in sabotaža predstavljata eni izmed najresnejših varnostnih groženj vojaškim bazam, saj lahko povzročita velike materialne posledice, izgubo življenj in zmanjšanje operativne

sposobnosti vojaških sil. Zaradi strateškega pomena so vojaške baze pogosto tarča terorističnih organizacij, uporniških skupin in drugih oboroženih akterjev.

Teroristični napadi so pogosto usmerjeni proti osebju, logističnim objektom, komunikacijskim sistemom in letalski infrastrukturi. Napadalci pri tem uporabljajo samomorilske napade, avtomobile bombe, infiltracijo v bazo in improvizirana eksplozivna sredstva (IED).

Posebno nevarnost predstavlja možnost infiltracije napadalcev med civilno osebje ali pogodbenike, ki imajo dostop do vojaških objektov. Zato sodobni sistemi zaščite vključujejo stroge postopke preverjanja identitete, nadzor dostopa in spremljanje sumljivih aktivnosti. (NATO, 2020)

Sabotaža vključuje namerno poškodovanje vojaške infrastrukture, komunikacijskih sistemov, energetskih objektov ali informacijskih omrežij z namenom zmanjšanja operativne sposobnosti baze. V sodobnem varnostnem okolju pogosto vključuje tudi kibernetske napade in elektronsko motenje sistemov. (US Army, 2021)

Eden najbolj znanih primerov je napad na Camp Bastion leta 2012 v Afganistanu, kjer je skupina napadalcev prebila zunanjo zaščito baze in poškodovala letalski del objekta. Dogodek je pokazal pomen usklajenega delovanja sistemov zaznavanja, fizičnega varovanja in hitrega odzivanja varnostnih sil. (US Department of Defense, 2013)



Slika 1: Posledice napada na Camp Bastion v Afganistanu leta 2012

Vir: US Department of Defense / NATO.

Za preprečevanje terorističnih in sabotažnih aktivnosti NATO uporablja fizične ter tehnične ukrepe, kot so zaščitne ograje, kontrolne točke, video nadzor, biometrični sistemi, patrulje in sistemi za zaznavanje eksplozivnih sredstev. Pomembno vlogo imajo tudi obveščevalna dejavnost, analiza tveganj in enote QRF za hitro posredovanje.

Primeri sodobnih napadov kažejo, da morajo vojaške baze stalno prilagajati varnostne postopke novim načinom delovanja napadalcev.

3.2 Raketni in minometni napadi

Raketni in minometni napadi predstavljajo eno najpogostejših groženj vojaškim bazam v sodobnih konfliktih. Napadalcem omogočajo izvajanje napadov z večjih razdalj brez neposrednega stika z varnostnimi silami, kar otežuje pravočasno zaznavanje in preprečevanje napadov. Zaradi mobilnosti, enostavne uporabe in nizkih stroškov so takšni sistemi pogosto uporabljeni pri asimetričnem bojevanju. (NATO, 2021)

Napadi so običajno usmerjeni proti letalskim stezam, skladiščem goriva in streliva, poveljniškim centrom, nastanitvenim območjem ter logistični infrastrukturi. Posebno nevarnost predstavljajo kratkotrajni napadi z mobilnimi izstrelišči, kjer napadalci po izstrelitvi hitro zapustijo območje delovanja.

Za zaščito pred takšnimi napadi NATO uporablja večplastni sistem zaščite, ki vključuje zgodnje zaznavanje, opozarjanje osebja, fizično zaščito objektov in aktivne obrambne sisteme. Pomembno vlogo imajo radarji za zaznavanje izstrelkov in sistemi C-RAM (Counter Rocket, Artillery and Mortar), namenjeni prestrezanju raketnih ter minometnih napadov. (US Army, 2021)



Slika 2: Sistem C-RAM za zaščito vojaških baz pred raketnimi in minometnimi napadi

Vir: US Army / NATO.

Pomemben del zaščite predstavlja tudi utrjevanje ključnih objektov z zaščitnimi zidovi, bunkerji in betonskimi pregradami ter razpršitev pomembne infrastrukture znotraj baze, s čimer se zmanjšujejo posledice napadov.

Pri zaščiti imajo pomembno vlogo tudi obveščevalna dejavnost, patruljiranje okolice baze in analiza območij, iz katerih bi lahko bili izvedeni napadi. Zgodnje odkrivanje priprav na napad omogoča preventivno delovanje in zmanjšuje tveganje za uspešen napad.

Primeri iz Afganistana in Iraka kažejo, da raketni in minometni napadi ostajajo stalna grožnja vojaškim bazam, zato mora biti zaščita zasnovana tako, da omogoča hitro zaznavanje groženj, učinkovito opozarjanje in zmanjševanje posledic napadov na infrastrukturo ter osebje.

Leta 2026 je NATO dodatno okrepil sisteme zračne in protiraketne zaščite v Turčiji zaradi nevarnosti balističnih raket iz območja Bližnjega vzhoda. Dogodki so pokazali pomen integriranih sistemov zgodnjega opozarjanja in protiraketne obrambe pri zaščiti vojaških baz ter kritične infrastrukture.

3.3 Brezpilotni sistemi (UAS)

Brezpilotni sistemi (UAS – Unmanned Aerial Systems) predstavljajo eno največjih sodobnih groženj vojaškim bazam. Zaradi nizke cene, enostavne dostopnosti in težkega zaznavanja so droni postali pogosto sredstvo za izvidovanje, nadzor ter izvajanje napadov. (NATO, 2022)

Brezpilotni sistemi se uporabljajo za zbiranje obveščevalnih podatkov, opazovanje premikov enot, fotografiranje infrastrukture in usmerjanje napadov. Poleg izvidniške vloge lahko nosijo tudi eksplozivna sredstva ali izvajajo napade na komunikacijske sisteme, letalsko infrastrukturo in skladišča orožja.

Posebno nevarnost predstavljajo majhni komercialni droni, ki jih je težko zaznati z običajnimi radarji. Zaradi majhne velikosti, nizke višine leta in tihega delovanja lahko predstavljajo resno grožnjo tudi dobro zaščitenim objektom.

Konflikti v Ukrajini, Siriji in na Bližnjem vzhodu so pokazali, da so brezpilotni sistemi postali pomemben del sodobnega bojevanja. Napadi z droni se pogosto uporabljajo za motenje delovanja baz, zbiranje podatkov ali izvajanje neposrednih napadov na infrastrukturo in osebje.

Za zaščito pred brezpilotnimi sistemi NATO uporablja radarje, sisteme za elektronsko motenje signalov, senzorje za zaznavanje dronov in posebne C-UAS sisteme (Counter-Unmanned Aircraft Systems), namenjene odkrivanju in nevtralizaciji brezpilotnih plovil. (US Department of Defense, 2021)



Slika 3: Counter-UAS sistem za zaznavanje in nevtralizacijo dronov

Vir: NATO / US Department of Defense.

Pomemben del zaščite predstavljajo tudi nadzor zračnega prostora, omejevanje uporabe dronov v bližini baz in usposabljanje varnostnih sil za prepoznavanje ter odzivanje na grožnje iz zraka.

Zaradi hitrega razvoja dronov morajo NATO baze redno posodabljati sisteme za zaznavanje in zaščito pred brezpilotnimi sistemi.

Primer napada na britansko vojaško bazo RAF Akrotiri na Cipru leta 2026 je pokazal, da brezpilotni sistemi predstavljajo resno grožnjo tudi za dobro zaščitene NATO baze. Napad je poudaril pomen sistemov C-UAS, radarjev za zaznavanje dronov ter hitrega odzivanja varnostnih sil pri zaščiti vojaške infrastrukture.

Sodobni razvoj brezpilotnih sistemov (FPV in roji dronov)

V zadnjih letih je opazen hiter razvoj tako imenovanih FPV (First Person View) dronov, ki operaterju omogočajo neposredno upravljanje s pomočjo kamere na brezpilotnem plovilu. Zaradi velike hitrosti, natančnosti in razmeroma nizkih stroškov predstavljajo pomembno grožnjo vojaškim bazam. Takšni droni se lahko uporabljajo za izvidovanje, opazovanje varnostnih postopkov ali za izvedbo natančnih napadov na vozila, skladišča in drugo pomembno infrastrukturo.

Posebno nevarnost predstavljajo tudi roji dronov (drone swarms), pri katerih več brezpilotnih sistemov deluje usklajeno in istočasno napade isti cilj. Takšen način delovanja lahko preobremeni klasične sisteme zračne obrambe in oteži pravočasno zaznavanje ter nevtralizacijo vseh groženj. Zaradi tega NATO razvija napredne sisteme umetne inteligence, ki omogočajo samodejno zaznavanje, razvrščanje in spremljanje več ciljev hkrati.

Učinkovita zaščita pred sodobnimi brezpilotnimi sistemi zato temelji na povezovanju radarjev, elektrooptičnih senzorjev, termovizijskih kamer, sistemov za elektronsko motenje in centrov za poveljevanje ter nadzor. Le usklajeno delovanje vseh elementov omogoča hitro prepoznavanje grožnje in pravočasno aktiviranje ustreznih zaščitnih ukrepov.

