МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародних відносин

Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

Освітня програма 291.00.01 «Суспільні комунікації»

БАКАЛАВРСЬКА РОБОТА
на тему:
ГІБРИДНИЙ ІНСТРУМЕНТАРІЙ ЯК СКЛАДОВА АГРЕСИВНОЇ ЗОВНІШНЬОЇ ПОЛІТИКИ РФ

Студентки 4 курсу
денної форми навчання
Шумейко Олени Володимирівни

Науковий керівник:
канд. політ. наук, доцент
доцент кафедри міжнародних відносин
Жовтенко Т.Г.

Київ – 2026

ЗМІСТ

ВСТУП

Актуальність обраної теми зумовлена глибокими трансформаціями сучасної системи міжнародної безпеки, у межах яких класичні форми збройного протистояння дедалі частіше поступаються комбінованим моделям впливу. Зміна характеру конфліктів супроводжується активним використанням інструментів, що поєднують інформаційний тиск, економічні важелі, кібероперації та обмежені силові дії. У цьому вимірі гібридна агресія російської федерації виступає одним із найбільш показових прикладів сучасних стратегій впливу. Україна опинилася в епіцентрі таких процесів, що надає дослідженню не лише теоретичного, але й виразного практичного значення. Поглиблений аналіз механізмів гібридної війни дозволяє краще зрозуміти логіку сучасних конфліктів і сформувати ефективні підходи до їх стримування.

Об’єктом дослідження виступають сучасні міжнародні безпекові процеси в умовах поширення гібридних форм конфліктів.

Предметом дослідження є інструменти, механізми та практика застосування гібридної агресії російської федерації, а також міжнародні підходи до протидії таким загрозам.

Метою дослідження є комплексний аналіз гібридної агресії російської федерації як сучасної форми зовнішньополітичного впливу, а також визначення ефективних механізмів міжнародного реагування та протидії.

Відповідно до поставленої мети визначено такі завдання дослідження:

– дослідити теоретичні підходи до розуміння сутності гібридної війни;

– проаналізувати основні інструменти та механізми гібридного впливу;

– охарактеризувати роль України як ключового об’єкта гібридної агресії російської федерації;

– встановити особливості практики застосування гібридних інструментів у міжнародному середовищі;

– визначити основні міжнародні механізми реагування та протидії гібридним загрозам;

– з'ясувати сучасні тенденції трансформації гібридної війни та їх вплив на міжнародну безпеку.

Теоретичне значення дослідження полягає у поглибленні наукових уявлень про природу гібридної війни, уточненні її структурних характеристик та виявленні закономірностей взаємодії різних інструментів впливу, що розвиває підходи до осмислення сучасних конфліктів, запропоновані Мері Калдор (Mary Kaldor)[1]. Проведений аналіз дозволяє конкретизувати уявлення про поєднання військових і невійськових засобів у межах єдиної стратегії впливу, що узгоджується з позиціями Френка Гоффмана (Frank Hoffman)[2], який розглядає гібридну війну як інтегровану модель застосування сили. Водночас результати дослідження уточнюють роль невизначеності та гнучкості у сучасних конфліктах, що співвідноситься з висновками Ендрю Мамфорда (Andrew Mumford) та Паскаля Карлуччі (Pascal Carlucci)[3], які акцентують увагу на трансформації традиційних форм війни. Отримані положення сприяють розвитку теоретичних підходів до аналізу сучасних конфліктів, дозволяють систематизувати інструменти гібридного впливу та визначити їх взаємозв'язки, що корелює з аналітичними підходами Маркуса Йоранссона (Markus Göransson)[4] щодо адаптивності сучасних стратегій. Крім того, результати дослідження розширюють наукове розуміння механізмів впливу на

---

[1] Kaldor M. In defence of new wars. *Stability: International Journal of Security and Development*. 2013. Vol. 2, No. 1. Article 4 DOI: https://doi.org/10.5334/sta.at.

