Integrated Deterrence Technology as an Effective Means of Ensuring the Security of European Union Countries Against the Backdrop of the Russian Threat

UDC 355.033.5(4-671:470) DOI: https://doi.org/10.15421/172648

Vysotskyi Oleksandr[1]
Dr.Sc., Full Prof., https://orcid.org/0000-0003-0712-8499, vysalek@gmail.com
Kulyk Tetyana[2]
Ph.D., Senior Researcher, Asso. Prof., http://orcid.org/0000-0003-4422-7533,Kulyk.T.V@nmu.one
Pashkevych Maryna[2]
Dr.Sc., Full Prof., https://orcid.org/0000-0003-3012-1690, pashkevych.m.s@nmu.one
Parkhomenko Yeva[2]
Bachelor Degree Student, https://orcid.org/0009-0005-3337-9621 parkhomenko.y.s@nmu.one
[1]Oles Honchar Dnipro National University (Dnipro, Ukraine)
[2]Dnipro University of Technology (Dnipro, Ukraine)

Abstract

Relevance. Russia's full-scale aggression against Ukraine has radically transformed the security environment in Europe and revealed the limitations of classical deterrence models, which rely primarily on military force or nuclear balance. For European Union countries, the Russian threat is complex and multidimensional, combining military pressure, information operations, economic and energy coercion, cyber activities, and political influence below the threshold of open warfare. Under such conditions, fragmented or sectoral approaches to security prove ineffective, which highlights the need to understand integrated deterrence not only as a strategy but as a comprehensive security technology.

The purpose of the article is to provide a systematic theoretical justification for integrated deterrence as an effective technology for ensuring the security of European Union countries in the context of the hybrid and multidomain Russian threat, to identify its structural elements and to determine the role of the information dimension as a system-forming factor in deterring actions below the threshold of war.

Results. The article proves that integrated deterrence should be considered as a technology of strategic influence based on the coordinated and mutually reinforcing use of military, political, economic and information tools. It is shown that deterrence is essentially a political process aimed at influencing the decision-making process of a potential aggressor, rather than a purely technical or military procedure. The central role of the information space, within which the perception of risks, costs and acceptable limits of aggressive behaviour is formed, is substantiated. The practice of the West's response to Russian aggression against Ukraine is analysed as an empirical example of the implementation of the logic of integrated deterrence.

Conclusions. The authors conclude that integrated deterrence is the most adequate and promising technology for ensuring the security of the European Union against the backdrop of the systemic Russian threat. Its effectiveness depends on the level of internal coordination, political unity, strategic communications and readiness for sustained collective action. Integrated deterrence enhances the ability of EU countries to counter hybrid aggression, strengthens resilience to sub-threshold coercion, and contributes to the formation of a stable European security architecture in the 21st century.

Keywords: integrated deterrence, European Union security, Russian threat, hybrid aggression, information deterrence, strategic communications, multi-domain security, international security

Технологія інтегрованого стримування як ефективний засіб забезпечення безпеки країн Європейського Союзу на тлі російської загрози

Висоцький Олександр[1], **Кулик Тетяна**[2], **Пашкевич Марина**[2], **Пархоменко Єва**[2]
[1]Дніпровський національний університет імені Олеся Гончара, (Дніпро, Україна)
[2]Національний технічний університет «Дніпровська політехніка», (Дніпро, Україна)

Анотація

Актуальність. Повномасштабна агресія росії проти України докорінно трансформувала безпекове середовище Європи та виявила обмеженість класичних моделей стримування, що спираються переважно на військову силу або ядерний баланс. Для країн Європейського Союзу російська загроза має комплексний, багатовимірний характер і поєднує військовий тиск, інформаційні операції, економічний та енергетичний примус, кібердіяльність і політичний вплив нижче порогу відкритої війни. За таких умов фрагментарні або секторальні підходи до безпеки виявляються неефективними, що актуалізує потребу в осмисленні інтегрованого стримування не лише як стратегії, а як цілісної технології забезпечення безпеки.

Мета статті полягає у системному теоретичному обґрунтуванні інтегрованого стримування як ефективної технології забезпечення безпеки країн Європейського Союзу в умовах гібридної та багатодоменної російської загрози, виявленні його структурних елементів та визначенні ролі інформаційного виміру як системоутворюючого чинника стримування дій нижче порогу війни.

Результати. У статті доведено, що інтегроване стримування слід розглядати як технологію стратегічного впливу, засновану на скоординованому та взаємопосиленому застосуванні військових, політичних, економічних та інформаційних інструментів. Показано, що стримування за своєю суттю є передусім політичним процесом, спрямованим на вплив на процес ухвалення рішень потенційного агресора, а не суто технічною або військовою процедурою. Обґрунтовано центральну роль інформаційного простору, в межах якого формується сприйняття ризиків, витрат і допустимих меж агресивної поведінки. Проаналізовано практику реагування Заходу на російську агресію проти України як емпіричний приклад реалізації логіки інтегрованого стримування.

Висновки. Зроблено висновок, що інтегроване стримування є найбільш адекватною та перспективною технологією забезпечення безпеки Європейського Союзу на тлі системної російської загрози. Його ефективність залежить від рівня внутрішньої координації, політичної єдності, стратегічних комунікацій і готовності до тривалої колективної дії. Інтегроване стримування підвищує спроможність країн ЄС протидіяти гібридній агресії, зміцнює стійкість до підпорогового примусу та сприяє формуванню стабільної архітектури європейської безпеки у XXI столітті.

Ключові слова: інтегроване стримування, безпека Європейського Союзу, російська загроза, гібридна агресія, інформаційне стримування, стратегічні комунікації, багатодоменна безпека, міжнародна безпека

Стаття надійшла / Article arrived: 25.12.2025 Схвалено до друку / Accepted: 26. 01.2026

Вступ.

Постановка проблеми. Сучасна міжнародна система переживає глибоку трансформацію, спричинену не лише зростанням стратегічної конкуренції між великою державою-агресором і західним демократичним світом, а й фундаментальною зміною самого характеру загроз безпеці. Російська збройна агресія проти України стала не просто регіональним конфліктом, а симптоматичним проявом нової парадигми – епохи «інтегрованих викликів», у якій військові, економічні, технологічні та інформаційні домени стратегічної взаємодії більше не існують окремо, а взаємопроникають, посилюючи один одного. У цих умовах класичні моделі стримування, зосереджені виключно на військовій силі чи ядерному балансі, втрачають свою ефективність, оскільки не спроможні адекватно реагувати на асиметричні, підпорогові форми агресії, що навмисно уникають чітких правових і політичних рамок. Особливо гостро це відчувається в інформаційному вимірі, де відсутність усталених норм поведінки, труднощі верифікації джерел, а також здатність швидко маніпулювати колективним сприйняттям створюють простір для систематичного підриву політичної стабільності, соціальної комунікації та довіри до інститутів. Водночас, саме інформаційний простір стає ключовим полем формування стримуючого ефекту – не через прямий примус, а через управління очікуваннями, вартістю ризиків і стратегічною доцільністю агресивних дій у свідомості потенційного противника. Таким чином, наявна фундаментальна проблема забезпечення надійного, передбачуваного та ефективного стримування в умовах, коли загрози є багатодоменні, інтегровані та навмисно нечіткі, а традиційні механізми стримування виявляються недостатніми. Ця проблема набуває особливої актуальності для країн Європейського Союзу, які опинилися в зоні ризику російської гібридної підпорогової агресії, але не завжди мають єдину, координовану та стратегічно цілісну відповідь. Тому наукове осмислення технології інтегрованого стримування – як системного підходу, що поєднує всі інструменти національної та колективної могутності – стає не лише теоретичною необхідністю, а й практичним імперативом безпеки країн Європейського Союзу.