3.4 Kibernetske in hibridne grožnje

Kibernetske in hibridne grožnje predstavljajo pomemben del sodobnega varnostnega okolja, saj lahko resno vplivajo na delovanje vojaških baz, komunikacijskih sistemov in operativnih zmogljivosti. Zaradi velike odvisnosti od informacijskih in komunikacijskih sistemov so sodobne vojaške baze vse bolj izpostavljene kibernetskim napadom. (CCDCOE, 2022)

Kibernetski napadi so pogosto usmerjeni proti komunikacijskim omrežjem, sistemom poveljevanja, radarjem, sistemom kontrole dostopa in logističnim ter informacijskim sistemom. Njihov namen je motenje delovanja baze, pridobivanje podatkov ali onemogočanje ključnih sistemov.

Posebno nevarnost predstavljajo napadi na energetske in komunikacijske sisteme, saj lahko povzročijo motnje pri delovanju varnostnih sistemov in zmanjšajo sposobnost usklajenega odzivanja varnostnih sil.

Hibridne grožnje vključujejo kombinacijo vojaških, informacijskih, kibernetskih in političnih aktivnosti z namenom destabilizacije delovanja vojaških objektov ter zmanjšanja obrambne sposobnosti države ali zavezništva. Pogosto vključujejo dezinformacije, elektronsko motenje, sabotaže in usklajene kibernetske napade.

Konflikti v Ukrajini in na Bližnjem vzhodu so pokazali, da sodobni napadi pogosto potekajo hkrati v fizičnem in digitalnem prostoru. Napadalci pri tem uporabljajo kombinacijo informacijskih operacij, kibernetskih napadov in delovanja brezpilotnih sistemov.

Za zaščito pred kibernetskimi in hibridnimi grožnjami NATO uporablja varnostne protokole, šifrirane komunikacije, nadzor omrežij, sisteme za zaznavanje vdorov in redno posodabljanje

informacijskih sistemov. Pomembno vlogo imajo tudi obveščevalna dejavnost, analiza tveganj in sodelovanje med državami članicami. (NATO CCDCOE, 2022)



Slika 4: Kibernetska zaščita vojaških sistemov

Vir: NATO CCDCOE

Sodobne grožnje zahtevajo povezovanje fizičnega in kibernetskega varovanja, saj napadi pogosto ciljajo več različnih sistemov hkrati. Zato mora biti zaščita vojaških baz zasnovana kot celovit sistem, ki omogoča hitro zaznavanje, preprečevanje in odzivanje na različne oblike ogrožanja.

4 SISTEM VAROVANJA VOJAŠKIH BAZ

Sistem varovanja vojaških baz vključuje fizične, tehnične in organizacijske ukrepe za zaščito osebja, infrastrukture, opreme in informacij pred različnimi varnostnimi grožnjami. Njegov namen je preprečevanje nepooblaščenega dostopa, zaznavanje nevarnosti ter učinkovito odzivanje na incidente. (AJP-3.14, 2024)

Tabela 2: Elementi sistema varovanja vojaških baz

Element varovanja	Namen	Primeri ukrepov
Fizično varovanje	Preprečevanje nepooblaščenega dostopa	Ograje, patrulje, kontrolne točke
Tehnično varovanje	Zaznavanje in spremljanje groženj	CCTV, senzorji, radarji
Kontrola dostopa	Omejevanje gibanja oseb in vozil	Biometrija, identifikacijske kartice
Obveščevalna dejavnost	Zgodnje zaznavanje nevarnosti	Analiza tveganj, zbiranje podatkov
QRF enote	Hitro odzivanje na incidente	Interventne patrulje
BDOC center	Koordinacija varnostnih aktivnosti	Nadzor in krizno upravljanje
C-UAS sistemi	Zaščita pred droni	Radarji, motilci signalov

Vir: prirejeno po NATO Force Protection konceptu

V okviru zveze NATO zaščita vojaških baz temelji na konceptu zaščite sil (Force Protection), ki vključuje usklajeno delovanje različnih varnostnih struktur, tehničnih sistemov in operativnih postopkov. Poseben pomen imajo fizično varovanje, nadzor dostopa, obveščevalna dejavnost, sistemi zgodnjega opozarjanja in enote za hitro posredovanje. (NATO, 2021)

Sodobne grožnje, kot so terorizem, brezpilotni sistemi, raketni napadi in kibernetsko delovanje, zahtevajo uporabo naprednih tehnologij in stalno prilagajanje varnostnih postopkov NATO, zato uporablja integrirane nadzorne sisteme, sisteme za zaznavanje dronov, avtomatizirane senzorje in napredne komunikacijske sisteme za izboljšanje zaščite vojaških objektov. (US Army, 2021)

4.1 Fizično varovanje

Fizično varovanje predstavlja temelj zaščite vojaških baz in je namenjeno preprečevanju nepooblaščenega dostopa in zaščiti osebja, infrastrukture ter opreme. Vključuje zaščitne ograje, kontrolne točke, patrulje, stražarska mesta in ovire za vozila. (US Army, 2021)

Pomemben del fizičnega varovanja predstavljajo kontrolne točke, kjer se izvajajo identifikacija oseb, pregled vozil in preverjanje dovoljenj za vstop. Za zaščito posebej pomembnih območij se uporabljajo dodatne ovire, omejitve gibanja in stalna prisotnost varnostnih sil.

Vojaške baze uporabljajo tudi opazovalne stolpe, bunkerje in utrjene položaje, namenjene nadzoru okolice ter zaščiti pred napadi. V območjih z višjo stopnjo ogroženosti se izvajajo redne patrulje znotraj in okoli baze.

Pomembno vlogo imajo vojaška policija, stražarske enote in druge varnostne sile, ki izvajajo nadzor območja, preverjanje sumljivih aktivnosti in posredovanje ob incidentih. (NATO, 2021)



Slika 5: Fizično varovanje vojaške baze z zaščitnimi ovirami in nadzornimi točkami

Vir: NATO / US Army

Za zmanjšanje nevarnosti napadov se uporabljajo tudi zaščitni zidovi, betonske pregrade, proti eksplozijske ovire in sistemi za usmerjanje gibanja vozil. Takšni ukrepi zmanjšujejo možnost nenadzorovanega vstopa in omejujejo posledice morebitnih napadov.

Fizično varovanje ostaja osnovni del zaščite vojaških baz, vendar je njegova učinkovitost odvisna od povezovanja s tehničnimi sistemi in hitrim odzivanjem varnostnih sil.

4.2 Tehnično varovanje (video nadzor, senzorji, kontrola dostopa)

Tehnično varovanje vključuje uporabo elektronskih in avtomatiziranih sistemov za zaznavanje, spremljanje in preprečevanje varnostnih groženj. Sodobne vojaške baze uporabljajo integrirane sisteme video nadzora, radarjev, senzorjev in kontrole dostopa za stalno spremljanje dogajanja znotraj ter okoli baze. (NATO, 2021)

Pomemben del tehničnega varovanja predstavlja video nadzor (CCTV), ki omogoča spremljanje ključnih območij, kontrolnih točk, skladišč in komunikacijskih objektov. Kamere so pogosto povezane s centri BDOC, kjer se izvajata nadzor in koordinacija varnostnih aktivnosti.

Za zaznavanje gibanja in nepooblaščenega dostopa se uporabljajo senzorji gibanja, infrardeči sistemi, termalne kamere in alarmni sistemi. Takšni sistemi omogočajo hitro odkrivanje sumljivih aktivnosti in pravočasno obveščanje varnostnih sil.

Pomembno vlogo imajo radarji in sistemi za nadzor zračnega prostora, namenjeni zaznavanju brezpilotnih sistemov in drugih zračnih groženj. NATO pri zaščiti baz uporablja sisteme C-UAS za odkrivanje, spremljanje in nevtralizacijo dronov. (US Department of Defense, 2021)

Za nadzor dostopa se uporabljajo elektronske identifikacijske kartice, biometrični sistemi, skenerji vozil in avtomatizirane kontrolne točke. Takšni sistemi zmanjšujejo možnost nepooblaščenega vstopa in izboljšujejo nadzor gibanja znotraj baze.



Slika 6: Sistem video nadzora in termovizijskih kamer v vojaški bazi

Vir: NATO / US Army

Sodobni sistemi tehničnega varovanja vključujejo povezovanje senzorjev, radarjev in komunikacijskih sistemov v enoten nadzorni sistem, ki omogoča hitrejšo analizo podatkov in učinkovitejše odzivanje na incidente.

Zaradi razvoja brezpilotnih sistemov, elektronskega motenja in kibernetskih groženj mora biti tehnično varovanje stalno prilagojeno novim oblikam ogrožanja in tehnološkemu razvoju varnostnih sistemov. Primer napada z brezpilotnimi sistemi na bazo RAF Akrotiri na Cipru leta 2026 je pokazal pomen sodobnih radarjev, sistemov C-UAS in integriranega nadzora zračnega prostora pri zaščiti NATO baz pred droni.

4.2.1 Varovanje pomorskih vojaških baz in zaščita pred brezpilotnimi plovili

Pomorske vojaške baze predstavljajo pomemben del obrambnega sistema držav članic zveze NATO, saj omogočajo podporo pomorskim operacijam, oskrbo vojaških ladij, vzdrževanje opreme in logistično podporo zavezniškim silam. Zaradi njihove strateške vloge so pogosto potencialna tarča različnih oblik ogrožanja, ki poleg klasičnih varnostnih tveganj vključujejo tudi sodobne grožnje iz morskega okolja.