[2] Hoffman F., Neumeyer M., Jensen B. The future of hybrid warfare. URL: https://www.csis.org/analysis/future-hybrid-warfare (date of access: 13.04.2026).

[3] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192–206. DOI: https://doi.org/10.1017/eis.2022.19.

[4] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449–471. DOI: https://doi.org/10.1080/14702436.2024.2365214.

політичні та соціальні процеси, що відповідає висновкам Аліни Полякової (Alina Polyakova) та Матьє Булега (Mathieu Boulègue)[5] про значення невизначеності у формуванні гібридних загроз. У сукупності це створює підґрунтя для подальших наукових досліджень у сфері міжнародних відносин та безпеки, зокрема у частині розробки нових концептуальних моделей протидії сучасним формам агресії.

Практичне значення полягає у можливості використання результатів дослідження для розробки ефективних стратегій протидії гібридним загрозам, удосконалення державної політики у сфері безпеки, а також підвищення рівня стійкості суспільства до зовнішніх впливів. Висновки роботи можуть бути застосовані у діяльності органів державної влади, аналітичних центрів та міжнародних організацій.

Структура роботи зумовлена метою і завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. У першому розділі розглядаються теоретичні засади дослідження гібридної війни. Другий розділ присвячений аналізу інструментів і механізмів гібридного впливу. У третьому розділі досліджується практика застосування гібридних інструментів російської федерації та міжнародні механізми протидії. Завершується робота формулюванням узагальнених висновків.

[5] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-conclusion/ (date of access: 13.04.2026)

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ГІБРИДНОЇ ВІЙНИ

1.1. Поняття та сутність гібридної війни

Поняття гібридної війни сформувалося як реакція на зміну характеру конфліктів у постбіполярний період, коли класичне протистояння регулярних армій перестало бути єдиною домінуючою формою силового впливу[6]. Вже на початку 2000-х років у військово-стратегічній думці з'являється усвідомлення того, що сучасні конфлікти дедалі частіше поєднують регулярні й нерегулярні методи ведення війни, доповнені інформаційними, економічними та кібернетичними інструментами[7]. Саме ця комбінація, що не вкладається у традиційні рамки «війни» або «миру», і стала основою концепту гібридної війни[8].

Одразу варто зауважити, що у науковому дискурсі відсутнє єдине універсальне визначення цього явища. Частина дослідників трактує гібридну війну як новий тип конфлікту, тоді як інші розглядають її як еволюцію вже існуючих форм боротьби. Так, у роботі британської науковиці Мері Калдор наголошується, що сучасні конфлікти загалом відходять від класичних міждержавних війн і набувають ознак так званих «нових війн», де ключову роль відіграють не стільки територіальні завоювання, скільки контроль над інформаційним простором, населенням і ресурсами[9]. У цьому вимірі гібридна війна постає як конкретизація ширшої трансформації природи конфліктів[10].

Водночас більш прикладні дослідження підкреслюють інструментальний вимір гібридності. Ендрю Мамфорд і Паскаль Карлуччі у статті «Гібридна війна:

---

[6] Kaldor M. In defence of new wars. Stability: International Journal of Security and Development. 2013. Vol. 2, No. 1. Article 4. P. 4

[7] Hoffman F., Neumeyer M., Jensen B. The future of hybrid warfare.

[8] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192.

[9] Ibid.

[10] Ibid.

продовження неоднозначності іншими засобами» визначають гібридну війну як продовження політики іншими засобами за умов принципової невизначеності та розмитості меж між різними формами насильства[11]. Така керована невизначеність не є випадковим явищем, вона виступає продуманим стратегічним підходом, що ускладнює ідентифікацію агресора, затримує міжнародну реакцію і дозволяє діяти нижче порогу колективної оборони[12].

