

СТРАТЕШКЕ ДИМЕНЗИЈЕ ОБЕЗБЕЂЕЊА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У ВОЈНИМ МРЕЖАМА У КОНТЕКСТУ САВРЕМЕНЕ ДОКТРИНЕ ОДБРАНЕ

Фјодор Тимеркан¹

Достављен: 19.6.2026.

Језик рада: Српски

Кориговано: 13.8.2026.

Тип рада: Прегледни рад

Прихваћен: 9.9.2026.

DOI број: 10.5937/vojdelo2603167T

Апстракт: Обезбеђивање информационе безбедности поста-
ло је критична компонента савремених војних способности
имајући у виду све већу зависност од умрежених система у области
командовања, контроле, комуникације и доношења одлука. Савре-
мене доктрине одбране све више препознају да војне мреже нису
само техничка инфраструктура већ и стратешка средства чији ин-
тегритет, расположивост и поверљивост непосредно утичу на опе-
ративну ефикасност и стратешку отпорност. У раду се разматрају
стратешке димензије обезбеђења информационе безбедности у
војним мрежама у контексту савремене доктрине одбране.

Истраживање анализира начин на који се питања информационе
безбедности интегришу у доктринарне оквире и процесе стратеш-
ког планирања, са посебним нагласком на њихову улогу у подршци
командовању и контроли, очувању надмоћи у одлучивању и јачању
отпорности на сајбер и хибридне претње. Применом концептуалног
и аналитичког приступа, у раду се указује на однос између обез-
беђења информационе безбедности, војне стратегије и политике
одбране, а не искључиво на техничке механизме заштите. Посебна
пажња посвећена је импликацијама пропуста у области информа-
ционе безбедности по оперативни континуитет и стратешку стабил-
ност у савременим конфликтним окружењима.

Анализа показује да делотворно осигурање информационе без-
бедности захтева свеобухватан приступ који обједињује техничке
мере са организационим, доктринарним и стратешким елементима.
У раду се заступа становиште да је интеграција обезбеђења инфор-
мационе безбедности у доктрину одбране од суштинског значаја за

¹ Војна академија Оружаних снага „Александру чел Бун”, Кишињев, Република Молдавија,
e-mail: timercantudor@yahoo.com, <https://orcid.org/0009-0001-6769-3556>

очување оперативног кредибилитета и обезбеђивање ефикасне употребе војних мрежа у савременом и будућем безбедносном окружењу.

Кључне речи: *обезбеђивање информационе безбедности, војне мреже, доктрина одбране, војна стратегија, сајбер и хибридне претње*

Увод

Савремено безбедносно окружење карактеришу трајно надметање, убрзана технолошка трансформација и постепено нестајање традиционалне разлике између рата и мира. Војне организације делују у оквиру континуума стратешког супарништва, у којем кинетичко ангажовање представља само једну од манифестација конфронтације. У таквом развојном окружењу информација је постала одлучујући елемент пројекције моћи и оперативне ефикасности.

Сајбер простор је данас формално признат као оперативни домен, заједно са копном, ваздушним простором, поморским простором и свемиром (NATO, 2020). Ово признање одражава више од концептуалне модернизације; оно потврђује структурну зависност савремених оружаних снага од дигиталне инфраструктуре. Војне мреже подржавају функције командовања и контроле, обједињавање обавештајних података, процесе циљања, координацију логистике и мултинационалну интероперабилност. Њихов интегритет непосредно утиче на оперативни темпо, тачност доношења одлука и преживљавање снага.

Савремена доктрина одбране све више наглашава мултидоменске операције, интеграцију здружених способности и убрзане циклусе одлучивања (U.S. Department of the Army, 2022). Ови развојни процеси додатно повећавају ослањање на безбедне и отпорне информационе системе. Мрежноцентрични приступи, иако унапређују ситуациону свест и координацију, истовремено проширују површину напада доступну противницима (Alberts & Garstka, 1998). Државни и недржавни актери искоришћавају рањивости путем напредних упорних претњи, манипулације ланцима снабдевања, сајбер шпијунаже, интеграције електронског ратовања и хибридних операција утицаја. У таквим условима обезбеђивање информационе безбедности превазилази оквири техничке администрације и постаје питање стратешке отпорности.

Војне мреже више нису изолована инфраструктура заштићена статичним периметарским одбранама. Оне представљају динамичне, дистрибуиране и међусобно повезане екосистеме. Коалиционе операције, мултинационалне команде и оквири интероперабилности захтевају размену података између различитих безбедносних архитектура и регулаторних окружења. Ова међусобна повезаност унапређује оперативне способности, али истовремено уводи системске рањивости. Стратешко обезбеђење зато мора да успостави равнотежу између отворености неопходне за сарадњу и контролисаног приступа неопходног за заштиту.