Аналіз попередніх досліджень та публікацій. Одним із перших проблему технологій безпеки як ефективних інструментів міжнародної політики поставив О.Ю.Висоцький в роботі «Технології національної безпеки у внутрішній та зовнішній політиці держави» (Vysotskyi, 2023). Також ним була осмислена проблема політичної безпеки держави в умовах нестабільності міжнародно-політичного середовища (Висоцький, 2021). Розвиток проблематики інтегрованого стримування безпосередньо пов'язаний із дослідженням С. Бланка, який обґрунтовує необхідність комплексної західної стратегії підтримки України та довгострокового збереження конвенційного стримування в Європі на лінії зіткнення росії та НАТО, що концептуально наближається до логіки інтегрованого стримування (Blank, 2024). К.Хеффлер, С.Гофманн і Ф.Меран аналізують феномен «полікризи» в ЄС та показують, як зовнішня військова загроза з боку росії стимулює зростання безпекових і оборонних компетенцій Союзу у взаємодії з НАТО, створюючи інституційні передумови для інтегрованого стримування (Hoeffler, Hofmann & Mérand, 2024). Дж.Вірц і Дж.Ларсен у своїх працях системно розкривають концепт інтегрованого стримування, наголошуючи, що йдеться не про перегляд класичної теорії стримування, а про її адаптацію до нових технологічних, соціальних та багаторівневих стратегічних умов (Wirtz & Larsen, 2023; 2024). Л.Фрідман, аналізуючи російсько-українську війну, демонструє відносну стійкість ядерного стримування та водночас виявляє межі російського залякування, що має принципове значення для формування збалансованої моделі інтегрованого стримування в Європі (Freedman, 2023). К.Лібізеллер критично переосмислює концепт «гібридної війни», застерігаючи від його надмірної універсалізації, що є важливим для коректного теоретичного вбудовування інформаційних та нефізичних компонентів у технологію інтегрованого стримування (Libiseller, 2023). М.Шенк і Н.Гайнек, досліджуючи синергію НАТО та ЄС у протидії інформаційним загрозам, запропонували модель «циркулярного інституціоналізму», яка розкриває роль експертного волонтерства та міжінституційної взаємодії як елементів сучасного стримування (Šenk & Hynek, 2025). Р.Роуз у своїй книзі «Європейська безпека: від України до Вашингтона» аналітично відтворює еволюцію європейської безпеки від холодної війни до повномасштабної російської агресії проти України, підкреслюючи критичну залежність ЄС від американського стримування та наголошуючи на необхідності інтеграції політичної, економічної та оборонної складових безпеки – що прямо актуалізує концепцію «інтегрованого стримування» в умовах системної російської загрози (Rose, 2025). Я.Кофронь і Я.Стаубер емпірично довели, що географічна близькість до росії залишається ключовим чинником зростання оборонних витрат європейських держав, що підсилює аргументацію на користь диференційованих підходів інтегрованого стримування в ЄС (Kofroň, & Stauber, 2021). Т.Хадано, спираючись на теорію Англійської школи, показав, як росія використовує багатосторонні інституції для трансформації фундаментальних інститутів міжнародного порядку, що потребує інституційно чутливих відповідей з боку ЄС у межах інтегрованого стримування (Hadano, 2024). Б.Мітракієв і Н.Димитров аналізували російські кампанії рефлексивного контролю щодо

демократичних союзників України, підкреслюючи важливість когнітивного та інформаційного вимірів у системі стримування (Mitrakiev & Dimitrov, 2024). М.Амадіо Вічере та М.Сус досліджували роль неформальних груп у відповіді ЄС на війну росії проти України, показуючи, що «компартменталізований мультилатералізм» стає практичним механізмом організації європейської безпеки (Amadio Viceré & Sus, 2025). Л.Кахішвілі та А.Фельдер продемонстрували трансформацію уявлень депутатів Європарламенту про безпеку після 2022 р., фіксуючи розширення безпекового порядку денного та посилення акценту на автономній ролі ЄС (Kakhishvili & Felder, 2025), що безпосередньо корелює з ідеєю інтегрованого стримування в умовах російської загрози. Проаналізовані роботи склали теоретичний фундамент та дозволили нам глибоко дослідити технологію інтегрованого стримування як ефективний засіб забезпечення безпеки ЄС в контексті російської загрози.

Метою статті є фундаментально осмислити та системно обґрунтувати технологію інтегрованого стримування як ефективний засіб забезпечення безпеки країн Європейського Союзу в умовах багатодоменної, асиметричної та гібридної російської загрози. Зокрема, дослідження спрямоване на виявлення специфіки інтегрованого стримування як комплексної технології, що поєднує військові, економічні, політичні та інформаційні інструменти державної могутності; з'ясувати роль інформаційного виміру як важливого елемента цієї технології; а також визначити умови, механізми та обмеження застосування інтегрованого стримування для запобігання агресивним діям нижче порогу війни, зокрема в інформаційному просторі.

Методологія. У дослідженні технології інтегрованого стримування як засобу забезпечення безпеки країн Європейського Союзу застосовано технологічний підхід, який виступає ключовим методологічним інструментом для аналізу сучасних міжнародних відносин (Висоцький, 2017; 2018). Цей підхід розглядає стримування не лише як політичну або військову стратегію, а як цілісну технологію влади – систематизований набір інструментів, процедур, дискурсів і інституційних механізмів, спрямованих на управління поведінкою потенційного агресора. Технологічний підхід слугує широкою евристичною призмою, що дозволяє інтегрувати загальнонаукові (порівняльний аналіз, системне мислення, історико-генетичний метод) та спеціальні методи (дискурс-аналіз, контент-аналіз стратегічних документів, концептуальне моделювання). Він дає змогу розглядати інтегроване стримування в інструментальному (як сукупність засобів досягнення стримувального ефекту) та трансформаційному (як чинник зміни структури стратегічної взаємодії) вимірах.

Результати дослідження.

Інтегроване стримування виходить із визнання того, що сучасні загрози проявляються одночасно у військовій, економічній, технологічній та інформаційній сферах, а отже ефективна відповідь потребує координації дій у цих вимірах. Інформаційний простір розглядається як повноцінний домен стратегічної взаємодії, у межах якого стримування набуває специфічних форм. Інформаційне стримування як складова інтегрованого підходу ґрунтується на управлінні сприйняттям, очікуваннями та оцінками витрат і вигід потенційного опонента. Формування передбачуваності реакцій, підвищення вартості інформаційних атак та зменшення їх стратегічної доцільності обумовлює потребу в інформаційному стримуванні, орієнтованому на вплив на процес ухвалення рішень ще до моменту реалізації інформаційних операцій, закріплюючи уявлення про їх обмежену ефективність або небажані наслідки. Включення інформаційного виміру до інтегрованого стримування відкриває перспективи для розвитку міжнародних підходів до регулювання та запобігання інформаційним війнам. Хоча формалізовані режими контролю в цій сфері залишаються обмеженими, дедалі більшого значення набувають практики встановлення норм відповідальної поведінки, підвищення прозорості інформаційної діяльності та координації між союзниками. Таким чином, інтегроване стримування створює рамку, в межах якої інформаційні операції розглядаються не ізольовано, а як елемент ширшої системи управління стратегічною стабільністю в умовах зростаючої невизначеності.