Суттєвим доповненням до цього підходу є позиція Френка Гоффмана та інших дослідників, які наголошують на синхронному використанні різних типів сили, від високотехнологічних військових операцій до дій нерегулярних формувань і інформаційних кампаній[13]. Йдеться не про випадкове поєднання, а про цілісну систему, де кожен інструмент підсилює інший. Обмежене застосування військової сили може супроводжуватися масштабною дезінформаційною кампанією, що змінює сприйняття подій як всередині країни-мішені, так і за її межами [14].

Якщо перейти до емпіричних проявів, російська практика останніх років демонструє чітко вибудувану конфігурацію такого підходу. Під час агресії проти України спостерігається поєднання регулярних військових операцій із діяльністю нерегулярних формувань, кібератаками на державну інфраструктуру та системними інформаційними кампаніями[15]. У дослідженні Майкла Бейкера, Джейкоба Бейкера та Фредеріка Беркла наголошується, що навіть сфера охорони здоров’я стала об’єктом впливу, де атаки на медичні установи, дезінформація щодо гуманітарних

---

[11] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192.

[12] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-conclusion/

[13] Hoffman F., Neumeyer M., Jensen B. The future of hybrid warfare. URL: https://www.csis.org/analysis/future-hybrid-warfare

[14] Giles K. The next phase of Russian information warfare. Riga: NATO Strategic Communications Centre of Excellence. 2016. URL: https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176

[15] Bachmann S.-D. D., Gunneriusson H. Russia’s hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. Georgetown Journal of International Affairs. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198

процесів і маніпуляції нормами міжнародного права використовувалися як інструменти тиску[16]. Це свідчить про вихід гібридної війни за межі суто військової сфери.

Дослідження Мауріціо Джері «Розуміння російської гібридної війни проти Європи в енергетичному секторі та в майбутньому безпековому вимірі “енергетика–ресурси–клімат”» демонструє, що енергетичний сектор став одним із ключових каналів впливу. Маніпуляції з постачанням енергоресурсів, створення штучних дефіцитів і використання залежності як політичного інструменту дозволяють досягати стратегічних цілей без відкритого втручання[17]. Цей економічний вплив супроводжується інформаційним забезпеченням, що формує відповідні інтерпретації у суспільстві.

Кібернетичний компонент гібридного інструментарію забезпечує новий рівень впливу. Його застосування не завжди супроводжується фізичними руйнуваннями, проте здатне суттєво впливати на функціонування держави[18]. Атаки на енергетичні системи, втручання у виборчі процеси, порушення роботи фінансових інституцій створюють ефект дестабілізації, який складно однозначно класифікувати.

На концептуальному рівні гібридні загрози слід розглянути у межах міжнародних організацій. Організація Північноатлантичного договору визначає їх як поєднання військових і невійськових засобів, спрямованих на підрив стабільності

[16] Baker M. S., Baker J., Burkle F. M. Russia’s hybrid warfare in Ukraine threatens both healthcare & health protections provided by international law. Annals of Global Health. 2023. Vol. 89, No. 1. Article 3. DOI: https://doi.org/10.5334/aogh.4022

[17] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future “energy-resources-climate” security nexus. Journal of Strategic Security. 2024. Vol. 17, No. 3. Article 2. URL: https://digitalcommons.usf.edu/jss/vol17/iss3/2/

[18] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. Security Science Journal. 2025. Vol. 6, No. 2. DOI: https://doi.org/10.37458/ssj.6.2.3.

держави[19]. Особливий акцент робиться на координації інструментів впливу, що передбачає комплексну відповідь, яка виходить за межі військової сфери[20].