Varovanje pomorskih baz temelji na enakih načelih večplastnega varovanja (Defense in Depth), vendar mora biti prilagojeno posebnostim obalnega in morskega prostora. Poleg varovanja kopenskega dela baze je potrebno zagotavljati tudi nadzor nad akvatorijem, pristaniškimi vhodi in območji, kjer so zasidrane vojaške ladje ali druga pomembna infrastruktura. V ta namen se uporabljajo: patruljna plovila, obalne opazovalnice, radarji za nadzor morskega prometa, elektrooptični sistemi, termovizijske kamere in sonarji za zaznavanje podvodnih groženj.

V zadnjih letih se kot nova varnostna grožnja vse pogosteje pojavljajo brezpilotna površinska plovila (USV – Unmanned Surface Vehicle) in podvodna brezpilotna plovila (UUV – Unmanned Underwater Vehicle). Zaradi relativno nizkih stroškov izdelave in težkega odkrivanja lahko predstavljajo resno nevarnost za vojaške ladje, pristaniško infrastrukturo, skladišča goriva in druga pomembna območja znotraj pomorskih baz. Takšna plovila se lahko uporabljajo za zbiranje obveščevalnih podatkov, opazovanje dejavnosti v pristanišču ali celo za izvajanje napadov z eksplozivnimi sredstvi.

Izkušnje sodobnih konfliktov so pokazale, da lahko brezpilotna plovila uspešno ogrozijo tudi dobro varovane pomorske objekte. Zato NATO namenja vedno več pozornosti razvoju sistemov za njihovo zgodnje zaznavanje in nevtralizacijo. Pomembno vlogo imajo integrirani nadzorni sistemi, ki združujejo podatke radarjev, sonarjev, kamer in drugih senzorjev v enotno

operativno sliko. Tako lahko operaterji v centru BDOC hitreje zaznajo morebitno grožnjo in uskladijo odziv varnostnih enot.

Za zaščito pristanišč se uporabljajo tudi fizične ovire, kot so zaščitne plavajoče pregrade, proti-diverzantske mreže in nadzorovani plovni koridorji, ki preprečujejo nepooblaščen dostop do vojaških plovil. Dodatno varnost zagotavljajo redne patrulje vojaške policije, pomorskih enot in potapljaške skupine, ki izvajajo preglede podvodnega dela pristaniške infrastrukture ter preverjajo morebitno prisotnost eksplozivnih naprav ali drugih nevarnih predmetov.

Učinkovito varovanje pomorskih vojaških baz zato zahteva tesno povezovanje fizičnega, tehničnega in organizacijskega varovanja. Poleg sodobnih tehnoloških rešitev imajo pomembno vlogo tudi stalna analiza tveganj, usposabljanje varnostnega osebja in sodelovanje med vojaškimi, pomorskimi ter obveščevalnimi strukturami. Le celovit pristop omogoča pravočasno zaznavanje groženj in učinkovito zaščito osebja, infrastrukture ter vojaških zmogljivosti pred vse bolj raznolikimi oblikami ogrožanja.

Zaradi razvoja brezpilotnih površinskih in podvodnih sistemov postaja varovanje pomorskih baz eno najhitreje razvijajočih se področij sistema Force Protection v okviru zveze NATO.

4.3 Organizacijski ukrepi (QRF, BDOC, obveščevalna dejavnost)

Organizacijski ukrepi predstavljajo pomemben del sistema varovanja vojaških baz, saj omogočajo usklajeno delovanje varnostnih sil, načrtovanje zaščite in hitro odzivanje na incidente. V okviru NATO so organizirani v sistem zaščite sil (Force Protection), katerega namen je zmanjšanje ranljivosti osebja, infrastrukture in opreme. (NATO, 2021)

Sistem zaščite sil vključuje načrtovanje varnostnih postopkov, analizo tveganj, nadzor dostopa, obveščevalno dejavnost in koordinacijo med različnimi vojaškimi ter varnostnimi strukturami. Pomemben del predstavljajo tudi standardni operativni postopki (SOP), ki določajo ravnanje ob različnih vrstah groženj in incidentov.

Za zagotavljanje učinkovite zaščite NATO uporablja različne stopnje varnostne pripravljenosti, ki se prilagajajo glede na oceno ogroženosti. Ob povečani nevarnosti se okrepijo patrulje, nadzor dostopa, tehnično varovanje in pripravljenost interventnih enot.

Redna usposabljanja in varnostne vaje izboljšujejo pripravljenost varnostnih sil ter odzivanje ob kriznih situacijah.

Sodobne grožnje zahtevajo stalno prilagajanje organizacijskih postopkov, povezovanje različnih varnostnih struktur in usklajeno delovanje fizičnega, tehničnega in informacijskega varovanja.

4.3.1 BDOC (Base Defense Operations Center)

BDOC (Base Defense Operations Center) predstavlja osrednji center za nadzor in koordinacijo varnostnih aktivnosti v vojaški bazi. Njegova naloga je spremljanje varnostnega stanja, usklajevanje delovanja varnostnih sil in koordinacija odzivanja ob incidentih. (US Army, 2021)

Center BDOC zbira podatke iz različnih virov, kot so video nadzor, radarji, senzorji, patrulje in obveščevalni sistemi. Na podlagi zbranih informacij se izvajata analiza varnostnega stanja in usmerjanje varnostnih aktivnosti znotraj baze.

Pomemben del delovanja BDOC predstavlja koordinacija med vojaško policijo, stražarskimi enotami, interventnimi skupinami in poveljstvom baze. Ob varnostnih incidentih center usmerja odzivanje enot, obvešča pristojne strukture in spremlja razvoj dogodkov.

BDOC ima pomembno vlogo tudi pri kriznem upravljanju, saj omogoča hitro sprejemanje odločitev in učinkovito komunikacijo med različnimi varnostnimi strukturami. V sodobnih vojaških bazah so BDOC centri povezani z integriranimi nadzornimi in komunikacijskimi sistemi, ki omogočajo stalno spremljanje varnostnega stanja.



Slika 7: Base Defense Operations Center (BDOC) – center za koordinacijo varovanja vojaške baze

Vir: NATO / US Department of Defense

Zaradi sodobnih groženj morajo BDOC centri omogočati hitro obdelavo podatkov, usklajeno odzivanje in povezovanje fizičnega, tehničnega ter informacijskega varovanja v enoten sistem zaščite.

4.3.2 QRF (Quick Reaction Force)

QRF (Quick Reaction Force) oziroma sile za hitro posredovanje predstavljajo posebej usposobljene vojaške enote za hitro odzivanje na varnostne incidente, napade in druge krizne situacije znotraj ali v bližini vojaške baze. V okviru zveze NATO imajo pomembno vlogo pri sistemu zaščite sil (Force Protection), saj omogočajo hitro ukrepanje ob zaznanih grožnjah. (NATO, 2021)

Naloga enot QRF je hitro posredovanje ob napadih, vdorih, sabotažah in drugih varnostnih incidentih znotraj ali v bližini vojaške baze. Enote so organizirane tako, da lahko v kratkem času aktivirajo osebje, prevzamejo bojni položaj in posredujejo na območju incidenta.

Pripadniki enot QRF so usposobljeni za boj v urbanem okolju, zaščito ključnih objektov, evakuacijo osebja in sodelovanje z drugimi varnostnimi strukturami. (AJP-3.14, 2024)

Pomemben del delovanja predstavlja sodelovanje s centrom BDOC (Base Defense Operations Center), ki koordinira varnostne aktivnosti in aktivira enote ob incidentih. Takšno sodelovanje omogoča hitrejše odločanje in učinkovitejše odzivanje na varnostne dogodke.

Naloge enot QRF vključujejo:

- hitro posredovanje ob napadih ali incidentih,
- zaščito ključnih objektov,
- izolacijo območja incidenta,
- nevtralizacijo napadalcev,
- pomoč pri evakuaciji osebja.

Enote uporabljajo različna vozila, komunikacijske sisteme in zaščitno opremo za hitro premikanje ter delovanje v različnih situacijah. V sodobnih vojaških bazah uporabljajo tudi sisteme za nočno opazovanje, termovizijske naprave in opremo za zaščito pred brezpilotnimi sistemi.



Slika 8: Enota QRF pri hitrem posredovanju v vojaški bazi

Vir: NATO / US Army

Pomemben del pripravljenosti predstavljajo redna usposabljanja in simulacijske vaje, s katerimi enote preverjajo učinkovitost postopkov in koordinacijo z drugimi varnostnimi strukturami.

4.3.3 Obveščevalna dejavnost

Obveščevalna dejavnost predstavlja pomemben del sistema varovanja vojaških baz, saj omogoča pravočasno zaznavanje groženj, zbiranje informacij in podporo pri načrtovanju zaščitnih ukrepov. V okviru NATO ima pomembno vlogo pri sistemu zaščite sil (Force Protection). (CCDCOE, 2022)

Namen obveščevalne dejavnosti je pridobivanje, analiza in posredovanje informacij o potencialnih nevarnostih, ki bi lahko ogrozile osebje, infrastrukturo ali delovanje vojaške baze. Na podlagi zbranih podatkov vodstvo baze sprejema odločitve o varnostnih ukrepih in stopnji pripravljenosti.

