

УДК:
351.86
327.84
343.53:004.738.
Оригинални научни рад
ДОИ: 10.5937/DB2601033L

Дипломатија и безбедност
Година 9.
Број 1/2026.
Стр. 33-54.

Бориша Лечић¹
Никола Трајковић²

СТРУКТУРАЛНИ И ФУНКЦИОНАЛНИ АСПЕКТИ ОБАВЕШТАЈНО-БЕЗБЕДНОСНИХ СИСТЕМА У ФУНКЦИЈИ КОЛЕКТИВНЕ БЕЗБЕДНОСТИ

Сажетак

Међународна безбедносна динамика 21. века одликује се наглашеном међузависношћу и појавом претњи, које надилазе капацитете појединачних држава. У таквим условима, колективна безбедност постаје важан механизам за очување стабилности и предвидљивости међународног поретка, док обавештајно-безбедносни системи представљају њен оперативни темељ. Циљ рада је анализа институционалне структуре и функционалних карактеристика ових система у оквиру три најзначајнија модела колективне безбедности: НАТО-а, Европске уније и Организације за уговор о колективној безбедности (ОДКБ). Посебна пажња је посвећена механизмима координације, размене информација и заједничког реаговања на савремене изазове, као што су тероризам, хибридне претње, сајбер-напади и дезинформационе кампање. Анализа показује да ефикасност колективних обавештајно-безбедносних система зависи пре свега од степена институционалне интеграције, техничке интероперабилности и политичког поверења међу државама чланицама. Закључује се да ће њихов будући развој зависити од способности међународних организација да ускладе националне интересе са заједничким безбедносним циљевима, те да ојачају механизме предиктивне и превентивне безбедности у дигиталном окружењу.

Кључне речи: *колективна безбедност, обавештајно-безбедносни системи, предиктивна безбедност, хибридне претње, сајбер безбедност*

¹ Факултет за правне и пословне студије „Др Лазар Вркатић”, Нови Сад, Србија, borisalecic@gmail.com

² Факултет за правне и пословне студије „Др Лазар Вркатић”, Нови Сад, Србија, ntrajkovickk93@gmail.com

УВОД

У последњим деценијама, глобални безбедносни поредак пролази кроз дубоке промене, које прате технолошка, политичка и друштвена превирања. Међудржавни конфликти све чешће добијају неконвенционалне форме, а границе између унутрашње и спољне безбедности постају све мање видљиве. Тероризам, хибридно ратовање, сајбер-претње и дезинформационе операције постали су саставни део савремених безбедносних изазова. У таквим условима, традиционални модели националне безбедности више не могу обезбедити поуздану заштиту, што доводи до развоја наднационалних механизма сарадње, заснованих на концепту колективне безбедности (Baullis, Smith & Owens, 2019). Управо у таквим околностима, улога обавештајно-безбедносних система добија суштински значај, јер од квалитета и брзине обраде информација зависи делотворност заједничког реаговања држава чланица (Jovanović, 2020).

Предмет овог истраживања јесте анализа структуре и функционалних карактеристика обавештајно-безбедносних система у оквиру колективне безбедности, са посебним освртом на три кључна модела: Северноатлантски савез (НАТО), Европску унију (ЕУ) и Организацију за уговор о колективној безбедности (ОДКБ). Циљ рада је да се утврди на који начин институционални оквир, политички односи и техничко-оперативни капацитети ових система утичу на њихову ефикасност у суочавању са савременим безбедносним изазовима, попут тероризма, хибридних претњи, сајбер-напада и ширења дезинформација.

Теоријско и практично значење ове теме се огледа у потреби да се боље разумеју механизми функционисања савремених обавештајних структура, које све више прелазе границе националних суверенитета и постају део наднационалних система колективног одлучивања. Разумевање њихових структурних и функционалних димензија доприноси унапређењу институционалне сарадње, формирању поузданих канала размене информација и јачању укупне отпорности међународних организација на безбедносне кризе.

Основна истраживачка хипотеза гласи да ефикасност обавештајно-безбедносних система колективне безбедности зависи пре свега од степена институционалне интеграције и политичког поверења између држава чланица. У циљу њене прецизније анализе, појам „степен институционалне интеграције” се у овом раду операционализује кроз више индикатора:

- нивое формалне институционалне централизације;
- степене правне усклађености и стандардизације процедура;
- обим и интензитет размене обавештајних података;
- нивое техничке интероперабилности система.

Помоћне хипотезе полазе од претпоставке да централизовани модели организације омогућавају брже и координираније реаговање на безбедносне претње, док правна усклађеност и политичка воља држава чланица представљају најбитније предуслове за делотворну обавештајну сарадњу.

У циљу емпиријске проверљивости постављене хипотезе, основни теоријски појмови (степен интеграције и ниво политичког поверења) операционализују се кроз скуп квалитативних индикатора, који омогућавају њихову компаративну анализу у оквиру одабраних регионалних безбедносних организација. Степен интеграције се посматра кроз следеће показатеље: ниво институционалне централизације и присуство сталних наднационалних тела са аутономним одлучивачким капацитетом; степен стандардизације процедура планирања и доношења одлука; обим и дубина заједничких оперативних механизма; степен обавезности одлука за државе чланице. Политичко поверење се дефинише кроз индикаторе који укључују: брзину и конзистентност реакције држава чланица у кризним ситуацијама; степен политичких блокада или консензусних застоја у процесу одлучивања; ниво размене обавештајних и стратешких информација; стабилност политичких односа унутар организације у условима спољнополитичких дивергенција. На основу овако дефинисаних индикатора, омогућава се компаративна анализа НАТО-а, ЕУ и ОДКБ-а као три различита модела институционалне безбедносне сарадње, при чему се њихов учинак посматра кроз однос између институционалне дубине интеграције и степена политичког поверења међу чланицама.

У раду се примењују аналитичко-компаративна метода и метода анализе садржаја релевантних докумената и стратешких концепата, као што су: NATO Strategic Concept (2022), EU Security Strategy (2020) и Статут ОДКБ-а (CSTO, 2002). Поред тога, у циљу превазилажења искључивог дескриптивног приступа, анализа ће бити допуњена студијама случаја, које омогућавају емпиријску проверу изведених закључака, укључујући вишегодишње операције НАТО-а у Авганистану, мисије ЕУ у Малију и деловање ОДКБ-а током кризе у Казахстану 2022. године. На овај начин омогућава се конкретније сагледавање ефективности различитих модела колективне безбедности у реалним условима.

ТЕОРИЈСКО ОДРЕЂЕЊЕ ПОЈМА КОЛЕКТИВНЕ БЕЗБЕДНОСТИ И ОБАВЕШТАЈНО-БЕЗБЕДНОСНИХ СИСТЕМА

Концепт колективне безбедности представља један од темељних стубова савременог међународног поретка и правне регулативе у области мира и стабилности. У теоријском смислу, он подразумева систем у којем државе

пристају да заједнички делују против сваке претње миру, без обзира на њен извор, а полазећи од претпоставке да је напад на једну чланицу – напад на све. Овај принцип, који је први пут јасно артикулисан у оквиру Друштва на-рода након Првог светског рата, свој пуни израз добија у Повељи Уједињених нација (1945), посебно у њеном VII поглављу, где се дефинише колективни одговор на угрожавање међународног мира и безбедности.

У међународном праву, колективна безбедност означава институцио-нализовану форму сарадње, у којој државе преносе део својих суверених ов-лашћења на међународну организацију, у циљу заједничког деловања против претњи које нарушавају општи мир (*Zakon o potvrđivanju konvencije UN protiv transnacionalnog organizovanog kriminala i dopunskih protokola*, 2001). За раз-лику од система савеза или колективне одбране, који се заснивају на заједнич-ком одговору на спољног непријатеља (као што је случај са НАТО-ом), колективна безбедност има универзални карактер и начелно обухвата све државе чланице међународне заједнице (Kupchan & Kupchan, 1995). Међу-тим, у пракси, овај идеални модел колективне акције се трансформише у пар-цијалне, регионалне или војно-политичке облике сарадње (Jovanović, 2020).

Савремени системи колективне безбедности, попут УН, НАТО-а, ЕУ или ОДКБ-а, функционишу на основу комбинације правних норми, поли-тичких обавеза и оперативних механизма координације (Rozanov & Douhan, 2013). У том оквиру, обавештајно-безбедносни системи представљају еле-мент који омогућава правовремено доношење одлука, планирање превен-тивних мера и координисано реаговање на кризне ситуације. Без поуздане обавештајне инфраструктуре, концепт колективне безбедности остаје у до-мену декларативне политике, јер заједничко деловање подразумева дељење тачних, проверених и благовремених информација (Bajagić, 2013; Gill, 2016).

Теоријски оквир овог рада се стога заснива на комбинацији реали-стичког приступа и либералног институционализма, уз допунске елементе конструктивизма. Реалистички приступ полази од претпоставке да државе делују у анархичном међународном систему, вођене сопственим интересима и настојањем да очувају моћ и безбедност (Waltz, 1979; Mearsheimer, 2001). У том смислу, обавештајно-безбедносни системи представљају инструмент националне моћи, док је сарадња ограничена степеном поверења и покла-пања интереса. Са друге стране, либерални институционализам наглашава улогу међународних институција у смањењу неизвесности, повећању транс-парентности и олакшавању сарадње међу државама (Keohane, 2005; Keohane & Nye, 1977). Колективна безбедност се посматра као институционални ме-ханизам, који омогућава координацију, размену информација и заједничко деловање, док обавештајно-безбедносни системи представљају основни ин-

струмент те сарадње. Коначно, конструктивистички приступ доприноси разумевању улоге норми, идентитета и политичке културе у обликовању поверења међу државама чланицама, што је од посебног значаја за анализу обавештајне сарадње, будући да дељење осетљивих информација подразумева висок степен међусобног поверења (Wendt, 1999; Adler, 2005).

Комбинација ових теоријских приступа омогућава свеобухватнију анализу различитих модела колективне безбедности, јер истовремено узима у обзир ограничења која произилазе из међудржавне конкуренције, као и потенцијале институционалне сарадње и утицај политичких и нормативних фактора. Овако постављен теоријски оквир представља основу за даљу компаративну анализу НАТО-а, ЕУ и ОДКБ-а, нарочито у погледу степена институционалне интеграције, политичког поверења и ефикасности обавештајно-безбедносне сарадње.

Полазећи од теоријског оквира, основна и помоћне хипотезе у раду се заснивају на претпоставци да степен институционалне интеграције, као категорија либералног институционализма, те ниво политичког поверења међу државама, који се у великој мери објашњава кроз конструктивистичке теорије, представљају одлучујуће факторе ефикасности обавештајно-безбедносних система; истовремено, ограничења те сарадње произилазе из структурних карактеристика међународног система, на које указује реалистички приступ.

Улога обавештајно-безбедносних система у остваривању колективне безбедности

Обавештајно-безбедносни системи обухватају скуп институција, процедура и техничких капацитета усмерених на прикупљање, обраду и анализу података од значаја за националну и међународну безбедност. У оквиру колективне безбедности, њихова улога се може теоријски тумачити кроз призму више приступа, у оквиру безбедносних студија и међународних односа.

Полазећи од концепата реализма, обавештајно-безбедносни системи представљају инструмент националне моћи, чија је примарна функција обезбеђивање стратешке предности, у условима анархичног међународног система (Waltz, 1979; Mearsheimer, 2001). У том контексту и у оквиру колективних аранжмана, државе задржавају контролу над информацијама, што ограничава степен њихове размене и условљава сарадњу преклапањем интереса. Са становишта либералног институционализма, обавештајно-безбедносни системи имају улогу механизма, који смањује неизвесност и омогућава ефикаснију координацију међу државама (Keohane, 2005). Према томе, њихова функција

у оквиру колективне безбедности је вишеструка: информативна, аналитичка, превентивна и оперативна (Trbojević & Malbašić, 2022).