Водночас варто розмежовувати поняття гібридних загроз і власне гібридної війни. Гібридні загрози можуть існувати ще до початку відкритого конфлікту і проявлятися через інформаційний тиск, економічний шантаж, кібератаки, підтримку радикальних груп, дипломатичні маніпуляції або спроби впливу на суспільну думку. Їхня мета полягає не завжди у негайному воєнному результаті, а часто у поступовому послабленні держави, зниженні довіри до інститутів влади, дестабілізації внутрішньої політичної ситуації та створенні умов для подальшої ескалації. Натомість гібридна війна є більш цілісною і скоординованою формою такого впливу, коли різні інструменти застосовуються не окремо, а як частини єдиної стратегії.

Це розмежування має принципове значення, оскільки не кожна гібридна загроза автоматично означає стан війни. Однак системне, тривале і цілеспрямоване використання таких загроз проти держави може поступово формувати ситуацію гібридного конфлікту. У цьому разі агресор прагне діяти у проміжному просторі між миром і війною, зберігаючи можливість заперечувати власну участь або подавати свої дії як внутрішню кризу країни-мішені. Отже гібридна війна небезпечна не лише через поєднання різних засобів впливу, а й через здатність маскувати справжній характер агресії.

Для кращого розуміння співвідношення різних форм конфліктів і місця гібридної війни доцільно звернутися до узагальненої моделі, яка відображає її положення між низькоінтенсивними конфліктами та повномасштабними війнами.

---

[19] Countering hybrid threats. North Atlantic Treaty Organization. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats/

[20] Ibid.

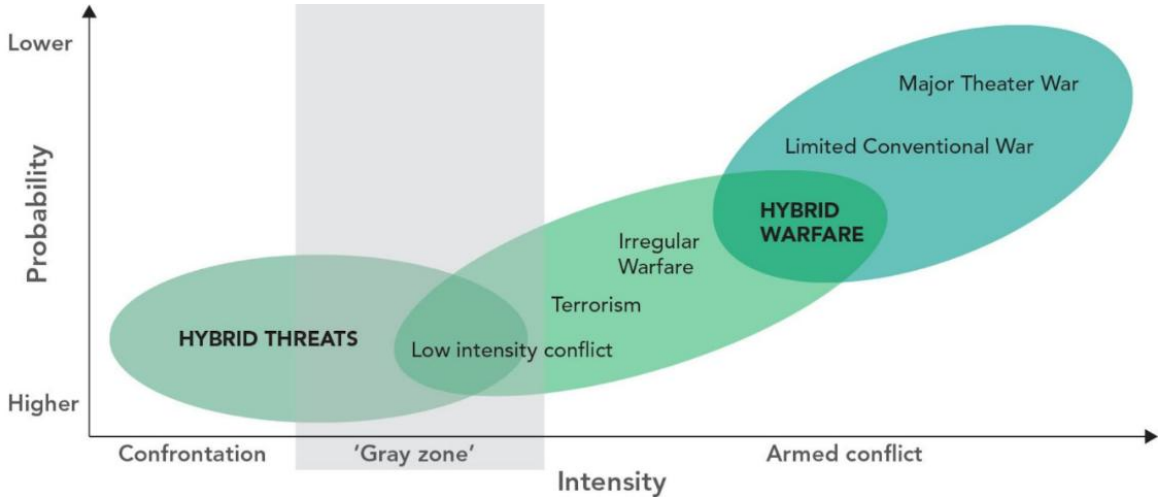

Рисунок 1.1 – Співвідношення гібридних загроз, гібридної війни та традиційних форм конфлікту

Джерело: Monaghan S. Countering Hybrid Warfare: So What for the Joint Force? National Defense University Press. 2019. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979787/countering-hybrid-warfare-so-what-for-the-joint-force/ (date of access: 21.04.2026).

Представлена схема демонструє, що гібридна війна займає проміжне положення між конфліктами з низькою інтенсивністю та обмеженими або масштабними війнами. Вона розвивається у зоні, яку часто визначають як «сіру», де рівень інтенсивності поступово зростає, а межі між різними формами протистояння залишаються нечіткими. Гібридні загрози можуть існувати ще до відкритого конфлікту, формуючи підґрунтя для подальшої ескалації. Гібридна війна здатна трансформуватися у більш інтенсивні форми, зберігаючи при цьому елементи непрямих дій.