Sodobne grožnje vključujejo teroristične aktivnosti, brezpilotne sisteme, raketne napade, sabotaže in kibernetske napade, zato mora biti obveščevalna dejavnost usmerjena v stalno spremljanje varnostnega okolja in prepoznavanje sumljivih aktivnosti.

Pomemben del predstavlja HUMINT (Human Intelligence), ki temelji na pridobivanju informacij preko osebnih virov, sodelovanja z lokalnim prebivalstvom in varnostnimi ter vojaškimi strukturami. Takšni podatki lahko pomagajo pri odkrivanju priprav na napade ali drugih varnostnih tveganjih.

Poleg človeških virov imajo pomembno vlogo tudi tehnične metode zbiranja podatkov, kot so SIGINT (Signals Intelligence), elektronski nadzor, analiza komunikacij in uporaba radarjev, video nadzora ter senzorjev. (US Army, 2021)

Pomemben del sodobne obveščevalne dejavnosti predstavlja tudi OSINT (Open Source Intelligence), ki temelji na analizi javno dostopnih virov, medijev, družbenih omrežij in spletnih platform.

Obveščevalna dejavnost ima pomembno vlogo pri analizi tveganj, saj omogoča prepoznavanje ranljivosti in prilagajanje sistema varovanja glede na aktualne varnostne razmere.

Pomembno je sodelovanje med obveščevalnimi strukturami, centrom BDOC in enotami QRF, saj hitro posredovanje informacij omogoča učinkovitejše odzivanje na incidente in aktiviranje varnostnih postopkov.

Izkušnje iz sodobnih konfliktov kažejo, da pravočasno zaznavanje groženj pomembno vpliva na učinkovitost sistema varovanja in zmanjšuje možnost uspešnih napadov na vojaške baze.

4.4 Večplastni sistem zaščite

Večplastni sistem zaščite temelji na povezovanju različnih varnostnih ukrepov v enoten sistem zaščite vojaške baze. Koncept »Defense in Depth« temelji na uporabi več obrambnih nivojev za zaznavanje, omejevanje in preprečevanje groženj. (AJP-3.14, 2024)

Sistem vključuje fizično varovanje, tehnične sisteme, organizacijske ukrepe ter obveščevalno dejavnost. Zunanja zaščita temelji na patruljah, radarjih, senzorjih in nadzoru okolice baze, srednja plast vključuje zaščitne ograje, kontrolne točke in nadzor dostopa, notranja zaščita pa varuje ključne objekte, kot so poveljniški centri, skladišča orožja in komunikacijski sistemi.

Pomemben del sistema predstavljajo video nadzor, alarmni sistemi, radarji, sistemi C-UAS in koordinacija med BDOC centrom, enotami QRF in varnostnimi silami. (US Army, 2021)

Sodobni sistemi zaščite vključujejo zaščito pred brezpilotnimi sistemi, elektronskim motenjem in kibernetskimi napadi. Pomembna značilnost večplastnega varovanja je prilagodljivost glede na stopnjo ogroženosti in vrsto grožnje.

Primeri sodobnih napadov v Turčiji in na Cipru leta 2026 so pokazali, da večplastni sistem zaščite omogoča učinkovitejše zaznavanje groženj in hitrejše odzivanje na raketne ter brezpilotne napade.

4.5 Varnostne stopnje in protokoli (FPCON)

FPCON (Force Protection Condition) predstavlja sistem varnostnih stopenj, ki ga NATO uporablja za določanje stopnje ogroženosti vojaških baz in izvajanje ustreznih zaščitnih ukrepov. Namen sistema je prilagajanje varnostnih postopkov glede na trenutno varnostno situacijo in zaznane grožnje. (NATO, 2021)

Tabela 3: FPCON varnostne stopnje v okviru NATO Force Protection sistema

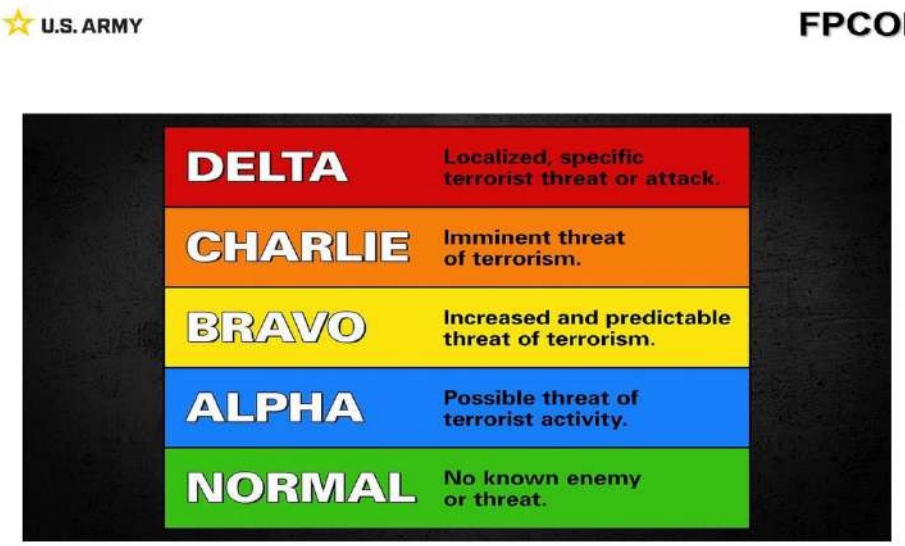
FPCON stopnja	Opis stopnje ogroženosti	Primer ukrepov
Normal	Običajna stopnja varnosti	Redni varnostni postopki
Alpha	Splošna možnost grožnje	Povečan nadzor dostopa
Bravo	Povečana nevarnost napada	Dodatne patrulje in pregledi
Charlie	Verjetna grožnja ali incident	Omejitev gibanja, višja pripravljenost
Delta	Neposredna ali izvedena grožnja	Zaprtje baze, maksimalni varnostni ukrepi

Vir: NATO Force Protection doctrine

Ob višji stopnji ogroženosti se povečajo: nadzor dostopa, število patrulj, pripravljenost enot QRF in obseg tehničnega nadzora. Sistem omogoča hitro prilagajanje zaščitnih ukrepov glede na obveščevalne podatke, varnostne incidente ali razvoj kriznih razmer. Ob povečanih napetostih na Bližnjem vzhodu leta 2026 je NATO v več bazah povečal stopnjo zaščite sil (FPCON) in okrepil sisteme zračne obrambe ter pripravljenost varnostnih enot.

Pri izvajanju FPCON ukrepov sodelujejo center BDOC, vojaška policija, obveščevalne službe, tehnični operaterji in enote QRF. Usklajeno delovanje vseh elementov omogoča učinkovitejše zaznavanje groženj in hitrejše odzivanje na incidente.

Sodobne grožnje, kot so terorizem, brezpilotni sistemi in hibridno delovanje, zahtevajo stalno prilagajanje varnostnih protokolov in redno izvajanje varnostnih vaj ter usposabljanj.



Slika 9: FPCON varnostne stopnje v okviru zaščite sil NATO

Vir: NATO Force Protection doctrine

Sistem FPCON danes predstavlja pomemben del sodobnega sistema varovanja vojaških baz, saj omogoča standardizirano, prilagodljivo in učinkovito upravljanje varnostnih tveganj v različnih operativnih okoljih.

4.6 Integracija varnostnih sistemov

Integracija varnostnih sistemov pomeni povezovanje fizičnih, tehničnih, organizacijskih in informacijskih elementov zaščite v enoten sistem varovanja vojaške baze. Namen integracije je

izboljšati zaznavanje groženj, hitrost odzivanja in koordinacijo med varnostnimi strukturami. (US Army, 2021)

V okviru NATO integrirani sistemi vključujejo video nadzor, radarje, senzorje gibanja, alarmne sisteme, kontrolo dostopa, komunikacijska omrežja in sisteme za zaznavanje brezpilotnih sistemov. Podatki se zbirajo in obdelujejo v centru BDOC, ki koordinira varnostne aktivnosti in odzivanje ob incidentih. (NATO, 2021)

Pomembna prednost integracije je samodejno povezovanje različnih sistemov. Ob zaznani grožnji lahko sistem aktivira kamere, sproži alarm in obvesti operaterje ter varnostne enote, kar omogoča hitrejše odzivanje.

Sodobni sistemi vključujejo tudi zaščito informacijskih omrežij pred kibernetskimi napadi, uporabo šifriranih komunikacij in sisteme za zaznavanje vdorov. (CCDCOE, 2022)

Pomemben del razvoja predstavljata avtomatizacija in uporaba umetne inteligence, ki omogočata analizo podatkov, prepoznavanje sumljivih aktivnosti in podporo pri odločanju varnostnih operaterjev.

Izkušnje iz sodobnih konfliktov kažejo, da integracija različnih varnostnih sistemov pomembno izboljšuje učinkovitost zaščite vojaških baz in zmanjšuje odzivni čas ob incidentih.

Poleg povezovanja posameznih tehničnih sistemov postaja vse pomembnejša tudi vzpostavitev skupne operativne slike (Common Operational Picture – COP), ki operaterjem v centru BDOC omogoča celovit pregled nad varnostnim stanjem vojaške baze. Na enem mestu so združeni podatki video nadzora, radarjev, senzorjev, kontrolnih točk, patrulj in obveščevalnih virov, kar omogoča hitrejše prepoznavanje morebitnih groženj in učinkovitejše odločanje. Takšen pristop zmanjšuje možnost napačne ocene razmer in izboljšuje koordinacijo med posameznimi varnostnimi enotami.

