

РОЗВИТОК ТА ОПЕРАТИВНЕ МИСТЕЦТВО ПОВІТРЯНИХ СИЛ

[DOI 10.33099/2786-7714-2026-1-10-5-19](https://doi.org/10.33099/2786-7714-2026-1-10-5-19)

УДК: 355.4:355.40:623.746

Габідулін Ібрагім Абдулович (кандидат технічних наук, доцент)
<https://orcid.org/0009-0009-7860-7818>

Центр досліджень армії, конверсії та роззброєння, Київ, Україна

Рукопис надійшов до редакції: 06.03.2026; Рукопис прийнято до друку після рецензування: 30.04.2026; Дата публікації: 17.06.2026

ГЕНЕЗИС ТА ЕВОЛЮЦІЯ КОНЦЕПЦІЇ A2/AD: ВІД ДЕТЕРМІНОВАНИХ СИСТЕМ ППО ДО МЕРЕЖЕЦЕНТРИЧНОГО ПРОТИБОРСТВА

У статті досліджується еволюція концепції “недопущення доступу / заперечення зони” (Anti-Access/Area Denial) та механізми її подолання у сучасних багатодомених операціях. На основі міждисциплінарного аналізу військових доктрин, теорії мережево-центричних бойових дій і сучасних операційних кейсів показано, що вирішальним чинником успіху стає не кількість платформ або вогнева міць, а рівень інтеграції сенсорів, засобів управління та систем ураження в єдину інформаційно-операційну архітектуру. Доведено, що руйнування інформаційної цілісності системи протиповітряної оборони може бути ефективнішим за її фізичне знищення. Обґрунтовано взаємозв'язок між теоретичними моделями управління в умовах інформаційної невизначеності та практичними результатами сучасних операцій. Зроблено висновок, що майбутні конфлікти визначатимуться здатністю сторін управляти інформаційним середовищем і темпом прийняття рішень, тоді як технологічна перевага виступає лише інструментом реалізації політичної стратегії.

Ключові слова: A2/AD, SEAD, DEAD, мережево-центрична війна, мережа ураження, інформаційне домінування, система управління військами, багатодоменні операції, протиповітряна оборона, бойові мережі, стратегія сучасної війни.

Вступ

Сучасний характер воєнних конфліктів визначається глибокою трансформацією співвідношення між технологіями, інформацією та управлінням. Одним із ключових феноменів цієї трансформації стала поява концепції Anti-Access/Area Denial (A2/AD), яку доцільно перекладати українською як концепція недопущення доступу та заперечення зони, що позначає системний комплекс заходів і засобів, спрямованих на обмеження свободи дій противника в операційному середовищі. Первісно сформована як асиметрична відповідь слабшої сторони на перевагу противника у проекції сили, ця концепція з часом перетворилася на універсальну модель побудови оборонних систем у різних доменах бойового простору.

У військово-теоретичному дискурсі A2/AD довгий час сприймалася як майже непроникна “зона обмеженого доступу”, подолання якої вимагало непропорційних ресурсів і ризиків. Водночас розвиток інформаційних технологій, мережових архітектур управління та алгоритмічних систем обробки даних поступово змінив уявлення про характер протиборства. З'ясувалося, що ключовою вразливістю інтегрованих оборонних систем є не їхня вогнева міць, а системна залежність від інформаційної цілісності та безперервності управління.

Актуальність дослідження зумовлена

необхідністю переосмислення ролі A2/AD у сучасній війні та визначення механізмів її подолання в умовах багатодомених операцій. Особливого значення це набуває для держав, які змушені протидіяти технологічно складним інтегрованим оборонним системам противника або, навпаки, розробляють власні інтегровані системи стримування.

Мета статті – дослідити еволюцію концепції A2/AD, виявити її системні вразливості та проаналізувати принципи сучасних операцій прориву таких систем у контексті розвитку військової теорії та практики.

Завдання дослідження:

- проаналізувати походження та розвиток концепції A2/AD;
- розглянути її місце у сучасній військовій доктрині;
- визначити роль інформаційного домінування у прориві оборонних систем;
- дослідити взаємозв'язок між технологічними, операційними та політико-стратегічними чинниками;
- сформулювати узагальнення щодо трансформації природи військової переваги.

Матеріали та методи

Дослідження ґрунтується на поєднанні теоретичного аналізу військових концепцій, аналізу відкритих джерел та порівняльного вивчення сучасних операцій протидії системам

A2/AD.

Матеріальною основою дослідження стали:

- доктринальні документи збройних сил США та НАТО, зокрема Joint Publication 3-01;
- наукові праці з теорії мережево-центричних операцій і управління бойовими системами;
- аналітичні матеріали міжнародних дослідницьких центрів (RAND, CSIS);
- відкриті джерела, що містять інформацію про перебіг сучасних військових операцій;
- публікації з питань розвитку систем протиповітряної оборони та концепції A2/AD.

У роботі використано комплекс взаємодоповнюючих методів дослідження.

Теоретичний аналіз і синтез застосовано для узагальнення існуючих підходів до розуміння концепції A2/AD та її еволюції у військовій доктрині.

Метод кейс-аналізу використано для реконструкції логіки конкретної операції прориву системи протиповітряної оборони, що дозволило дослідити взаємодію елементів SEAD/DEAD, функціонування сенсорних мереж та механізми руйнування інформаційної цілісності оборонної системи.

Порівняльний аналіз застосовано для зіставлення ієрархічних та мережевих архітектур управління бойовими системами, зокрема моделей kill chain і kill web.

Системний підхід дозволив розглядати систему A2/AD не лише як сукупність окремих засобів ураження, а як інтегровану інформаційно-керуючу структуру, у якій сенсори, канали зв'язку, центри управління та засоби ураження функціонують як єдина мережа.

Крім того, використано елементи концептуального моделювання, що дозволило інтерпретувати результати сучасних операцій у контексті теорії управління складними системами та математичних моделей деградації централізованих структур управління в умовах інформаційного перевантаження.

Поєднання зазначених методів забезпечило можливість інтегрувати доктринальний, операційний та стратегічний рівні аналізу і сформуванню цілісного уявлення про механізми подолання систем A2/AD у сучасних багатодомених операціях.

Результати

1. Концепція A2/AD як система та еволюція підходів до її подолання

1.1. Походження концепції A2/AD. Концепція A2/AD сформувалася не як абстрактна теоретична модель, а як практична відповідь на конкретний стратегічний дисбаланс періоду Холодної війни [1, 2]. Радянський Союз, усвідомлюючи свою обмежену спроможність до глобальної проєкції сили на океанських театрах у порівнянні зі Сполученими Штатами Америки, зробив ставку на асиметричні засоби стримування [3].

Сутність цього підходу полягала не у прагненні знищити авіаносні ударні групи противника, а у створенні таких умов, за яких їх застосування

ставало б надмірно ризикованим з військової та політичної точки зору [1]. Далекобійна авіація, протикорабельні ракети, ешелонувана протиповітряна оборона, розгалужена мережа радіолокаційних засобів і централізована система управління утворювали архітектуру стримування, покликану обмежити свободу дій противника ще до початку активної фази бойових дій [2].

У цьому первісному вигляді A2/AD функціонувала передусім як інструмент стратегічного стримування, а не як концепція “непроникної оборони”, що є принципово важливим для коректного розуміння її подальшої еволюції [3].

1.2. A2/AD як предмет західної військово-теоретичної дискусії. Після завершення Холодної війни концепція A2/AD не зникла, а зазнала концептуальної реконцептуалізації в західній військово-теоретичній думці, насамперед у контексті зростання військових спроможностей Китаю, Ірану та Російської Федерації [2].

У 2000–2010-х роках вона стала предметом системних досліджень і стратегічних дискусій у провідних аналітичних центрах оборонної політики, зокрема в роботах Center for Strategic and Budgetary Assessments [1], RAND Corporation [5] та International Institute for Strategic Studies [6].

У цих дослідженнях A2/AD розглядалася вже не лише як оборонна модель слабшої сторони, а як комплексна операційно-стратегічна архітектура, здатна обмежувати свободу дій навіть технологічно переважаючого противника та змінювати баланс сил на регіональному рівні [4].

1.3. Критика концепції A2/AD у військово-морській доктрині США. Важливий етап переосмислення A2/AD пов'язаний з критикою, висловленою тодішнім начальником військово-морських операцій США (Chief of Naval Operations) адміралом Джоном Річардсоном у програмному документі [7].

Він наголошував, що термін A2/AD є зручним аналітичним ярликом, але водночас небезпечним спрощенням, оскільки формує уявлення про статичну “зону заборони”, тоді як у реальності йдеться про динамічну систему взаємопов'язаних спроможностей.

Річардсон пропонував змістити фокус з питання “як прорватися в зону” на питання руйнування системи, що цю зону створює і підтримує. Такий підхід передбачав багатодоменні дії, інтеграцію морського, повітряного, кібернетичного та електромагнітного середовищ, а також цілеспрямований вплив на систему управління, розвідки та прийняття рішень противника [7].

Ця логіка стала важливим концептуальним містком між теоретичними дискусіями початку 2000-х років і подальшою доктринальною фіксацією підходів до протидії A2/AD у багатодомених операціях.