Сучасні дослідження підкреслюють адаптивність гібридної стратегії. У дослідженні «Російське бачення нових війн та повномасштабне вторгнення в Україну» Маркус Йоранссон звертає увагу на постійне коригування інструментів

залежно від реакції противника[21]. Це означає, що гібридна війна не має фіксованої структури, вона змінюється разом із середовищем[22]. Така гнучкість підвищує ефективність впливу і ускладнює протидію[23].

Ця адаптивність пов'язана з використанням «сірих зон» міжнародного права, тобто значна частина дій не підпадає під чіткі визначення агресії, що дозволяє уникати прямої відповідальності[24]. А. Полякова та М. Булег наголошують, що саме ця невизначеність забезпечує ефективність гібридної стратегії, оскільки вона ускладнює формування консолідованої відповіді[25].

У підсумку гібридну війну доцільно розглядати як інтегровану систему впливу, що поєднує військові, інформаційні, економічні та кібернетичні інструменти. Її ключовими характеристиками виступають розмитість меж між війною і миром, адаптивність, гнучкість і орієнтація на досягнення політичних результатів без відкритої ескалації. Системність забезпечує ефективність гібридної стратегії, водночас створюючи суттєві виклики для сучасної системи міжнародної безпеки[26].

1.2. Класифікація та інструменти гібридного впливу

Класифікація інструментів гібридного впливу потребує не лише формального групування, а передусім виявлення їхньої функціональної ролі у досягненні стратегічних цілей держави-агресора[27]. Якщо на попередньому етапі аналізу увага

---

[21] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. Defence Studies. 2024. Vol. 24, No. 3. P. 449
[22] Ibid.
[23] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-conclusion/
[24] Ibid.
[25] Ibid.
[26] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192.
[27] Ibid.

зосереджувалася на загальних характеристиках гібридної війни як феномену, то подальше дослідження логічно переходить до прикладного рівня, де визначальне значення має не саме існування інструментів, а їх конкретне використання, поєднання та ефект у реальному політичному середовищі[28]. Такий підхід дозволяє розкрити внутрішню структуру гібридного впливу, де кожен елемент має власну функцію, але не може бути повністю зрозумілий поза системою взаємодії з іншими[29].

У сучасних наукових підходах відбувається відхід від спрощених моделей класифікації. Поділ на військові та невійськові інструменти виявляється недостатнім, оскільки не відображає складності сучасних стратегій впливу[30]. Доцільним є багатовимірний підхід, який дозволяє аналізувати гібридну війну як динамічну систему, де інструменти взаємодіють у часі та просторі[31]. У такій системі інформаційно-комунікаційні, кібернетичні, економічно-ресурсні, політико-інституційні, силові та інфраструктурно-дестабілізаційні механізми не просто співіснують, а утворюють взаємопов'язану мережу впливу, яка забезпечує досягнення стратегічних результатів.

Для більш наочного відображення цієї взаємодії варто звернутися до узагальненої моделі, яка демонструє, як різні інструменти формують єдину систему.

---

[28] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. Defence Studies. 2024. Vol. 24, No. 3. P. 449

[29] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192

[30] Ibid.

[31] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. Defence Studies. 2024. Vol. 24, No. 3. P. 449

Рисунок 2.1 – Інтегрована модель інструментів гібридного впливу

Джерело: Blasco Robledo F. J. La guerra híbrida. Sociedad Argentina de Estudios Estratégicos y Globales. 2022. URL: https://saeeg.org/index.php/2022/09/12/la-guerra-hibrida/ (date of access: 21.04.2026).