Прелазак са реактивне сајбер безбедности на безбедносну архитектуру засновану на отпорности одражава доктринарно прилагођавање адаптивним противницима. Апсолутна заштита је недостижна у оспораваном сајбер простору. Стратешка предност лежи у способности откривања, ограничавања, опоравка и прилагођавања, уз истовремено очување оперативног континуитета. Концепти као што су слојевита одбрана, архитектура нултог поверења, инжењеринг заснован на принципу безбедности од самог пројектовања и континуирано праћење све више се уграђују у војно планирање. Они не представљају техничке преференције, већ стратешке нужности (U.S. Department of Defense, 2023).

Интеграција вештачке интелигенције, аутономних система и инфраструктуре засноване на облаку додатно усложњава безбедносно окружење. Алгоритми за подршку одлучивању, платформе за фузију сензорских података и предиктивна аналитика зависе од интегритета података и поузданости софтвера. Компромитовање на нивоу података или алгоритама може искривити оперативну свест и стратешко расуђивање. Зато обезбеђење информационе безбедности мора да обухвати заштиту порекла података, валидацију алгоритама и безбедно управљање животним циклусом дигиталних способности (European Commission, 2020).

Компромитовање мреже носи стратешке последице које превазилазе непосредни оперативни поремећај. Безбедносни пробоји подривају кредибилитет одвраћања, излажу рањивости структуре снага и могу изменити противничке процене. У савременом окружењу перцепција сајбер слабости може бити стратешки штетна у истој мери као и деградација физичке силе. Обезбеђење информационе безбедности, сходно томе, непосредно доприноси националној отпорности и стратешком сигнализирању.

Ефикасна примена захтева усклађеност доктрине, политике, организационе структуре и оперативне културе. Сајбер безбедност не може остати ограничена на специјализоване техничке јединице. Она мора бити интегрисана у командну одговорност, процесе планирања и режиме обуке. Дисциплина у дигиталним праксама, свест на нивоу руководства и институционализована безбедносна култура представљају суштинске компоненте стратешког обезбеђења.

У ери обележеној убрзаним протоком информација и сажетим циклусима одлучивања, заштита војних мрежа неодвојива је од очувања борбене моћи. Дигитална инфраструктура представља и рањивост и стратешко средство. Обезбеђивање њене отпорности више није помоћна функција; оно је темељни захтев савремене доктрине одбране.

Стратешко позиционирање информационе безбедности у оквиру савремене доктрине одбране

Савремено безбедносно окружење одређено је трајним стратешким надметањем, убрзаном технолошком трансформацијом и нарушавањем јасних граница између мира и сукоба. У таквом оквиру војна ефикасност не зависи само од кинетичких способности већ и од интегритета дигиталне инфраструктуре која подржава командни ауторитет и оперативну координацију. Обезбеђење информационе безбедности стога се позиционира као саставни део доктрине одбране, а не као споредна техничка функција.

Формално признавање сајбер простора као оперативног домена мења начин на који се рањивост и заштита концептуализују у војном планирању. Савезничка доктрина утврђује да су комуникационо-информациони системи (*Communication and Information Systems – CIS*) средства од критичног значаја за извршење мисије, чија је заштита неопходна за очување оперативног континуитета на стратешком, оперативном и тактичком нивоу. Информационо обезбеђење, дефинисано кроз заштиту расположивости, интегритета и поверљивости информација и информационих система, непосредно условљава ефикасност процеса командовања и контроле.

Оперативна доктрина додатно наглашава да савремене здружене операције зависе од синхронизованих ефеката у копненом, поморском, ваздушном, свемирском и сајбер домену. Ова интеграција омогућава се посредством међусобно повезаних дигиталних мрежа које обједињују улазне податке са сензора, обавештајне производе, податке о циљевима и логистичке информације у јединствена окружења за доношење одлука. Свако нарушавање ових система производи каскадне оперативне последице: успоравање циклуса одлучивања, искривљену ситуациону свест и смањену синхронизацију снага (NATO Standardization Office, 2025).

Структурна централност војних мрежа концептуално је приказана архитектуром Информационе мреже Министарства одбране Сједињених Америчких Држава (*Department of Defense Information Network – DoDIN*), раније познате као Глобална информациона мрежа (*Global Information Grid*). Овај модел одражава међусобно повезану дигиталну окосницу која подржава здружене и комбиноване операције.

На Слици 1 приказана је интеграција оперативних домена посредством заједничке дигиталне инфраструктуре. Она истиче критичну доктринарну реалност – оперативна ефикасност неодвојива је од поузданости мреже. Иста повезаност која омогућава брзу координацију истовремено проширује површину напада доступну противницима. У таквим условима механизми обезбеђења постају стратешки омогућавајући фактори континуитета мисије.