1.4. SEAD і DEAD як практичні механізми подолання A2/AD. Після того як у військово-морській і міжвидовій доктрині США було

поставлено під сумнів уявлення про А2/AD як “непроникну зону”, логічно постало питання чи не можна її подолати, а як саме це робиться на практиці. Відповіддю стали концепції SEAD і DEAD, які задовго до появи самого терміна А2/AD сформували ядро американського підходу до боротьби з протиповітряною обороною противника.

Походження термінів. Операції придушення засобів ППО активно застосовувалися вже під час війни у В’єтнамі, коли стало очевидно, що радянські зенітно-ракетні комплекси С-75 створюють якісно нову загрозу для авіації [8]. Сам термін SEAD (Suppression of Enemy Air Defenses) сформувався у 1970-х роках у процесі доктринального осмислення бойового досвіду.

Початково SEAD означав тимчасове придушення елементів ППО – шляхом радіоелектронної боротьби, вогневого ураження, демонстративних маневрів і примусу розрахунків ЗРК до вимкнення радарів. Його стандартизоване визначення закріпилося в американських та натівських нормативних документах і сьогодні визначається як комплекс дій із нейтралізації, тимчасового приглушення або знищення засобів протиповітряної оборони противника [9].

Надалі, у 1980–1990-х роках, у професійній військовій літературі США з’являється більш жорстке поняття DEAD (Destruction of Enemy Air Defenses) – фізичне знищення елементів системи ППО: радарів, пускових установок, командних пунктів і вузлів зв’язку. Якщо SEAD мав на меті “осліпити” оборону на певний час, то DEAD – вивести її з ладу структурно.

У сучасній американській доктрині ці поняття розглядаються не як альтернативні, а як взаємодоповнюючі фази єдиного процесу [9].

Доктринальне закріплення. У документі *Joint Publication 3-01 Countering Air and Missile Threats* SEAD і DEAD зафіксовані як складові системної боротьби з повітряними й ракетними загрозами [9]. Документ прямо виходить з того, що сучасна протиповітряна оборона є мережевою системою, а отже її нейтралізація потребує:

- порушення сенсорного рівня (радіолокація, оптико-електронні засоби);
- руйнування або дезорганізації системи управління і зв’язку (С2);
- фізичного ураження ключових вузлів у критичні моменти.

Таким чином, SEAD і DEAD у доктрині США – це інструменти розриву kill chain противника, що безпосередньо пов’язує їх із критикою А2/AD як статичної “бульбашки” [11].

Історичний досвід застосування. Класичним прикладом ефективного застосування SEAD/DEAD стала кампанія НАТО проти Югославії у 1999 році, детально проаналізована Бенджаміном Лембетом [12]. Попри обмежені масштаби фізичних втрат, сербська ППО була позбавлена можливості діяти як єдине ціле, що забезпечило коаліції повну свободу дій у повітрі.

Цей досвід закріпив ключовий висновок:

знищення всієї ППО не є необхідною умовою повітряного панування – достатньо зруйнувати її зв’язність, керованість і передбачуваність.

Логічний перехід до Каракаса. Саме в цій логіці слід розглядати і події в Каракасі у 2026 році. Операція “Absolute Resolve” [13, 14, 15] продемонструвала класичну послідовність SEAD → DEAD:

- спочатку – радіоелектронне “осліплення” і дезорганізація сенсорів;
- далі – точкове фізичне ураження активованих елементів;
- у підсумку – розпад системи ППО як єдиного механізму.

Це дозволяє перейти до наступного підрозділу – аналізу того, як саме kill chain венесуельської ППО була зламана і чому наступаюча сторона діяла вже в логіці kill web, що принципово змінює характер протиборства.

1.5. Kill chain і kill web: структурна вразливість А2/AD. Однією з ключових причин провалу венесуельської системи А2/AD стала асиметрія логік управління бойовими діями, що проявилася у зіткненні двох різних моделей ураження: kill chain та kill web.

Концепція kill chain як послідовної моделі ураження сформувалася в межах розвитку американської військової доктрини та передбачає лінійну послідовність дій – від виявлення до ураження цілі (Find-Fix-Track-Target-Engage-Assess). У мережево-центричному вимірі ця модель описується як функціонально зв’язаний ланцюг сенсорів, командних пунктів і засобів ураження [9, 10].

Мережева модель ураження, kill web або battle networks, розвинулася як еволюція мережевоцентричних підходів у багатодомених операціях і передбачає множинність шляхів передачі інформації та прийняття рішень [16, 10]. На відміну від kill chain, вона не потребує жорсткої послідовності та має надлишкові канали обробки даних, що забезпечує стійкість до втрати окремих елементів.

Традиційна архітектура протиповітряної оборони, на якій ґрунтувалася оборона Каракаса, відповідала логіці kill chain – лінійного ланцюга ураження з централізованим управлінням [3]. Така модель характерна для індустріальної епохи війни й передбачає жорстку залежність між сенсорами, командними пунктами та ефекторами.

У венесуельському випадку ця логіка проявлялася у зв’язці:

- китайських радарів метрового діапазону JY-27,
- централізованих пунктів управління,
- зенітно-ракетних комплексів С-300 [13, 14].

Порушення будь-якого з ключових елементів цього ланцюга – передусім сенсорного або командного – призводило до розриву всієї системи ураження. Саме це і було досягнуто на етапі SEAD шляхом радіоелектронного впливу на радіолокаційні засоби, що позбавило ЗРК можливості отримувати цілевказання. Подальші

дії DEAD завершили руйнування цієї архітектури шляхом фізичного знищення активних вузлів.

На противагу цьому, атакуюча сторона діяла у логіці kill web – мережевої моделі ураження, що є розвитком мережевоцентричної війни [10, 16]. У такій моделі:

- сенсори, платформи управління та засоби ураження не мають жорсткої ієрархії;
- інформація агрегується з багатьох джерел;
- рішення можуть ухвалюватися децентралізовано;
- втрата окремого вузла не призводить до деградації всієї системи.

У ході операції Absolute Resolve цю логіку забезпечували:

- багатоцільові літаки F-35 як багатоспектральні сенсори,
- розвідувальні БПЛА, зокрема RQ-170 Sentinel [17-19],
- платформи радіоелектронної боротьби,
- інтегровані системи злиття даних і управління типу Lattice [20, 21].

Таким чином, навіть у разі втрати окремих сенсорів або каналів зв'язку загальна картина бою зберігалася, а система управління залишалася функціонально стійкою.

Зіткнення kill chain та kill web у Каракасі продемонструвало принципову обмеженість класичних A2/AD-архітектур, побудованих на централізованому управлінні. Система ППО виявилася вразливою не через нестачу засобів ураження, а через структурну нездатність зберегти цілісність управління в умовах багатодоменного впливу.

Саме цей структурний фактор пояснює швидкий колапс венесуельської системи A2/AD після початку операції.

2. Практичне подолання A2/AD: кейс Венесуели.

2.1. Передопераційне середовище та підготовка кампанії. Як показано в попередньому розділі, структурна вразливість централізованих A2/AD-архітектур проявляється насамперед у сфері управління та інформаційної цілісності. Тому практичне подолання таких систем починається задовго до першого кінетичного удару.

Фундаментом операції є формування операційного середовища, у якому противник поступово втрачає здатність діяти як інтегрована система. Йдеться не лише про розвідувальну підготовку, а про комплекс дипломатичних, інформаційних, економічних і психологічних заходів, спрямованих на ізоляцію цілі та зниження стійкості її військової структури.

Такий підхід відповідає принципам загальної (тотальної) стратегії, сформульованим Андре Бофром [22], згідно з якими військова дія має завершувати процес, уже підготовлений політичними, інформаційними та психологічними інструментами впливу. У цьому сенсі кінетична фаза операції є не початком, а кульмінацією довготривалої системної кампанії.

У випадку Венесуели підготовчий етап включав поступове формування сприятливого міжнародного середовища, інформаційний тиск, демонстрацію сили та розгортання розвідувальних можливостей, що дозволило перейти до активної фази вже за умов частково дезорганізованої системи управління [13, 14].

2.2. Фаза SEAD: дезінтеграція сенсорного поля A2/AD. Першою військовою фазою подолання системи A2/AD є не знищення засобів противника, а позбавлення їх здатності бачити та координуватися. У доктринальних документах Збройних Сил США цей етап визначається як SEAD – придушення систем протиповітряної оборони шляхом впливу на їхні сенсори, канали зв'язку та систему управління [9].

Згідно з положеннями [9], SEAD передбачає комплекс дій, спрямованих на тимчасове або часткове виведення елементів ППО з функціонального стану, не обов'язково їх фізичне знищення. Йдеться насамперед про порушення інформаційної цілісності системи – саме того елементу, на якому тримається будь-яка архітектура A2/AD.

У випадку венесуельської операції ключовою ціллю першої фази стало сенсорне поле протиповітряної оборони, зокрема далекобійні радіолокаційні станції, що забезпечували дальнє виявлення та цілевказання зенітним ракетним комплексам [13, 14].

Порушення їхньої роботи призводить до системного ефекту:

- розривається інформаційний зв'язок між сенсором і пусковою установкою;
- руйнується ланцюг прийняття рішення;
- кожна батарея ППО змушена діяти ізольовано;
- система втрачає властивість цілісності.

Саме в цьому проявляється фундаментальна відмінність між знищенням засобу і знищенням системи. Зенітний комплекс може залишатися фізично неушкодженим, але без сенсорного поля та мережевої координації він перетворюється на локальний автономний вузол із різко зниженими можливостями.