Поняття інтегрованого стримування розуміється в теорії міжнародної безпеки як намір досягати стримувального ефекту шляхом всебічної та стратегічно спроєктованої інтеграції національних інструментів влади. Центральним операційним процесом залишається саме стримування, тоді як концепція інтегрованого стримування передусім стосується характеру та поєднання засобів, за допомогою яких цей ефект досягається.

Аналіз стримування як практики державної політики ґрунтується на двох ключових вихідних положеннях. По-перше, об'єктом стримувального впливу є процес ухвалення рішення про ініціювання агресії в уявленні потенційного агресора – конкретного лідера або вузького кола осіб, які здійснюють стратегічний вибір. Політичні лідери та уряди оцінюють ризики й можливості застосування сили у спосіб, що часто є ідіосинкратичним і формується під впливом глибоко вкорінених переконань, уявлень та сприйняття реальності. По-друге, стримування за своєю суттю є передусім політичним, а не технічним феноменом. Воно залежить від інтересів, влади, інформації та рішучості, так само як і рішення про війну є політичним судженням, а не раціоналізованим

розрахунком балансу сил (Lindsay, 2020, p. 14). Ці обставини істотно ускладнюють практику стримування. Хоча класична теорія стримування формувалася як відповідь на технологічний виклик, пов'язаний із появою ядерної зброї, у реальній політичній практиці стримування не функціонує як лінійна шкала об'єктивно вимірюваних параметрів, які можна механістично коригувати, а являє собою складний процес формування суб'єктивних уявлень і впливу на політичні судження, що за своєю природою є нестабільними та важко передбачуваними. Стримування означає зусилля, спрямовані на запобігання здійсненню небажаної дії з боку іншого актора, яким у сфері безпеки є зазвичай держави або недержавна збройна група. Отже, стримування принципово відрізняється від спорідненого поняття примусу, яке означає застосування тиску з метою змусити іншу сторону здійснити певну дію.

Держави можуть прагнути стримувати інших акторів від здійснення широкого спектра дій. В сучасних умовах поняття стримування певною мірою втратило аналітичну чіткість, оскільки його дедалі частіше використовують як універсальну політичну відповідь на будь-яку поведінку або потенційну подію, що сприймається як загроза національним інтересам. Однак, стримування за своєю суттю передбачає, принаймні частково, наявність переконливих загроз відплати, здатних накласти такі витрати, які істотно змінюють розрахунок ризиків з боку опонента У випадку багатьох дій конкурентів, що здійснюються нижче порогу збройного конфлікту, сформувати заздалегідь подібні переконливі загрози вкрай складно. Поведінка агресора в таких ситуаціях часто не є достатньо відверто ворожою або неприйнятною, щоб виправдати серйозні погрози у відповідь: відповідні дії можуть не порушувати міжнародне право, не виглядати агресивними або створювати надмірні ризики ескалаційних спіралей. У сукупності це означає, що погрози жорстко покарати дії, які не досягають порогу війни, є складними з погляду їхньої переконливості та ефективності За таких умов у значній частині повсякденної конкурентної взаємодії держави змушені зосереджуватися не стільки на стримуванні відповідних дій, скільки на пом'якшенні їхніх наслідків або на активній конкуренції у відповідних сферах. Отже, під час формулювання будь-якого стримувального виклику чи політики принципово важливо враховувати низку ключових розрізнень, які визначають характер стримувальних зусиль (Mazarr et al., 2021, p. 82).

По-перше, будь-яка політика стримування насамперед визначається тією ворожою дією, якій вона має запобігти. У класичному розумінні поняття стримування зазвичай застосовується до відносно вузької категорії потенційних дій – масштабної агресивної війни (Huth, 1999). Зростання ролі відносно агресивних дій нижче порогу війни, зокрема кібератак або інформаційного примусу, призводить до того, що дедалі частіше йдеться про необхідність стримування окремих, особливо демонстративних та конфронтаційних форм такої діяльності. Мається на увазі обмежене коло дій нижче порогу війни, які, попри відсутність формального збройного конфлікту, характеризуються значним військовим або квазі-військовим ефектом та виразним ворожим наміром. Інший підхід до концептуалізації форм стримування пов'язаний із розрізненням за масштабом і характером інструментів державної політики, що застосовуються для досягнення стримувальних цілей. Частина теоретиків наполягає на вузькому тлумаченні «інструментарію стримування», розглядаючи його передусім як використання військових погроз для запобігання військовим діям з боку опонента (Mazarr, et al., 2021, p. 3–5).

Другий підхід до розуміння стримування полягає в розширенні набору інструментів, за допомогою яких може формуватися стримувальний ефект. У цьому випадку стримування не обмежується виключно військовими погрозами, а включає застосування невійськових засобів у відповідь на військову агресію, зокрема економічні санкції, політичну ізоляцію, інформаційний або інші форми державного тиску. Такий підхід виходить з припущення, що загроза значущих немілітарних витрат може впливати на розрахунки потенційного агресора так само, як і загроза прямого військового протистояння (Mazarr & Ke, 2024, p. 6).

Третє, ще ширше, розуміння стримування виходить за межі виключно загрози та включає механізм поєднання стримування і заспокоєння. В межах цього підходу вважається, що для запобігання агресії необхідно враховувати базові безпекові побоювання потенційного противника та, за певних умов, адресувати їх через обмеження власної поведінки, переговори, компроміси або публічні гарантії. Мазар підкреслює, що сама по собі загроза може бути недостатньою для ефективного стримування, а в окремих випадках дії, спрямовані на посилення стримування, можуть мати протилежний ефект, оскільки вони поглиблюють відчуття загрози у іншої сторони та стимулюють ескалаційну логіку (Morgan, 2019, p. 52).

Класична типологія форм стримування залежно від механізму впливу на рішення агресора визначає стримування шляхом відмови (deterrence by denial) та стримування шляхом покарання (deterrence by punishment). Стримування шляхом відмови спрямоване на унеможливлення досягнення агресором бажаних цілей, зокрема через створення ефективної оборони та демонстрацію готовності її застосувати. Стримування шляхом покарання ґрунтується на загрозі ширших, часто непрямих наслідків агресії, які завдають шкоди агресору поза межами конкретного театру дій. Хоча ці два підходи не є взаємовиключними

і можуть застосовуватися паралельно, треба уникати спрощеного уявлення про їх ефективність. Здатність стримування шляхом відмови або покарання впливати на поведінку агресора значною мірою залежить від його сприйняття, упереджень та інтерпретацій, а не від об'єктивно вимірюваних показників. Отже, стримування не є лінійною моделлю, в якій можна точно визначити поріг достатності, а залишається політично й психологічно зумовленим процесом.