Слика 1: Шематски приказ Глобалне информационе мреже. Глобална информациона мрежа (GIG) обухвата сваки систем, опрему, софтвер или услугу Министарства одбране САД који преносе, чувају или обрађују информације Министарства одбране САД, као и све друге повезане услуге неопходне за постизање информационе надмоћи

Извор: National Institute of Standards and Technology (NIST, 2007)

Концептуални темељи мрежноцентричног ратовања додатно потврђују ову зависност. Заједничка ситуациона свест и дистрибуиране архитектуре одлучивања повећавају оперативну агилност, али истовремено појачавају системску рањивост уколико се не може гарантовати интегритет података. У дигитално међусобно повезаним структурама снага, компромитовање информација непосредно се претвара у оперативну деградацију (Alberts & Garstka, 1998).

Стратешки позиционирано обезбеђење информационе безбедности због тога испуњава три основне функције:

- Ø прво, одржава надмоћ у одлучивању заштитом интегритета токова података у оквиру сажетих оперативних временских рокова;
- Ø друго, ублажава системску рањивост насталу услед мрежне међузависности и мултинационалне интероперабилности;

Ø треће, јача кредибилитет одвраћања смањивањем подстицаја противника да искористе уочене сајбер слабости.

У савременој доктрини одбране обезбеђење информационе безбедности представља заштитни слој дигиталног нервног система војске. Његова робусност одржава оперативну кохерентност, институционални кредибилитет и стратешку стабилност. Његов неуспех производи ефекте упоредиве са поремећајима у традиционалним доменима ратовања.

Поред оперативне зависности, стратешко позиционирање обезбеђења информационе безбедности мора се разумети и кроз призму процене ризика на нивоу националне одбране. Војни доносиоци одлука све више процењују сајбер ризик не само у техничком смислу већ и у односу на обезбеђење мисије. Обезбеђење мисије односи се на способност одбрамбених институција да наставе са извршавањем суштинских функција у неповољним условима (U.S. Department of Defense, 2016). У овом оквиру безбедне мреже третирају се као критични омогућавајући фактори остваривања циљева националне одбране. Поремећај који погађа стратешке командне мреже, центре за обједињавање обавештајних података или системе за управљање логистиком има импликације које превазилазе тактичку непријатност; он утиче на кредибилитет пројекције снага и поузданост савезништва.

Друга димензија односи се на интероперабилност у мултинационалним окружењима. Савремене операције ретко се одвијају изоловано. Здружене наменске снаге, командне структуре НАТО-а и коалиционо распоређивање захтевају безбедну размену података између хетерогених система. То уводи структурну напетост између оперативне отворености и безбедносне контроле. Прекомерна подела информација на затворене целине подрива сарадњу, док прекомерна повезаност повећава изложеност. Обезбеђење информационе безбедности услед тога има улогу као механизам уравнотежавања између интеграције и заштите. Доктрина све више разматра овај изазов кроз стандардизоване безбедносне протоколе, федеративне системе управљања идентитетом и слојевите контроле приступа (NATO, 2023).

Стратешко позиционирање додатно је ојачано улогом сајбер отпорности у положењу одвраћања. Традиционално одвраћање ослањало се на видљиве војне способности. У дигиталној ери сама отпорност постаје инструмент сигнализација. Противник који уочава ојачане мреже, способност брзог опоравка и робусне механизме реаговања на инциденте може преиспитати очекиване добити од сајбер упада. Насупрот томе, системске рањивости подстичу испитивање слабости и ескалацију. У том смислу обезбеђење информационе безбедности доприноси стратешкој стабилности обликујући противничке процене ризика.

Убрзање дигиталне трансформације у оквиру оружаних снага додатно појачава ово позиционирање. Миграција ка облаку, интеграција вештачке интелигенције и оперативни модели засновани на подацима повећавају ефикасност, али истовремено појачавају зависност. Програми модернизације одбране им-

плицитно проширују површину напада. Без доктринарно уграђених механизма обезбеђења, модернизација носи ризик стварања крхкости. Савремена доктрина одбране отуда све више у циклусе развоја способности уграђује принципе безбедности од самог пројектовања, обезбеђујући да заштита буде уграђена на нивоу архитектуре, а не додата тек након распоређивања (U.S. Department of Defense, 2023).

Узете заједно, ове димензије показују да је обезбеђење информационе безбедности тесно повезано са стратешком спремношћу, кохезијом савезништва и кредибилитетом одвраћања. Оно није додатак оперативној способности; оно успљева поузданост војне моћи у дигитално оспораваном окружењу.