Схема ілюструє, що гібридна стратегія не має чітко визначених меж між окремими видами діяльності. Дипломатичний, економічний, конвенційний, нерегулярний та інформаційний компоненти взаємно накладаються, формуючи спільний простір впливу[32]. Центральне розташування гібридної війни вказує на її інтегративний характер, адже вона не існує як ізольований тип дій, а виникає внаслідок взаємодії різних інструментів[33]. Це означає, що ефект досягається не через домінування одного елементу, а через їх координацію, що створює складну і водночас гнучку структуру впливу.

[32] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192
[33] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. Defence Studies. 2024. Vol. 24, No. 3. P. 449

Інформаційно-комунікаційні інструменти відіграють фундаментальну роль у цій системі, оскільки формують базове середовище сприйняття[34]. Вони поширюють певні повідомлення та визначають рамки інтерпретації подій, у яких інші дії виглядають логічними або виправданими[35]. Робота з інформаційним простором передбачає тривале і послідовне формування наративів, які закріплюються через різні канали комунікації. Це створює умови, за яких навіть об'єктивні події можуть сприйматися крізь призму заздалегідь сформованих уявлень.

Кібернетичні інструменти розширюють можливості впливу за рахунок технічних засобів. Вони дозволяють втручатися у функціонування цифрових систем, створюючи збої, які мають безпосередній вплив на управління, економіку та безпеку[36]. Особливість цих інструментів полягає у їх здатності діяти приховано і швидко, що підвищує їх ефективність. Навіть обмежені за масштабом операції можуть мати значний ефект, якщо вони спрямовані на критично важливі елементи інфраструктури[37]. Важливо зазначити, що кібероперації часто поєднуються з інформаційними кампаніями, які пояснюють їх наслідки у вигідному для агресора ключі.

Економічно-ресурсні інструменти формують довгострокову основу гібридного впливу. Вони спрямовані на створення залежностей, які обмежують можливості держави-цілі у прийнятті рішень. Використання енергетичних ресурсів, інвестиційних механізмів або торговельних зв'язків дозволяє формувати ситуацію, у якій економічні фактори перетворюються на політичні важелі[38]. Такий вплив не

---

[34] Ibid.
[35] Ibid.
[36] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. Webology. 2021. Vol. 18, No. 4. P. 1720
[37] Ibid.
[38] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. Journal of Strategic Security. 2024. Vol. 17, No. 3. Article 2. URL: https://digitalcommons.usf.edu/jss/vol17/iss3/2/

завжди має очевидний характер, але його наслідки можуть бути суттєвими і тривалими.

Політико-інституційні інструменти спрямовані на трансформацію внутрішнього середовища держави. Вони реалізуються через вплив на політичні процеси, підтримку окремих акторів та формування нової конфігурації влади[39]. Особливість цього впливу полягає у його непрямому характері. Зміни відбуваються через внутрішні механізми, що створює ілюзію їх автономності. Це ускладнює виявлення джерела впливу і робить протидію менш ефективною[40].

Силові інструменти у гібридній стратегії мають обмежений і вибірковий характер. Вони застосовуються не для досягнення масштабної перемоги, а для зміни ситуації у конкретних точках. Використання нерегулярних формувань або обмежених військових дій дозволяє досягати результатів без переходу до відкритого конфлікту[41]. Такий підхід забезпечує гнучкість і знижує ризики ескалації.

Інфраструктурно-дестабілізаційні інструменти спрямовані на підрив функціонування ключових систем держави[42]. Їх вплив проявляється у матеріальних втратах, формуванні відчуття нестабільності. Порушення роботи енергетичних, транспортних або комунікаційних систем створює додатковий психологічний ефект, який підсилює загальний вплив[43].

Комбіновані інструменти становлять особливу категорію, оскільки поєднують кілька форм впливу. У цьому випадку вирішальне значення має не кожен інструмент окремо, а їх послідовність і взаємодія. Кібернетичний вплив може поєднуватися з інформаційною кампанією і економічним тиском, створюючи комплексний ефект

---

[39] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-conclusion/
[40] Ibid.
[41] Ibid.
[42] McWilliams A., Legnér M. Threat assessments and heritage in the age of hybrid warfare. International Journal of Heritage Studies. 2024. Vol. 30, No. 12. P. 1379
[43] Ibid.