Такий ефект відповідає логіці оперативного мистецтва, сформульованій у класичній стратегічній теорії [22], згідно з якою найефективніший спосіб зламати оборону полягає не в її фізичному руйнуванні, а в позбавленні противника свободи організованої дії. Як зазначав Андре Бофр, стратегія прагне позбавити противника свободи дії.

У практичному вимірі це означає перехід від класичної моделі протидії ППО – прямого знищення позицій – до моделі інформаційного осліплення системи. Саме тому в сучасних операціях SEAD дедалі частіше реалізується засобами радіоелектронної боротьби, кібероперацій та багатодоменного впливу, тоді як кінетичні удари здійснюються після втрати системою здатності до скоординованої реакції [9, 10].

У практичному вимірі це означає перехід від класичної моделі протидії ППО – прямого знищення позицій – до моделі інформаційного осліплення системи. Саме тому в сучасних операціях SEAD дедалі частіше реалізується засобами радіоелектронної боротьби, кібероперацій та багатодоменного впливу, тоді як кінетичні удари здійснюються після втрати системою здатності до скоординованої реакції [9, 10].

У розглянутій операції ключову роль відіграла інтегруюча цифрова архітектура управління бойовим середовищем типу Lattice [20, 21], яка забезпечувала зведення даних від розрізнених сенсорів у єдину оперативну картину.

Основними пасивними сенсорами виступали малопомітні літаки F-35, оснашені комплексом радіоелектронної розвідки AN/ASQ-239, що дозволяє визначати координати радіолокаційних станцій за їхнім випромінюванням без увімкнення власного радара [17].

Наступною ланкою були літаки радіоелектронної боротьби EA-18G Growler, які здійснювали спрямоване придушення сигналів радіолокаційних станцій. Для операторів ППО це означало втрату достовірної повітряної обстановки та неможливість формування цілевказання.

Після дезорганізації сенсорного поля координати передавалися ударним платформам (B-1B, F/A-18), які застосовували високоточні засоби ураження великої дальності, зокрема ракети AGM-158 JASSM. Таким чином реалізовувався принцип сучасної операційної війни: кінетичний удар наноситься лише після втрати противником системної здатності реагувати як єдине ціле.

2.3. Мережево-центричний контур управління операцією. Ключовою передумовою ефективності операції стало не лише технічне переважання засобів ураження, а наявність інтегрованого інформаційно-управлінського контуру, що об'єднував сенсори, аналітичні модулі та виконавчі платформи в єдину систему.

Така архітектура відповідає концепції мережевоцентричної війни (network-centric warfare), описаній у фундаментальній праці [10], де підкреслюється, що вирішальною перевагою сучасних сил є не кількість платформ, а рівень інформаційної інтеграції між ними.

У межах цієї логіки сенсорні системи – стелс-авіація, розвідувальні БпЛА, космічні засоби спостереження та радіоелектронна розвідка – формують єдине поле даних, яке в реальному часі обробляється алгоритмічними системами підтримки рішень і передається засобам ураження [9, 10].

Подібна архітектура отримала в сучасній військовій теорії назву мережі ураження (kill web) [16]. На відміну від класичного “ланцюга ураження” (kill chain), де кожна ланка жорстко залежить від попередньої, у мережевій моделі втрата окремого сенсора або платформи не призводить до руйнування системи в цілому,

оскільки функціональність автоматично перерозподіляється між іншими елементами мережі.

Саме така логіка забезпечує стійкість операцій у середовищі інформаційного протиповітряного протидії, де противник активно застосовує засоби радіоелектронного впливу та кібероперації. У цьому сенсі сучасна операція придушення ППО є не просто застосуванням високоточної зброї, а результатом функціонування складної кібернетичної системи управління боєм [11].

2.4. Фаза DEAD: фізична нейтралізація елементів системи A2/AD. Після досягнення інформаційної переваги та дезінтеграції сенсорного поля противника логічним продовженням операції стала фаза DEAD – безпосереднє фізичне знищення елементів системи протиповітряної оборони. На відміну від етапу SEAD, метою якого є тимчасове придушення функціонування ППО, фаза DEAD передбачає остаточну ліквідацію ключових вузлів оборонної архітектури, включаючи радіолокаційні станції, пускові установки, командні пункти та засоби зв'язку [9].

У доктринальному вимірі цей етап розглядається як завершальна стадія боротьби за домінування в повітрі, коли противник уже позбавлений здатності координувати оборону та змушений діяти фрагментарно [9]. Ефективність DEAD визначається не кількістю нанесених ударів, а точністю вибору моменту їх застосування – тобто тоді, коли система управління ППО вже втратила функціональну цілісність.

У розглянутій операції ця логіка проявилася у класичній формі: після дезорганізації інформаційного поля оборони радіолокаційні комплекси, що періодично активувалися для уточнення обстановки, автоматично ставали демаскуючими цілями. Будь-яке випромінювання сенсора миттєво фіксувалося засобами пасивної радіотехнічної розвідки і використовувалося для наведення високоточної зброї [13].

Подібна схема відповідає принципам багатодомених операцій: сенсор, система обробки даних і засіб ураження функціонують як інтегрована система [10]. За таких умов навіть короткочасне включення радара може призводити до втрати позиції через її технічне самовикриття.

За наявними відкритими оцінками, у фазі фізичного знищення елементів оборони могли застосовуватися високоточні боеприпаси повітряного базування великої дальності, що запускалися з платформ, розташованих поза зоною ураження зенітних ракетних комплексів [13, 23]. Такий підхід мінімізує ризики для ударної авіації та дозволяє проводити системне “розбирання” оборонної архітектури противника без входження у зону його вогневого впливу.

Ключовим наслідком цього етапу стало перетворення формально багаторівневої системи протиповітряної оборони на набір ізольованих, неузгоджених елементів. Втрата зв'язку між сенсорами, командними пунктами та пусковими

установками означала фактичний розрив класичного ланцюга ураження (kill chain) оборонної сторони [10]. Натомість атакуюча сторона діяла в рамках мережі ураження (kill web) [16], що забезпечувало їй структурну стійкість навіть у разі втрати окремих платформ або каналів зв'язку.

Таким чином, фаза DEAD не була самостійною операцією, а стала закономірним результатом попереднього руйнування інформаційної цілісності оборонної системи. Саме послідовність “дезорганізація → ізоляція → знищення” демонструє сучасну логіку подолання A2/AD-архітектур, де вирішальну роль відіграє не масованість удару, а системність впливу.

2.5. Домінування в повітрі як операційний перелом. Досягнення домінування в повітрі історично вважається ключовою умовою успішного ведення сучасних операцій. У доктринальних документах США воно визначається як такий ступінь контролю повітряного простору, за якого противник не здатний ефективно перешкоджати діям власних сил [9]. Саме цей стан означає не просто перевагу в повітрі, а втрату противником можливості впливати на перебіг операції як системою.

У розглянутому кейсі перелом настав не в момент першого удару, а тоді, коли оборонна система втратила здатність формувати узгоджену повітряну обстановку. Після руйнування сенсорного поля та фізичного знищення ключових вузлів ППО противник опинився в ситуації інформаційної деградації. Засоби виявлення та управління більше не забезпечували цілісного контролю повітряного простору, що означало фактичну втрату ініціативи в повітрі.

Такий момент відповідає класичним принципам оперативного мистецтва: перелом досягається не тоді, коли противник повністю знищений, а тоді, коли він втрачає можливість організовано діяти. Саме тому сучасні концепції подолання A2/AD роблять акцент не на масованості ударів, а на послідовному руйнуванні функціональних зв'язків системи [1].

Водночас досягнуте домінування в повітрі не є статичним станом. У багатодоменному середовищі воно підтримується безперервною роботою сенсорів, систем управління та засобів ураження, інтегрованих у мережеву архітектуру [10]. Отже, домінування – це не одноразова подія, а динамічний процес, який залежить від здатності сторони підтримувати безперервність інформаційного циклу “спостереження, орієнтації, рішення та дії” (Observe–Orient–Decide–Act, OODA) [24].

У сучасних дослідженнях оперативного мистецтва, що аналізують бойові мережі (battle networks), підкреслюється, що саме інформаційна цілісність виступає центром ваги системи [16]. Втрата цієї цілісності означає системну деградацію, навіть якщо частина засобів ураження формально зберігається.

Таким чином, у межах цієї операції

домінування в повітрі стало не наслідком чисельної або технічної переваги, а результатом правильно вибудованої послідовності дій:

дезінтеграція сенсорів → руйнування управління → ізоляція вузлів → точкове знищення.

Саме така логіка дедалі частіше визначає характер сучасних кампаній і пояснює, чому навіть складні багаторівневі системи оборони можуть втрачати ефективність за відносно короткої строки.

2.6. Операція як модель сучасного прориву A2/AD. Розглянута операція демонструє принципово важливу зміну у способах подолання систем A2/AD. Якщо у традиційній військовій думці прорив оборони асоціювався з концентрацією сил і масованим ударом, то сучасна практика підтверджує іншу закономірність: ефективність досягається через дезорганізацію системи управління противника, а не через фронтальне знищення його засобів.