Четвертий аспект характеру стримування, стосується часу та масштабу. Безпосереднє (immediate) стримування означає найбільш відому, короткострокову й конкретно спрямовану форму стримування, зосереджену на запобіганні безпосередній загрозі агресії. У ситуаціях, коли існують ознаки неминучого нападу, і стримувальні заходи спрямовані на вплив на конкретне рішення про початок агресивних дій. Дії держави, спрямовані на посилення загроз або демонстрацію готовності до відповіді, є складовими політики безпосереднього стримування. Загальне (general) стримування має більш довгостроковий і контекстуальний характер й полягає у формуванні стійкого співвідношення витрат і вигод у сприйнятті одного або кількох потенційних агресорів, що в цілому знижує їхню схильність до агресивної поведінки. Загальне стримування не орієнтоване на конкретну кризу чи загрозу, а функціонує як постійний фон стратегічної взаємодії (Mazarr & Ke, 2024, p. 7).

П'ятий фактор стосується об'єкта стримування. Центральне стримування передбачає зусилля держави, спрямовані на запобігання нападу безпосередньо на неї саму. Розширене (extended) стримування, своєю чергою, означає стримування агресії проти третіх сторін і ґрунтується на готовності держави застосувати свої ресурси для захисту союзників або партнерів (Mazarr, & Ke, 2024, p. 7).

Сукупність цих п'яти чинників демонструє складність встановлення простих і вимірюваних причинно-наслідкових зв'язків між окремими заходами, такими як військові інвестиції, нарощування сил, заходи у сфері безпекового співробітництва або інші політичні кроки, та фактичними результатами стримування. Один і той самий інструмент або дія може мати різні наслідки залежно від того, чи йдеться про стримування шляхом позбавлення або покарання, про безпосереднє чи загальне стримування, а також залежно від того, на якого саме потенційного агресора вони спрямовані. Як зауважує П.Морган, у сучасному дискурсі концепт стримування дедалі частіше використовується для опису широкого спектра ситуацій і дій, спрямованих на припинення, зменшення або пом'якшення загроз національним інтересам (Morgan, 2019, p. 52). Якщо концепція інтегрованого стримування піде цим шляхом, вона ризикує перетворитися на синонім загальної стратегії національної безпеки, тобто на позначення інтегрованого застосування всіх інструментів державної потуги для досягнення будь-яких стратегічних цілей. Таким чином, необхідно обмежувати завдання стримувальних стратегій запобіганням масштабному застосуванню сили, передусім ядерній або конвенційній агресії, а також, за певних умов, найбільш інтенсивним і насильницьким формам дій нижче порогу війни, які передбачають значне застосування військової сили (Mazarr & Ke, 2024, p. 7).

Таким чином, сучасне розуміння стримування, окреслене через п'ять ключових вимірів: характер запобіжної дії, інструментарій, механізм впливу, часовий горизонт і об'єкт стримування, засвідчує, що стримування більше не може розглядатися виключно як військово-технічна або кризово-орієнтована практика. Стратегія стримування дедалі виразніше набуває рис комплексної політико-стратегічної діяльності, спрямованої на формування стійких моделей поведінки в умовах тривалої стратегічної конкуренції. Інформаційна складова стає не допоміжним, а системоутворюючим елементом стримування, оскільки саме через інформаційний простір здійснюється вплив на сприйняття намірів, витрат, ризиків і допустимих меж дій. В умовах цифровізації, зростання швидкості інформаційних потоків і розширення спектра дій нижче порогу війни стримування має враховувати та передбачати нові форми впливу, які не підпадають під класичні моделі військового протиборства, але безпосередньо впливають на стабільність міжнародної системи. Стримування постає як одна з ключових стратегій міжнародного регулювання та запобігання інформаційним війнам, спрямована не стільки на реактивне покарання, скільки на попереджувальне формування таких умов, за яких інформаційна агресія втрачає свою стратегічну доцільність.

Поняття міждоменного стримування (cross-domain deterrence) означає використання спроможностей в одному домені з метою нейтралізації загроз або комбінації загроз в іншому домені, передусім у ситуаціях, коли держава має відносну вразливість або обмежені можливості в певній сфері. Концепція міждоменного стримування сформувалася в середині 2000-х років у відповідь на зростання ролі космічного та кіберпростору у військових операціях, які поступово долучилися до традиційних операційних доменів суходолу, моря та повітря. У своєму початковому вигляді вона була зосереджена насамперед на взаємодії саме бойових доменів у контексті стримування, що робить її концептуально вужчою, ніж пізніша ідея інтегрованого стримування. Міждоменного стримування багато в чому збігається з інтегрованим підходом, а саме яким чином перетин доменів або комбінування інструментів державної влади може забезпечувати додатковий стримувальний ефект. Важливою відмінністю міждоменного

стримування є те, що воно не передбачає обов'язкової глибокої інтеграції спроможностей різних сфер, а радше спирається на дискретне застосування дій в одному домені для досягнення ефекту в іншому. Тобто міждоменне стримування не є повноцінною стратегією «синхронізованого впливу», але вже містить у собі перехресні ефекти, які згодом були розвинені в концепції інтегрованого стримування (Lindsay, & Gartzke, 2019, p.3).

Практика міждоменного стримування тісно пов'язана з трансформацією характеру стратегічної конкуренції. Якщо США традиційно покладалися на переваги у здатності інтегрувати повітряні, морські та космічні операції, то такі держави, як Китай, росія та Іран, дедалі активніше використовують нові технології для досягнення стратегічних переваг у тих сферах, де їхні конвенційні військові можливості є обмеженими. У відповідь на це зростає увага до немілітарних або нетрадиційних інструментів впливу, які можуть компенсувати дисбаланс сил і забезпечувати стримувальний ефект без прямого застосування військової сили. Міждоменне стримування пов'язане з підвищеними ризиками хибної інтерпретації сигналів та неконтрольованої ескалації. Перенесення дій з одного домену в інший може сприйматися опонентом як ознака розширення конфлікту, що здатне провокувати превентивні або ескалаційні кроки у відповідь. Особливо це стосується таких доменів, як кіберпростір і космос, де дії можуть бути інтерпретовані як підготовка до масштабнішого нападу. Окремі дослідження вказують на потенційний стабілізуючий ефект складної «мозаїки» міждоменних зв'язків, оскільки вона знижує вирішальність будь-якого одиничного кроку та зменшує ризик різкої ескалації в межах одного домену (Mallory, 2018, p. 6-8).

У концепції міждоменного стримування інформаційний простір набуває значення як домен, через який можуть створюватися стримувальні ефекти, непропорційні витратам і без прямого застосування військової сили. Інформаційні операції дозволяють переносити конкуренцію з доменів, де держава має відносні обмеження, у сферу, де асиметричні інструменти впливу можуть забезпечувати відчутний стратегічний ефект. Інформаційний домен виступає як об'єктом захисту, та й активним середовищем реалізації міждоменних стримувальних стратегій. Однак, застосування інформаційних засобів у рамках міждоменного стримування ускладнює інтерпретацію намірів і сигналів. Інформаційні впливи можуть одночасно сприйматися як елемент політичного тиску, підготовка до ширших дій або як автономна форма стратегічного протиборства, що підвищує ризики хибних оцінок і небажаної ескалації. Багатозначність інформаційного домену демонструє як його стримувальний потенціал, так і обмеження міждоменного підходу, вказуючи на потребу більш узгодженого та комплексного бачення стримування в умовах сучасної стратегічної конкуренції.