- На информативном нивоу, задатак система је да обезбеди релевантне податке о потенцијалним изворима претњи, било да се ради о војним, терористичким, сајбер или хибридним активностима.
- На аналитичком нивоу, обавештајне службе процењују ризике, идентификују обрасце понашања и формирају заједничке процене ситуације, које се прослеђују политичким и војним телима колективне безбедности.
- На превентивном нивоу, ове службе доприносе раном упозоравању и антиципацији конфликта.
- На оперативном плану, омогућавају ефикаснију координацију током заједничких мисија, војних вежби и кризних интервенција (Trbojević & Malbašić, 2022).

Из перспективе конструктивизма, аспект обавештајно-безбедносне сарадње се односи на улогу поверења, норми и заједничких идентитета (Wendt, 1999). Дељење осетљивих информација не представља само техничко питање, већ зависи од перцепције поузданости партнера и политичке културе сарадње.

Значај обавештајно-безбедносних система у колективним аранжманима постаје још већи у ери информационог друштва и дигиталних технологија. Обим и сложеност безбедносних претњи превазилазе могућности појединачних држава, што доводи до развоја интегрисаних механизма размене података. Ипак, у складу са реалистичким увидима, ова сарадња остаје ограничена различитим нивоима поверења, правним режимима заштите података и политичким интересима (Matić, 2025).

Поред институционалних и техничких аспеката, обавештајно-безбедносна сарадња има и изразиту политичку димензију. Она подразумева висок ниво међусобног поверења и усаглашавање стратешких приоритета. Сходно томе, ефикасност колективних обавештајних структура се може разумети као резултат интеракције институционалних механизма (либерализам), структурних ограничења (реализам) и нормативних фактора (конструктивизам), што представља полазну основу за даљу компаративну анализу различитих модела колективне безбедности.

**Типологија обавештајно-безбедносне сарадње:
политичко-стратешки, војни и цивилни аспекти**

Ради бољег разумевања функционалног обухвата обавештајно-безбедносних система у оквиру колективне безбедности, могуће је идентификовати три основна аспекта сарадње: политичко-стратешки, војни и цивилни.

- Политичко-стратешки аспект обухвата размену информација и процена на највишем нивоу одлучивања, између министарстава спољних послова, безбедносних савета и међународних тела, задужених за планирање и спровођење безбедносне политике. Са реалистичког становишта, овај ниво сарадње одражава покушај држава да усагласе перцепцију претњи, али уз задржавање контроле над битним информацијама. У оквиру НАТО-а, на пример, такву улогу имају North Atlantic Council и Intelligence Committee, док у ЕУ исту функцију обавља Политички и безбедносни комитет (PSC).
- Војни аспект обухвата оперативне обавештајне структуре, које делују у оквиру заједничких мисија, вежби или операција. Из перспективе либерализма, овај ниво сарадње представља најразвијенији облик институционалне координације, јер се заснива на стандардизованим процедурама, интероперабилности и заједничким оперативним циљевима. NATO Joint Intelligence and Security Division, као и EU Military Staff Intelligence Directorate представљају типичне примере таквих структура. Ове компоненте су најразвијеније, јер се ослањају на стандардизоване процедуре и техничке капацитете чланица.
- Цивилни аспект се односи на сарадњу у области унутрашње безбедности, полицијских и контраобавештајних послова, борбе против тероризма, организованог криминала и сајбер-претњи. Конструктивистички гледано, овај сегмент сарадње у великој мери зависи од постојања заједничких норми, правних стандарда и међусобног поверења. У тим оквирима, превасходну улогу играју институције, попут Еуропола (Europol), Фронтекса (Frontex), као и специјализовани центри за анализу и размену информација. Цивилни сегмент обавештајне сарадње има растући значај, будући да се граница између унутрашње и спољне безбедности све више брише, а већина савремених претњи има транснационални карактер.

У савременим међународним околностима, ефикасност колективне безбедности зависи од способности да се ови различити аспекти повежу у јединствен, функционалан систем размене информација и координисаног

одлучивања. Комбинација институционалних механизма, структурних ограничења и нормативних предуслова омогућава свеобухватно разумевање начина на који функционишу савремени обавештајно-безбедносни системи у оквиру колективне безбедности. Само таква интегрисана структура омогућава правовремено препознавање претњи, спречавање ескалације криза и очување поверења међу државама чланицама.

МОДЕЛИ ОБАВЕШТАЈНО-БЕЗБЕДНОСНЕ САРАДЊЕ У МЕЂУНАРОДНИМ ОРГАНИЗАЦИЈАМА

Развој међународних механизма обавештајно-безбедносне сарадње одражава промене у глобалној безбедносној архитектури након Другог светског рата. Док су рани модели били засновани на билатералним односима и *ad hoc* разменама информација, савремени системи колективне безбедности заснивају се на институционализованим структурама, које интегришу националне службе у заједнички оквир планирања, анализе и деловања. У овом поглављу се анализирају три најзначајнија модела: Северноатлантски савез, Европска унија и Организација за уговор о колективној безбедности. Сваки од њих рефлектује специфичне политичке, правне и организационе приступе обавештајно-безбедносној сарадњи.

НАТО – институционална структура и механизми обавештајне сарадње

НАТО представља најразвијенији пример колективног безбедносног система са функционално интегрисаном обавештајном компонентом. Од оснивања 1949. године, Савез је пролазио кроз бројне трансформације, али је обавештајна сарадња остала фундаментална за његову оперативну способност и политичку кохезију. Савремени институционални оквир НАТО обавештајне структуре је дефинисан реформама из 2016. године, којима су формиране две централне компоненте: NATO Intelligence Division и JISD (Joint Intelligence and Security Division), смештене у седишту Савеза, у Бриселу.

JISD делује као централни чвор обавештајно-безбедносне мреже Савеза. Његова основна функција је обједињавање и анализа информација које достављају националне службе држава чланица, као и развој заједничких процена безбедносне ситуације. JISD обухвата и NATO Intelligence Fusion Centre (NIFC), који се налази у Молсворту (Molesworth, Уједињено Краљевство), а

који омогућава стално прикупљање и анализу података из различитих извора: војних, сателитских, дипломатских и отворених. Ова структура омогућава брзо реаговање и континуирано информисање политичких и војних органа Савеза, пре свега Северноатлантског савета (НАС) и Војног комитета.

Основна иновација у НАТО приступу последњих година јесте развој концепта „предиктивне безбедности”, заснованог на употреби вештачке интелигенције, анализе великих скупова података (big data analytics) и машинског учења за антиципацију безбедносних трендова и потенцијалних криза. Усвајањем NATO AI Strategy (2021), Савез је формализовао оквир за коришћење алгоритама аналитике у проценама ризика, логистичким операцијама, сајбер одбрани и ситуационом мапирању (НАТО, 2024). Овим приступом НАТО прелази из фазе реактивног одговора у фазу проактивног, заснованог на предиктивним моделима и интегрисаној аналитици.

Механизми дељења података у оквиру НАТО-а су уређени вишеслојним системом класификације и поверљивости, са јасно дефинисаним протоколима за размену између чланица и партнерских држава. Иако су, формално, све чланице равноправне у приступу обавештајним информацијама, у пракси постоји асиметрија: највеће државе (САД, Велика Британија, Француска) задржавају контролу над кључним обавештајним ресурсима и делују као главни „донатори” информација. Ипак, координација унутар JISD и NIFC омогућава високу интероперабилност, што се показало пресудним током операција у Авганистану, Либији и Источној Европи.

Мини студија случаја: НАТО – Авганистан:

Интервенција НАТО-а у Авганистану (2001-2021), кроз мисију ISAF, представља један од најзначајнијих примера примене колективне безбедности у пракси (НАТО, 2022; Farrell et al., 2013). У контексту обавештајно-безбедносне сарадње, ова операција показује висок степен институционалне интеграције и развијене механизме координације међу државама чланицама (Johnson, 2018).

Обавештајна сарадња у Авганистану заснивала се на заједничким аналитичким структурама, дељењу података у реалном времену и интеграцији националних обавештајних служби у јединствени оперативни систем (Phythian, 2013; Gill & Phythian, 2018). Овакав модел је омогућио висок ниво ситуационе свести, прецизније планирање операција и ефикасније реаговање на безбедносне претње.

Ипак, упркос техничкој и организационој ефикасности, случај Авганистана указује на ограничења оваквог модела. Разлике у националним ин-

тересима, као и селективност у дељењу осетљивих информација, утицале су на квалитет заједничких процена. Поред тога, недовољна повезаност обавештајних налаза са дугорочним политичким стратегијама довела је до несразмере између оперативне успешности и коначних исхода мисије (Jones, 2009).

Овај случај потврђује да висок степен институционалне интеграције, карактеристичан за НАТО, омогућава ефикасну оперативну сарадњу, али да њена укупна успешност остаје условљена политичком кохезијом и стратешким консензусом држава чланица (Farrell et al., 2013; Johnson, 2018).

Европска унија – институционална мрежа и цивилно-војна обавештајна координација

За разлику од НАТО-а, који се заснива на војној структури и концепту колективне одбране, Европска унија је развила сложен систем обавештајно-безбедносне сарадње у оквиру Заједничке безбедносне и одбрамбене политике, која је део шире Заједничке спољне и безбедносне политике. Ова политика је настала као одговор на растућу потребу ЕУ да изгради аутономне капацитете за процену и реаговање на безбедносне кризе, без потпуног ослањања на НАТО.

Централна институција у овом систему је EU Intelligence and Situation Centre (EU INTCEN), који делује у оквиру Европске службе за спољне послове (EEAS). INTCEN има улогу аналитичког центра, који обрађује обавештајне податке достављене од држава чланица и партнерских служби, али сам не поседује сопствене изворе прикупљања информација. Његова мисија је да производи такозване strategic intelligence assessments, односно заједничке процене безбедносне ситуације, које се користе у доношењу политичких одлука на нивоу Савета ЕУ и Европског парламента (Nomikos, 2014).

Поред INTCEN-а, значајну улогу у војном сегменту има EU Military Staff Intelligence Directorate (EUMS INT), који обезбеђује војно-обавештајну подршку планирању и спровођењу заједничких мисија и операција. EUMS INT је интегрисан у структуру Војног штаба ЕУ (EUMS), а сарађује са националним војним обавештајним службама кроз мрежу Military Intelligence Officers Working Group (INT WG). Ова координација омогућава повезивање цивилних и војних компоненти, што ЕУ разликује од класичних војних савеза.

Европска унија је у последњој деценији развила и бројне специјализоване агенције, које допуњују обавештајно-безбедносни систем: Europol, Frontex, Eurojust, European Union Satellite Centre (SatCen) и Hybrid Fusion Cell, која делује у оквиру EEAS-а и бави се анализом хибридних претњи.

Ове институције чине мрежу која повезује унутрашњу и спољнополитичку безбедност, чиме се остварује јединствен европски концепт „свеобухватне безбедности” (comprehensive security).

За разлику од НАТО-а, обавештајна сарадња унутар ЕУ има изражено цивилни карактер, а нагласак је на информационој и аналитичкој интеграцији, а не на заједничким оперативним капацитетима. Ограничења проистичу из чињенице да државе чланице задржавају суверенитет над својим обавештајним службама и не желе да деле осетљиве податке. Ипак, ЕУ систематски гради поверење кроз заједничке обуке, стандардизоване процедуре и правне инструменте заштите информација.

Мини студија случаја: ЕУ – Мали:

Ангажовање ЕУ у Малију, кроз мисије као што су EUTM Mali и EUCAP Sahel Mali, представља пример специфичног приступа колективној безбедности, заснованог на цивилно-војној координацији и институционалној сарадњи (EUTM Mali, 2020; European Union, 2021).