Ключовим фактором стала інтеграція сенсорів, засобів РЕБ, платформ ураження і командних систем у єдину бойову мережу [9, 10]. Саме така архітектура дозволила здійснювати дії не послідовно, а паралельно, що різко скорочує цикл прийняття рішень і створює ефект операційної асиметрії. У результаті сторона, яка діяла в мережевій логіці, нав'язала противнику темп подій, з яким той не зміг синхронізувати свої реакції.

Цей висновок узгоджується з положеннями сучасної теорії оперативного мистецтва, згідно з якою вирішальним фактором стає здатність інтегрувати дії в різних доменах у єдиний інформаційний цикл [16]. У такій системі навіть складна оборонна архітектура може втратити стійкість, якщо порушується взаємодія її елементів.

Принципове значення має також різниця в логіці функціонування систем. Оборонна сторона діяла у межах класичного kill chain – структурованого ланцюга прийняття рішень. Натомість наступальна сторона застосовувала архітектуру kill web – розподілену мережу, здатну адаптуватися до втрат окремих вузлів [10, 16]. Саме ця різниця пояснює, чому навіть часткове порушення каналів зв'язку спричинило системну деградацію оборони.

Таким чином, операція підтверджує кілька фундаментальних закономірностей сучасної війни:

- інформаційна перевага набуває більшого значення, ніж суто платформна;
- швидкість інтеграції систем перевищує за значенням концентрацію маси сил;
- мережеві структури демонструють вищу стійкість порівняно з жорстко ієрархічними;
- руйнування контурів управління часто є ефективнішим, ніж пряме знищення бойових засобів.

У сукупності це дозволяє трактувати розглянутий кейс не як ізольований епізод, а як прояв тенденції формування нового типу операцій,

у яких головним об'єктом впливу стає система прийняття рішень противника.

Саме тому подібні операції дедалі частіше розглядаються у військовій теорії як модель майбутніх кампаній проти складних багаторівневих оборонних систем.

3. Стратегічні уроки сучасних операцій прориву A2/AD

3.1. Трансформація природи воєнної переваги. Розглянутий кейс свідчить про трансформацію природи військової переваги у сучасних конфліктах. Якщо в класичній військовій теорії вирішальним фактором вважалася кількісна концентрація сил або технологічна перевага окремих засобів ураження, то сучасні операції демонструють зростання ролі системної інтеграції [3, 10].

У межах індустріальної моделі війни перевага асоціювалася з масою сил, дальністю ураження та гарантованою відповіддю. Проте в умовах мережево-центричного протиборства визначальним чинником стає здатність об'єднати сенсори, системи управління, засоби впливу та аналітичні алгоритми в єдиний операційний контур [10].

Таким чином, перевага поступово зміщується від окремої платформи до архітектури взаємодії. Система, що забезпечує швидке злиття даних, скорочений цикл прийняття рішень і адаптивність у багатодомному середовищі, отримує структурну перевагу навіть за відсутності абсолютної технічної домінації.

У таких умовах навіть технологічно потужна оборонна система може втратити ефективність, якщо вона не здатна підтримувати інформаційну цілісність та стійкість управління [11]. Саме тому у сучасній військовій думці дедалі частіше наголошується, що центром ваги стає не фізичний компонент сил, а здатність системи підтримувати безперервність інформаційного циклу.

3.2. Від платформи до мережі: нова логіка сили. Порівняльний аналіз показує, що традиційна модель бойових дій базувалася на концепції платформи – танка, літака, корабля як основної одиниці сили.

Натомість сучасна війна переходить до мережевої логіки, у якій платформа є лише вузлом системи [10, 11]. Вирішального значення набуває не ізольована бойова спроможність окремого засобу, а його включеність у єдиний інформаційно-управлінський контур.

У межах мережевої архітектури:

- знищення окремої платформи не призводить до руйнування системи в цілому;
- функції можуть перерозподілятися між вузлами;
- управління набуває розподіленого характеру;
- швидкість реакції зростає завдяки інформаційній синхронізації [10].

Це підтверджує висновок сучасної теорії мережевоцентричних операцій: бойова ефективність визначається не кількістю сил, а якістю зв'язків між ними [10, 24]. Саме

взаємозв'язки, а не окремі платформи, стають головним джерелом переваги, оскільки дозволяють скорочувати цикл “спостереження – орієнтації – прийняття рішення – дії” (OODA) [24].

Практичним доктринальним втіленням цієї логіки є концепція Joint All-Domain Command and Control (JADC2) – інтегрованої системи міжвидового управління, що об'єднує сенсори, командні центри та засоби ураження у всіх доменах бойового простору (повітряному, наземному, морському, космічному та кіберпросторі) в єдину інформаційно-керуючу мережу [25]. Її мета полягає у забезпеченні переваги в швидкості прийняття рішень та формуванні спільної операційної картини, що дозволяє синхронізувати дії різнорідних сил у реальному часі.

У цьому контексті платформа перестає бути основним елементом сили й перетворюється на модуль у ширшій системі управління.

3.3. Пріоритет інформаційного домінування. Події засвідчили, що ключовим об'єктом боротьби стає інформаційне середовище бою. Контроль над інформацією дозволяє:

- формувати картину бойової обстановки;
- прогнозувати поведінку противника;
- скорочувати цикл прийняття рішень;
- випереджувати противника в темпі операції [11, 6].

У цьому контексті актуалізується класичний принцип стратегічної теорії, сформульований Лідделлом Гартом: “Стратегія прагне позбавити противника свободи дій” [26]. Сучасна інтерпретація цього положення пов'язана не лише з фізичним обмеженням маневру, а й із порушенням здатності противника адекватно сприймати обстановку та приймати узгоджені рішення.

У мережевоцентричному середовищі такий ефект досягається шляхом дезорганізації інформаційних потоків, порушення сенсорних мереж, перевантаження або фрагментації каналів управління, а також створення когнітивної невизначеності [11]. У результаті інформаційна дезінтеграція системи управління може виявитися ефективнішою, ніж її пряме фізичне руйнування.

Це узгоджується з ширшим теоретичним висновком сучасної військової науки: контроль над інформацією трансформується у форму стратегічної сили. За певних умов саме здатність підтримувати інформаційну цілісність і скорочувати власний цикл рішень може нейтралізувати навіть технологічно сильнішого противника [24, 10].

Отже, інформаційне домінування поступово переходить із допоміжного елемента бойових дій у категорію їх центральної умови.

3.4. Політико-стратегічний вимір операцій. Операції сучасного типу мають не лише військовий, а й стратегічно-політичний вимір. Як підкреслював Андре Бофр, війна є передусім боротьбою волі, а не матеріальних ресурсів [22]. З цього випливає фундаментальний висновок: навіть

найуспішніша військова операція не гарантує досягнення стратегічної мети, якщо вона не підкріплена політичними, дипломатичними, інформаційними та економічними заходами [22, 27].

Аналіз сучасних кампаній демонструють кілька закономірностей:

- темп і швидкість військової фази істотно впливають на формування стратегічного результату [27];
- легітимність підсумку може мати більше значення, ніж масштаб тактичного успіху [22];
- міжнародна реакція здатна змінити баланс сил після завершення операції [9];
- рівень внутрішньої підтримки суспільства визначає стійкість досягнутого результату [26].

Таким чином, військовий успіх виступає лише одним елементом ширшої системи стратегічної дії. Якщо він не інтегрований у загальну політичну архітектуру післяопераційного врегулювання, тактична перемога може не трансформуватися у стабільний стратегічний результат.

Цей висновок узгоджується з класичною стратегічною логікою: ефективна стратегія – це не максимізація руйнування, а досягнення бажаного політичного стану з мінімально необхідним застосуванням сили [26]. Саме тому сучасні високотехнологічні операції доцільно оцінювати не лише за показниками бойової ефективності, а й за їх здатністю формувати керований політичний результат.

3.5. Значення для розвитку військової теорії. З наукової точки зору розглянутий кейс становить інтерес як емпіричний матеріал для перевірки низки теоретичних положень, що тривалий час існували переважно у вигляді концептуальних моделей або аналітичних припущень у дослідженнях мережево-центричних операцій та систем A2/AD.

По-перше, аналіз свідчить про переваги мережевої організації бойових систем над жорстко ієрархічною. Система, побудована як розподілена мережа взаємопов'язаних вузлів, демонструє вищу стійкість до втрат окремих елементів, ніж централізована структура управління. Цей висновок узгоджується з положеннями теорії мережево-центричних операцій, відповідно до якої бойова ефективність визначається рівнем інформаційної інтеграції, а не лише кількістю сил або характеристиками окремих платформ [11, 28].

По-друге, спостерігається підтвердження тези про те, що інформаційна перевага здатна частково нівелювати технічну. Навіть складні системи протиповітряної оборони можуть втрачати ефективність якщо порушується цілісність їх інформаційного контуру, тобто зв'язок між сенсорами, центрами управління і засобами ураження [11, 29].

По-третє, помітно зростає роль швидкості інтеграції систем. В умовах сучасного бою вирішальним чинником стає не максимальна дальність ураження або потужність окремої платформи, а здатність системи швидко збирати,

обробляти та передавати інформацію між вузлами мережі. У цьому сенсі темп інформаційного циклу безпосередньо трансформується у темп операції [6, 11].

По-четверте, розглянутий кейс узгоджується з принципом, сформульованим у класичній стратегічній теорії: дезорганізація системи противника може бути ефективнішою за її пряме фізичне знищення. Руйнування структур управління, сенсорних полів і каналів зв'язку здатне призвести до колапсу всієї бойової архітектури навіть за збереження значної частини матеріальних ресурсів [25, 30].