Адаптоване стримування (tailored deterrence) ґрунтується на посиленні контекстуалізації стримування та відмові від універсальних, стандартизованих стратегій на користь адаптації стримувальних заходів до конкретних акторів, ситуацій і типів загроз (Johnson & Kelly, 2014, p. 2). Стримування розглядається як процес, що має бути налаштований під специфічні умови ухвалення рішень потенційного агресора, включно з індивідуальними особливостями лідерства, інституційною структурою влади та політичною динамікою. Ключовим елементом адаптованого стримування є орієнтація на конкретного адресата стримувального сигналу, державу, домінантного лідера, вузьке коло політичних або військових еліт чи окремі центри ухвалення рішень, які безпосередньо формують курс дій. Відповідно, стримувальні загрози, стимули та комбінація інструментів державної потуги мають бути сконструйовані таким чином, щоб максимізувати вплив саме на ці групи або осіб. Адаптоване стримування створює своєрідний міст до концепції інтегрованого стримування. Якщо інтегроване стримування визначає широкий спектр доступних інструментів і способів їх поєднання, то адаптоване стримування задає принципи їх вибору та конфігурації залежно від конкретного суперника і типу виклику. У Стратегії національної оборони США 2022 року інтегроване стримування прямо пов'язується з необхідністю адаптації до «конкретних конкурентів і викликів» (U.S. Department of Defense, 2022).

Аналіз стратегічної культури потенційного агресора в межах адаптованого стримування включає історичний досвід, національну ідентичність, роль військових інституцій, домінантні уявлення про застосування сили та сприйняття ризику. Оскільки стримування є інтерактивним процесом, що значною мірою залежить від комунікації стримувальних сигналів, ефективність таких сигналів визначається тим, як вони інтерпретуються в межах конкретної стратегічної культури. Проте, існують й обмеження цього підходу. Критики застерігають від надмірної впевненості у здатності точно ідентифікувати ключові центри формування рішень і передбачити реакцію опонента. Обмеженість розвідувальної інформації, когнітивні упередження та динамічність політичних процесів можуть призводити до хибних припущень і переоцінки ефективності індивідуально налаштованих стримувальних стратегій. Попри це, навіть у теоретичному вимірі стримування не може бути ефективним без урахування специфіки конкретних ситуацій і адресатів, що й становить базову основу адаптованого стримування (Larkin, 2011, p. 55).

Концепція інтегрованого стримування була

викладена у Стратегії національної оборони США 2022 р. (U.S. Department of Defense, 2022) й передбачала узгоджене й безперервне застосування можливостей у межах різних доменів ведення бойових дій, географічних театрів, усього спектра конфлікту, а також інших інструментів національної могутності США у тісній координації з союзниками й партнерами. Додатковою опорою цієї концепції залишався безпечний, надійний та ефективний ядерний стримувальний потенціал. За визначенням колишнього міністра оборони Л. Остіна, інтегроване стримування полягає у «використанні наявних спроможностей, створенні нових та їх розгортанні у взаємопов'язаних і мережевих формах, адаптованих до регіонального безпекового середовища та реалізованих у зростаючому партнерстві з союзниками» (Mazarr & Ke, 2024, p. 13).

Сутність інтегрованого стримування відображає уявлення про те, що в умовах посилення ревізіоністських намірів потенційних супротивників США можуть найефективніше зміцнювати стримування різних форм звичайної військової агресії та високоінтенсивної діяльності в сірій зоні шляхом кращого узгодження власних інструментів впливу та поглиблення інтеграції з партнерами. Концептуальною передумовою інтегрованого стримування є визнання того, що регіональні військові тенденції протягом понад двох десятиліть розвивалися не на користь США, унаслідок чого оборонна політика потребувала переорієнтації на відновлення переконливості та дієвості американських зобов'язань у сфері воєнної безпеки. Посилення інтеграції покликане створити синергетичні ефекти, здатні підвищити загальний стримувальний ефект (U.S. Department of Defense, 2022).

Досягнення цілей інтегрованого стримування потребує двох взаємопов'язаних форм інтеграції: внутрішньої та зовнішньої. Внутрішня інтеграція стосується узгодження дій між різними елементами уряду США та Об'єднаних збройних сил, тоді як зовнішня передбачає поглиблення співпраці та взаємосумісності з союзниками й партнерами. Причинно-наслідковий зв'язок між підвищенням рівня інтеграції та посиленням стримувального ефекту становить центральну ідею документу. Зміни у військових спроможностях і амбіціях потенційних супротивників суттєво підвищили ризики для союзників і партнерів США, а також для ширших американських інтересів, унаслідок чого низка базових припущень оборонного планування пост «холодної війни» втратила актуальність. У відповідь на це ключовим завданням визначено підвищення бойової спроможності Збройних сил США таким чином, щоб вони були здатні виконувати основні воєнні місії навіть за відсутності попереднього рівня домінування. Створення більш боєздатних збройних сил розглядається як головна мета концепції інтегрованого стримування. Основний аргумент Стратегії полягає в тому, що найбільш реалістичний шлях до посилення бойової спроможності полягає у максимізації наявної бойової потужності шляхом тісного поєднання всіх її складових. Інтегроване стримування постає як теорія реалізації, оскільки ідеться про способи, за допомогою яких скоординоване державне управління дозволяє максимізувати ефект від уже наявних і запланованих можливостей. Використання синергії, як усередині американських структур, так і разом із союзниками, є найбільш перспективним шляхом зміцнення стримування. Хоча цей підхід не був повністю реалізований до початку повномасштабного вторгнення росії в Україну, подальша стратегія США щодо стримування ескалації та покарання агресії розглядалась як один із найбільш наочних емпіричних прикладів логіки інтегрованого стримування (U.S. Department of Defense, 2022).

У відповідь на агресію росії проти України США поєднали зусилля з багатьох доменів і різних сегментів державної влади з метою досягнення стримувального та карального ефекту. До цього комплексу заходів увійшли військова допомога й підготовка, обмін розвідувальною інформацією, дипломатичні дії, економічний примус і підтримка, а також багатосторонні зусилля з координації дій союзників і партнерів. Демонструючи модель справді всеосяжної національної відповіді на агресію, США створили прецедент, який може бути застосований превентивно у майбутніх конфліктах для обіцянки здатності позбавляти агресора досягнення його цілей, накладати суттєві витрати та підвищувати стійкість держави-жертви агресії. Досвід України засвідчує, що інтегроване стримування може бути концептуалізоване щонайменше на двох рівнях. Перший, вужчий рівень має тактико-операційний характер і зосереджується на створенні синергії між різними ефектами. Другий, ширший рівень має геостратегічний вимір і передбачає застосування загальнодержавних підходів («whole-of-government») до стримування та конфлікту загалом. У межах вузького підходу акцент робиться на ініціативах із посилення внутрішньої інтеграції, зокрема таких як спільне у всіх доменах командування та контроль (Joint All-Domain Command and Control (JADC2)), а також на операційній взаємосумісності з союзниками й партнерами. Ширше розуміння інтегрованого стримування виходить за межі суто військових питань і охоплює поєднання військових, економічних, політичних та інформаційних інструментів, які можуть використовуватися для погроз, стримування і, за необхідності, покарання агресорів у більш комплексний і взаємопосилювальний спосіб. Заходи з нарощування спроможностей розглядаються як один із ключових елементів інтегрованого стримування, оскільки вони безпосередньо зміцнюють здатність США до ефективного ведення бойових дій у межах

ширшого багатовимірного стримувального підходу. Водночас центральний меседж Стратегії 2022 р. полягав в тому, що окремі покращення спроможностей, хоч і є необхідними, самі по собі не є достатніми для досягнення ключових стримувальних цілей. Вони мають супроводжуватися цілеспрямованими зусиллями з інтеграції американських можливостей і видів діяльності таким чином, щоб створювати нові форми синергії та підвищувати бойову достовірність оперативних планів США (Mazarr, & Ke, 2024, p. 15).