Обавештајно-безбедносна сарадња се у овом контексту одвијала кроз интеграцију аналитичких капацитета, размену информација између цивилних и војних структура, као и сарадњу са локалним актерима (Bossong & Rhinard, 2016; Duke, 2019). Овај модел је омогућио боље разумевање безбедносног окружења и подршку изградњи институционалних капацитета државе домаћина.

Међутим, за разлику од НАТО-а, обавештајна сарадња у оквиру ЕУ се карактерише већом зависношћу од политичког консензуса и добровољног учешћа држава чланица (Smith, 2013). Ово је утицало на спорије доношење одлука и ограничену оперативну ефикасност у кризним ситуацијама.

Случај Малија показује да модел аналитичке интеграције и нормативне координације, који карактерише структуре ЕУ, доприноси дугорочној стабилизацији и изградњи институција, али да истовремено има ограничења у погледу брзине и интензитета реаговања (Duke, 2019; Bossong & Rhinard, 2016).

Организација за уговор о колективној безбедности (ОДКБ)

Организација за уговор о колективној безбедности (ОДКБ), основана 2002. године, као наследник споразума из 1992, представља регионални безбедносни савез постсовјетских држава предвођен Руском Федерацијом. У институционалном смислу, ОДКБ комбинује елементе колективне одбране

и политичко-безбедносне координације, али са изразито централизованим и хијерархиским моделом обавештајне сарадње.

Обавештајно-безбедносна компонента ОДКБ-а функционише кроз систем координације националних служби, у оквиру којег примарну улогу имају руски безбедносни и обавештајни органи. Иако су државе чланице (Белорусија, Јерменија, Казахстан, Киргистан и Таџикистан) формално обавезане на размену података од значаја за колективну безбедност, у пракси задржавају висок степен контроле над информацијама, што доводи до селективне и асиметричне сарадње. Оперативни капацитети Савеза су усмерени пре свега на борбу против тероризма, екстремизма, трговине наркотицима и граничне безбедности у Централној Азији.

Посебан институционални механизам представља Регионална анти-терористичка структура (РАТС) са седиштем у Ташкенту, која делује као централна платформа за размену обавештајних података о тероризму, екстремизму и транснационалним претњама (Рајић & Гајић, 2020). Активности РАТС-а обухватају вођење заједничких база података, координацију операција и организацију заједничких вежби, нарочито у региону Централне Азије. Ипак, упркос формалној институционализацији, обим и дубина сарадње у великој мери зависе од политичке воље и односа са Руском Федерацијом (Rozanov & Douhan, 2013; Allison, 2018).

У том смислу, функционисање ОДКБ-а се може тумачити кроз реалистичку призму, где доминација једне силе и асиметрија моћи обликују обрасце сарадње. За разлику од институционално развијенијих модела, као што су НАТО и ЕУ, где постоје релативно стабилни механизми заједничке анализе и доношења одлука, у оквиру ОДКБ-а институције имају ограничену аутономију, док одлуке остају у домену националних политичких елита.

Ограничења овог модела постају видљива у конкретним кризним ситуацијама. Током политичке кризе у Белорусији (2020), као и безбедносних изазова у Јерменији (2022), обавештајна координација и заједничко деловање су били спори, селективни и условљени националним интересима, што указује на ограничен дomet колективног механизма. Насупрот томе, интервенција у Казахстану 2022. године је показала да систем може бити оперативан у условима високог степена политичког консензуса, али и да је та ефикасност у значајној мери зависна од иницијативе и капацитета Руске Федерације.

Мини студија случаја: ОДКБ – Казахстан:

Интервенција ОДКБ-а у Казахстану 2022. године је најзначајнији пример практичне примене механизма колективне безбедности у оквиру ове

организације (Chathamhouse, 2023). У условима унутрашње политичке кризе и безбедносне нестабилности, обавештајно-безбедносна сарадња је омогућила брзу процену ситуације и доношење одлуке о ангажовању заједничких снага. Операција је реализована у кратком року, што указује на способност координације и мобилизације ресурса, у условима високог степена политичког консензуса (Chatham House, 2023).

Ипак, овај случај истовремено открива структурна ограничења система. Обавештајна сарадња је била ослоњена на капацитете Руске Федерације, док је улога осталих чланица била секундарна. Ово указује на асиметричан карактер сарадње и ограничен степен институционалне аутономије (Stronski, 2022).

Случај Казахстана потврђује да ОДКБ може бити оперативно ефикасан у специфичним условима, али да његова укупна функционалност зависи од политичке воље и доминације једног актера, што је апсолутно у складу са реалистичким тумачењем међународних односа (Parezanović, 2022).

Компаративни преглед: институционални, правни и политички аспекти

Компаративна анализа ова три модела указује на то да се обавештајно-безбедносна сарадња, у оквиру колективне безбедности, развија кроз различите институционалне парадигме. НАТО представља високо интегрисан, војно оријентисан систем, са развијеним аналитичким и техничким капацитетима, али и са израженом асиметријом између водећих и мањих чланица. Европска унија нуди модел цивилно-војне координације, који почива на аналитичкој интеграцији и политичком консензусу, док ОДКБ функционише као централизована, политички вођена структура, са ограниченим степеном институционалне аутономије.

У погледу нивоа интеграције, НАТО се истиче највишим степеном оперативне повезаности и стандардизације, док ЕУ има хоризонталан модел, који подстиче поверење, али спорије реагује у кризним ситуацијама. ОДКБ, иако формално поседује заједничке органе, фактички зависи од политичке воље и ресурса Русије.

Правни оквир у НАТО-у и ЕУ се заснива на јасно дефинисаним уговорима, процедурама и механизмима контроле, док ОДКБ карактеришу неформални аранжмани и одсуство систематске правне регулативе о обавештајној размени.

Када је реч о поверењу међу чланицама, оно је најразвијеније у оквиру ЕУ, где се поверење гради кроз институционалне процедуре и заједничке политике, док у НАТО-у поверење почива на стратешком партнерству и дугорочној војној сарадњи. У оквиру ОДКБ-а, међутим, поверење је претежно политичко и неретко инструментализовано, у складу са регионалним интересима.

У целини посматрано, три анализирана модела илуструју три различита концепта интеграције обавештајно-безбедносних система:

- НАТО – модел оперативне централизације, са нагласком на војну ефикасност и предиктивну аналитику;
- ЕУ – модел аналитичке интеграције, усмерен на баланс између безбедности и суверенитета;
- ОДКБ – модел политичке централизације, заснован на доминацији једне државе и ограниченој институционалној координацији.

Ови модели показују да је успех обавештајно-безбедносне сарадње у колективним оквирима условљен степеном институционалне зрелости, правне интегрисаности и политичке кохезије међу чланицама. Другим речима, обавештајна интеграција није само техничко, већ пре свега политичко питање поверења и заједничких вредности. Уочене разлике између три модела колективне безбедности постају посебно видљиве у конкретним кризним ситуацијама, које омогућавају емпиријску проверу њихове ефикасности.

У оквиру НАТО-а, операције у Авганистану представљају пример високог степена оперативне интеграције и развијене обавештајне сарадње. Заједничке обавештајне структуре су омогућиле континуирану размену података, координацију активности и релативно висок ниво ситуационе свести на терену. Но, упркос техничкој и организационој ефикасности, овај случај указује на ограничења дугорочне стратешке успешности, што потврђује да оперативна супериорност не мора нужно довести до политички одрживих исхода.

Са друге стране, ЕУ је кроз своје мисије у Малију показала специфичности свог модела, који се заснива на цивилно-војној координацији и аналитичкој интеграцији. Обавештајно-безбедносна сарадња у овом контексту омогућила је подршку локалним институцијама и управљање кризом, али је истовремено показала ограничења у брзини реаговања и зависност од политичког консензуса држава чланица.

У случају ОДКБ-а, реакција на кризу у Казахстану 2022. године представља најјаснији пример оперативне примене колективног механизма. Брза интервенција указује на способност мобилизације у условима високог степена политичког сагласја, али истовремено потврђује да је ефикасност овог

система у великој мери условљена улогом и капацитетима Руске Федерације, као доминантног актера.

Упоредна анализа ових случајева показује да се ефикасност обавештајно-безбедносне сарадње не може посматрати само кроз институционалне карактеристике, него и кроз њену примену у конкретним политичким и безбедносним оквирима. Док НАТО демонстрира висок ниво оперативне интеграције, ЕУ показује предности у домену нормативне и аналитичке координације, а ОДКБ функционише као политички условљен механизам, чија ефикасност варира у зависности од степена консензуса међу чланицама.

ФУНКЦИЈЕ ОБАВЕШТАЈНО-БЕЗБЕДНОСНИХ СИСТЕМА У КОЛЕКТИВНОЈ БЕЗБЕДНОСТИ

У савременим међународним односима, обавештајно-безбедносни системи постају неизоставни инструменти деловања у оквиру колективне безбедности. Њихове функције нису искључиво оперативног карактера, већ обухватају читав спектар активности, од раног упозоравања и процене ризика, преко планирања и спровођења заједничких мисија, до заштите информација, сајбер безбедности и политичке координације међу државама чланицама. У савременом окружењу, које карактеришу динамичне, вишедимензионалне и често нетрадиционалне претње, способност обавештајних система да ефикасно функционишу постаје директно повезана са стабилношћу и кредибилитетом колективне безбедности као концепта (Орашић, 2005).

Превентивна и аналитичка функција – систем раног упозоравања

Превентивна функција обавештајно-безбедносних система се огледа у способности антиципације безбедносних претњи, пре него што оне прерасту у отворене конфликте. Систем раног упозоравања (early warning system) представља централни елемент те функције. Он омогућава идентификацију потенцијалних криза на основу интеграције података из различитих извора: политичких, војних, економских, технолошких и друштвених (Kriendler, 2006).

У оквиру НАТО-а и ЕУ развијени су софистицирани модели предиктивне аналитике, који се ослањају на обраду великих скупова података (big data analytics) и вештачку интелигенцију (AI). Ови алати омогућавају препознавање образаца понашања и корелација које указују на ране фазе дестабилизације, хибридних операција или терористичких активности. Такав

приступ мења традиционалну парадигму обавештајног рада, јер се акценат помера са ретроспективне анализе ка предиктивној безбедности, чији је циљ превентивно деловање (Muti, 2021).

На плану Европске уније, Европски систем за ситуациону свест (EU SITCEN, данас EU INTCEN) обавља функцију интегрисаног аналитичког центра, прикупљајући податке из дипломатских мисија, националних служби и партнерских организација. Улога таквих тела није само техничка, већ и политичка. Она формулишу заједничке безбедносне процене које служе као основа за одлуке Савета ЕУ у оквиру Заједничке безбедносне и одбрамбене политике.

За разлику од НАТО-а и ЕУ, у оквиру ОДКБ-а, систем раног упозоравања није у потпуности институционализован на наднационалном нивоу. Обавештајно-безбедносна анализа углавном остаје у надлежности националних служби, док заједнички механизми имају пре свега координациону, а не аналитичку функцију. Иако постоје одређени облици сарадње у области раног откривања претњи, укључујући активности повезане са РАТС-ом, ови механизми су ограниченог домета и усмерени превасходно на борбу против тероризма и екстремизма. Недостатак интегрисаних аналитичких платформи и заједничких система предиктивне обраде података умањује способност благовременог препознавања сложених хибридних и дигиталних претњи.

Функција раног упозоравања подразумева и континуирано праћење такозваних „механих” индикатора ризика, попут промена у јавном мњењу, миграционих токова, политичке нестабилности и активности на друштвеним мрежама. Тиме обавештајно-безбедносни систем прелази из класичног војног оквира у интердисциплинарни домен, где се комбинују безбедносни, политички и социотехнолошки елементи.

Оперативна функција – координација мисија и заједничких операција

Оперативна функција обавештајно-безбедносних система огледа се у планирању, подршци и спровођењу заједничких мисија и операција у оквиру колективне безбедности. На овом нивоу, обавештајни капацитети обезбеђују ситуациону свест (situational awareness), пружају логистичке и аналитичке податке командним структурама и омогућавају тактичку координацију међу јединицама различитих земаља.