Отже, подібні операції мають значення не лише як приклади військового планування, але й як джерело емпіричного матеріалу для розвитку сучасної військової теорії. Вони дозволяють уточнювати моделі функціонування бойових систем, поглиблювати розуміння інформаційного виміру війни та вдосконалювати підходи до підготовки командного складу.

3.6. Теоретична верифікація мережево-центричної переваги: кореляція математичної моделі та бойової практики. Особливу наукову цінність для аналізу сучасних операцій прориву A2/AD становить зіставлення емпіричних результатів бойових дій із теоретичними моделями управління складними системами. У цьому контексті показовою є концептуальна відповідність між практичними наслідками досліджуваної операції та результатами дослідження Шовкошитного і Василенка, присвяченого ураженню нестационарних групових цілей [31].

У зазначеній роботі показано, що в умовах інформаційної невизначеності та динамічного середовища ієрархічні системи управління можуть демонструвати різке зниження ефективності після перевищення певного порогу інформаційного навантаження на вузли прийняття рішень. Ключовим фактором виступає не фізичне знищення елементів системи, а перевантаження каналів обробки даних, що призводить до втрати узгодженості між її складовими.

Аналіз емпіричних подій демонструє подібну закономірність. Під впливом радіоелектронних перешкод інтегрована система протиповітряної оборони перестає функціонувати як стабільна оборонна структура і переходить у режим нестійкої інформаційної системи. Радари працюють імпульсно, сигнали змінюють характеристики, канали зв'язку стають нестабільними, а операційна картина повітряної обстановки втрачає достовірність.

За таких умов система фактично набуває характеристик об'єкта, який у теоретичній моделі описується як нестационарна групова ціль. Це створює ситуацію, коли порушення інформаційних зв'язків між елементами системи призводить до її швидкої функціональної деградації.

Порівняльний аналіз дозволяє виявити структурну асиметрію протиборчих систем. Оборонна архітектура, побудована за ієрархічним

принципом, виявляється вразливою до інформаційного перевантаження, тоді як мережево-центрична система з розподіленим управлінням зберігає функціональність завдяки можливості перерозподілу ролей між вузлами.

Методологічно така відповідність має принципове значення. Вона свідчить про конвергенцію результатів, коли математичне моделювання та емпіричний аналіз бойових дій приводять до подібних висновків щодо закономірностей функціонування складних військових систем.

Отже, результати дослідження Шовкошитного та Василенко можна розглядати як теоретичну інтерпретацію механізмів деградації ієрархічних систем управління під впливом інформаційного перевантаження, тоді як розглянутий кейс демонструє можливу практичну реалізацію подібних процесів на операційному рівні.

3.7. *Методичні наслідки для підготовки офіцерів.* Аналіз сучасних операцій подолання систем А2/AD демонструє закономірність, яка має важливе значення для викладання оперативного мистецтва та теорії управління військами. Ефективність бойових систем визначається не лише технічними характеристиками озброєння, а насамперед архітектурою інформаційної взаємодії між елементами системи. Практика сучасних операцій узгоджується з висновками математичних моделей управління складними системами: після перевищення певного порогу інформаційного навантаження централізовані структури втрачають керованість швидше, ніж мережеві.

З педагогічної точки зору це означає необхідність зміщення акцентів підготовки офіцерів від платформи-орієнтованого мислення до системного розуміння бойового простору як інтегрованої мережі сенсорів, засобів управління та засобів впливу. Саме такий підхід дозволяє майбутнім командирам адекватно оцінювати характер сучасної війни та приймати рішення у умовах інформаційної нестабільності.

Таблиця №1

Порівняльні характеристики ієрархічних та мережевих систем управління

Критерій	Ієрархічна система управління	Мережева система управління
Архітектура	Централізована вертикаль	Розподілена мережа вузлів
Стійкість до втра	Критична залежність від вузлів управління	Висока живучість через резервування функцій
Швидкість реакції	Обмежена швидкістю передачі команд	Висока завдяки паралельній обробці
Адаптивність	Низька, зміни потребують централізованих рішень	Висока, вузли можуть перебирати функції
Вразливість до РЕБ	Висока – порушення зв'язку	Нижча – мережа перебудовується

	руйнує систему	
Масштабованість	Обмежена структурою	Практично необмежена
Поведінка в умовах невизначеності	Деградація управління	Самоорганізація системи
Тип переваги	Платформна	Архітектурна
Операційна логіка	Лінійна (kill chain)	Нелінійна (kill web / бойова мережа ураження)
Стратегічна ефективність	Залежить від чисельності сил	Залежить від якості інтеграції



Рисунок 1. Порівняльна схема моделей kill chain та kill web

Проміжний висновок розділу. Аналіз сучасних операцій прориву систем А2/AD демонструє якісну трансформацію характеру воєнної переваги. Вирішальним фактором стає не сама по собі вогнева міць або кількість платформ, а здатність сторони створювати, підтримувати та захищати інтегроване інформаційне середовище бойових дій. Перевага поступово переходить від окремих засобів ураження до архітектури їх взаємодії.

У таких умовах навіть технічно потужна оборонна система може втратити ефективність, якщо порушується її інформаційна цілісність або деградує швидкість прийняття рішень. Таким чином, сучасні конфлікти дедалі більше набувають характеру боротьби за контроль над інформаційним середовищем поля бою.

4. *Політико-стратегічні наслідки операцій прориву А2/AD*

Технічна картина подолання системи А2/AD – включаючи застосування фаз SEAD/DEAD, руйнування ланцюга ураження (kill chain) та перевагу мережевої архітектури над ієрархічною – набуває стратегічного значення лише тоді, коли вона інтегрована у політичну логіку операції та підпорядкована чітко визначеному кінцевому стану.

У військово-стратегічній теорії війна розглядається не як змагання масштабів руйнування, а як боротьба волі [22], у межах якої удари по критичних системах управління та символах влади спрямовані насамперед на зміну поведінки противника та підрив його здатності до організованого опору.

4.1. *Соціально-політичний вимір стратегії: боротьба волі.* Військово-операційний успіх має

стратегічну цінність лише тоді, коли він інтегрований у ширшу політичну логіку. Як наголошував Андре Бофр, війна є не змаганням руйнувань, а змаганням волі; саме здатність впливати на волю противника визначає результат конфлікту [22]. Ця класична теза підтверджується сучасною стратегічною аналітикою: військова стратегія спрямована на використання ресурсів так, щоб зменшити волю противника до опору та забезпечити досягнення політичних цілей.

У венесуельському кейсі ключовим чинником стала не лише деградація системи ППО, а психологічний ефект демонстрації вразливості центру влади. Дослідник цивільно-військових відносин Джон Полга-Хечимовіч зазначає [32], що стійкість режиму Мадуро значною мірою ґрунтувалася на механізмах так званого “захисту від переворотів” (coup-proofing). Такі механізми передбачають тісне переплетення політичних та військових еліт, унаслідок чого збройні сили стають інструментом підтримки режиму, а не автономним державним інститутом.

Аналітична стаття [33] попереджає, що навіть успішне усунення авторитарного лідера не гарантує демократичного результату: після падіння персоналістського режиму можуть зберігатися силові та клієнтельні мережі попереднього режиму, створюючи ризик “керованого авторитаризму”, а не інституційної трансформації.

Аналітик Майкл Шуркін [34] у своїх лекційних матеріалах з військової стратегії також наголошує, що військові операції мають сенс лише як елемент цілісної політичної стратегії, де дипломатичні, інформаційні й економічні інструменти є невід’ємними складовими стратегії поряд із військовими діями. Без цієї інтеграції навіть блискавичні перемоги не дають стійкого результату.

4.2. Руйнування ілюзії безпеки як стратегічний ефект. У випадку досліджуваної операції ключовим результатом стало не лише ураження сенсорних елементів ППО, а підлив базового припущення керівництва режиму щодо захищеності центру влади. Це означає руйнування психологічного базису системи стримування. Коли система оборони перестає гарантувати безпеку столиці або стратегічних активів, політична структура режиму може почати втрачати стійкість навіть за наявності значного залишкового військового потенціалу.

Це підтверджує тезу стратегічної теорії: вирішальним є не фізичне знищення сил, а психологічний перелом у противника, який змушує його відмовитися від продовження боротьби [22].

4.3. Соціально-економічна мотивація військових еліт. Аналіз поведінки військового керівництва свідчить, що стійкість режиму значною мірою залежить від характеру мотивації офіцерського корпусу. Якщо лояльність базується не на ідеологічних переконаннях чи національній ідентичності, а на доступі до економічних

ресурсів, то втрата гарантій їх збереження може швидко зруйнувати готовність до опору [32].

У такій ситуації технологічна перевага противника виступає каталізатором політичної дестабілізації, але не його першопричиною. Вона лише активує внутрішні слабкості системи.

4.4. Пастка післяопераційної стабілізації. Операційний успіх не тотожний стратегічній перемозі. Усунення політичного керівництва режиму не означає автоматичного демонтажу його інституційної структури. Апарат безпеки, економічні мережі, адміністративна вертикаль і зовнішні союзники можуть зберегтися та трансформуватися в нову форму керованої авторитарності [32].

Це створює стратегічну пастку: швидка військова перемога здатна породити довготривалу нестабільність, якщо не забезпечено політичні, дипломатичні та інституційні умови для стабілізації після завершення операції.