У площині інформаційного стримування концепція інтегрованого стримування набуває форми цілеспрямованого стратегічного сигналу про неминучість відповіді на агресивні дії, незалежно від домену, в якому вони здійснюються. Центральним елементом такого сигналу є публічне й інституційно закріплене повідомлення, зафіксоване у стратегічних документах США, про те, що ревізіоністська поведінка не залишатиметься без наслідків. Це повідомлення не зводиться до конкретних погроз чи сценаріїв застосування сили, а формує стійке очікування, що будь-яка агресія, включно з діями в інформаційному просторі або іншими формами підпорогового примусу, буде включена до ширшого розрахунку покарання. Інформаційна складова інтегрованого стримування працює як самостійний інструмент формування уявлень потенційного агресора про структуру ризиків і як допоміжний канал комунікації. Донесення думки про стримування через покарання принаймні буде застосоване у разі провалу стримування через відмову, створює для ревізіоністських акторів ситуацію принципової невизначеності щодо меж допустимого. Вони не можуть з упевненістю розраховувати на безкарність дій у «сірих» або інформаційних доменах, оскільки відповідь може бути відкладеною, асиметричною та реалізованою через поєднання військових, економічних, політичних і інформаційних засобів. Таким чином, інформаційне стримування в межах інтегрованого підходу не обмежується попередженням або контрнаративами, а виконує системоутворюючу функцію: пов'язує окремі дії агресора в єдину рамку стратегічної відповідальності, що є ключовим чинником стримування в умовах сучасної стратегічної конкуренції, де межі між війною і миром, військовими та немілітарними діями, інформаційним впливом і силовим примусом є принципово розмитими.

Ключове, хоча й не завжди прямо артикульоване, припущення концепції інтегрованого стримування полягає в тому, що саме глибша інтеграція інструментів державної влади США, у поєднанні з діями союзників і партнерів, є найбільш перспективним засобом посилення стримувального ефекту в сучасних умовах. Проте, трансформація характеру війни у бік мережево-технологічних форм ведення операцій об'єктивно вимагає більш комплексної інтеграції. За відсутності такої інтеграції США не зможуть суттєво підвищити бойову переконливість власних сил. Стратегія національної безпеки визначає інтегроване стримування як «безшовне поєднання можливостей з метою переконати потенційних супротивників, що вартість їхніх ворожих дій перевищує очікувані вигоди». При цьому наголошується, що інтегроване стримування передбачає ефективнішу координацію, мережування та інновації, аби будь-який конкурент, який прагне здобути перевагу в одному домені, усвідомлював можливість відповіді в багатьох інших. Такий підхід не скасовує традиційної ролі переконливих конвенційних і стратегічних спроможностей, а підсилює їх, дозволяючи точніше формувати сприйняття ризиків і витрат потенційним агресором у будь-який момент і в будь-якому домені. Відповідно, «ядром інтегрованого стримування» прямо визначено розвиток, поєднання та координацію наявних переваг для досягнення максимального ефекту (U.S. Department of Defense, 2022).

Концепція інтегрованого стримування відрізняється від попередніх уявлень про міждоменне стримування тим, що в сучасному технологічному та геополітичному середовищі ефективність стримування залежить від системної синергії різних можливостей, тобто комплексне поєднання військових, політичних, економічних, інформаційних та інших інструментів. У суто військово-операційному вимірі, в умовах мережевої війни та зростаючої ролі інформації й автоматизації, різні форми інтеграції стають не додатковою перевагою, а передумовою ефективності. Саме посилення синергій розглядається як спосіб досягти більш негайного і водночас стійкішого стримувального ефекту.

Попри концептуальну привабливість технології інтегрованого стримування, дослідники звертають увагу на низку структурних і практичних обмежень, які ускладнюють її реалізацію в умовах сучасної стратегічної конкуренції. Технологія інтегрованого стримування істотно підвищує складність комунікації стримувальних сигналів. Чим більш багатовимірною є стратегія, з поєднанням військових, економічних, дипломатичних та інформаційних інструментів, тим важче забезпечити однозначне сприйняття намірів і «червоних ліній» потенційним противником. В інформаційному середовищі це підвищує ризик шуму, суперечливих сигналів і помилкових інтерпретацій, що може не посилювати, а послаблювати стримувальний ефект. Концепція інтегрованого стримування значною мірою спирається на припущення, що держава-ініціатор здатна досить точно зрозуміти, як її дії інтерпретуються конкретним лідером або елітною групою. В умовах інформаційної асиметрії, культурних відмінностей і навмисної дезінформації це припущення є вразливим. Інформаційний простір лише посилює цю проблему, оскільки наративи можуть бути переосмислені, спотворені або використані самим

противником для внутрішньої мобілізації. Ризик хибної впевненості, коли формалізовані інтегровані підходи можуть створювати ілюзію контролю над ескалацією та ефективністю сигналів, проявляється у вірі, що правильно скоординовані повідомлення, санкції та демонстрації спроможностей автоматично транслюються у бажаний ефект. Проте, стримування залишається політичним процесом, а не технічною процедурою, і не піддається повній оптимізації.

Технологія інтегрованого стримування стикається з проблемою внутрішньої координації, сутність якого полягає в тому, що поєднання численних інструментів і акторів (від військових структур до дипломатії та інформаційних інституцій) ускладнює узгодження повідомлень і дій. Для інформаційного стримування це означає ризик фрагментованого сигналювання, коли різні елементи державної політики транслюють несумісні або взаємно нівелюючі меседжі. Обмеження ефективності технології інтегрованого стримування також пов'язане з ескалаційною невизначеністю. Інтеграція дій у різних доменах може непередбачувано підвищувати ставки, особливо коли інформаційні операції перетинаються з військовими або кібердіями. У такій ситуації противник може інтерпретувати інтегровані сигнали як підготовку до ширшого конфлікту, навіть якщо намір полягає у стримуванні, що підриває стабілізуючу функцію стратегії.

Асиметрія застосування технології інтегрованого стримування проявляється в тому, що авторитарні режими з централізованим контролем над інформаційним простором можуть легше координувати інтегровані дії, ніж відкриті суспільства, де інформаційне середовище є плюралістичним і менш керованим, що створює структурний виклик для інформаційного стримування з боку демократичних держав. До того ж, з'являється ризик концептуального розмивання. Якщо інтегроване стримування охоплює надто широкий спектр дій - від військового планування до інформаційної політики загалом, - воно може перетворитися на узагальнену метафору державної активності, в разі чого стримування перестає бути чітко артикульованим механізмом запобігання агресії, зокрема в інформаційному просторі. Отже, у сукупності ці зауваження дозволяють стверджувати, що технологія інтегрованого стримування створює важливі можливості для розвитку інформаційного стримування, але водночас висуває підвищені вимоги до якості комунікації, розуміння сприйняття противника та контролю ескалації. В інформаційному вимірі ці обмеження проявляються найбільш гостро, що робить його водночас ключовим елементом і найбільш уразливою складовою технології інтегрованого стримування.