Оперативна отпорност и мултидоменска интеграција војних мрежа

Оперативна отпорност представља функционални израз обезбеђења информационе безбедности у извођењу савремених војних операција. У савременој доктрини операције се све више схватају као мултидоменске, синхронизоване у копненом, ваздушном, поморском, свемирском и сајбер домену, што захтева континуирану размену података и интегрисане командне структуре (U.S. Department of the Army, 2022).

Мултидоменске операције (*multi-domain operations* – MDO) сажимају циклусе одлучивања и појачавају зависност од дигиталне инфраструктуре (NATO Cooperative Cyber Defence Centre of Excellence, 2020). Командовање и контрола (*command and control* – C2), обједињавање обавештајних података, координација циљања и логистичка подршка ослањају се на непрекинуте токове података између дистрибуираних јединица и виших ешалона командовања. Приручници који се баве операцијама у оспораваним окружењима наглашавају значај одржавања оперативног темпа у условима поремећаја и противничког ометања. У таквим условима отпорност постаје одлучујуће својство војних мрежа.

Отпорност се разликује од традиционалне одбрамбене безбедности. Класична заштита заснована на периметру полазила је од претпоставке о препознатљивим границама и епизодичним претњама. Савремена окружења претњи су трајна, адаптивна и хибридна. Противници интегришу сајбер упаде, електронско ратовање и информационе операције како би деградирали поузданост мреже и створили когнитивно трење унутар командних система. Оперативна доктрина признаје да снаге морају очекивати деградиране комуникације и оспоравана информационе окружења као уобичајено стање ратовања, а не као изузетак (U.S. Department of Defense, 2018).

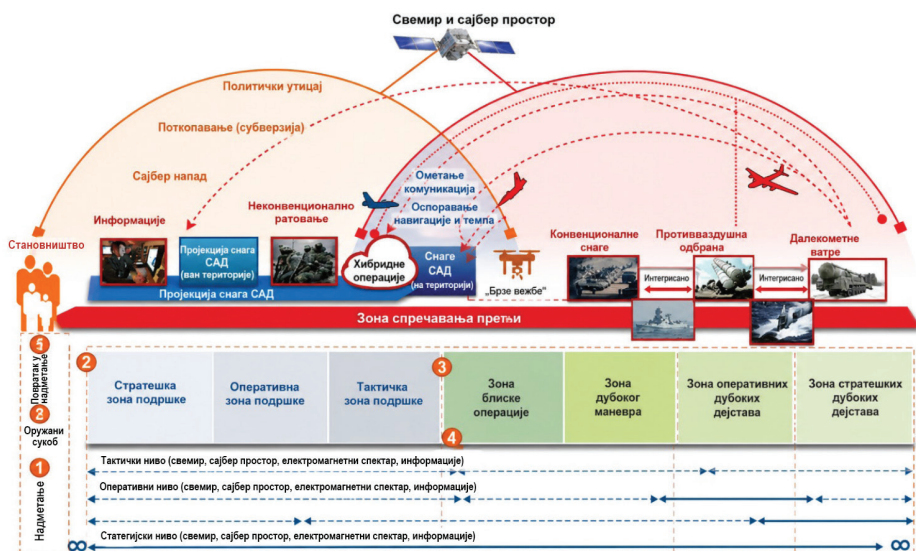
У овом оквиру, оперативна отпорност војних мрежа почива на четири структурна принципа:

- Ø редундантност – обезбеђивање алтернативних комуникационих путева и дистрибуираних архитектура;
- Ø сегментација – ограничавање латералног кретања унутар компромитованих система;
- Ø континуирано праћење – откривање аномалија у реалном времену;
- Ø способност брзог опоравка – обнављање функција од критичног значаја за мисију без стратешког одлагања.

Ови механизми подржавају оно што доктрина означава као континуитет мисије у оспораваним доменима.

Интеграција сајбер способности у оперативнo планирање додатно учвршћује овај приступ. Концепти мултидоменске битке изричито препознају операције у сајбер простору као средство обликовања и подршке маневру у другим доменима. Ова међузависност подразумева да отказ мреже у сајбер слоју производи таласне ефекте у кинетичким доменима. Компромитована веза за пренос података може пореметити циклусе циљања; деградиране сателитске комуникације могу утицати на навигацију и синхронизацију; манипулисани обавештајни токови могу искривити оперативну процену.

Архитектура отпорних војних мрежа може се концептуализовати као слојеви-та одбрана усклађена са оперативним функцијама.



Слика 2: Слојевити модел оперативне отпорности у мултидоменским војним мрежама (<https://capssindia.org/americas-multi-domain-operations-at-250-a-strategy-concept-or-mirage/>).

Овај слојевити модел одражава доктринарну реалност: отпорност је кумулативна. Отказ на нижим слојевима преноси се навише, утичући на оперативне и стратешке исходе. Насупрот томе, робусна заштита на темељним слојевима стабилизује функције мисије на вишим нивоима.