У оквиру НАТО-а, ова функција се институционално остварује преко JISD-а, који интегрише војне, контраобавештајне и безбедносне податке и дистрибуира их релевантним командама. Такав систем омогућава брзо реа-

говање, планирање мисија и подршку мултинационалним операцијама од Авганистана до балтичких држава.

У оквиру Европске уније, сличну улогу има EUMS INT, који у сарадњи са цивилним компонентама пружа обавештајну подршку мировним мисијама и операцијама кризног менаџмента. На тај начин се обезбеђује вертикална интеграција информација, од националног нивоа до стратешког центра одлучивања у Бриселу (EUMS INT, 2020).

Иако ОДКБ формално располаже колективним снагама за брзо реаговање и заједничким командним структурама, у пракси је степен интеграције обавештајних података нешто нижи него у оквиру НАТО-а. Размена информација се одвија билатерално, а не кроз јединствени аналитички систем, што утиче на ниво ситуационе свести и ефикасност координације током операција. Па ипак, ОДКБ показује одређене тактичке предности у односу на НАТО и ЕУ системе. То су способности брзе мобилизације и ефикасне оперативне координације, што указује на функционалност система у специфичним кризним ситуацијама.

Оперативна функција у савременом окружењу добија додатну димензију кроз сајбер и хибридне операције, које захтевају висок степен међуинституционалне координације и дигиталне интероперабилности. Брзина реаговања у таквим ситуацијама зависи од способности обавештајних структура да ефикасно комбинују податке из војних и цивилних извора.

Контраобавештајна и заштитна функција – безбедност информација и сајбер домен

Ефикасно функционисање колективне безбедности претпоставља постојање поузданих механизма заштите информација, инфраструктуре и комуникационих канала. Контраобавештајна функција обавештајно-безбедносних система је усмерена на спречавање инфилтрације, цурења поверљивих података и страног утицаја унутар институција колективне безбедности. У том смислу, безбедност информација није само техничко, већ и политичко питање поверења међу државама чланицама.

НАТО, на пример, примењује високо стандардизоване протоколе за класификацију и заштиту информација (NATO Security Policy, C-M(2002)49), док се унутар ЕУ спроводи систем заштите података према стандардима EU Classified Information. Поред класичне заштите информација, улога обавештајно-безбедносних система је проширена на сајбер домен, који је од 2016. године званично признат као „оперативни простор” деловања НАТО-а.

Сајбер безбедност и заштита инфраструктуре постају приоритети у колективним аранжманима. Напади на комуникационе мреже, дезинформационе кампање и сајбер-саботаже угрожавају интегритет и кредибилитет система, па обавештајне службе развијају заједничке протоколе за детекцију, анализу и реаговање. Тиме граница између обавештајног и техничког деловања ишчежава, а колективна безбедност прелази у дигитални и алгоритамски оквир.

Политичко-координациона функција – изградња поверења и дељење ризика

Једна од најбитнијих, али уједно и недовољно анализираних функција обавештајно-безбедносних система у оквиру колективне безбедности јесте политичко-координациона функција. Она подразумева како техничку размену података, тако и усклађивање националних безбедносних политика, изградњу међусобног поверења и институционализацију механизма заједничког одлучивања (Keohane, 2005). Размена обавештајних података представља изразито политички процес, јер државе деле информације које имају стратешку вредност и чије откривање може произвести многе безбедносне ризике. Због тога је степен обавештајне сарадње директно условљен нивоом поверења међу државама чланицама, што ову функцију чини централном, за разумевање ефикасности колективних безбедносних система (Kydd, 2005).

У оквиру НАТО-а, политичко-координациона функција је развијена кроз високо институционализоване механизме, који укључују редовне консултације, заједничке безбедносне процене и стандардизоване процедуре размене информација. Овакав модел омогућава релативно висок ниво поверења, али истовремено не елиминише у потпуности селективност у дељењу осетљивих података, посебно оних од различитих националних интереса. ЕУ развија политичко-координациону функцију кроз комплексну мрежу институција и механизма, као што су SIENA систем Europol-а, као и аналитичке структуре попут EU INTCEN-а (Europol, 2025). Међутим, за разлику од НАТО-а, овај модел се у доброј мери ослања на политички консензус и добровољност, што доприноси изградњи поверења, али истовремено успорава процес доношења одлука. Насупрот томе, у оквиру ОДКБ, политичко-координациона функција има изразито асиметричан карактер. Поверење није институционализовано у истој мери, него се углавном заснива на политичким односима са доминантним актером. У таквим условима, размена обавештајних података је условљена националним интересима, што ограничава степен стварне интеграције система. Међутим, управо овај централизовани

модел омогућава брже усаглашавање ставова и ефикасности доношење одлука у ситуацијама када постоји висок степен политичке сагласности, што може представљати оперативну предност у односу на сложеније и консензусом условљене механизме карактеристичне за НАТО и ЕУ.

Посебан аспект политичко-координационе функције представља концепт *Burden sharing*, односно заједничко преузимање одговорности и ризика. У високо интегрисаним системима, као што је НАТО, овај концепт подразумева расподелу војних и финансијских ресурса, те дељење обавештајних ризика и одговорности за доношење одлука. У оквиру ЕУ, он има нешто ширу политичко-економску димензију, док је у ОДКБ принцип ограничен доминацијом једног актера, што свакако доводи до неравномерне расподеле одговорности.

Аналитички посматрано, политичко-координациона функција представља везу између институционалне интеграције и ефикасности обавештајно-безбедносних система. Управо кроз механизме поверења и координације, институционалне структуре добијају стварну оперативну вредност. Стога, овај аспект директно потврђује полазну хипотезу рада, према којој ефикасност колективних безбедносних система зависи од степена институционалне интеграције и политичког поверења међу државама чланицама.

Нови изазови – хибридне претње, дезинформације и дигитална сфера

У последњој деценији се појављује нова генерација безбедносних изазова, која значајно трансформише традиционалне моделе обавештајно-безбедносног деловања. Хибридне претње, дезинформационе кампање, сајбер-напади и манипулација информацијама у дигиталном простору делују испод прага отвореног сукоба, али имају потенцијал да дестабилизују политичке системе и наруше друштвену кохезију (Singer & Brooking, 2018). Ефикасност колективне безбедности све више зависи од способности обавештајно-безбедносних система, да функционишу као интегрисане мреже за рано откривање, анализу и неутрализацију сложених, вишедимензионалних претњи (Nye, 2016). Овај изазов још јаче наглашава значај институционалне интеграције и политичког поверења, као темељних варијабли, постављених у хипотези рада.

У оквиру НАТО-а, одговор на хибридне претње се развија кроз институционализоване механизме, као што су „центри изврсности за сајбер одбрану и стратешке комуникације”. Висок степен техничке интеграције омогућава брзу размену података и координацију одговора, али и даље постоје ограничења у погледу дељења осетљивих информација и усклађивања националних приступа, нарочито у домену сајбер операција. ЕУ развија спе-

цифичан приступ, заснован на нормативној регулацији, заштити дигиталног простора и борби против дезинформација, кроз институције као што су Europol и специјализовани тимови за стратешке комуникације. Овај модел доприноси јачању отпорности друштава и институција, али је и даље ограничен сложеним процесима доношења одлука и различитим нивоима дигиталне спремности држава чланица. С друге стране, ОДКБ у мањој мери развија институционализоване механизме за суочавање са хибридним претњама, ослањајући се пре свега на националне капацитете и билатералну сарадњу. Иако постоје одређени облици координације, укључујући активности повезане са РАТС-ом, недостатак транспарентности и ограничен степен институционалне интеграције умањују ефикасност заједничког деловања у дигиталној сфери. У појединим анализама се указује на то да се овакав модел делимично ослања и на индиректне облике деловања, кроз партнерске и парадржавне актере, што може повећати флексибилност реаговања, али истовремено усложњава координацију и контролу у оквиру колективног система (Renz, 2016; Giles, 2016).

Упоредна анализа показује да се разлике између ових система продубљују у условима нових безбедносних изазова. Док НАТО задржава предност у техничко-оперативној координацији, ЕУ развија нормативно-институционалну отпорност, а ОДКБ, иако ограничен политичким и структурним факторима, проактивно делује кроз сарадњу са „прокси” сектором (Mumford, 2013). Ове разлике потврђују да у условима дигиталне трансформације безбедности, институционална интеграција и поверење међу државама чланицама постају још значајнији фактори ефикасности (Buzan & Wæver, 2003). Савремени обавештајно-безбедносни системи више не функционишу као затворене националне структуре, него као динамичне, технолошки посредоване мреже, чија успешност зависи од способности за координацију, размену информација и заједничко деловање у реалном времену (Rid, 2020).

Слабости обавештајно-безбедносних система колективне безбедности

Упркос дигиталној трансформацији и технолошком напретку, савремени обавештајно-безбедносни системи организација колективне безбедности се суочавају са низом унутрашњих ограничења. Та ограничења се могу посматрати кроз три међусобно повезана аспекта: структурне, политичке и оперативно-техничке слабости.

- Структурне слабости се огледају у сложености и фрагментацији међународних организација, као и у ограниченој интероперабилности

њихових подсистема. Разлике у технолошким стандардима, софтверским решењима, класификацији информација и безбедносним процедурама отежавају стварање јединственог обавештајног простора (Lowenthal, 2025).

- Политичке слабости се испољавају кроз дефицит поверења међу државама чланицама и учесталу политичку инструментализацију обавештајних података. Више аутора указује и на недовољну демократску и цивилну контролу над обавештајним структурама у оквиру колективне безбедности (Betts, 2007; Gill, 2016; Vjelajac, 2017). Такве слабости не само да умањују ефикасност система, него могу и нарушити његов кредибилитет у очима јавности.
- Оперативно-техничке слабости проистичу из преоптерећености информацијама, фрагментације база података и растуће сајбер-рањивости мрежа које повезују чланице. Иако концепт предиктивне безбедности тежи антиципацији ризика, у пракси се често суочава са кашњењем у обради података и недостатком времена за одлучивање у реалним ситуацијама (Mijalković, 2011).

У ширем смислу, највећа слабост обавештајно-безбедносних система колективне безбедности се огледа у трајној напетости између националне суверености и колективне солидарности. Док свака држава настоји да задржи контролу над сопственим обавештајним ресурсима, истовремено се очекује заједничко реаговање у кризама, које превазилазе појединачне капацитете (Allison, 2018). Ова контрадикција нарочито долази до изражаја у савременим конфликтима, као што су Украјина – Русија и Хамас – Израел, где колективни механизми деловања показују ограничену ефикасност, услед различитих политичких интереса и интерпретација безбедносних приоритета.

ЗАКЉУЧАК

На основу спроведене теоријске и емпиријске анализе, може се закључити да односи између нивоа институционалне интеграције и политичког поверења представљају идеалан аналитички оквир за разумевање функционисања савремених регионалних безбедносних организација.

Резултати компаративне анализе НАТО-а, ЕУ и ОДКБ-а указују да виши степен институционалне интеграције не производи аутоматски и виши ниво политичке кохезије, већ да се ефекти интеграције у значајној мери посредују кроз политичко поверење међу државама чланицама. У том смислу,

институционална архитектура представља неопходан, али не и довољан услов ефикасног колективног деловања.

Студије случаја потврђују ову релацију на различите начине. НАТО демонстрира висок степен оперативне ефикасности, али и повремене политичке несугласице, које ограничавају његову кохерентност у сложеним кризама. ЕУ показује виши ниво институционалне формализације и дугорочне стабилизационе капацитете, али уз изражену спорост у кризном одлучивању, услед хетерогености политичких интереса држава чланица. ОДКБ, са друге стране, показује већу брзину реакције у одређеним кризним ситуацијама, али и изражену зависност од доминантне улоге једне чланице, што ограничава његову институционалну аутономију.