Висновки.

В умовах трансформації сучасної міжнародної системи безпеки, розмивання меж між війною і миром та поширення підпорогових, гібридних і багатодоменних форм агресії класичні моделі стримування, зосереджені переважно на військовому або ядерному вимірі, є концептуально та практично недостатніми для забезпечення безпеки держав Європейського Союзу. Російська агресивна політика щодо України та європейського безпекового простору загалом засвідчила системний характер загроз, які поєднують військові, економічні, інформаційні, енергетичні та політико-дипломатичні інструменти впливу в єдину технологію примусу і дестабілізації. У цьому контексті інтегроване стримування постає не як чергова варіація традиційної теорії стримування, а як цілісна технологія управління стратегічною поведінкою потенційного агресора, що ґрунтується на скоординованому та взаємопосиленому застосуванні всього спектра інструментів державної та наддержавної потуги. Доведено, що саме технологічний підхід дозволяє адекватно осмислити інтегроване стримування як системно організований процес, що включає вироблення стратегічних сигналів, інституційну координацію, управління сприйняттям ризиків і витрат, а також формування довгострокових моделей стримувальної поведінки в умовах тривалої стратегічної конкуренції. Велике значення для здійснення технології інтегрованого стримування має інформаційний вимір, який виступає важливим елементом цієї технології. З'ясовано, що інформаційне стримування виходить далеко за межі контрпропаганди чи реагування на дезінформаційні кампанії та полягає у формуванні стійких уявлень потенційного агресора про неминучість політичних, економічних і стратегічних наслідків агресивних дій незалежно від домену їх здійснення. В умовах, коли значна частина російської агресії реалізується нижче порогу відкритої війни, саме інтеграція інформаційних, економічних і політичних інструментів у єдину стримувальну рамку підвищує переконливість та ефективність стримування. Дослідження також підтвердило, що для країн Європейського Союзу інтегроване стримування має не лише теоретичне, а й безпосереднє практичне значення. ЄС, перебуваючи в зоні прямої або опосередкованої дії російської загрози, потребує узгодженої, стратегічно цілісної та довгострокової моделі безпеки, яка виходить за межі фрагментарних або реактивних заходів. Інтегроване стримування створює концептуальну основу для поєднання оборонних спроможностей, санкційної політики, енергетичної безпеки, стратегічних комунікацій і партнерської взаємодії з НАТО та США в єдину технологію забезпечення безпеки. Водночас наголошено, що ефективність цієї технології прямо залежить від рівня внутрішньої координації в межах ЄС, політичної єдності держав-членів і готовності до тривалої стратегічної конкуренції. Технологія інтегрованого стримування є найбільш адекватною відповіддю на системну та багатовимірну російську

загрозу в сучасних умовах. Вона дозволяє не лише підвищити стійкість країн Європейського Союзу до агресивних дій нижче порогу війни, а й сформувати довгострокову архітектуру безпеки, засновану на поєднанні стримування шляхом відмови, покарання та управління стратегічними очікуваннями. Таким чином, технологія інтегрованого стримування постає як ключовий інструмент забезпечення безпеки ЄС у XXI столітті та як перспективний напрям подальших наукових і прикладних досліджень у галузі міжнародних відносин і безпекових студій.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Висоцький, О. Ю. (2017). Легітимаційні технології в міжнародних відносинах. *Науково-теоретичний альманах Грані*. 2017. № 20 (10). P. 98-104. https://doi.org/10.15421/1717138

Висоцький, О.Ю. (2018). Електронна дипломатія як інструмент пропаганди. *Політологічний вісник*, 81. С.51-59. https://doi.org/10.17721/2415-881x.2018.81.51-59

Висоцький, О. (2021). Політична безпека держави в умовах нестабільності міжнародно-політичного середовища. *Науково-теоретичний альманах Грані*, *24*(2), 13-23. https://doi.org/10.15421/172110

Amadio Viceré, M.G., Sus, M. Organizing European security through informal groups: insights from the European Union's response to the Russian war in Ukraine. *Int Polit* 62, 931–946 (2025). https://doi.org/10.1057/s41311-024-00657-7

Blank, S. J. (2024). Ukraine and an Integrated Deterrence Strategy. *Orbis,* 68(3), 491–511. https://doi.org/10.1016/j.orbis.2024.05.009

Boyan Mitrakiev, Noncho Dimitrov. (2024). Russian Reflexive Control Campaigns Targeting Political Realignment of Ukraine's Democratic Allies: Critical Review and Conceptualization. *Information & Security: An International Journal,* 55, no. 3, 299-330. https://doi.org/10.11610/isij.5519

Freedman, L. (2023). The Russo-Ukrainian War and the Durability of Deterrence. *Survival*, *65*(6), 7–36. https://doi.org/10.1080/00396338.2023.2285598

Hadano, T. 2024. Agents, multilateral institutions, and fundamental institutional change in international society: The case of Russia's peacekeeping policy. *European Journal of International Security* 9, 78–96. https://doi.org/10.1017/eis.2023.22

Hoeffler, C., Hofmann, S. C., & Mérand, F. (2024). The polycrisis and EU security and defence competences. *Journal of European Public Policy*, *31*(10), 3224–3248. https://doi.org/10.1080/13501763.2024.2362762

Huth, P.K. (1999). Deterrence and international conflict: Empirical Findings and Theoretical Debates. *Annual Review of Political Science, 2, 25-48.* https://doi.org/10.1146/annurev.polisci.2.1.25

Johnson, M., & Kelly, T. K. (2014). Tailored deterrence: Strategic context to guide Joint Force 2020. *Joint Force Quarterly,* 74(3), 22–29. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_22-29_Johnson-Kelly.pdf

Kakhishvili, L., Felder, A. (2025). The Russian invasion of Ukraine and changes in MEPs' conceptions of security. *Int Polit* 62, 1084–1096 https://doi.org/10.1057/s41311-024-00646-w

Kofroň J., & Stauber, J. (2021): The impact of the Russo-Ukrainian conflict on military expenditures of European states: security alliances or geography? *Journal of Contemporary European Studies,* https://doi.org/10.1080/14782804.2021.1958201

Larkin, S. P. (2011). The limits of tailored deterrence. *Joint Force Quarterly,* 63(4), 47–57. https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1051&context=jfq-full-issue

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies,* 46(4). https://doi.org/10.1080/01402390.2023.2177987

Lindsay, J. R. (2020). *Information technology and military power*. New York: Cornell University Press.

Lindsay, J. R., & Gartzke, E. (Eds.). (2019). *Cross-domain deterrence: Strategy in an era of complexity.* Oxford University Press.