Додатна димензија односи се на коалиционе операције. НАТО и партнерске снаге делују у оквиру федеративних мрежних архитектура које морају да успоставе равнотежу између интероперабилности и суверенитета (NATO, 2023). Оквири федеративног умрежавања мисија захтевају заједничке стандарде, уз истовремено очување националне контроле над осетљивим подацима. Ова структурна сложеност повећава значај стандардизованих процедура сајбер одбране и координисаних механизма реаговања на инциденте.

Оперативна отпорност зависи и од обуке и процедуралне дисциплине. Доктрина на терену наглашава да јединице морају бити способне да делују у условима деградираних комуникација и делимичног отказа система. Вежбе све чешће симулирају сценарије сајбер-електромагнетног ометања ради провере процедура опоравка и командне прилагодљивости. Отпорност, због тога, није само технолошка већ и процедурална и когнитивна (U.S. Department of the Army, 2022).

У савременим мултидоменским операцијама безбедне мреже нису пасивни омогућавајући фактори. Оне представљају простор маневра. Њихова заштита захтева синхронизацију између јединица за сајбер одбрану, оперативних команданата и стратешког руководства. Обезбеђење војних мрежа постаје предуслов за одржавање оперативне иницијативе у оспораваним окружењима.

Поред структурне редундантности и слојевите заштите, оперативна отпорност мора се анализирати и у односу на сајбер-електромагнетни спектар. Савремена доктрина све више третира сајбер простор и електромагнетни спектар као интегрисано бојиште. Електронско ратовање, ускраћивање приступа спектру, ометање сигнала и сајбер упади делују координисано ради нарушавања снага зависних од мрежа. У таквом окружењу војне мреже морају бити пројектоване тако да функционишу у условима смањеног пропусног опсега, повремене повезаности и оспоравања спектра. Отпорност стога подразумева адаптивне комуникационе путеве, агилност у коришћењу спектра и децентрализоване командне способности које могу функционисати у условима делимичне изолације (U.S. Department of Defense, 2018).

Још једна критична димензија односи се на интегритет података у оперативним окружењима подржаним вештачком интелигенцијом. Мултидоменске операције ослањају се на фузију сензорских података, аутоматизоване системе подршке циљању и предиктивну аналитику. Ови системи зависе од поузданих скупова података. Манипулација улазним подацима, било путем сајбер упада, лажирања сигнала или алгоритамског тровања, може произвести искривљене оперативне излазе без непосредног онеспособљавања мрежне инфраструктуре. То представља рањивост вишег реда. Стратегије дигиталне модернизације

одбране све више препознају потребу за обезбеђивањем порекла података, процеса валидације модела и софтверских ланаца снабдевања као интегралних компоненти оперативног обезбеђења (European Commission, 2020).

Оперативна отпорност мора бити уграђена и у методологије планирања. Са-временно оперативно пројектовање укључује матрице процене ризика којима се вреднују рањивости у различитим доменима (U.S. Department of the Army, 2022). Међутим, процена сајбер ризика разликује се од традиционалне процене кинетичких претњи. Сајбер претње могу остати латентне све до активирања, а њихов оперативни утицај може се развијати нелинеарно. То захтева динамичко моде-лирање ризика и континуирану процену рањивости уграђену у циклусе операти-вног планирања.

Управљање, одвраћање и технолошки суверенитет у војном информационом обезбеђењу

Стратешко обезбеђење информационе безбедности превазилази оперативну отпорност и техничку архитектуру. На највишем нивоу оно је обликовано структу-рама управљања, положајем одвраћања и степеном технолошког суверенитета који држава задржава. Војне мреже функционишу у оквиру националних правних оквира, савезничких обавеза, индустријских зависности и механизма политич-ког надзора. Њихова заштита отуда постаје питање стратешког управљања, а не искључиво оперативног руковођења.

Ефикасно управљање почиње јасноћом надлежности. Одговорности у об-ласти сајбер одбране морају бити разграничене између стратешких командних нивоа, оперативних штабова и специјализованих сајбер јединица. Здружена доктрина наглашава јединство командовања и синхронизоване ефекте у разли-читим доменима (NATO Standardization Office, n.d.). У сајбер домену фрагмен-тација одговорности ствара пукотине које противник може искористити. Сходно томе, одбрамбене институције све више централизују сајбер надзор, уз очување децентрализованог оперативног извршења.

Кохерентност политике подједнако је критична. Стандарди информацио-не безбедности, прописи о набавкама, протоколи класификације и механизми пријављивања инцидената морају функционисати у оквиру јединственог доктри-нарног усмерења. НАТО оквири наглашавају значај усклађених безбедносних стандарда у савезничким мрежама ради очувања интероперабилности без угро-жавања националне контроле. Управљање због тога представља везивно ткиво које повезује савезничку интеграцију и суверену власт (NATO, 2023).