На основу наведеног, хипотеза да виши степен институционалне интеграције доприноси већој ефикасности и стабилности безбедносне сарадње може се сматрати потврђеном у значајној, али не и апсолутној мери. Емпиријски налази указују да је однос између интеграције и ефикасности посредован политичким поверењем, институционалним дизајном и природом стратешких интереса држава чланица.

Допринос овог истраживања огледа се у развоју компаративног аналитичког оквира, који повезује теоријске приступе међународним односима са праксом функционисања регионалних безбедносних организација, као и у идентификацији политичког поверења као неопходне варијабле, која посредује између институционалне структуре и оперативне ефикасности.

Практичне импликације рада произилазе непосредно из резултата анализе. Утврђено је да унапређење ефикасности колективних обавештајно-безбедносних система захтева:

- даље јачање институционалне интеграције и стандардизације процедура;
- развој поузданих механизма заштите и размене података;
- унапређење политичке координације и изградње поверења међу државама чланицама.

Ове препоруке су директно изведене из уочених слабости у анализираним системима, те представљају логичан наставак емпиријских налаза рада.

Посматрано у целини, рад показује да ефикасност колективне безбедности у савременим условима не зависи само од техничких капацитета, већ пре свега од способности институција да обезбеде поверење, координацију и заједничко деловање у условима све сложенијег безбедносног окружења, које постаје примарна карактеристика 21. века.

Boriša Lečić¹
Nikola Trajković²

STRUCTURAL AND FUNCTIONAL ASPECTS OF INTELLIGENCE AND SECURITY SYSTEMS IN THE FUNCTION OF COLLECTIVE SECURITY

Abstract

The international security dynamics of the twenty-first century are characterized by pronounced interdependence and the proliferation of threats that transcend the capacities of individual states. Under such conditions, collective security has become a significant mechanism for preserving the stability and predictability of the international order, while intelligence and security systems constitute its operational foundation. The aim of this paper is to analyse the institutional structure and functional characteristics of these systems within the framework of the three most significant models of collective security: the North Atlantic Treaty Organization (NATO), the European Union (EU), and the Collective Security Treaty Organization (CSTO). Particular attention is devoted to mechanisms of coordination, information exchange, and joint responses to contemporary challenges such as terrorism, hybrid threats, cyberattacks, and disinformation campaigns. The analysis demonstrates that the effectiveness of collective intelligence and security systems primarily depends on the degree of institutional integration, technical interoperability, and political trust among member states. It is concluded that their future development will depend on the ability of international organizations to reconcile national interests with common security objectives and to strengthen mechanisms of predictive and preventive security within the digital environment.

Keywords: *collective security, intelligence and security systems, predictive security, hybrid threats, cybersecurity*

¹ Faculty of Law and Business Studies "Dr Lazar Vrkatić", Novi Sad, Serbia, borisalecic@gmail.com

² Faculty of Law and Business Studies "Dr Lazar Vrkatić", Novi Sad, Serbia, ntrajkovickk93@gmail.com

INTRODUCTION

In recent decades, the global security order has undergone profound transformations accompanied by technological, political, and social upheavals. Interstate conflicts increasingly assume unconventional forms, while the boundaries between internal and external security have become progressively less distinct. Terrorism, hybrid warfare, cyber threats, and disinformation operations have become integral components of contemporary security challenges. Under such circumstances, traditional models of national security can no longer provide reliable protection, which has led to the development of supranational mechanisms of cooperation based on the concept of collective security (Baylis, Smith & Owens, 2019). It is precisely in such circumstances that the role of intelligence and security systems acquires fundamental importance, as the effectiveness of joint responses by member states depends upon the quality and speed of information processing (Jovanović, 2020).

The subject of this research is the analysis of the structure and functional characteristics of intelligence and security systems within the framework of collective security, with particular reference to three key models: the North Atlantic Treaty Organization (NATO), the European Union (EU), and the Collective Security Treaty Organization (CSTO). The aim of the paper is to determine the manner in which the institutional framework, political relations, and technical-operational capacities of these systems influence their effectiveness in addressing contemporary security challenges such as terrorism, hybrid threats, cyberattacks, and the dissemination of disinformation.

The theoretical and practical significance of this topic is reflected in the need for a better understanding of the functioning of contemporary intelligence structures, which increasingly transcend the boundaries of national sovereignty and become components of supranational systems of collective decision-making. Understanding their structural and functional dimensions contributes to the enhancement of institutional cooperation, the establishment of reliable channels for information exchange, and the strengthening of the overall resilience of international organizations to security crises.

The principal research hypothesis posits that the effectiveness of intelligence and security systems within collective security arrangements depends primarily on the degree of institutional integration and political trust among member states. For the purpose of a more precise analysis, the concept of the “degree of institutional integration” is operationalized in this paper through several indicators:

- levels of formal institutional centralization;
- degrees of legal harmonization and procedural standardization;
- the scope and intensity of intelligence sharing;
- levels of technical interoperability among systems.

The auxiliary hypotheses proceed from the assumption that centralized organizational models enable more rapid and coordinated responses to security threats, whereas legal harmonization and the political will of member states constitute the most important preconditions for effective intelligence cooperation.

In order to ensure the empirical verifiability of the proposed hypothesis, the principal theoretical concepts (degree of integration and level of political trust) are operationalized through a set of qualitative indicators that enable their comparative analysis within selected regional security organizations. The degree of integration is examined through the following indicators: the level of institutional centralization and the existence of permanent supranational bodies possessing autonomous decision-making capacities; the degree of procedural standardization in planning and decision-making processes; the scope and depth of joint operational mechanisms; and the degree to which decisions are binding upon member states. Political trust is defined through indicators that include: the speed and consistency of member-state responses in crisis situations; the degree of political blockages or consensus-related deadlocks in decision-making processes; the level of intelligence and strategic information exchange; and the stability of political relations within the organization under conditions of foreign-policy divergence. On the basis of these indicators, a comparative analysis of NATO, the EU, and the CSTO is undertaken as three distinct models of institutional security cooperation, whereby their performance is assessed through the relationship between the institutional depth of integration and the degree of political trust among member states.

The paper employs the analytical-comparative method and the method of content analysis of relevant documents and strategic concepts, such as the NATO Strategic Concept (2022), the EU Security Strategy (2020), and the CSTO Charter (CSTO, 2002). Furthermore, in order to overcome the limitations of an exclusively descriptive approach, the analysis will be supplemented by case studies that enable the empirical verification of the derived conclusions, including NATO's long-term operations in Afghanistan, EU missions in Mali, and the activities of the CSTO during the crisis in Kazakhstan in 2022. In this manner, a more concrete assessment of the effectiveness of different models of collective security under real-world conditions is made possible.

THEORETICAL DEFINITION OF THE CONCEPT OF COLLECTIVE SECURITY AND INTELLIGENCE AND SECURITY SYSTEMS

The concept of collective security constitutes one of the fundamental pillars of the contemporary international order and the legal framework governing peace and stability. In theoretical terms, it denotes a system in which states agree to act jointly against any threat to peace, regardless of its source, based on the assumption that an attack against one member constitutes an attack against all. This principle, first clearly articulated within the framework of the League of Nations following the First World War, found its fullest expression in the Charter of the United Nations (1945), particularly in Chapter VII thereof, which defines the collective response to threats against international peace and security.

In international law, collective security denotes an institutionalized form of cooperation in which states transfer a portion of their sovereign authority to an international organization for the purpose of undertaking joint action against threats that undermine

general peace (Zakon o potvrđivanju konvencije UN protiv transnacionalnog organizovanog kriminala i dopunskih protokola, 2001). Unlike systems of alliances or collective defence, which are based on a common response to an external adversary (as is the case with NATO), collective security possesses a universal character and, in principle, encompasses all member states of the international community (Kupchan & Kupchan, 1995). In practice, however, this ideal model of collective action is transformed into partial, regional, or military-political forms of cooperation (Jovanović, 2020).

Contemporary systems of collective security, such as the UN, NATO, the EU, and the CSTO, operate on the basis of a combination of legal norms, political commitments, and operational coordination mechanisms (Rozanov & Douhan, 2013). Within this framework, intelligence and security systems constitute the element that enables timely decision-making, the planning of preventive measures, and coordinated responses to crisis situations. Without a reliable intelligence infrastructure, the concept of collective security remains within the realm of declaratory policy, since joint action presupposes the sharing of accurate, verified, and timely information (Bajagić, 2013; Gill, 2016).

The theoretical framework of this paper is therefore based on a combination of the realist approach and liberal institutionalism, supplemented by elements of constructivism. The realist approach proceeds from the assumption that states operate within an anarchic international system, guided by their own interests and the pursuit of power and security (Waltz, 1979; Mearsheimer, 2001). In this regard, intelligence and security systems constitute an instrument of national power, while cooperation is limited by the degree of trust and the convergence of interests. By contrast, liberal institutionalism emphasizes the role of international institutions in reducing uncertainty, increasing transparency, and facilitating cooperation among states (Keohane, 2005; Keohane & Nye, 1977). Collective security is viewed as an institutional mechanism that enables coordination, information exchange, and joint action, while intelligence and security systems represent the principal instrument of such cooperation. Finally, the constructivist approach contributes to an understanding of the role of norms, identities, and political culture in shaping trust among member states, which is of particular significance for the analysis of intelligence cooperation, given that the sharing of sensitive information presupposes a high degree of mutual trust (Wendt, 1999; Adler, 2005).

The combination of these theoretical approaches enables a more comprehensive analysis of different models of collective security, as it simultaneously takes into account the constraints arising from interstate competition, as well as the potential of institutional cooperation and the influence of political and normative factors. Such a theoretical framework provides the foundation for a further comparative analysis of NATO, the EU, and the CSTO, particularly with regard to the degree of institutional integration, political trust, and the effectiveness of intelligence and security cooperation.

Proceeding from this theoretical framework, the principal and auxiliary hypotheses of the paper are based on the assumption that the degree of institutional integration, as a category of liberal institutionalism, and the level of political trust among states, which is largely explained through constructivist theories, constitute decisive factors in the ef-

fectiveness of intelligence and security systems; at the same time, the limitations of such cooperation stem from the structural characteristics of the international system, as emphasized by the realist approach.

The role of intelligence and security systems in the realization of collective security

Intelligence and security systems encompass a set of institutions, procedures, and technical capacities directed toward the collection, processing, and analysis of data relevant to national and international security. Within the framework of collective security, their role may be theoretically interpreted through the prism of several approaches within security studies and international relations.

Proceeding from the concepts of realism, intelligence and security systems constitute an instrument of national power whose primary function is to secure strategic advantage under conditions of an anarchic international system (Waltz, 1979; Mearsheimer, 2001). In this context, and within collective arrangements, states retain control over information, which limits the degree of its exchange and conditions cooperation upon the overlap of interests. From the perspective of liberal institutionalism, intelligence and security systems serve as a mechanism that reduces uncertainty and enables more effective coordination among states (Keohane, 2005). Accordingly, their function within collective security is multifaceted: informational, analytical, preventive, and operational (Trbojević & Malbašić, 2022).

- At the informational level, the task of the system is to provide relevant data on potential sources of threats, whether they involve military, terrorist, cyber, or hybrid activities.
- At the analytical level, intelligence services assess risks, identify behavioural patterns, and formulate joint situational assessments, which are subsequently transmitted to the political and military bodies of collective security.
- At the preventive level, these services contribute to early warning and the anticipation of conflicts.
- At the operational level, they enable more effective coordination during joint missions, military exercises, and crisis interventions (Trbojević & Malbašić, 2022).

From the perspective of constructivism, the dimension of intelligence and security cooperation pertains to the role of trust, norms, and shared identities (Wendt, 1999). The sharing of sensitive information does not constitute merely a technical issue, but depends upon perceptions of partner reliability and the political culture of cooperation.