4.5. Узагальнення стратегічного рівня. Проведений аналіз дозволяє сформулювати такі стратегічні закономірності:

- технологічна перевага виступає інструментом реалізації стратегії, а не самодостатньою умовою перемоги;
- швидкість військової фази має стратегічний сенс лише за наявності чіткої політичної мети та плану післяопераційної стабілізації;
- легітимність результату важливіша за масштаб ураження;
- внутрішня мотивація суспільства та еліт визначає довгострокову стійкість результатів операції.

У цьому контексті сучасні операції прориву A2/AD слід розглядати не лише як технологічний або оперативний феномен, а як інтегроване стратегічне явище, де військові дії, інформаційний вплив і політична логіка становлять єдину систему.

4.6. Порівняльний контекст: технологія проти волі. Порівняння з досвідом сучасних воєнних конфліктів демонструє принципову закономірність: технологічна перевага не гарантує перемоги, якщо противник має високу мотивацію до опору. Навпаки, навіть обмежені матеріальні ресурси можуть частково компенсуватися високим рівнем суспільної консолідації та екзистенційною мотивацією до опору.

Водночас планування подібних операцій потребує врахування внутрішньополітичної структури противника. Історичний досвід демонструє, що навіть технологічно успішні військові кампанії можуть призводити до стратегічної нестабільності, якщо не враховано характер суспільної підтримки режиму, конфігурацію еліт та потенціал внутрішньої консолідації. У таких умовах військовий успіх не гарантує формування стабільного політичного порядку після завершення бойових дій.

Отже, справжня стратегічна “зона заборони доступу” може формуватися не лише системами озброєння, а й моральною стійкістю суспільства та

його готовністю до тривалого опору.

Таким чином, системи A2/AD мають подвійну природу. З одного боку, вони є сукупністю технічних засобів оборони, а з іншого – інструментом стратегічного стримування, який впливає на процес прийняття рішень противником. Руйнування інформаційної цілісності такої системи підриває не лише її технічні можливості, а й психологічний ефект стримування, що значно прискорює деградацію всієї оборонної архітектури.

Проведений політико-стратегічний аналіз свідчить, що сучасні операції прориву A2/AD є інструментом досягнення політичних результатів, а не самоціллю. Їхня ефективність визначається здатністю інтегрувати військові дії в ширшу систему стратегічного впливу – дипломатичного, інформаційного та економічного. Саме ця інтеграція перетворює тактичний успіх на довгострокову стратегічну перевагу.

Обговорення

Отримані результати дослідження свідчать про системну трансформацію характеру сучасних операцій прориву A2/AD. Аналіз кейсу показав, що вирішальним фактором успіху є не кількісна перевага у засобах ураження, а рівень інтеграції сенсорних, інформаційних та ударних компонентів у єдину мережеву архітектуру управління.

Проведене дослідження дозволило встановити такі закономірності:

1. Деградація ієрархічної системи ППО відбувається передусім через інформаційне перевантаження її вузлів управління.

2. Порушення цілісності сенсорного поля призводить до втрати ситуаційної обізнаності швидше, ніж фізичне знищення окремих елементів системи.

3. Мережева архітектура забезпечує суттєве прискорення циклу прийняття рішень, що формує асиметричну перевагу навіть за обмежених ресурсів.

Таким чином, результати підтверджують гіпотезу про пріоритет інформаційної інтеграції над платформенною перевагою.

Отримані висновки узгоджуються з:

- теорією мережевоцентричних операцій [11],
- концепцією боротьби волі [22],
- принципом непрямого підходу [26],
- положеннями сучасних доктрин [6],
- математичними моделями управління в умовах інформаційної невизначеності [31].

Особливо важливою є кореляція між теоретичними розрахунками українських авторів щодо деградації управління при перевищенні порогу інформаційного шуму та емпіричними даними сучасних операцій. Це свідчить про універсальність виявлених закономірностей.

Наукова новизна дослідження полягає у:

- інтеграції технічного аналізу операції з політико-стратегічним виміром;
- поєднанні концепції SEAD/DEAD з теорією руйнування волі противника;

• інтерпретації A2/AD як інформаційної системи, а не лише сукупності ракетних платформ;

• формулюванні критерію сучасної стратегічної ефективності через зміну раціональності війни для противника.

У роботі здійснено спробу інтегрувати операційно-технічний аналіз із політико-стратегічною інтерпретацією, що дозволяє розглядати A2/AD як інформаційну систему, а не лише як сукупність озброєнь.

Практична цінність отриманих результатів полягає у можливості їх використання в системі професійної підготовки військових фахівців, зокрема при викладанні дисциплін, пов'язаних із теорією сучасних операцій, організацією управління військами та протидією інтегрованим системам протиповітряної оборони. Запропонований підхід до інтерпретації A2/AD як інформаційно-керуючої системи може бути застосований під час розроблення навчальних програм, тренувальних сценаріїв і штабних моделювань. Результати дослідження також можуть бути враховані у процесі вдосконалення архітектур систем управління та під час формування вимог до стійкості бойових мереж в умовах інформаційного впливу та радіоелектронної боротьби. Крім того, зроблені висновки можуть бути використані при розробленні методичних рекомендацій щодо підвищення адаптивності підрозділів у багатодоменному середовищі та при оцінці ефективності мережевих рішень у сучасних конфліктах.

Подальші дослідження доцільно спрямувати на поглиблене вивчення механізмів інтеграції мережево-центричних систем управління у багатодоменних операціях, а також на аналіз стійкості ієрархічних оборонних структур в умовах інформаційного перевантаження та радіоелектронного впливу. Особливу увагу варто приділити емпіричній перевірці моделей деградації систем управління при перевищенні порогових значень інформаційного шуму, що дозволить уточнити математичні залежності між щільністю сигналів, пропускну здатністю каналів і швидкістю прийняття рішень. Перспективним напрямом є також порівняльний аналіз різних архітектур бойових мереж з метою визначення оптимального співвідношення централізації та децентралізації управління. Окремого вивчення потребує взаємозв'язок між технологічною інтеграцією систем і психологічною стійкістю військових структур, оскільки сучасні операції демонструють, що інформаційна дезорганізація може мати стратегічні наслідки навіть без масштабного фізичного ураження. Результати таких досліджень можуть бути використані як у військово-теоретичній площині, так і в практиці підготовки командного складу та розроблення нових доктринальних підходів.

Проведене дослідження підтверджує, що сучасні операції прориву систем A2/AD є не лише технологічним явищем, а комплексним стратегічним процесом, у якому інформаційна

інтеграція, мережеве управління та політична логіка становлять єдину систему. Саме ця інтеграція визначає характер і результат сучасних воєнних конфліктів.

Висновки

Проведений аналіз демонструє, що сучасні операції прориву систем A2/AD відображають глибинну трансформацію характеру війни. Якщо в індустріальну епоху вирішальним фактором виступала маса вогневих засобів і технічна перевага платформ, то в умовах цифровізованого поля бою визначальним стає рівень інтеграції сенсорів, засобів управління, ударних систем та аналітичних алгоритмів у єдину мережеву архітектуру.

Досліджений кейс підтверджує кілька фундаментальних закономірностей сучасного воєнного мистецтва.

По-перше, інформаційне домінування здатне нейтралізувати навіть технологічно розвинуту систему оборони. Руйнування сенсорного поля, порушення передачі даних та дезорганізація управління призводять до втрати боєздатності швидше, ніж фізичне знищення озброєння. У цьому сенсі системи A2/AD доцільно розглядати не лише як сукупність ракетних і радіолокаційних платформ, а передусім як інформаційно-керуючі системи, стійкість яких визначається цілісністю мережі сенсорів, каналів зв'язку та центрів прийняття рішень.

По-друге, мережева архітектура бойових систем демонструє стійкість, принципово недосягну для ієрархічних структур. У розподіленій мережі знищення окремих вузлів не руйнує функціональну цілісність системи, тоді як централізовані системи управління зазнають каскадної деградації після втрати ключових елементів. Саме ця структурна різниця пояснює ефективність сучасних концепцій бойових мереж (kill web) у протистоянні традиційним ієрархічним архітектурам (kill chain).

По-третє, швидкість інтеграції систем стає важливішою за їхню кількість або індивідуальні характеристики. Перевагу отримує сторона, здатна швидше об'єднати розвідку, управління та ураження в єдиний інформаційний цикл, скорочуючи час від виявлення до удару. У такій логіці ключовим фактором виступає не лише технологія озброєння, а здатність системи підтримувати безперервність циклу спостереження, орієнтації, рішення та дії (OODA).

По-четверте, результати дослідження свідчать про структурну асиметрію між мережевими системами наступу та оборони. Розподілені мережі сенсорів і платформ наступальної сторони здатні масштабуватися та адаптуватися швидше, ніж інтегровані оборонні архітектури, які потребують централізованого управління та стабільної інформаційної інфраструктури. Унаслідок цього мережеві системи наступу демонструють вищу еволюційну гнучкість, що поступово знижує ефективність традиційних A2/AD-архітектур.

По-п'яте, сучасні операції мають нерозривний військово-політичний характер. Військовий успіх набуває стратегічного значення лише тоді, коли він

синхронізований із політичною метою, дипломатичною підготовкою та інформаційною стратегією. Без цієї інтеграції навіть технічно бездоганна операція може не привести до бажаного результату.