Mallory, K. (2018). *New challenges in cross-domain deterrence* (RAND Expert Insights). RAND Corporation. https://www.rand.org/pubs/perspectives/PE259.html

Mazarr, M. J., & Ke, I. (2024). *Integrated deterrence as a defense planning concept* (RAND Expert Insights). RAND Corporation. https://www.rand.org/pubs/perspectives/PEA2263-1.html

Mazarr, M. J., Cheravitch, J., Hornung, J. W., & Pezard, S. (2021). What deters and why: Applying a framework to assess deterrence of gray zone aggression (Research Report No. RR-3142-A). RAND Corporation. https://www.rand.org/pubs/research_reports/RR3142.html

Morgan, P. M. (2019). The past and future of deterrence theory. In J. R. Lindsay & E. Gartzke (Eds.), *Cross-domain deterrence: Strategy in an era of complexity* (pp. 50–65). Oxford University Press.

Rose, Richard. (2025). European security : from Ukraine to Washington / Richard Rose. London ; New York : Bloomsbury Academic.

Šenk, M., & Hynek, N. (2025). NATO/EU synergies against information warfare: a "circulatory institutionalist" model of expert voluntarism. *European Security*, 1–22. https://doi.org/10.1080/09662839.2025.2566519

U.S. Department of Defense. (2022). The National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-national-defense-strategy-npr-mdr.pdf

Vysotskyi, O. (2023). National Security Technologies in the Domestic and Foreign Policy of the State. *Scientific and Theoretical Almanac Grani*, *26*(3), 126-133. https://doi.org/10.15421/172358

Wirtz, J. J., & Larsen, J. A. (2024). Wanted: a strategy to integrate deterrence. *Defense & Security Analysis*, *40*(3), 361–378. https://doi.org/10.1080/14751798.2024.2352943

Wirtz, J., & Larsen, J. (2023). Who Does Deterrence? The Politics and Strategy of Integrated Deterrence. *The RUSI Journal*, *168*(6), 14–20. https://doi.org/10.1080/03071847.2023.2288133

REFERENCES

Amadio Viceré, M.G., & Sus, M. (2025). Organizing European security through informal groups: insights from the European Union's response to the Russian war in Ukraine. *Int Polit* 62, 931–946. https://doi.org/10.1057/s41311-024-00657-7

Blank, S. J. (2024). Ukraine and an Integrated Deterrence Strategy. *Orbis,* 68(3), 491–511. https://doi.org/10.1016/j.orbis.2024.05.009

Boyan Mitrakiev, Noncho Dimitrov. (2024). Russian Reflexive Control Campaigns Targeting Political Realignment of Ukraine's Democratic Allies: Critical Review and Conceptualization. Information & Security: *An International Journal*, 55, no. 3, 299-330. https://doi.org/10.11610/isij.5519

Freedman, L. (2023). The Russo-Ukrainian War and the Durability of Deterrence. *Survival*, *65*(6), 7–36. https://doi.org/10.1080/00396338.2023.2285598

Hadano, T. 2024. Agents, multilateral institutions, and fundamental institutional change in international society: The case of Russia's peacekeeping policy. *European Journal of International Security*, 9, 78–96. https://doi.org/10.1017/eis.2023.22

Hoeffler, C., Hofmann, S. C., & Mérand, F. (2024). The polycrisis and EU security and defence competences. *Journal of European Public Policy*, *31*(10), 3224–3248. https://doi.org/10.1080/13501763.2024.2362762

Huth, P.K. (1999). Deterrence and international conflict: Empirical Findings and Theoretical Debates. *Annual Review of Political Science, 2, 25-48.* https://doi.org/10.1146/annurev.polisci.2.1.25

Johnson, M., & Kelly, T. K. (2014). Tailored deterrence: Strategic context to guide Joint Force 2020. *Joint Force Quarterly,* 74(3), 22–29. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_22-29_Johnson-Kelly.pdf

Kakhishvili, L., Felder, A. (2025). The Russian invasion of Ukraine and changes in MEPs' conceptions of security. *Int Polit* **62**, 1084–1096 https://doi.org/10.1057/s41311-024-00646-w

Kofroň J., & Stauber, J. (2021): The impact of the Russo-Ukrainian conflict on military expenditures of European states: security alliances or geography? *Journal of Contemporary European Studies,* https://doi.org/10.1080/14782804.2021.1958201

Larkin, S. P. (2011). The limits of tailored deterrence. Joint Force Quarterly, 63(4), 47–57. https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1051&context=jfq-full-issue

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. Journal of Strategic Studies, 46(4). https://doi.org/10.1080/01402390.2023.2177987

Lindsay, J. R. (2020). *Information technology and military power*. New York: Cornell University Press.

Lindsay, J. R., & Gartzke, E. (Eds.). (2019). *Cross-domain deterrence: Strategy in an era of complexity.* Oxford University Press.

Mallory, K. (2018). New challenges in cross-domain deterrence (RAND Expert Insights). RAND Corporation. https://www.rand.org/pubs/perspectives/PE259.html

Mazarr, M. J., & Ke, I. (2024). Integrated deterrence as a defense planning concept (RAND Expert Insights). RAND Corporation. https://www.rand.org/pubs/perspectives/PEA2263-1.html

Mazarr, M. J., Cheravitch, J., Hornung, J. W., & Pezard, S. (2021). What deters and why: Applying a framework to assess deterrence of gray zone aggression (Research Report No. RR-3142-A). RAND Corporation. https://www.rand.org/pubs/research_reports/RR3142.html

Morgan, P. M. (2019). The past and future of deterrence theory. In J. R. Lindsay & E. Gartzke (Eds.), *Cross-domain deterrence: Strategy in an era of complexity* (pp. 50–65). Oxford University Press.

Rose, Richard. (2025). *European security : from Ukraine to Washington*. Richard Rose. London ; New York : Bloomsbury Academic.

Šenk, M., & Hynek, N. (2025). NATO/EU synergies against information warfare: a "circulatory institutionalist" model of expert voluntarism. *European Security*, 1–22. https://doi.org/10.1080/09662839.2025.2566519

U.S. Department of Defense. (2022). The National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-national-defense-strategy-npr-mdr.pdf

Vysotskyi, O. (2021). Politychna bezpeka derzhavy v umovakh nestabilnosti mizhnarodno-politychnoho seredovyshcha. *Naukovo-teoretychnyy almanakh Hrani. Scientific and Theoretical Almanac Grani,* 24(2), 13–23. https://doi.org/10.15421/172110

Vysotskyi, O. (2023). National Security Technologies in the Domestic and Foreign Policy of the State. *Scientific and Theoretical Almanac Grani*, *26*(3), 126-133. https://doi.org/10.15421/172358

Vysotskyi, O. Yu. (2018). Elektronna diplomatyya yak instrument propagandy. *Politolohichnyi visnyk*, 81, 51–59. https://doi.org/10.17721/2415-881x.2018.81.51-59

Vysotskyi, O.Yu. (2017). Lehitymatsiyni tekhnolohiyi v mizhnarodnykh vidnosynakh. *Naukovo-teoretychnyy almanakh Hrani. Scientific and Theoretical Almanac Grani,* 20(10), 98-104. https://doi.org/10.15421/1717138

Wirtz, J. J., & Larsen, J. A. (2024). Wanted: a strategy to integrate deterrence. *Defense & Security Analysis*, *40*(3), 361–378. https://doi.org/10.1080/14751798.2024.2352943

Wirtz, J., & Larsen, J. (2023). Who Does Deterrence? The Politics and Strategy of Integrated Deterrence. *The RUSI Journal*, *168*(6), 14–20. https://doi.org/10.1080/03071847.2023.2288133