The significance of intelligence and security systems within collective arrangements becomes even greater in the era of the information society and digital technologies. The scale and complexity of security threats exceed the capacities of individual states, leading to the development of integrated mechanisms for data exchange. Nevertheless, in accordance with realist insights, such cooperation remains constrained by differing levels

of trust, legal regimes governing data protection, and political interests (Matić, 2025).

In addition to institutional and technical aspects, intelligence and security cooperation also possesses a pronounced political dimension. It presupposes a high level of mutual trust and the alignment of strategic priorities. Accordingly, the effectiveness of collective intelligence structures may be understood as the result of the interaction of institutional mechanisms (liberalism), structural constraints (realism), and normative factors (constructivism), which constitutes the starting point for a further comparative analysis of different models of collective security.

Typology of intelligence and security cooperation: political-strategic, military, and civilian aspects

For the purpose of a better understanding of the functional scope of intelligence and security systems within the framework of collective security, it is possible to identify three principal aspects of cooperation: political-strategic, military, and civilian.

- The political-strategic aspect encompasses the exchange of information and assessments at the highest levels of decision-making, among ministries of foreign affairs, security councils, and international bodies responsible for the planning and implementation of security policy. From a realist perspective, this level of cooperation reflects the efforts of states to harmonize their perceptions of threats while retaining control over critical information. Within NATO, for example, such a role is performed by the North Atlantic Council and the Intelligence Committee, while within the EU the same function is exercised by the Political and Security Committee (PSC).
- The military aspect encompasses operational intelligence structures functioning within joint missions, exercises, or operations. From the perspective of liberalism, this level of cooperation represents the most developed form of institutional coordination, as it is based on standardized procedures, interoperability, and common operational objectives. The NATO Joint Intelligence and Security Division, as well as the EU Military Staff Intelligence Directorate, constitute typical examples of such structures. These components are the most highly developed, as they rely on standardized procedures and the technical capacities of member states.
- The civilian aspect relates to cooperation in the field of internal security, police and counterintelligence affairs, the fight against terrorism, organized crime, and cyber threats. From a constructivist perspective, this segment of cooperation largely depends upon the existence of common norms, legal standards, and mutual trust. Within this framework, institutions such as Europol, Frontex, and specialized centres for analysis and information exchange play a predominant role. The civilian dimension of intelligence cooperation is acquiring increasing importance, as the distinction between internal and external security is becoming progressively blurred and the majority of contemporary threats possess a transnational character.

Under contemporary international circumstances, the effectiveness of collective security depends upon the ability to integrate these different aspects into a unified and functional system of information exchange and coordinated decision-making. The com-

bination of institutional mechanisms, structural constraints, and normative preconditions enables a comprehensive understanding of the manner in which contemporary intelligence and security systems operate within the framework of collective security. Only such an integrated structure makes possible the timely identification of threats, the prevention of crisis escalation, and the preservation of trust among member states.

MODELS OF INTELLIGENCE AND SECURITY COOPERATION IN INTERNATIONAL ORGANIZATIONS

The development of international mechanisms of intelligence and security cooperation reflects changes in the global security architecture following the Second World War. Whereas early models were based on bilateral relations and ad hoc information exchanges, contemporary systems of collective security rely upon institutionalized structures that integrate national services into a common framework of planning, analysis, and action. This chapter examines the three most significant models: the North Atlantic Treaty Organization, the European Union, and the Collective Security Treaty Organization. Each of them reflects specific political, legal, and organizational approaches to intelligence and security cooperation.

NATO – institutional structure and mechanisms of intelligence cooperation

NATO represents the most developed example of a collective security system with a functionally integrated intelligence component. Since its establishment in 1949, the Alliance has undergone numerous transformations, yet intelligence cooperation has remained fundamental to its operational capability and political cohesion. The contemporary institutional framework of NATO's intelligence structure was defined through the reforms of 2016, which established two central components: the NATO Intelligence Division and the JISD (Joint Intelligence and Security Division), located at the Alliance's headquarters in Brussels.

The JISD functions as the central hub of the Alliance's intelligence and security network. Its primary function is the consolidation and analysis of information provided by the national services of member states, as well as the development of joint assessments of the security environment. The JISD also encompasses the NATO Intelligence Fusion Centre (NIFC), located in Molesworth (United Kingdom), which enables the continuous collection and analysis of data derived from various sources, including military, satellite, diplomatic, and open-source channels. This structure facilitates rapid response and continuous briefing of the Alliance's political and military bodies, primarily the North Atlantic Council (NAC) and the Military Committee.

The principal innovation in NATO's approach in recent years has been the development of the concept of "predictive security", based on the use of artificial intelli-

gence, big data analytics, and machine learning for the anticipation of security trends and potential crises. Through the adoption of the NATO AI Strategy (2021), the Alliance formalized a framework for the use of algorithmic analytics in risk assessment, logistical operations, cyber defence, and situational mapping (NATO, 2024). Through this approach, NATO is moving from a phase of reactive response to a phase of proactive action based on predictive models and integrated analytics.

Data-sharing mechanisms within NATO are regulated through a multilayered system of classification and confidentiality, with clearly defined protocols governing exchanges among member states and partner countries. Although all member states are formally equal in terms of access to intelligence information, in practice there exists a degree of asymmetry: the largest states (the United States, the United Kingdom, and France) retain control over key intelligence resources and act as the principal “providers” of information. Nevertheless, coordination within the JISD and the NIFC enables a high degree of interoperability, which proved decisive during operations in Afghanistan, Libya, and Eastern Europe.

Mini case study: NATO – Afghanistan:

NATO’s intervention in Afghanistan (2001-2021), conducted through the ISAF mission, represents one of the most significant examples of the practical application of collective security (NATO, 2022; Farrell et al., 2013). In the context of intelligence and security cooperation, this operation demonstrates a high degree of institutional integration and well-developed mechanisms of coordination among member states (Johnson, 2018).

Intelligence cooperation in Afghanistan was based on joint analytical structures, real-time data sharing, and the integration of national intelligence services into a unified operational system (Phythian, 2013; Gill & Phythian, 2018). Such a model enabled a high level of situational awareness, more precise operational planning, and more effective responses to security threats.

Nevertheless, despite its technical and organizational effectiveness, the Afghan case reveals the limitations of such a model. Differences in national interests, as well as selectivity in the sharing of sensitive information, affected the quality of joint assessments. Furthermore, the insufficient linkage between intelligence findings and long-term political strategies resulted in a discrepancy between operational success and the ultimate outcomes of the mission (Jones, 2009).

This case confirms that the high degree of institutional integration characteristic of NATO enables effective operational cooperation, but that its overall success remains contingent upon the political cohesion and strategic consensus of member states (Farrell et al., 2013; Johnson, 2018).

European Union – institutional network and civil-military intelligence coordination

Unlike NATO, which is founded upon a military structure and the concept of collective defence, the European Union has developed a complex system of intelligence and security cooperation within the framework of the Common Security and Defence Policy, which forms part of the broader Common Foreign and Security Policy. This policy emerged as a response to the growing need for the EU to develop autonomous capacities for assessing and responding to security crises without complete reliance upon NATO.

The central institution within this system is the EU Intelligence and Situation Centre (EU INTCEN), which operates within the European External Action Service (EEAS). INTCEN functions as an analytical centre that processes intelligence data provided by member states and partner services, although it does not possess its own information-gathering capabilities. Its mission is to produce so-called strategic intelligence assessments, namely joint evaluations of the security environment that are used in political decision-making at the level of the Council of the European Union and the European Parliament (Nomikos, 2014).

In addition to INTCEN, a significant role in the military segment is performed by the EU Military Staff Intelligence Directorate (EUMS INT), which provides military intelligence support for the planning and implementation of joint missions and operations. EUMS INT is integrated into the structure of the EU Military Staff (EUMS) and cooperates with national military intelligence services through the Military Intelligence Officers Working Group (INT WG). This coordination enables the integration of civilian and military components, distinguishing the EU from traditional military alliances.

Over the last decade, the European Union has also developed a number of specialized agencies that complement its intelligence and security system: Europol, Frontex, Eurojust, the European Union Satellite Centre (SatCen), and the Hybrid Fusion Cell, which operates within the EEAS and is responsible for the analysis of hybrid threats. Together, these institutions constitute a network linking internal and external security, thereby realizing the distinctive European concept of “comprehensive security”.

Unlike NATO, intelligence cooperation within the EU possesses a markedly civilian character, with emphasis placed on informational and analytical integration rather than on common operational capabilities. Its limitations stem from the fact that member states retain sovereignty over their intelligence services and remain reluctant to share sensitive information. Nevertheless, the EU systematically builds trust through joint training programmes, standardized procedures, and legal instruments for information protection.

Mini case study: EU – Mali:

The EU’s engagement in Mali, through missions such as EUTM Mali and EUCAP Sahel Mali, represents an example of a specific approach to collective security based on civil-military coordination and institutional cooperation (EUTM Mali, 2020; European Union, 2021).

In this context, intelligence and security cooperation was conducted through the integration of analytical capacities, the exchange of information between civilian and military structures, and cooperation with local actors (Bossong & Rhinard, 2016; Duke, 2019). This model enabled a more comprehensive understanding of the security environment and supported the development of institutional capacities within the host state.

However, unlike NATO, intelligence cooperation within the EU is characterized by a greater dependence upon political consensus and the voluntary participation of member states (Smith, 2013). This has contributed to slower decision-making processes and limited operational effectiveness in crisis situations.

The case of Mali demonstrates that the model of analytical integration and normative coordination characteristic of EU structures contributes to long-term stabilization and institution-building, while simultaneously exhibiting limitations with regard to the speed and intensity of response (Duke, 2019; Bossong & Rhinard, 2016).

Collective Security Treaty Organization (CSTO)

The Collective Security Treaty Organization (CSTO), established in 2002 as the successor to the 1992 agreement, represents a regional security alliance of post-Soviet states led by the Russian Federation. In institutional terms, the CSTO combines elements of collective defence and political-security coordination, albeit through a highly centralized and hierarchical model of intelligence cooperation.

The intelligence and security component of the CSTO functions through a system of coordination among national services, within which Russian security and intelligence bodies play the primary role. Although member states (Belarus, Armenia, Kazakhstan, Kyrgyzstan, and Tajikistan) are formally obliged to exchange information relevant to collective security, in practice they retain a high degree of control over such information, resulting in selective and asymmetrical cooperation. The Alliance's operational capacities are directed primarily toward combating terrorism, extremism, drug trafficking, and ensuring border security in Central Asia.

A particularly important institutional mechanism is the Regional Anti-Terrorist Structure (RATS), headquartered in Tashkent, which serves as the central platform for the exchange of intelligence concerning terrorism, extremism, and transnational threats (Rajić & Gajić, 2020). The activities of RATS include the maintenance of joint databases, the coordination of operations, and the organization of joint exercises, particularly within the Central Asian region. Nevertheless, despite its formal institutionalization, the scope and depth of cooperation depend to a considerable extent upon political will and relations with the Russian Federation (Rozanov & Douhan, 2013; Allison, 2018).

In this regard, the functioning of the CSTO may be interpreted through a realist lens, whereby the dominance of a single power and asymmetries of power shape patterns of cooperation. Unlike institutionally more developed models such as NATO and the EU, where relatively stable mechanisms of joint analysis and decision-making exist, institu-

tions within the CSTO possess limited autonomy, while decisions remain largely within the domain of national political elites.

The limitations of this model become evident in specific crisis situations. During the political crisis in Belarus (2020), as well as the security challenges in Armenia (2022), intelligence coordination and collective action proved slow, selective, and conditioned by national interests, indicating the limited reach of the collective mechanism. By contrast, the intervention in Kazakhstan in 2022 demonstrated that the system can operate effectively under conditions of a high degree of political consensus, while also revealing that such effectiveness is significantly dependent upon the initiative and capacities of the Russian Federation.