По-шосте, розвиток концепції A2/AD має чітко виражений асиметричний характер. Історично вона формується передусім у державах, які поступаються потенційному противнику у можливостях глобальної проєкції сили, але прагнуть обмежити його свободу дій у власному регіоні. У таких умовах системи протиповітряної оборони, протикорабельні ракети, засоби радіоелектронної боротьби та мережеві сенсорні комплекси використовуються для створення так званих "зон заборони доступу", що підвищують ризик і вартість військового втручання для сильнішої сторони. Саме тому концепція A2/AD найбільш активно розвивається державами, які прагнуть компенсувати асиметрію сил шляхом підвищення оборонної стійкості у визначених географічних регіонах.

Наукова новизна дослідження полягає у комплексному поєднанні трьох рівнів аналізу, які традиційно розглядаються окремо:

1. Доктринального рівня – систематизації еволюції концепції A2/AD та механізмів її подолання.
2. Операційного рівня – реконструкції логіки сучасної інтегрованої операції із застосуванням мережево-центричних систем.
3. Стратегічного рівня – оцінки політичних наслідків технологічного домінування.

На відміну від більшості робіт, що розглядають A2/AD переважно як технічну або тактичну проблему, дана стаття демонструє, що її подолання є насамперед системною задачею управління інформаційним середовищем бою.

Отримані результати можуть бути використані:

- у навчальному процесі військових навчальних закладів;
- при підготовці доктринальних документів;
- у плануванні операцій протидії інтегрованим системам ППО;
- у дослідженнях розвитку мережево-центричних концепцій ведення війни.

Таким чином, сучасна війна дедалі більше набуває характеру боротьби за контроль над інформаційною реальністю поля бою. Стратегічна перевага майбутнього визначатиметься не кількістю озброєнь як такою, а здатністю держави створювати інтегровані мережеві системи управління бойовими діями та підтримувати їхню інформаційну цілісність у багатодоменному середовищі.

Список використаних джерел

- [1.] A. Krepinevich, B. Watts, and R. Work, Meeting the Anti-Access and Area-Denial Challenge. Washington, DC, USA: Center for Strategic and Budgetary Assessments, 2003. [Online]. Available: <https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf>
- [2.] K. Dobija, "The political and military aspects of creating anti-access/area-denial systems," Safety & Defense, 2021, Available: <https://doi.org/10.37105/sd.143>.

- [3.] M. van Creveld, *The Transformation of War*. New York, NY, USA: Free Press, 1991.
- [4.] S. M. I. Imam and S. Ullah, "Anti-access area denial capabilities: Implications for strategic stability," *Journal of Security & Strategic Analyses*, 2020, Available: <https://thesvi.org/wp-content/uploads/2020/09/JSSA-Vol-VI-no-1-17-42.pdf>
- [5.] E. V. Larson et al., *Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy*. Santa Monica, CA, USA: RAND Corporation, 2004.
- [6.] D. Barrie, "Anti-access/area denial: Bursting the 'no-go' bubble?," *International Institute for Strategic Studies*, Apr. 2019. [Online]. Available: <https://www.iiss.org/online-analysis/military-balance/2019/04/anti-access-area-denial-russia-and-crimea/>
- [7.] J. M. Richardson, "Design for maintaining maritime superiority," *Naval War College Review*, vol. 69, no. 2, Art. no. 4, 2016. [Online]. Available: <https://digitalcommons.usnwc.edu/cgi/viewcontent.cgi?article=1093&context=nwc-review>
- [8.] B. S. Lambeth, *The Transformation of American Air Power*. Ithaca, NY, USA: Cornell University Press, 2000.
- [9.] U.S. Department of Defense, "Joint Publication 3-01: Countering Air and Missile Threats," 2018. [Online]. Available: <https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/JointDoctrine-CounteringAirandMissileThreats.pdf>
- [10.] D. S. Alberts and R. E. Hayes, *Power to the Edge: Command and Control in the Information Age*. Washington, DC, USA: CCRP, 2003.
- [11.] B. S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment*. Santa Monica, CA, USA: RAND Corporation, 2001. [Online]. Available: https://www.rand.org/pubs/monograph_reports/MR1365.html
- [12.] "Why did Venezuela's air defense fail in US' Caracas raid?," *Army Technology*. [Online]. Available: <https://www.army-technology.com/features/why-did-venezuelas-air-defence-fail-in-us-caracas-raid/>
- [13.] J. A. López Díaz, "La caída del régimen en Venezuela: El concepto Anti-Acceso / Denegación de Área (A2AD) es sólo un acrónimo y no es invulnerable," *Asociación Española de Militares Escritores*, Jan. 8, 2026. [Online]. Available: <https://militaresescritores.es/noticias/la-caida-del-regimen-en-venezuela-el-concepto-anti-acceso-denegacion-de-area-a2ad-es-solo-un-acronimo-y-no-es-invulnerable-coronel-de-im-lopez-diaz/>
- [14.] G. Dubois, "Cómo el dominio aéreo de EE. UU. dismanteló la defensa antiaérea venezolana para capturar a Nicolás Maduro," *Aviacionline*. [Online]. Available: https://www.aviacionline.com/espanol/defensa/como-el-dominio-aereo-de-ee-uu--dismantelo-la-defensa-antiaerea-venezolana-para-capturar-a-nicolas-maduro_a6959c8a97a89b44e006d9698/
- [15.] B. Jensen, "Operational Art in the Age of Battle Networks," *Center for Strategic and International Studies (CSIS)*. [Online]. Available: <https://www.csis.org/analysis/chapter-4-operational-art-age-battle-networks/>
- [16.] C. Gordon and G. Hadley, "Military Operations: Airpower and Absolute Resolve," *Air & Space Forces Magazine*. [Online]. Available: <https://www.airandspaceforces.com/article/military-operations-airpower-and-absolute-resolve/>
- [17.] "RQ-170 Sentinel," *Air & Space Forces Magazine*. [Online]. Available: <https://www.airandspaceforces.com/weapons/rq-170/>
- [18.] "What to Know About the RQ-170 Drone, Venezuela, and Stealthy ISR," *Air & Space Forces Magazine*. [Online]. Available: <https://www.airandspaceforces.com/what-to-know-rq-170-drone-venezuela-stealthy-isr/>
- [19.] "Anduril's Lattice: a trusted dual use – commercial and military – platform for public safety, security, and defense," *Anduril*. [Online]. Available: <https://www.anduril.com/news/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/>
- [20.] "Army Selects Anduril's Lattice for IBCS-M Program," *ExecutiveBiz*. [Online]. Available: <https://www.executivebiz.com/articles/army-anduril-lattice-ibcs-m-program/>
- [21.] A. Beaufre, *Introduction à la stratégie*. Paris, France: Armand Colin, 1963. [Online]. Available: <https://gallica.bnf.fr/ark:/12148/bpt6k3328314d>
- [22.] "What US aircraft were used in Operation Absolute Resolve?," *Army Technology*. [Online]. Available: <https://www.army-technology.com/features/what-us-aircraft-were-used-in-operation-absolute-resolve/>
- [23.] J. R. Boyd, *A Discourse on Winning and Losing*, G. T. Hammond, Ed. Maxwell AFB, AL, USA: Air University Press, 2018. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.pdf
- [24.] E. G. Fillman, "Suppression of Enemy Air Defenses (SEAD) Battle Tracking Challenges in Contested Environments," *ALSSA*. [Online]. Available: <https://www.alssa.mil/News/Article/2543194/suppression-of-enemy-air-defenses-sead-battle-tracking-challenges-in-contested/>
- [25.] B. H. Liddell Hart, *Strategy*. London, U.K.: Faber & Faber, 1967.
- [26.] M. Shurkin et al., *French Army Approaches to Networked Warfare*. Santa Monica, CA, USA: RAND Corporation, 2022. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2946/RAND_RR2946.pdf
- [27.] A. Martinez et al., "Simulating autonomous drone behaviors in an A2AD environment," *Journal of Defense Modeling and Simulation*, 2024, Available: <https://doi.org/10.1177/15485129241288236>
- [28.] S. Markiewicz and M. Wrzosek, "Required operational capabilities of the recognition subsystem in the A2/AD system," *Safety & Defense*, 2023, Available: <https://doi.org/10.37105/sd.193>
- [29.] N. Świętochowski and D. Rewak, "The role of artillery in combating A2/AD systems," *Scientific Journal of the Military University of Land Forces*, 2021, <https://doi.org/10.5604/01.3001.0014.9797>
- [30.] І. І. Шовкошитний та О. А. Василенко, "Математична модель застосування рою ударних безпілотних літальних апаратів для ураження нестационарних групових цілей із використанням елементів штучного інтелекту," *Повітряна міць України*, no. 2(9), pp. 48-56, 2025. [Online]. Available: <https://sap.nuou.org.ua/article/view/343255>
- [31.] J. Polga-Hecimovich and K. Anderson, "Assessing the capabilities of Venezuela's military and armed groups," *War on the Rocks*. [Online]. Available: <https://warontherocks.com/episode/the-insider/42610/assessing-the-capabilities-of-venezuelas-military-and-armed-groups/>
- [32.] O. J. Pérez, "After Maduro: Trump's Managed Authoritarianism Trap in Venezuela," *War on the Rocks*, Jan. 2026. [Online]. Available: <https://warontherocks.com/2026/01/after-maduro-trumps-managed-authoritarianism-trap-in-venezuela/>
- [33.] M. Shurkin, "Thoughts on Military Strategy and War with Venezuela," *Pax Americana*, YouTube lecture. [Online]. Available: <https://www.youtube.com/watch?v=mW-L5XPLJwQ>

Ibragim Gabidulin (Candidate Technical Science, Associate Professor)

<https://orcid.org/0009-0009-7860-7818>

Center for Army, Conversion and Disarmament Studies

GENESIS AND EVOLUTION OF A2/AD CONCEPTS: FROM DETERMINISTIC SYSTEMS TO NETWORK-CENTRIC WARFARE

This article examines the evolution of the Anti-Access/Area Denial (A2/AD) concept and the mechanisms for overcoming it in contemporary multi-domain operations. Based on an interdisciplinary analysis of military doctrines, the theory of network-centric warfare, and recent operational case studies, the study demonstrates that the decisive factor of success is not the number of platforms or firepower, but the level of integration of sensors, command-and-control assets, and strike systems within a unified information-operational architecture.