Pomemben del sodobnih integriranih sistemov predstavlja tudi povezovanje zaščite pred zračnimi in pomorskimi grožnjami. Poleg sistemov C-UAS za zaznavanje brezpilotnih letalnikov NATO postopoma vključuje tudi sisteme za zaznavanje brezpilotnih površinskih in podvodnih plovil, predvsem pri varovanju pomorskih vojaških baz in pristanišč. Združevanje podatkov različnih senzorjev omogoča zgodnejše odkrivanje nevarnosti in pravočasno aktiviranje ustreznih zaščitnih ukrepov.

Nadaljnji razvoj varnostnih sistemov temelji na uporabi umetne inteligence, strojnega učenja in avtomatizirane analize podatkov. Takšni sistemi lahko samodejno prepoznajo nenavadne

vzorce gibanja oseb ali vozil, zaznajo prisotnost brezpilotnih sistemov in operaterjem predlagajo najprimernejše ukrepe za odzivanje. Čeprav končno odločitev še vedno sprejme odgovorna oseba, uporaba naprednih tehnologij bistveno prispeva k hitrejšemu odločanju in učinkovitejšemu varovanju vojaških baz.

Integracija vseh varnostnih podsistemov zato predstavlja enega ključnih dejavnikov sodobnega sistema varovanja vojaških baz in pomembno prispeva k večji odpornosti proti sodobnim varnostnim grožnjam.

5 ANALIZA PRIMEROV IN INCIDENTOV

Analiza primerov napadov na vojaške baze omogoča boljše razumevanje sodobnih varnostnih groženj in učinkovitosti zaščitnih ukrepov. Sodobni konflikti so pokazali, da so vojaške baze pogosto tarča terorističnih napadov, raketnega obstreljevanja, brezpilotnih sistemov in sabotaž. (NATO, 2021)

Primeri iz Afganistana, Iraka in drugih kriznih območij kažejo, da lahko tudi dobro zaščitene baze postanejo ranljive zaradi pomanjkljivega nadzora, počasnega odzivanja ali uporabe novih načinov napadov.

Pri analizi primerov bodo obravnavani uporabljeni načini napadov, odzivanje varnostnih sil, delovanje sistemov zaščite in ključne ugotovitve za izboljšanje varovanja vojaških baz.

Poseben poudarek bo namenjen primerjavi različnih sistemov zaščite in analizi ranljivosti, ki so se pokazale med sodobnimi vojaškimi operacijami.

5.1 Izbrane vojaške baze

Za analizo sistemov varovanja in sodobnih groženj so bile izbrane vojaške baze, ki so bile v preteklosti izpostavljene različnim oblikam napadov. Primeri omogočajo primerjavo varnostnih ukrepov, odzivanja varnostnih sil in učinkovitosti sistema zaščite v različnih operativnih okoljih.

Izbrane baze so:

- Camp Bastion v Afganistanu,
- Al Asad Airbase v Iraku,
- Balad Air Base v Iraku.

Gre za pomembne vojaške objekte, ki so imeli ključno logistično in operativno vlogo v NATO in koalicijskih operacijah. Zaradi strateškega pomena so bile pogosto tarča terorističnih, raketnih in drugih asimetričnih napadov. (US Army, 2021)

Analiza primerov bo osredotočena na uporabljene varnostne ukrepe, način izvedbe napadov, odzivanje varnostnih sil in ključne ugotovitve za izboljšanje sistema varovanja vojaških baz.

5.1.1 Camp Bastion – Afganistan

Camp Bastion je bila ena največjih vojaških baz v Afganistanu in pomembno logistično ter operativno središče sil NATO in ISAF. Baza je bila uporabljena za nastanitev vojaškega osebja,

letalske operacije, skladiščenje opreme in podporo vojaškim operacijam v regiji. (US Department of Defense, 2013)

Septembra 2012 je bila baza tarča obsežnega terorističnega napada, v katerem je skupina napadalcev prebila zunanjo zaščito baze in napadla letalski del objekta. V napadu je bilo uničenih več letal, poškodovana infrastruktura in ubitih več pripadnikov varnostnih sil.

Napadalci so izkoristili pomanjkljiv nadzor določenih delov perimetra in element presenečenja. Dogodek je pokazal, da lahko tudi dobro zaščitene vojaške baze postanejo ranljive ob usklajenih asimetričnih napadih. Napad je pokazal pomanjkljivosti pri nadzoru zunanjega perimetra in počasno zaznavanje vdora, kar je omogočilo dostop napadalcev do pomembnega dela baze.

Po napadu so bili okrepljeni sistemi fizičnega varovanja, nadzor perimetra, tehnični sistemi zaznavanja in pripravljenost enot QRF. Poseben poudarek je bil namenjen izboljšanju koordinacije med varnostnimi strukturami in hitrejšemu odzivanju ob incidentih.

Napad na Camp Bastion velja za enega pomembnejših primerov sodobnih napadov na vojaške baze, saj je pokazal pomen večplastnega varovanja, obveščevalne dejavnosti in stalnega prilagajanja varnostnih sistemov sodobnim grožnjam.



Slika 10: Vojaška baza Camp Bastion v Afganistanu

Vir: NATO / ISAF

5.1.2 Al Asad Airbase – Irak

Al Asad Airbase je ena največjih vojaških baz v Iraku in pomembno operativno središče iraških in zavezniških sil. Baza ima pomembno vlogo pri letalskih operacijah, logistični podpori in usposabljanju vojaških enot. (US Air Force, 2020)

Januarja 2020 je bila baza tarča raketnega napada, pri katerem je bilo izstreljenih več balističnih raket. Napad je povzročil poškodbe infrastrukture in pokazal ranljivost vojaških baz pred napadi z večjih razdalj.

Kljub obsežnemu napadu je sistem zgodnjega opozarjanja omogočil pravočasno obveščanje osebja in zmanjšanje števila žrtev. Pomembno vlogo so imeli utrjeni objekti, alarmni sistemi in organizirani postopki zaščite sil.

Dogodek je pokazal pomen radarjev, sistemov zgodnjega zaznavanja in kriznega odzivanja pri zaščiti vojaških baz pred raketnimi napadi. Po napadu so bili okrepljeni sistemi zračne obrambe, zaščita infrastrukture in varnostni postopki v primeru posrednega ognja.

Napad na Al Asad Airbase je pokazal, da sodobne vojaške baze potrebujejo učinkovite sisteme opozarjanja, zaščite infrastrukture in hitro odzivanje za zmanjševanje posledic raketnih napadov.



Slika 11: Al Asad Airbase v Iraku

Vir: US Air Force / NATO

5.1.3 Balad Air Base – Irak

Balad Air Base je pomembna vojaška baza v Iraku, ki se uporablja za letalske operacije, logistično podporo in vzdrževanje vojaške opreme. Zaradi strateškega pomena je bila večkrat tarča raketnih napadov in drugih varnostnih incidentov. (US Air Force, 2021)

Baza je bila v preteklosti pogosto izpostavljena raketnemu in minometnemu obstreljevanju, usmerjenemu proti letalski infrastrukturi, nastanitvenim območjem in logističnim objektom. Takšni napadi so povzročali materialno škodo in motnje pri izvajanju operacij.

Pomemben del zaščite baze so predstavljali sistemi zgodnjega opozarjanja, utrjeni objekti, zaščitne pregrade in patruljiranje okolice baze. Za zmanjšanje posledic napadov so bili uporabljeni tudi alarmni sistemi in postopki hitrega umika osebja v zaščitne objekte.

Napadi na Balad Air Base so pokazali pomen stalnega nadzora okolice baze, učinkovitega opozarjanja in hitrega odzivanja varnostnih sil pri zaščiti osebja ter infrastrukture.

Izkušnje iz Iraka so pokazale, da morajo biti sistemi varovanja prilagodljivi in sposobni odzivanja na dolgotrajne asimetrične grožnje ter ponavljajoče se napade.



Slika 12: Balad Air Base v Iraku

Vir: US Air Force / NATO

5.2 Primerjava sistemov varovanja

Primerjava izbranih vojaških baz kaže, da učinkovito varovanje temelji na povezovanju fizičnih, tehničnih in organizacijskih ukrepov zaščite. Kljub različnim operativnim razmeram imajo analizirane baze podobne elemente zaščite, kot so nadzor dostopa, video nadzor, patruljiranje, sistemi zgodnjega opozarjanja in enote QRF. (NATO, 2021)

Tabela 4: Primerjava sistemov varovanja izbranih vojaških baz

Vojaška baza	**Glavne grožnje**	**Ključni varnostni ukrepi**	**Ugotovljene ranljivosti**
Camp Bastion	Teroristični napadi	Ograje, patrulje, QRF	Preboj zunanje zaščite
Al Asad Airbase	Raketni napadi	C-RAM, radarji, bunkerji	Ranljivost pred posrednim ognjem
Balad Air Base	Minometni in raketni napadi	Video nadzor, utrjeni objekti	Pogosti napadi na infrastrukturo

Vir: lastna analiza na podlagi NATO in javno dostopnih virov

Analiza primerov kaže, da noben posamezen varnostni ukrep ne zagotavlja popolne zaščite. Učinkovit sistem temelji na večplastnem varovanju, povezovanju različnih sistemov zaščite in usklajenem delovanju varnostnih struktur.