Mini case study: CSTO – Kazakhstan:

The CSTO intervention in Kazakhstan in 2022 constitutes the most significant example of the practical application of collective security mechanisms within this organization (Chatham House, 2023). Under conditions of internal political crisis and security instability, intelligence and security cooperation enabled a rapid assessment of the situation and the adoption of a decision to deploy joint forces. The operation was carried out within a short timeframe, indicating the capacity for coordination and resource mobilization under conditions of a high degree of political consensus (Chatham House, 2023).

At the same time, however, this case reveals the structural limitations of the system. Intelligence cooperation relied predominantly upon the capacities of the Russian Federation, while the role of the other member states remained secondary. This points to the asymmetrical character of cooperation and the limited degree of institutional autonomy (Stronski, 2022).

The Kazakhstan case confirms that the CSTO can be operationally effective under specific circumstances, but that its overall functionality depends upon political will and the dominance of a single actor, which is entirely consistent with the realist interpretation of international relations (Parezanović, 2022).

Comparative overview: institutional, legal, and political aspects

A comparative analysis of these three models indicates that intelligence and security cooperation within the framework of collective security develops through different institutional paradigms. NATO represents a highly integrated, military-oriented system characterized by advanced analytical and technical capacities, but also by a pronounced asymmetry between leading and smaller member states. The European Union offers a model of civil-military coordination based on analytical integration and political consensus, whereas the CSTO functions as a centralized, politically driven structure with a limited degree of institutional autonomy.

With regard to the level of integration, NATO is distinguished by the highest degree of operational interconnectedness and standardization, while the EU employs a horizontal model that fosters trust but responds more slowly in crisis situations. The CSTO, although formally possessing common institutions, is in practice dependent upon the political will and resources of Russia.

The legal framework of NATO and the EU is based upon clearly defined treaties, procedures, and oversight mechanisms, whereas the CSTO is characterized by informal arrangements and the absence of a systematic legal framework governing intelligence exchange.

With regard to trust among member states, it is most highly developed within the EU, where trust is built through institutional procedures and common policies, whereas within NATO it rests upon strategic partnership and long-term military cooperation. Within the CSTO, however, trust is predominantly political and is frequently instrumentalized in accordance with regional interests.

Taken as a whole, the three models analysed illustrate three distinct concepts of intelligence and security system integration:

- NATO – a model of operational centralization, with an emphasis on military effectiveness and predictive analytics;
- EU – a model of analytical integration, aimed at balancing security and sovereignty;
- CSTO – a model of political centralization, based upon the dominance of a single state and limited institutional coordination.

These models demonstrate that the success of intelligence and security cooperation within collective frameworks is conditioned by the degree of institutional maturity, legal integration, and political cohesion among member states. In other words, intelligence integration is not merely a technical issue but, above all, a political question of trust and shared values. The differences identified among the three models of collective security become particularly evident in specific crisis situations, which enable an empirical assessment of their effectiveness.

Within NATO, operations in Afghanistan constitute an example of a high degree of operational integration and advanced intelligence cooperation. Joint intelligence structures enabled continuous information exchange, coordination of activities, and a relatively high level of situational awareness in the field. Nevertheless, despite their technical and organizational effectiveness, this case highlights the limitations of long-term strategic success, confirming that operational superiority does not necessarily lead to politically sustainable outcomes.

By contrast, through its missions in Mali, the EU demonstrated the specific features of its model, which is based upon civil-military coordination and analytical integration. Intelligence and security cooperation in this context facilitated support for local institutions and crisis management, while simultaneously revealing limitations in response speed and dependence upon political consensus among member states.

In the case of the CSTO, the response to the crisis in Kazakhstan in 2022 constitutes the clearest example of the operational application of a collective mechanism. The rapid intervention indicates a capacity for mobilization under conditions of a high degree of political agreement, but at the same time confirms that the effectiveness of this system is largely conditioned by the role and capacities of the Russian Federation as the dominant actor.

A comparative analysis of these cases demonstrates that the effectiveness of intelligence and security cooperation cannot be assessed solely through institutional characteristics, but must also be examined through its application within specific political and security contexts. While NATO demonstrates a high level of operational integration, the EU exhibits advantages in the domain of normative and analytical coordination, whereas the CSTO functions as a politically conditioned mechanism whose effectiveness varies according to the degree of consensus among its member states.

FUNCTIONS OF INTELLIGENCE AND SECURITY SYSTEMS IN COLLECTIVE SECURITY

In contemporary international relations, intelligence and security systems have become indispensable instruments of action within the framework of collective security. Their functions are not exclusively operational in nature, but encompass an entire spectrum of activities, ranging from early warning and risk assessment, through the planning and implementation of joint missions, to information protection, cybersecurity, and political coordination among member states. In a contemporary environment characterized by dynamic, multidimensional, and often non-traditional threats, the capacity of intelligence systems to function effectively becomes directly linked to the stability and credibility of collective security as a concept (Opačić, 2005).

Preventive and analytical function – the early warning system

The preventive function of intelligence and security systems is reflected in their capacity to anticipate security threats before they escalate into open conflicts. The early warning system constitutes the central element of this function. It enables the identification of potential crises through the integration of data from diverse sources, including political, military, economic, technological, and social domains (Kriendler, 2006).

Within NATO and the EU, sophisticated models of predictive analytics have been developed that rely upon big data analytics and artificial intelligence (AI). These tools facilitate the identification of behavioural patterns and correlations indicative of the early stages of destabilization, hybrid operations, or terrorist activities. Such an approach transforms the traditional paradigm of intelligence work, as the emphasis shifts from retrospective analysis toward predictive security, the objective of which is preventive action (Muti, 2021).

At the level of the European Union, the European Union Situation Centre (EU SITCEN, now EU INTCEN) performs the function of an integrated analytical centre, collecting information from diplomatic missions, national services, and partner organizations. The role of such bodies is not merely technical, but also political. They formulate common security assessments that serve as the basis for decisions of the Council of the European Union within the framework of the Common Security and Defence Policy.

Unlike NATO and the EU, within the CSTO the early warning system is not fully institutionalized at the supranational level. Intelligence and security analysis largely remains within the competence of national services, while common mechanisms primarily perform a coordinating rather than an analytical function. Although certain forms of cooperation in the field of early threat detection exist, including activities associated with RATS, these mechanisms are limited in scope and are primarily focused on combating terrorism and extremism. The absence of integrated analytical platforms and common predictive data-processing systems reduces the capacity for the timely identification of complex hybrid and digital threats.

The early warning function also entails the continuous monitoring of so-called “soft” risk indicators, such as changes in public opinion, migration flows, political instability, and activity on social media platforms. In this way, the intelligence and security system moves beyond the traditional military framework into an interdisciplinary domain in which security, political, and socio-technological elements are combined.

Operational function – coordination of missions and joint operations

The operational function of intelligence and security systems is reflected in the planning, support, and implementation of joint missions and operations within the framework of collective security. At this level, intelligence capabilities provide situational awareness, supply logistical and analytical information to command structures, and facilitate tactical coordination among units from different countries.

Within NATO, this function is institutionally realized through the JISD, which integrates military, counterintelligence, and security information and disseminates it to relevant commands. Such a system enables rapid response, mission planning, and support for multinational operations ranging from Afghanistan to the Baltic states.

Within the European Union, a similar role is performed by EUMS INT, which, in cooperation with civilian components, provides intelligence support for peacekeeping missions and crisis-management operations. In this manner, vertical integration of information is ensured, from the national level to the strategic decision-making centre in Brussels (EUMS INT, 2020).

Although the CSTO formally possesses collective rapid reaction forces and joint command structures, in practice the degree of intelligence integration is somewhat lower than within NATO. Information exchange is conducted bilaterally rather than through a unified analytical system, which affects the level of situational awareness and the effec-

tiveness of operational coordination. Nevertheless, the CSTO demonstrates certain tactical advantages in comparison with NATO and EU systems. These include the capacity for rapid mobilization and effective operational coordination, indicating the functionality of the system in specific crisis situations.

In the contemporary environment, the operational function acquires an additional dimension through cyber and hybrid operations, which require a high degree of inter-institutional coordination and digital interoperability. The speed of response in such situations depends upon the ability of intelligence structures to effectively integrate information derived from both military and civilian sources.

Counterintelligence and protective function – information security and the cyber domain

The effective functioning of collective security presupposes the existence of reliable mechanisms for the protection of information, infrastructure, and communication channels. The counterintelligence function of intelligence and security systems is directed toward preventing infiltration, the leakage of classified information, and foreign influence within the institutions of collective security. In this respect, information security is not merely a technical issue, but also a political question of trust among member states.

NATO, for example, applies highly standardized protocols for the classification and protection of information (NATO Security Policy, C-M(2002)49), while within the European Union data protection is implemented according to the standards of EU Classified Information. In addition to the traditional protection of information, the role of intelligence and security systems has expanded into the cyber domain, which has been officially recognized since 2016 as an “operational domain” of NATO activity.

Cybersecurity and infrastructure protection have become priorities within collective arrangements. Attacks against communication networks, disinformation campaigns, and cyber sabotage threaten the integrity and credibility of these systems, prompting intelligence services to develop joint protocols for detection, analysis, and response. Consequently, the boundary between intelligence and technical activity is increasingly disappearing, and collective security is evolving into a digital and algorithmic framework.

Political-coordination function – building trust and sharing risks

One of the most important, yet simultaneously underexplored, functions of intelligence and security systems within collective security frameworks is the political-coordination function. It encompasses not only the technical exchange of information but also the alignment of national security policies, the development of mutual trust, and the institutionalization of joint decision-making mechanisms (Keohane, 2005). Intelligence sharing constitutes an inherently political process, as states exchange information of

strategic value whose disclosure may generate significant security risks. Consequently, the degree of intelligence cooperation is directly conditioned by the level of trust among member states, making this function central to understanding the effectiveness of collective security systems (Kydd, 2005).

Within NATO, the political-coordination function has been developed through highly institutionalized mechanisms that include regular consultations, joint security assessments, and standardized information-sharing procedures. Such a model facilitates a relatively high level of trust, while not entirely eliminating selectivity in the sharing of sensitive information, particularly information linked to specific national interests. The EU develops its political-coordination function through a complex network of institutions and mechanisms, such as Europol's SIENA system and analytical structures such as EU INTCEN (Europol, 2025). However, unlike NATO, this model relies to a considerable extent on political consensus and voluntary participation, which contributes to trust-building but simultaneously slows the decision-making process. In contrast, within the CSTO, the political-coordination function exhibits a markedly asymmetrical character. Trust is not institutionalized to the same extent but is largely based on political relations with the dominant actor. Under such conditions, intelligence sharing is conditioned by national interests, thereby limiting the degree of genuine system integration. Nevertheless, this centralized model enables faster alignment of positions and more efficient decision-making in situations characterized by a high degree of political consensus, which may constitute an operational advantage compared to the more complex and consensus-dependent mechanisms characteristic of NATO and the EU.

A particularly important dimension of the political-coordination function is the concept of burden sharing, that is, the collective assumption of responsibilities and risks. In highly integrated systems such as NATO, this concept entails the distribution of military and financial resources, as well as the sharing of intelligence risks and decision-making responsibilities. Within the EU, burden sharing assumes a somewhat broader political and economic dimension, whereas within the CSTO the principle remains constrained by the dominance of a single actor, resulting in an uneven distribution of responsibilities.

From an analytical perspective, the political-coordination function represents the link between institutional integration and the effectiveness of intelligence and security systems. It is precisely through mechanisms of trust and coordination that institutional structures acquire real operational value. Consequently, this aspect directly confirms the central hypothesis of this study, according to which the effectiveness of collective security systems depends upon the degree of institutional integration and political trust among member states.