кризи[44]. Така синхронізація дозволяє досягати результатів, які були б неможливими при використанні окремих інструментів.

У практичному вимірі саме узгодженість інструментів визначає ефективність гібридного впливу[45]. Різні механізми використовуються одночасно, створюючи багатовекторний тиск, який складно нейтралізувати окремими заходами. Це вимагає комплексного підходу до аналізу і протидії, оскільки розгляд окремих інструментів не дає повного уявлення про механізм впливу.

Окремої уваги потребує механізм взаємодії інструментів гібридного впливу. Небезпека полягає в наявності різних засобів тиску та здатності агресора поєднувати їх у певній послідовності. На практиці гібридний вплив рідко починається з відкритого застосування сили. Частіше він розгортається поступово: спочатку формується інформаційне тло, далі створюються або посилюються внутрішні суперечності, після цього активізуються політичні, економічні, кібернетичні та силові інструменти. Через це гібридна стратегія має не лінійний, а хвилеподібний характер. Вона може посилюватися або послаблюватися залежно від міжнародної реакції, внутрішньої стійкості держави-мішені та готовності суспільства критично сприймати інформаційні повідомлення. Зазначені етапи не слід розглядати як усталений або універсальний алгоритм гібридного впливу. Їхня послідовність може змінюватися залежно від конкретних обставин, типу держави-мішені, рівня її інституційної стійкості, характеру міжнародної реакції та стратегічних цілей агресора. В одних випадках вплив може починатися з інформаційної підготовки, в інших – з економічного тиску, кібератак або політико-інституційного розхитування. Так само силовий компонент не завжди є завершальним етапом: він може з’являтися раніше, діяти паралельно з іншими

[44] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. Webology. 2021. Vol. 18, No. 4. P. 1720

[45] Countering hybrid threats. North Atlantic Treaty Organization. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats/

інструментами або тимчасово відходити на другий план. Тому подана етапність має аналітичний характер і використовується для пояснення типової логіки розгортання гібридної стратегії, а не для фіксації жорсткої послідовності дій[46].

Першим етапом гібридного впливу може виступати підготовка інформаційного середовища. Її суть полягає у поступовому нав'язуванні потрібних агресору пояснень, оцінок і образів. На цьому етапі ще може не бути відкритого конфлікту, однак у суспільстві вже формуються сумніви щодо легітимності влади, ефективності державних інститутів, здатності армії, міжнародної підтримки або доцільності євроінтеграційного чи безпекового курсу. Інформаційний вплив працює не лише через пряме поширення неправдивих повідомлень. Часто він діє тонше: через перебільшення реальних проблем, виривання фактів із ширшого контексту, емоційне загострення окремих тем, створення відчуття безвиході або недовіри. У цьому полягає одна з ключових особливостей гібридного інструментарію: він використовує не лише вигадані, а й реальні вразливості держави, перетворюючи їх на засіб політичного тиску.

Інституційне розхитування можна визначити як другий етап. Воно пов'язане з цілеспрямованим послабленням довіри до державних органів, правоохоронної системи, судів, армії, виборчих процедур, органів місцевого самоврядування та медіа. У цьому випадку інформаційні інструменти поєднуються з політико-інституційними. Наприклад, агресор може підтримувати ті сили, які зацікавлені у радикалізації суспільної дискусії, посиленні протестних настроїв або блокуванні рішень, важливих для безпеки держави. При цьому зовнішній вплив часто подається як внутрішній політичний процес. Ця маскувальна здатність робить гібридні інструменти особливо складними для виявлення, тому що вони не завжди виглядають як пряма агресія.