The research shows that disrupting the informational integrity of an air defense system may be more effective than its physical destruction. The paper also substantiates the relationship between theoretical models of command and control under conditions of informational uncertainty and the practical outcomes of modern military operations.

It is concluded that future conflicts will increasingly be determined by the ability of opposing sides to manage the information environment and accelerate decision-making cycles, while technological superiority serves primarily as an instrument for implementing political strategy.

The findings of the study may contribute to the development of military doctrine, operational planning, and professional military education related to countering integrated air defense systems and A2/AD architectures.

Keywords: A2/AD, SEAD, DEAD, network-centric warfare, **kill web**, information dominance, command and control systems, multi-domain operations, air defense, battle networks, modern military strategy.

References

- [1.] A. Krepinevich, B. Watts, and R. Work, Meeting the Anti-Access and Area-Denial Challenge. Washington, DC, USA: Center for Strategic and Budgetary Assessments, 2003. [Online]. Available: <https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf>
- [2.] K. Dobija, "The political and military aspects of creating anti-access/area-denial systems," Safety & Defense, 2021, Available: <https://doi.org/10.37105/sd.143>.
- [3.] M. van Creveld, The Transformation of War. New York, NY, USA: Free Press, 1991.
- [4.] S. M. I. Imam and S. Ullah, "Anti-access area denial capabilities: Implications for strategic stability," Journal of Security & Strategic Analyses, 2020, Available: <https://thesvi.org/wp-content/uploads/2020/09/JSSA-Vol-VI-no-1-17-42.pdf>
- [5.] E. V. Larson et al., Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy. Santa Monica, CA, USA: RAND Corporation, 2004.
- [6.] D. Barrie, "Anti-access/area denial: Bursting the 'no-go' bubble?," International Institute for Strategic Studies, Apr. 2019. [Online]. Available: <https://www.iiss.org/online-analysis/military-balance/2019/04/anti-access-area-denial-russia-and-crimea/>
- [7.] J. M. Richardson, "Design for maintaining maritime superiority," Naval War College Review, vol. 69, no. 2, Art. no. 4, 2016. [Online]. Available: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1093&context=nwc-review>
- [8.] B. S. Lambeth, The Transformation of American Air Power. Ithaca, NY, USA: Cornell University Press, 2000.
- [9.] U.S. Department of Defense, "Joint Publication 3-01: Countering Air and Missile Threats," 2018. [Online]. Available: <https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/JointDoctrine-CounteringAirandMissileThreats.pdf>
- [10.] D. S. Alberts and R. E. Hayes, Power to the Edge: Command and Control in the Information Age. Washington, DC, USA: CCRP, 2003.
- [11.] B. S. Lambeth, NATO's Air War for Kosovo: A Strategic and Operational Assessment. Santa Monica, CA, USA: RAND Corporation, 2001. [Online]. Available: https://www.rand.org/pubs/monograph_reports/MRI365.html
- [12.] "Why did Venezuela's air defense fail in US' Caracas raid?," Army Technology. [Online]. Available: <https://www.army-technology.com/features/why-did-venezuelas-air-defence-fail-in-us-caracas-raid/>
- [13.] J. A. López Díaz, "La caída del régimen en Venezuela: El concepto Anti-Acceso / Denegación de Área (A2AD) es sólo un acrónimo y no es invulnerable," Asociación Española de Militares Escritores, Jan. 8, 2026. [Online]. Available: <https://militaresescritores.es/noticias/la-caida-del-regimen-en-venezuela-el-concepto-anti-acceso-denegacion-de-area-a2ad-es-solo-un-acronimo-y-no-es-invulnerable-coronel-de-im-lopez-diaz/>
- [14.] G. Dubois, "Cómo el dominio aéreo de EE. UU. desmanteló la defensa antiaérea venezolana para capturar a Nicolás Maduro," Aviacionline. [Online]. Available: https://www.aviacionline.com/espanol/defensa/como-el-dominio-aereo-de-ee-uu-desmantelo-la-defensa-antiaerea-venezolana-para-capturar-a-nicolas-maduro_a6959c8a97a89b44e006d9698/
- [15.] B. Jensen, "Operational Art in the Age of Battle Networks," Center for Strategic and International Studies (CSIS). [Online]. Available: <https://www.csis.org/analysis/chapter-4-operational-art-age-battle-networks/>
- [16.] C. Gordon and G. Hadley, "Military Operations: Airpower and Absolute Resolve," Air & Space Forces Magazine. [Online]. Available: <https://www.airandspaceforces.com/article/military-operations-airpower-and-absolute-resolve/>
- [17.] "RQ-170 Sentinel," Air & Space Forces Magazine. [Online]. Available: <https://www.airandspaceforces.com/weapons/rq-170/>
- [18.] "What to Know About the RQ-170 Drone, Venezuela, and Stealthy ISR," Air & Space Forces Magazine. [Online]. Available: <https://www.airandspaceforces.com/what-to-know-rq-170-drone-venezuela-stealthy-isr/>
- [19.] "Anduril's Lattice: a trusted dual use – commercial and

- military – platform for public safety, security, and defense," Anduril. [Online]. Available: <https://www.anduril.com/news/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/>
- [20.] "Army Selects Anduril's Lattice for IBCS-M Program," ExecutiveBiz. [Online]. Available: <https://www.executivebiz.com/articles/army-anduril-lattice-ibcs-m-program/>
- [21.] A. Beaufre, Introduction à la stratégie. Paris, France: Armand Colin, 1963. [Online]. Available: <https://gallica.bnf.fr/ark:/12148/bpt6k3328314d>
- [22.] "What US aircraft were used in Operation Absolute Resolve?," Army Technology. [Online]. Available: <https://www.army-technology.com/features/what-us-aircraft-were-used-in-operation-absolute-resolve/>
- [23.] J. R. Boyd, A Discourse on Winning and Losing, G. T. Hammond, Ed. Maxwell AFB, AL, USA: Air University Press, 2018. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.pdf
- [24.] E. G. Fillman, "Suppression of Enemy Air Defenses (SEAD) Battle Tracking Challenges in Contested Environments," ALSSA. [Online]. Available: <https://www.alssa.mil/News/Article/2543194/suppression-of-enemy-air-defenses-sead-battle-tracking-challenges-in-contested/>
- [25.] B. H. Liddell Hart, Strategy. London, U.K.: Faber & Faber, 1967.
- [26.] M. Shurkin et al., French Army Approaches to Networked Warfare. Santa Monica, CA, USA: RAND Corporation, 2022. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2946/RAND_RR2946.pdf
- [27.] A. Martinez et al., "Simulating autonomous drone behaviors in an A2AD environment," Journal of Defense Modeling and Simulation, 2024, Available: <https://doi.org/10.1177/15485129241288236>.
- [28.] S. Markiewicz and M. Wrzosek, "Required operational capabilities of the recognition subsystem in the A2/AD system," Safety & Defense, 2023, Available: <https://doi.org/10.37105/sd.193>.
- [29.] N. Świętochowski and D. Rewak, "The role of artillery in combating A2/AD systems," Scientific Journal of the Military University of Land Forces, 2021, <https://doi.org/10.5604/01.3001.0014.9797>.
- [30.] I. Shovkoshytnyi and O. Vasylenko, "Mathematical model of the use of a swarm of strike unmanned aerial vehicles to engage non-stationary group targets using elements of artificial intelligence," Air Power of Ukraine, no. 2(9), pp. 48-56, 2025. [Online]. Available: <https://sap.nuou.org.ua/article/view/343255>
- [31.] J. Polga-Hecimovich and K. Anderson, "Assessing the capabilities of Venezuela's military and armed groups," War on the Rocks. [Online]. Available: <https://warontherocks.com/episode/the-insider/42610/assessing-the-capabilities-of-venezuelas-military-and-armed-groups/>
- [32.] O. J. Pérez, "After Maduro: Trump's Managed Authoritarianism Trap in Venezuela," War on the Rocks, Jan. 2026. [Online]. Available: <https://warontherocks.com/2026/01/after-maduro-trumps-managed-authoritarianism-trap-in-venezuela/>
- [33.] M. Shurkin, "Thoughts on Military Strategy and War with Venezuela," Pax Americana, YouTube lecture. [Online]. Available: <https://www.youtube.com/watch?v=mW-L5XPLJwQ>