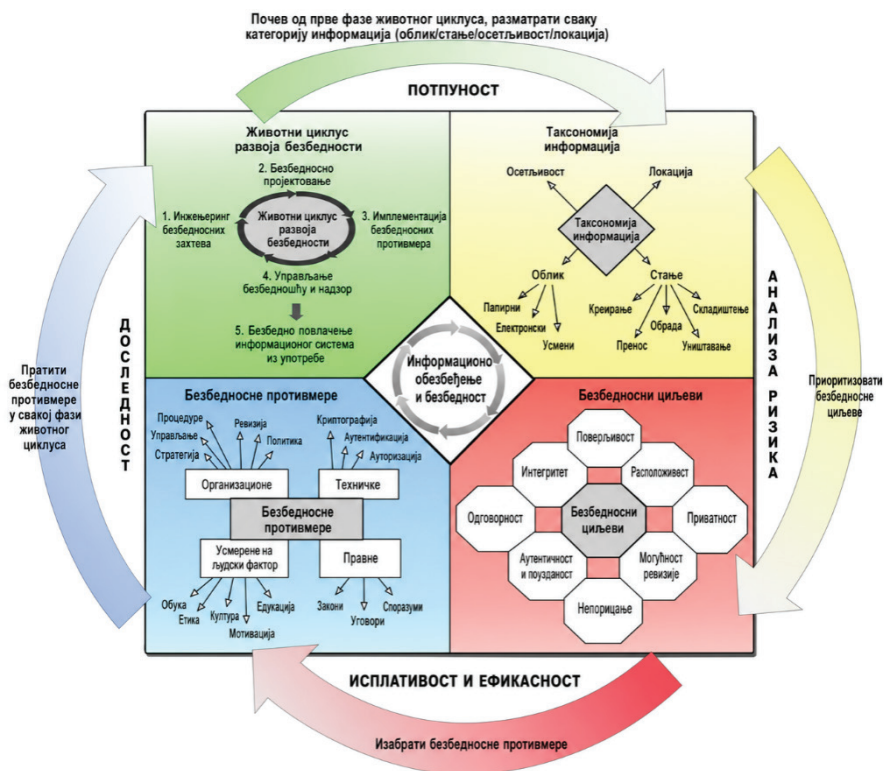
Одвраћање у дигиталном домену уводи додатну сложеност. Класично од-враћање ослањало се на видљиве способности и јасно приписиве последице.

Сајбер простор усложњава атрибуцију и пропорционалан одговор. Ипак, стратешки документи све више препознају отпорност и способност реаговања као компоненте положаја одвраћања. Противник који процењује вредност сајбер упада мора узети у обзир не само потенцијалне добити већ и брзину опоравка браниоца, способност узвратног деловања и механизме савезничке подршке (NATO, 2020).

Осигуравање информационе безбедности стога доприноси одвраћању на два комплементарна начина. Прво, смањењем рањивости оно умањује очекивану ефикасност противничких операција. Друго, демонстрирањем координисаног управљања и спремности, оно сигнализира припремљеност. Стратешка комуникација у вези са сајбер способностима све више постаје део националних одбрамбених наратива. Ова димензија сигнализирања утиче на противничке процене ризика чак и у одсуству кинетичке ескалације.

Технолошки суверенитет представља још један одлучујући фактор. Војне мреже зависе од хардверских компоненти, софтверских платформи, инфраструктуре у облаку и ланаца снабдевања који могу излазити изван националне јурисдикције. Прекомерно ослањање на спољне добављаче уводи стратешки ризик. Рањивости ланца снабдевања, уграђена „задња врата“ и непрозирност животног циклуса софтвера могу да подривају дугорочно обезбеђење. Због тога агенде модернизације одбране наглашавају безбедне ланце снабдевања, поуздане добављаче и развој домаћих способности (U.S. Department of Defense, 2023).

Суверенитет не подразумева изолацију. Мултинационалне операције захтевају интероперабилне системе. Стратешки изазов лежи у успостављању равнотеже између међузависности и аутономије. Федеративни мрежни модели и архитектуре нултог поверења нуде делимична решења, омогућавајући сарадњу без безусловног поверења. Међутим, механизми управљања морају обезбедити да националне информације од критичног значаја остану заштићене у оквиру савезничких структура.