New challenges – hybrid threats, disinformation, and the digital domain

Over the past decade, a new generation of security challenges has emerged, significantly transforming traditional models of intelligence and security activity. Hybrid threats, disinformation campaigns, cyberattacks, and information manipulation in the dig-

ital sphere operate below the threshold of open conflict but possess the capacity to destabilize political systems and undermine social cohesion (Singer & Brooking, 2018). The effectiveness of collective security increasingly depends on the ability of intelligence and security systems to function as integrated networks for the early detection, analysis, and neutralization of complex, multidimensional threats (Nye, 2016). This challenge further underscores the importance of institutional integration and political trust as the fundamental variables underlying the study's hypothesis.

Within NATO, responses to hybrid threats have been developed through institutionalized mechanisms such as Centres of Excellence for Cyber Defence and Strategic Communications. A high degree of technical integration enables rapid information exchange and coordinated responses, although limitations persist regarding the sharing of sensitive information and the harmonization of national approaches, particularly in the field of cyber operations. The EU has developed a distinct approach based on normative regulation, digital-space protection, and counter-disinformation efforts through institutions such as Europol and specialized strategic communications teams. This model contributes to strengthening the resilience of societies and institutions but remains constrained by complex decision-making procedures and varying levels of digital preparedness among member states. Conversely, the CSTO has developed institutionalized mechanisms for addressing hybrid threats to a much lesser extent, relying primarily on national capabilities and bilateral cooperation. Although certain forms of coordination exist, including activities associated with RATS, the lack of transparency and the limited degree of institutional integration reduce the effectiveness of collective action in the digital sphere. Some analyses suggest that this model partially relies on indirect forms of activity through partner and para-state actors, which may enhance flexibility in response but simultaneously complicates coordination and control within the collective system (Renz, 2016; Giles, 2016).

Comparative analysis demonstrates that the differences among these systems become more pronounced under conditions of emerging security challenges. While NATO retains an advantage in technical-operational coordination, the EU develops normative and institutional resilience, whereas the CSTO, despite being constrained by political and structural factors, acts proactively through cooperation with proxy actors (Mumford, 2013). These differences confirm that, in the context of the digital transformation of security, institutional integration and trust among member states become even more significant determinants of effectiveness (Buzan & Wæver, 2003). Contemporary intelligence and security systems no longer function as closed national structures but rather as dynamic, technologically mediated networks whose success depends on their capacity for coordination, information sharing, and collective action in real time (Rid, 2020).

Weaknesses of intelligence and security systems in collective security

Despite digital transformation and technological advancement, contemporary intelligence and security systems within collective security organizations face a range of

internal limitations. These constraints may be examined through three interconnected dimensions: structural, political, and operational-technical weaknesses.

- Structural weaknesses are reflected in the complexity and fragmentation of international organizations, as well as in the limited interoperability of their subsystems. Differences in technological standards, software solutions, information-classification systems, and security procedures complicate the creation of a unified intelligence environment (Lowenthal, 2025).
- Political weaknesses manifest themselves through deficits of trust among member states and the frequent political instrumentalization of intelligence information. Numerous scholars also point to insufficient democratic and civilian oversight of intelligence structures within collective security frameworks (Betts, 2007; Gill, 2016; Bjelajac, 2017). Such weaknesses not only diminish system effectiveness but may also undermine its public credibility.
- Operational-technical weaknesses arise from information overload, fragmented databases, and the growing cyber-vulnerability of networks connecting member states. Although the concept of predictive security seeks to anticipate risks, in practice it frequently encounters delays in data processing and insufficient time for decision-making in real-world situations (Mijalković, 2011).

More broadly, the principal weakness of intelligence and security systems within collective security arrangements lies in the enduring tension between national sovereignty and collective solidarity. While each state seeks to retain control over its own intelligence resources, collective responses are simultaneously expected in crises that exceed individual national capacities (Allison, 2018). This contradiction is particularly evident in contemporary conflicts such as the Russia–Ukraine war and the Hamas–Israel conflict, where collective mechanisms have demonstrated limited effectiveness as a result of divergent political interests and competing interpretations of security priorities.

CONCLUSION

Based on the theoretical and empirical analysis conducted, it may be concluded that the relationship between the level of institutional integration and political trust constitutes an appropriate analytical framework for understanding the functioning of contemporary regional security organizations.

The results of the comparative analysis of NATO, the EU, and the CSTO indicate that a higher degree of institutional integration does not automatically generate a higher level of political cohesion. Rather, the effects of integration are significantly mediated by political trust among member states. In this regard, institutional architecture represents a necessary, but not sufficient, condition for effective collective action.

The case studies confirm this relationship in different ways. NATO demonstrates a high degree of operational effectiveness, but also experiences occasional political disagreements that limit its coherence in complex crises. The EU exhibits a higher level of

institutional formalization and long-term stabilization capacity, yet is characterized by considerable slowness in crisis decision-making due to the heterogeneity of member states' political interests. The CSTO, by contrast, demonstrates greater responsiveness in certain crisis situations, while simultaneously exhibiting a pronounced dependence on the dominant role of a single member state, which constrains its institutional autonomy.

On the basis of the foregoing, the hypothesis that a higher degree of institutional integration contributes to greater effectiveness and stability of security cooperation may be regarded as confirmed to a significant, though not absolute, extent. The empirical findings indicate that the relationship between integration and effectiveness is mediated by political trust, institutional design, and the nature of the strategic interests of member states.

The contribution of this research lies in the development of a comparative analytical framework that connects theoretical approaches in international relations with the practical functioning of regional security organizations, as well as in identifying political trust as a necessary variable mediating the relationship between institutional structure and operational effectiveness.

The practical implications of the study derive directly from the findings of the analysis. It has been established that enhancing the effectiveness of collective intelligence and security systems requires:

- further strengthening of institutional integration and the standardization of procedures;
- the development of reliable mechanisms for information protection and information sharing;
- the enhancement of political coordination and the strengthening of trust among member states.

These recommendations are directly derived from the weaknesses identified within the analyzed systems and therefore constitute a logical extension of the study's empirical findings.

Viewed as a whole, this study demonstrates that the effectiveness of collective security under contemporary conditions depends not only on technical capabilities but, above all, on the capacity of institutions to foster trust, coordination, and collective action within an increasingly complex security environment, which has become one of the defining characteristics of the twenty-first century.

REFERENCE LIST

Adler, E. (2005). *Communitarian international relations: The epistemic foundations of international relations*. Routledge.

Allison, R. (2018). Protective integration and coordination of security policy: A comparison of the SCO and the CSTO. *The Chinese Journal of International Politics*, 11(3), 297–338.

- Bajagić, M. (2013). *Obaveštajna aktivnost u funkciji izgradnje sistema nacionalne bezbednosti*. Kriminalističko-policijska akademija.
- Baylis, J., Smith, S., & Owens, P. (2019). *The globalization of world politics* (8th ed.). Oxford University Press.
- Betts, R. K. (2007). *Enemies of intelligence*. Columbia University Press.
- Bjelajac, Ž. (2017). *Bezbednosna kultura*. Univerzitet Privredna akademija.
- Bossong, R., & Rhinard, M. (2016). *Theorizing internal security co-operation in the European Union*. Oxford University Press.
- Buzan, B., & Wæver, O. (2003). *Regions and powers*. Cambridge University Press.
- Carnegie Endowment for International Peace. (2022). *Lessons learned from the Kazakhstan crisis*. <https://carnegieendowment.org/posts/2022/02/lessons-learned-from-the-kazakhstan-crisis>
- Chatham House. (2023). *How to intervene symbolically: The CSTO in Kazakhstan*. <https://www.chathamhouse.org/2023/06/how-intervene-symbolically-csto-kazakhstan>
- Collective Security Treaty Organization. (2002). *Charter of the Collective Security Treaty Organization*. <https://en.odkb-csto.org>
- Duke, S. (2019). *The European External Action Service and EU intelligence*. *Intelligence and National Security*, 34(1), 1–17.
- European External Action Service. (2020). *Intelligence Directorate of the EU Military Staff (EUMS INT)*. <https://veteransforbritain.uk>
- European Union. (2021). *EU Security Union Strategy*. <https://eur-lex.europa.eu>
- Europol. (2025). *Secure Information Exchange Network Application (SIENA)*. <https://www.europol.europa.eu>
- EUTM Mali. (2020). *European Union Training Mission in Mali*. https://www.eeas.europa.eu/eutm-mali/eutm-mali-european-union-training-mission-mali-military-mission_und_en
- Farrell, T., Rynning, S., & Terriff, T. (2013). *Transforming military power since the Cold War*. Cambridge University Press.
- Galeotti, M. (2019). *Russian political war*. Routledge.
- Gill, P. (2016). *Intelligence governance and democratisation*. Routledge.
- Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (2nd ed.). Polity Press.
- Giles, K. (2016). *Russia's 'new' tools for confronting the West*. Chatham House.
- Johnson, T. H. (2018). *Taliban narratives*. Oxford University Press.

Jovanović, M. (2020). *Ujedinjene nacije i iluzije kolektivne bezbednosti*. <https://ius.bg.ac.rs/wp-content/uploads/2020/11/ILUZIJE-KOLEKTIVNE-BEZBEDNOSTI.pdf>

Jones, S. G. (2009). *In the graveyard of empires*. W. W. Norton & Company.

Keohane, R. O. (2005). *After hegemony*. Princeton University Press.

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence*. Little, Brown and Company.

Kriendler, J. (2006). *NATO intelligence and early warning*. Conflict Studies Research Centre.

Kupchan, C. A., & Kupchan, C. (1995). *The promise of collective security*. *International Security*, 20(1), 52–61.

Kydd, A. H. (2005). *Trust and mistrust in international relations*. Princeton University Press.

Lowenthal, M. M. (2025). *Intelligence: From secrets to policy*. CQ Press.

Matić, G. D. (2025). *Informaciona bezbednost u ICT sistemima*. https://nsa.gov.rs/extfile/sr/4443/IB_IKT_sa_TP_skripta2025.pdf

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton & Company.

Mijalković, S. (2011). Obaveštajno-bezbednosne službe. *Bezbednost*, 53(1), 74–92.

Mumford, A. (2013). *Proxy warfare*. Polity Press.

NATO. (2022). *NATO Strategic Concept*. <https://www.nato.int>

NATO. (2024). *Summary of NATO's Artificial Intelligence strategy*. <https://www.nato.int>

Nomikos, J. M. (2014). *EU INTCEN analysis*. <https://www.rieas.gr/images/editorial/NomikosEUintelligence15.pdf>

Nye, J. S. (2016). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.

Opačić, M. (2005). *Reforma sistema kolektivne bezbednosti UN*. https://bezbednost.org/wp-content/uploads/2020/06/opai_m__2005__reforma_sistema_kolektivne_bezbednos.pdf

Parezanović, M. (2022). *Operacija ODKB u Kazahstanu*. *Baština*, 57. <https://scindeks-clanci.ceon.rs/data/pdf/0353-9008/2022/0353-90082257141P.pdf>

Phythian, M. (2013). *Understanding the intelligence cycle*. Routledge.

Rajić, N., & Gajić, A. (2020). Odnos ODKB sa ŠOS i NATO. *Politika nacionalne bezbednosti*, 11(1), 147–178.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*, 22(3), 283–300.

Rid, T. (2020). *Active measures*. Farrar, Straus and Giroux.

Rozanov, A. A., & Douhan, A. F. (2013). *Collective Security Treaty Organization 2002–2012*. Geneva Centre for the Democratic Control of Armed Forces.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar*. Houghton Mifflin Harcourt.

Smith, K. E. (2013). *EU foreign policy*. Polity Press.

Trbojević, M., & Malbašić, Z. (2022). *Bezbednosno-obaveštajni sistemi*. Službeni glasnik.

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.

Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Zakon o potvrđivanju konvencije UN protiv transnacionalnog organizovanog kriminala i dopunskih protokola. (2001). *Službeni list SRJ*, br. 6/2001.