Pomembno vlogo imajo tudi obveščevalna dejavnost, analiza tveganj in stalno prilagajanje zaščitnih ukrepov glede na razvoj sodobnih groženj.

5.3 Analiza napadov na vojaške baze

Analiza izbranih primerov kaže, da sodobne vojaške baze ostajajo ranljive predvsem pred asimetričnimi in tehnološko naprednimi grožnjami. Napadi v Afganistanu in Iraku so pokazali pomen pravočasnega zaznavanja groženj, učinkovitega nadzora perimetra ter hitrega odzivanja varnostnih sil.

Pri večini napadov so napadalci izkoristili element presenečenja, pomanjkljiv nadzor določenih območij ali uporabo napadov z večjih razdalj. Posebno nevarnost predstavljajo raketni napadi, brezpilotni sistemi in infiltracija napadalcev v bližino baze.

Analiza primerov kaže, da fizično varovanje samo po sebi ni dovolj za učinkovito zaščito vojaških baz. Pomembno vlogo imajo povezovanje tehničnih sistemov, obveščevalna dejavnost, sistemi zgodnjega opozarjanja in koordinacija med varnostnimi strukturami.

Pomemben dejavnik zaščite predstavljajo tudi BDOC centri in enote QRF, ki omogočajo hitrejše odzivanje ob incidentih ter zmanjševanje posledic napadov.

Sodobni konflikti kažejo, da morajo biti sistemi varovanja prilagodljivi in sposobni odzivanja na različne vrste groženj, vključno s kibernetskimi in hibridnimi napadi. NATO zato razvija večplastne sisteme zaščite, ki združujejo fizično, tehnično in organizacijsko varovanje.

Aktualni primeri iz leta 2026, povezani z raketnimi grožnjami v Turčiji in napadi z brezpilotnimi sistemi na RAF Akrotiri na Cipru, kažejo, da sodobne vojaške baze ostajajo izpostavljene kombinaciji raketnih, zračnih in hibridnih groženj. Dogodki potrjujejo pomen večplastnega sistema zaščite, sistemov zgodnjega opozarjanja in hitrega odzivanja varnostnih sil.

5.4 Ključne ugotovitve (Lessons Learned)

Analiza sodobnih napadov na vojaške baze kaže, da učinkovito varovanje temelji na povezovanju fizičnih, tehničnih in organizacijskih ukrepov zaščite. Noben posamezen sistem ne zagotavlja popolne varnosti, zato je pomemben večplastni pristop varovanja. (NATO, 2021)

Pomembno vlogo imajo zgodnje zaznavanje groženj, obveščevalna dejavnost, nadzor dostopa in hitro odzivanje varnostnih sil. Primeri iz Afganistana in Iraka so pokazali, da lahko počasno odzivanje ali pomanjkljiv nadzor povečata ranljivost vojaških baz.

Posebno nevarnost predstavljajo brezpilotni sistemi, raketni napadi in hibridne grožnje, ki zahtevajo uporabo naprednih tehničnih sistemov, radarjev, sistemov C-UAS in zaščite komunikacijskih ter informacijskih omrežij.

Pomembna ugotovitev je tudi pomen koordinacije med centrom BDOC, enotami QRF, obveščevalnimi strukturami in drugimi varnostnimi silami. Usklajeno delovanje omogoča hitrejše sprejemanje odločitev in učinkovitejše odzivanje ob incidentih.

Tabela 5: Ključne ugotovitve sodobnih napadov na vojaške baze

Ugotovitev	Pomen za varovanje
Potrebno je zgodnje zaznavanje groženj	Skrajšanje odzivnega časa
Droni predstavljajo veliko grožnjo	Potrebni C-UAS sistemi
Fizično varovanje samo ni dovolj	Potrebna integracija sistemov
Pomembna je obveščevalna dejavnost	Preventivno odkrivanje napadov
Hiter odziv QRF zmanjšuje posledice	Učinkovitejša zaščita osebja

Vir: (Lastni vir)

Sodobni konflikti kažejo, da morajo biti sistemi varovanja stalno prilagojeni novim oblikam groženj in tehnološkemu razvoju sodobnega bojevanja.

6 RAZPRAVA IN PRIPOROČILA

Sodobno varnostno okolje kaže, da so vojaške baze izpostavljene vedno bolj kompleksnim grožnjam, ki vključujejo terorizem, raketne napade, brezpilotne sisteme in kibernetsko ter hibridno delovanje. Zaradi tega mora biti sistem varovanja zasnovan kot večplasten in prilagodljiv sistem zaščite. (NATO, 2021)

Analiza teoretičnih izhodišč in primerov napadov je pokazala, da učinkovito varovanje temelji na povezovanju fizičnega varovanja, tehničnih sistemov, obveščevalne dejavnosti in organizacijskih ukrepov. Pomembno vlogo imajo tudi sistemi zgodnjega opozarjanja, nadzor dostopa, center BDOC in enote QRF.

Sodobni konflikti so pokazali, da tradicionalni sistemi zaščite pogosto niso dovolj učinkoviti proti asimetričnim in tehnološko naprednim grožnjam. Poseben izziv predstavljajo brezpilotni sistemi in kibernetski napadi, ki zahtevajo uporabo naprednih sistemov zaznavanja, zaščite komunikacij in hitrega odzivanja.

V nadaljevanju bodo predstavljene ključne ugotovitve raziskave, interpretacija rezultatov in predlogi za izboljšanje sistema varovanja vojaških baz v okviru NATO.

6.1 Interpretacija rezultatov

Rezultati raziskave potrjujejo, da varovanje vojaških baz temelji na povezovanju fizičnih, tehničnih in organizacijskih ukrepov zaščite. Učinkovit sistem varovanja vključuje nadzor dostopa, tehnične sisteme zaznavanja, obveščevalno dejavnost in hitro odzivanje varnostnih sil. (AJP-3.14, 2024)

Analiza primerov napadov je pokazala, da sodobne grožnje pogosto vključujejo kombinacijo različnih načinov delovanja, kot so raketni napadi, brezpilotni sistemi, sabotaže in kibernetske aktivnosti. Zaradi tega mora biti zaščita vojaških baz zasnovana kot večplasten sistem varovanja.

Rezultati potrjujejo tudi pomembno vlogo centrov BDOC in enot QRF pri koordinaciji varnostnih aktivnosti in odzivanju ob incidentih. Pomembna dejavnika zaščite sta pravočasno zaznavanje groženj in učinkovita komunikacija med varnostnimi strukturami.

Raziskava je pokazala, da imajo sodobne tehnologije pomembno vlogo pri izboljšanju zaščite vojaških baz. Poseben pomen imajo radarji, sistemi C-UAS, video nadzor, avtomatizirani senzorji in sistemi za zaščito informacijskih omrežij.

Na podlagi analiziranih primerov je mogoče ugotoviti, da sodobne grožnje zahtevajo stalno prilagajanje varnostnih sistemov, redno usposabljanje osebja in razvoj novih zaščitnih rešitev za zmanjševanje ranljivosti vojaških baz.

6.2 Predlogi za izboljšanje varovanja

Na podlagi analize sodobnih groženj in primerov napadov je mogoče ugotoviti, da je za učinkovitejšo zaščito vojaških baz potrebno stalno izboljševanje varnostnih sistemov in prilagajanje novim oblikam ogrožanja.

Pomemben ukrep predstavlja nadgradnja sistemov za zaznavanje brezpilotnih sistemov, predvsem radarjev, senzorjev in sistemov C-UAS za odkrivanje ter nevtralizacijo dronov. (NATO, 2022)

Za izboljšanje zaščite je pomembno tudi povezovanje video nadzora, alarmnih sistemov, radarjev in komunikacijskih omrežij v enoten nadzorni sistem, ki omogoča hitrejšo analizo podatkov in učinkovitejše odzivanje ob incidentih.

Poseben poudarek mora biti namenjen zaščiti informacijskih in komunikacijskih sistemov pred kibernetskimi napadi. Pomembni ukrepi vključujejo uporabo šifriranih komunikacij, sistemov za zaznavanje vdorov in redno posodabljanje programske opreme.