Слика 3: Стратешки оквир обезбеђења информационе безбедности
(https://link.springer.com/chapter/10.1007/978-3-030-64351-5_9)

Стратешка димензија односи се на правне и нормативне структуре. Сајбер операције укрштају се са међународним правом, правилима ангажовања и савезничким обавезама. Механизми управљања морају дефинисати прагове за реаговање, процедуре атрибуције и протоколе координације са цивилним властима. Замагљивање граница између цивилне и војне инфраструктуре у сајбер простору захтева интегрисане механизме цивилно-војне координације. Националне стратегије сајбер безбедности све више одражавају овај интегрисани приступ.

Узети заједно, управљање, одвраћање и технолошки суверенитет одређују стратешко окружење у којем функционише оперативна отпорност. Без кохерентног управљања, отпорност постаје фрагментисана. Без кредибилног одвраћања, отпорност остаје реактивна. Без технолошког суверенитета, отпорност постаје споља зависна (Schmitt, 2017).

У савременом безбедносном окружењу војно информационо обезбеђење због тога није само техничка дисциплина већ стратешки инструмент. Оно подржава оперативни континуитет, јача кохезију савезништва и обликује противничке процене. Његова стратешка вредност не лежи само у спречавању поремећаја већ и у очувању слободе деловања у оспораваном дигиталном бојишту.

Закључак

Савремено одбрамбено окружење потврђује да је војна моћ неодвојива од отпорности њене дигиталне архитектуре. Обезбеђење информационе безбедности превазишло је оквири техничке заштите и данас представља структурни предуслов оперативне кохерентности и стратешког кредибилитета. Савремене оружане снаге не користе мреже само као средство; оне посредством њих функционишу. Командовање, обједињавање обавештајних података, логистичко обезбеђење и синхронизација здружених ватрених дејстава зависе од интегритета токова података у оспораваним доменима (NATO, 2020; U.S. Department of Defense, 2023).

Анализа показује да се обезбеђење информационе безбедности остварује у три међусобно зависне димензије. Прво, оно је доктринарно утемељено у признавању сајбер-простора као оперативног домена и у развоју вишедоменских операција. Друго, на оперативном нивоу испољава се кроз механизме отпорности чија је сврха очување континуитета извршења мисије у условима сајбер-електромагнетног супротстављања. Треће, на стратешком нивоу њиме се управља посредством институционалних овлашћења, положаја у систему одвраћања и технолошког суверенитета.

Оперативна отпорност издваја се као одлучујућа карактеристика савремених војних мрежа. Апсолутна заштита није ни остварива нити је доктринарно реалистична. Циљ је очување континуитета функционисања под притиском, односно одржавање способности командовања упркос покушајима ометања. Редундантност, сегментација, децентрализовано извршавање и механизми брзог опоравка нису технички луксуз, већ оперативна нужност у окружењима у којима се деградација способности очекује, а не представља изузетак.

На стратешком нивоу, кохерентност управљања одређује да ли ће се отпорност преточити у кредибилан одбрамбени положај. Јасно дефинисана одговорност у командовању, усклађени стандарди, безбедне праксе набавке и координација у оквиру савеза обезбеђују да се заштита и поузданост мрежа не фрагментишу дуж институционалних граница. Истовремено, видљива отпорност доприноси одвраћању тако што утиче на процену ризика потенцијалног противника. Снага способна да апсорбује последице сајбер-агресије и да се од њих опорави умањује перципирану корисност такве агресије.

Технолошки суверенитет додатно условљава дугорочно обезбеђење. Зависност од рањивих ланаца снабдевања или нетранспарентних дигиталних екосис-

тема уводи структурне ризике. Стратешка аутономија у критичним дигиталним способностима јача националну отпорност, уз истовремено очување интероперабилности у оквиру савеза. Равнотежа између интеграције и суверенитета представља једну од кључних противречности савремене одбрамбене политике.

У безбедносном окружењу које карактеришу трајно надметање и брзе технолошке промене, обезбеђење информационе безбедности мора се посматрати као трајна стратешка функција. Оно подржава оперативну ефикасност, јача кохезију савеза и чува слободу деловања у оспораваном дигиталном борбеном простору. Заштита војних мрежа више није помоћни задатак; она представља темељни предуслов кредибилне одбране у двадесет првом веку.

Стратешке димензије изложене у овом раду потврђују ширу доктринарну трансформацију: дигитална отпорност сада представља саставни део борбене моћи. Тамо где су токови информација безбедни и отпорни, могуће је задржати оперативну иницијативу. Тамо где су они рањиви, стратешки положај слаби. У савременом ратовању, одбрана мрежа неодвојива је од одбране државе.

Литература

[1] Alberts, D. S., & Garstka, J. J. (1998). Network centric warfare: Developing and leveraging information superiority. CCRP Publication Series. https://www.dodccrp.org/files/Alberts_NCW.pdf

[2] European Commission. (2020). EU cybersecurity strategy for the digital decade. <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy-digital-decade>

[3] NATO. (2020). NATO 2030: United for a new era. <https://www.nato.int/nato2030/>

[4] NATO. (2023). Comprehensive cyber defence policy. https://www.nato.int/cps/en/natohq/topics_78170.htm

[5] NATO Cooperative Cyber Defence Centre of Excellence. (2020). Cyber threats and NATO 2030: Horizon scanning and analysis. <https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030/>

[6] NATO Standardization Office. (2022). Allied Joint Doctrine (AJP-01), Edition F, Version 1. North Atlantic Treaty Organization. https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP_01_EdF_with_UK_elements.pdf

[7] NATO Standardization Office. (2025). Allied Joint Doctrine for the Conduct of Operations (AJP-3), Edition D, Version 1. North Atlantic Treaty Organization. https://assets.publishing.service.gov.uk/media/6964e72799fbd498faecce2/AJP_3_Ed_D_V1-O.pdf

[8] NATO Standardization Office. (2020). Allied joint doctrine for cyberspace operations (AJP-3.20). https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[9] NATO Standardization Office. (2024). Allied Joint Doctrine for Communication and Information Systems (AJP-6), Edition B, Version 1. North Atlantic Treaty Organization. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

[10] National Institute of Standards and Technology. (2007). Global Information Grid (GIG). Computer Security Resource Center Glossary https://csrc.nist.gov/glossary/term/global_information_grid

[11] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. <https://doi.org/10.1017/9781316822524>

[12] Sellitto, G. P., Aranha, H., Masi, M., & Pavleska, T. (2020). Security and safety by design in the Internet of Actors: An architectural approach. In M. Freitag, A. Kinra, H. Kotzab, H.-J. Kreowski, & K.-D. Thoben (Eds.), Subject-Oriented Business Process Management. The Digital Workplace – Nucleus of Transformation (Communications in Computer and Information Science, Vol. 1278, pp. 133–142). Springer, Cham. https://doi.org/10.1007/978-3-030-64351-5_9

[13] Singh, K. (2025). America's multi-domain operations at 250: A strategy, concept or mirage? Centre for Aerospace Power and Strategic Studies (CAPSS). <https://capssindia.org/americas-multi-domain-operations-at-250-a-strategy-concept-or-mirage/>

[14] U.S. Department of Defense. (2018). Joint publication (JP) 3-12: Cyberspace operations. Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[15] U.S. Department of Defense. (2023). 2023 Department of Defense cyber strategy. <https://media.defense.gov/2023/Aug/25/2003288669/-1/-1/1/2023-DOD-CYBER-STRATEGY.PDF>

[16] U.S. Department of Defense. (2016). DoD directive 3020.40: Mission assurance. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf>

[17] U.S. Department of the Army. (2022). Field manual (FM) 3-0: Operations. https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1024908

Резиме

Обезбеђивање информационе безбедности постало је критична компонента савремених војних способности имајући у виду све већу зависност од умрежених система у области командовања, контроле, комуникације и доношења одлука. Савремене доктрине одбране све више препознају да војне мреже нису само техничка инфраструктура већ и стратешка средства чији интегритет, расположивост и поверљивост непосредно утичу на оперативну ефикасност и стратешку отпорност. У раду се разматрају стратешке димензије обезбеђења информационе безбедности у војним мрежама у контексту савремене доктрине одбране.

Истраживање анализира начин на који се питања информационе безбедности integriшу у доктринарне оквире и процесе стратешког планирања, са посебним нагласком на њихову улогу у подршци командовању и контроли, очувању надмоћи у одлучивању и јачању отпорности на сајбер и хибридне претње. При-

меном концептуалног и аналитичког приступа, у раду се указује на однос између обезбеђења информационе безбедности, војне стратегије и политике одбране, а не искључиво на техничке механизме заштите. Посебна пажња посвећена је импликацијама пропуста у области информационе безбедности по оперативни континуитет и стратешку стабилност у савременим конфликтним окружењима.

Анализа показује да делотворно осигурање информационе безбедности захтева свеобухватан приступ који обједињује техничке мере са организационим, доктринарним и стратешким елементима. У раду се заступа становиште да је интеграција обезбеђења информационе безбедности у доктрину одбране од суштинског значаја за очување оперативног кредибилитета и обезбеђивање ефикасне употребе војних мрежа у савременом и будућем безбедносном окружењу.

Кључне речи: *обезбеђивање информационе безбедности, војне мреже, доктрина одбране, војна стратегија, сајбер и хибридне претње*

© 2026 Аутор. Објавило *Војно дело* (<http://www.vojnodelo.mod.gov.rs>). Ово је чланак отвореног приступа и дистрибуира се у складу са лиценцом Creative Commons (<http://creativecommons.org/licenses/by/4.0/>).