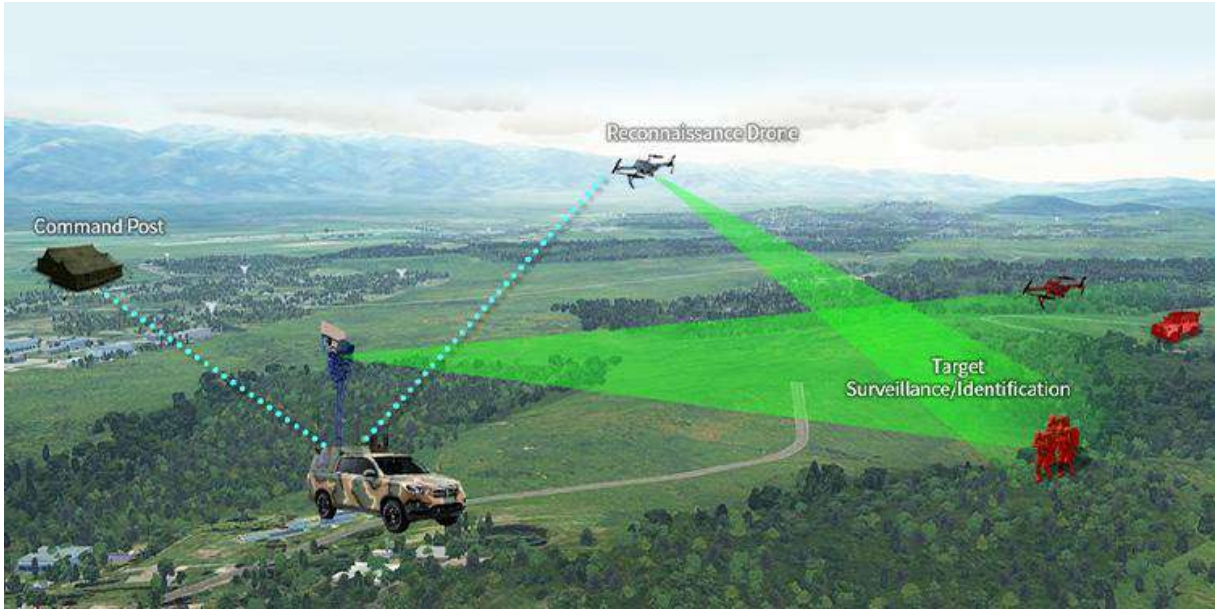
Pomembno vlogo imajo tudi redna usposabljanja, varnostne vaje in preverjanje pripravljenosti varnostnih struktur, saj izboljšujejo koordinacijo med enotami BDOC, QRF in drugimi varnostnimi silami.

Tabela 6: Predlogi za izboljšanje sistema varovanja vojaških baz

Področje izboljšave	**Predlagani ukrepi**	**Namen**
Zaščita pred droni	Uvedba C-UAS sistemov	Zaznavanje in nevtralizacija UAS
Kibernetska varnost	Nadgradnja zaščite omrežij	Preprečevanje kibernetskih napadov
Video nadzor	Uporaba AI analitike	Hitrejše zaznavanje groženj
Fizično varovanje	Dodatne zaščitne ovire	Večja zaščita perimetra
Usposabljanje osebja	Redne varnostne vaje	Izboljšanje pripravljenosti
Krizno upravljanje	Izboljšanje koordinacije BDOC	Hitrejše odzivanje na incidente

Vir: (Lastni vir)

Sodobne varnostne grožnje zahtevajo stalno prilagajanje zaščitnih sistemov in uporabo sodobnih tehnologij za zaznavanje ter preprečevanje napadov. Prihodnji razvoj varovanja vojaških baz bo temeljil predvsem na integraciji različnih varnostnih sistemov, avtomatizaciji in zaščiti pred brezpilotnimi ter kibernetskimi grožnjami.



Slika 13: Sodobni integrirani sistemi varovanja vojaških baz

Vir: NATO / Defense Technology

Slika prikazuje povezovanje sodobnih sistemov varovanja, kot so video nadzor, radarji, senzorji, sistemi C-UAS in komunikacijska omrežja, v enoten sistem zaščite vojaške baze. Integracija različnih sistemov omogoča hitrejše zaznavanje groženj in učinkovitejše odzivanje varnostnih sil. Sodobni primeri napadov na vojaške baze kažejo potrebo po nadaljnjem razvoju sistemov C-UAS, protiraketne zaščite, avtomatiziranega zaznavanja groženj in integracije umetne inteligence v varnostne sisteme NATO baz.

V prihodnje bo razvoj sistemov varovanja vojaških baz vse bolj temeljil na povezovanju naprednih tehnologij, avtomatizacije in umetne inteligence. Sistemi bodo sposobni samodejno analizirati podatke različnih senzorjev, zaznavati nenavadne dogodke in opozarjati operaterje na morebitne varnostne grožnje. Takšne rešitve bodo omogočale hitrejše odločanje in učinkovitejše usklajevanje delovanja varnostnih sil.

Posebna pozornost bo namenjena zaščiti pred brezpilotnimi sistemi vseh vrst. Poleg zračnih dronov bo treba razvijati tudi zmogljivosti za zaznavanje in nevtralizacijo brezpilotnih površinskih in podvodnih plovil, ki predstavljajo vedno večjo nevarnost predvsem za pomorske

vojaške baze in pristanišča. Zaradi hitrega razvoja teh tehnologij bo potrebno stalno posodabljanje sistemov zaznavanja, komunikacijskih omrežij in zaščitnih ukrepov.

Pomemben dejavnik prihodnjega razvoja ostaja tudi usposabljanje osebja. Ne glede na tehnološki napredek je učinkovitost sistema varovanja še vedno odvisna od strokovno usposobljenih pripadnikov, njihovega poznavanja postopkov in sposobnosti hitrega ter usklajenega odzivanja ob varnostnih incidentih. Redne vaje, simulacije različnih scenarijev in sodelovanje med državami članicami NATO bodo tudi v prihodnje predstavljali pomemben element razvoja sistema zaščite sil.

6.3 Omejitve raziskave

Raziskava temelji predvsem na analizi strokovne literature, NATO doktrin, javno dostopnih dokumentov in študij primerov, zato ne vključuje zaupnih ali operativnih podatkov o konkretnih sistemih varovanja vojaških baz.

Omejitev raziskave predstavlja tudi dejstvo, da številni podatki o zaščiti vojaških objektov zaradi varnostnih razlogov niso javno dostopni. Zaradi tega so bili obravnavani predvsem splošni koncepti zaščite sil, organizacijski modeli in javno znani primeri napadov.

Analiza primerov temelji na javno dostopnih informacijah o napadih v Afganistanu in Iraku, zato vseh operativnih podrobnosti ni bilo mogoče vključiti v raziskavo.

Omejitev predstavlja tudi hitro spreminjanje sodobnih groženj in razvoj novih tehnologij, zaradi česar se sistemi varovanja vojaških baz stalno prilagajajo in posodabljajo.

Kljub omejitvam raziskava omogoča vpogled v osnovne elemente sistema varovanja vojaških baz in sodobne varnostne grožnje, s katerimi se sooča NATO v sodobnem varnostnem okolju.

6.4 Preverjanje hipotez

Interpretacija preverjanja hipotez

Na podlagi analize strokovne literature, NATO doktrin in izbranih študij primerov je mogoče ugotoviti, da so bile vse tri postavljene hipoteze potrjene. Raziskava je pokazala, da učinkovito varovanje vojaških baz temelji na medsebojno povezani uporabi fizičnih, tehničnih in organizacijskih ukrepov, ki skupaj tvorijo večplastni sistem zaščite v skladu s konceptom Defense in Depth.

Prva hipoteza je bila potrjena, saj analiza potrjuje, da posamezen varnostni ukrep sam po sebi ne zagotavlja zadostne zaščite. Visoka stopnja varnosti je dosežena predvsem z integracijo različnih elementov sistema varovanja, kot so fizične ovire, tehnični nadzorni sistemi, kontrola dostopa, obveščevalna dejavnost in usklajeno delovanje varnostnega osebja.

Potrjena je bila tudi druga hipoteza, saj so študije primerov pokazale, da imajo zgodnje zaznavanje groženj, učinkovit nadzor dostopa in hitro ter usklajeno poveljevanje ključno vlogo pri zmanjševanju posledic varnostnih incidentov. Delovanje centra BDOC in enot QRF pomembno prispeva k pravočasnemu odzivanju in učinkovitemu obvladovanju kriznih razmer.

Tretja hipoteza je bila prav tako potrjena. Razvoj brezpilotnih sistemov, hibridnih groženj in drugih sodobnih oblik ogrožanja zahteva stalno prilagajanje sistemov varovanja in uvajanje novih tehnoloških rešitev. Uporaba sistemov C-UAS, naprednih senzorjev, umetne inteligence in integriranih nadzornih sistemov postaja nepogrešljiv del sodobnega varovanja vojaških baz v okviru zveze NATO.

Rezultati raziskave potrjujejo, da mora biti sistem varovanja vojaških baz zasnovan celovito in prilagodljivo. Le s stalnim razvojem zaščitnih zmogljivosti, usposabljanjem osebja in uvajanjem novih tehnologij je mogoče učinkovito odgovoriti na spreminjajoče se varnostne grožnje sodobnega varnostnega okolja.

Tabela 7: Hipoteze in ugotovitve

Hipoteza	Ugotovitev	Status
H1	Varovanje vojaških baz temelji na povezovanju fizičnih, tehničnih in organizacijskih ukrepov v enoten sistem zaščite.	Potrjena
H2	Zgodnje zaznavanje groženj, nadzor dostopa in usklajeno poveljevanje predstavljajo ključne dejavnike učinkovitega varovanja.	Potrjena
H3	Brezpilotni sistemi, kibernetske in hibridne grožnje zahtevajo uporabo naprednih in večplastnih zaščitnih rešitev.	Potrjena

Vir: (Lastni vir)

7 SKLEP

Diplomsko delo je obravnavalo sistem varovanja vojaških baz v okviru zveze NATO in analiziralo ključne varnostne ukrepe za zaščito osebja, infrastrukture ter vojaške opreme pred sodobnimi varnostnimi grožnjami. Na podlagi analize strokovne literature, NATO doktrin in študij primerov napadov na vojaške baze je bilo ugotovljeno, da učinkovito varovanje temelji na povezovanju različnih varnostnih ukrepov v celovit sistem zaščite.

Raziskava je pokazala, da koncept Defense in Depth predstavlja temelj sodobnega varovanja vojaških baz, saj omogoča večplastno zaščito, zgodnje zaznavanje groženj, učinkovit nadzor dostopa in hitro ter usklajeno odzivanje varnostnih sil. Pomembno vlogo imajo fizično varovanje, tehnični sistemi, obveščevalna dejavnost, center BDOC in enote QRF, ki skupaj zagotavljajo visoko stopnjo zaščite vojaških objektov. Analiza je pokazala, da noben posamezen varnostni ukrep ne zagotavlja zadostne zaščite, temveč je uspešnost sistema odvisna predvsem od njihovega medsebojnega povezovanja in usklajenega delovanja.

Pomemben del raziskave je predstavljala analiza sodobnih varnostnih groženj, ki se v zadnjih letih hitro spreminjajo. Poleg klasičnih oblik ogrožanja, kot so teroristični napadi, sabotaže ter raketni in minometni napadi, postajajo vse pomembnejše tudi brezpilotni sistemi, kibernetski napadi in različne hibridne grožnje. Prav zaradi njihove raznolikosti morajo biti sistemi varovanja vojaških baz prilagodljivi, tehnološko napredni in sposobni hitrega odzivanja na nepredvidljive varnostne dogodke.

Analiza študij primerov Camp Bastion, Al Asad Airbase in Balad Air Base je pokazala, da so bili uspešni napadi pogosto posledica kombinacije različnih dejavnikov, kot so pomanjkljiva zgodnja zaznava groženj, nezadostno usklajevanje varnostnih struktur ali omejene zmogljivosti za pravočasno odzivanje. Obravnavani primeri hkrati potrjujejo, da lahko pravočasno delovanje centrov BDOC, enot QRF in sodobnih sistemov nadzora pomembno zmanjša posledice napadov ter izboljša varnost osebja in infrastrukture.

Na podlagi izvedene raziskave so bile preverjene postavljene hipoteze.

Hipoteza H1, da varovanje vojaških baz temelji na integraciji fizičnih, tehničnih in organizacijskih ukrepov, je bila **potrjena**. Analiza strokovne literature, NATO doktrin in obravnavanih primerov je pokazala, da posamezni ukrepi sami po sebi ne zagotavljajo zadostne stopnje zaščite, temveč morajo delovati kot medsebojno povezan sistem.

Hipoteza H2, da so ključni dejavniki učinkovitega varovanja zgodnje zaznavanje groženj, nadzor dostopa in usklajeno poveljevanje, je bila **potrjena**. Ugotovitve kažejo, da pravočasno odkrivanje nevarnosti, učinkovita organizacija sistema varovanja in hitro odločanje pomembno prispevajo k zmanjšanju tveganj ter uspešnemu odzivanju na varnostne incidente.

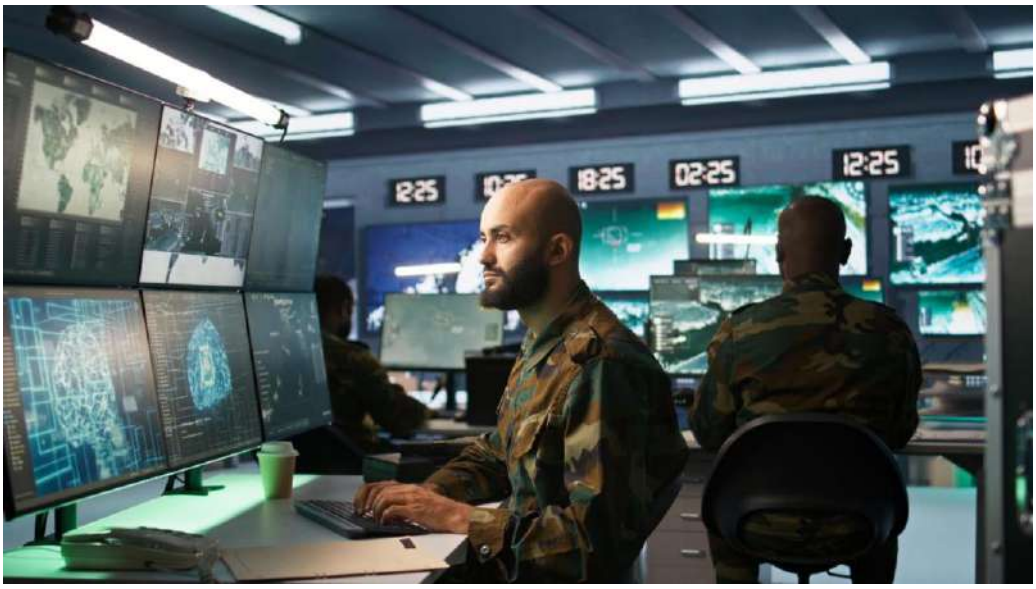
Hipoteza H3, da sodobne grožnje, predvsem brezpilotni sistemi, zahtevajo uvedbo večplastnih in tehnološko naprednih zaščitnih ukrepov, je bila prav tako **potrjena**. Razvoj brezpilotnih sistemov, kibernetskih groženj in drugih sodobnih oblik ogrožanja zahteva uporabo naprednih sistemov zaznavanja, umetne inteligence, avtomatiziranega nadzora in integriranih rešitev za zaščito vojaških baz.

Na podlagi ugotovitev raziskave je mogoče zaključiti, da bodo prihodnji sistemi varovanja vojaških baz vse bolj temeljili na povezovanju različnih informacijskih in varnostnih sistemov v enotno operativno okolje. Uporaba umetne inteligence pri analizi podatkov, avtomatiziranih nadzornih sistemov, naprednih senzorjev in sistemov za zaznavanje ter nevtralizacijo brezpilotnih letalnikov bo predstavljala pomemben korak pri izboljšanju zaščite vojaških objektov. Poleg tehnološkega razvoja bo pomembno tudi nadaljnje usposabljanje varnostnega osebja, izvajanje skupnih vaj in stalno posodabljanje varnostnih postopkov glede na nove oblike ogrožanja.

Pomembno vlogo bo imelo tudi sodelovanje med državami članicami zveze NATO, saj sodobne varnostne grožnje pogosto presegajo nacionalne okvire. Izmenjava informacij, skupno načrtovanje zaščitnih ukrepov, standardizirani postopki in uporaba skupnih doktrin omogočajo učinkovitejše preprečevanje, zaznavanje in obvladovanje kriznih situacij. Prav mednarodno sodelovanje predstavlja eno izmed ključnih prednosti sistema kolektivne varnosti in pomembno prispeva k zaščiti vojaških baz ter varnosti zavezniških sil.

Diplomsko delo potrjuje, da sodobnega sistema varovanja vojaških baz ni mogoče zagotavljati zgolj s fizičnim varovanjem, temveč je nujno povezovanje organizacijskih postopkov, sodobnih tehnologij in usposobljenega osebja. Celovit, večplasten in prilagodljiv sistem varovanja predstavlja temelj učinkovite zaščite vojaških baz ter pomembno prispeva k ohranjanju operativne sposobnosti, zaščiti osebja, infrastrukture in vojaške opreme ter varnosti sil zveze NATO. Ugotovitve diplomskega dela lahko predstavljajo tudi izhodišče za nadaljnje raziskave na področju razvoja sistemov Force Protection, zaščite pred brezpilotnimi sistemi in uporabe umetne inteligence pri zagotavljanju varnosti vojaških objektov.

.



Slika 14: Prihodnost varovanja vojaških baz v okviru NATO

Vir: NATO / Defense Innovation

8 VIRI IN LITERATURA

Army, U. S. (2021). Base Defense Handbook. Washington D.C.: Department of the Army.

Committee, H. o. (26. Marec 2014). Afghanistan—Camp Bastion Attack.

Defense, U. S. (2013). Camp Bastion Attack Investigation Report. Washington D.C.: Department of Defense.

Defense, U. S. (2022). Base Defense Operations. Washington D.C.: Department of Defense.

Democracies, F. f. (16. junij 2025). U.S. Forces in the Middle East: Under Attack and Defending Israel.

JAVERNIK, I. (JUNIJ 2010). VAROVANJE VOJAŠKIH OBJEKTOV.

JINSA. (2025). Iran Projectile Tracker: Attacks Against U.S. Troops Resume.

MAŠALINA, N. K. (MAJ 2022). VAROVANJE VOJAŠNIC S PRIPADAJOČIMI OBJEKTI. LJUBLJANA.

Media, I. S. (junij. 23 2025). Drone attacks on Iraqi military bases.

Nato. (2021). NATO Force Protection Doctrine and Military Base Security.

Nato. (december 2022). NATO STANDARD AJP-01.

Nato. (2022). NATO Strategic Concept 2022. Madrid: North Atlantic Treaty Organization.

Nato. (21. October 2024). Allied Joint Doctrine for Force Protection (AJP-3.14), Edition B Version 1.

Nato. (2025). NATO Cooperative Cyber Defence Centre of Excellence.

Reuters. (23. junij 2025). Iran fires missiles at US base in Qatar, Trump calls for peace.