[46] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192

Третій етап може бути пов’язаний з економічним і ресурсним тиском. Його функція полягає у створенні ситуації залежності або нестабільності. Якщо держава залежить від певного ринку, енергетичного ресурсу, логістичного маршруту, фінансового потоку або критичного імпорту, ця залежність може бути використана як інструмент впливу. Економічний тиск не завжди має форму відкритих санкцій чи блокади. Він може проявлятися через зміну умов торгівлі, штучне ускладнення постачання, маніпулювання цінами, дестабілізацію енергетичного сектору, підтримку тіньових економічних схем або створення невизначеності для інвесторів. У поєднанні з інформаційною кампанією такі дії можуть породжувати в суспільстві відчуття економічної кризи, навіть якщо її масштаби ще не є критичними.

Кібернетичний вплив є ще одним компонентом гібридного впливу. Наразі його значення зростає через цифровізацію державного управління, фінансових послуг, енергетики, транспорту, медицини, освіти та комунікацій. Кібератаки у гібридній стратегії виконують кілька функцій: вони можуть безпосередньо порушувати роботу важливих систем, створювати психологічний ефект небезпеки, коли громадяни починають сумніватися у здатності держави захистити критичну інфраструктуру; кібероперації можуть використовуватися для отримання інформації, подальшого шантажу або підготовки інформаційних кампаній. У зв’язку з наведеними чинниками кібернетичний інструмент рідко існує окремо. Він або готує подальші дії, або супроводжує їх, або посилює вже наявну кризу.

Наступний етап впливу може передбачати силовий або напівсиловий тиск. У гібридній війні він не завжди має вигляд повномасштабного вторгнення. Значно частіше йдеться про локальні провокації, діяльність диверсійних груп, підтримку незаконних збройних формувань, демонстрацію сили біля кордонів, використання приватних військових структур або організацію заворушень. Такий інструмент виконує подвійну функцію. З одного боку, він створює реальну загрозу безпеці. З іншого боку, він підсилює інформаційний та політичний тиск, оскільки суспільство починає жити в умовах постійного очікування ескалації. Силовий компонент у

гібридній стратегії часто залишається обмеженим за масштабом, але значним за психологічним ефектом.

Особливе місце займають інфраструктурно-дестабілізаційні інструменти. Їхнє завдання полягає у тому, щоб порушити нормальний ритм життя суспільства. Якщо не працює енергетична система, транспорт, зв'язок, банківські сервіси або медична інфраструктура, населення починає відчувати не лише матеріальні труднощі, а й втрату контролю над повсякденністю. У цьому сенсі інфраструктурна дестабілізація має не тільки технічний, а й соціально-психологічний характер. Вона змушує людей сприймати кризу як постійну, а державу - як недостатньо спроможну. Тому удари по інфраструктурі або створення загрози її функціонуванню часто поєднуються з інформаційними повідомленнями, які мають посилити паніку, недовіру або втому.

Варто підкреслити, що гібридний вплив не завжди спрямований на негайну перемогу. Нерідко його метою є поступове виснаження держави-мішені. Таке виснаження може бути політичним, економічним, психологічним, військовим або дипломатичним. Держава змушена постійно витрачати ресурси на реагування, пояснення, спростування, захист інфраструктури, стабілізацію суспільних настроїв і підтримку міжнародної довіри. Агресор, своєю чергою, може змінювати інструменти залежно від ситуації: якщо один канал впливу втрачає ефективність, активізується інший. Наприклад, після невдалої інформаційної кампанії може посилюватися кібертиск; після економічного тиску - політичні провокації; після військової ескалації - дипломатичні маніпуляції або спроби нав'язати вигідне трактування подій.

У цьому полягає відмінність гібридного впливу від звичайного набору ворожих дій. Окремо кібератака, дезінформація, економічний шантаж або політичне втручання можуть розглядатися як самостійні загрози. Проте в межах гібридної стратегії вони набувають іншої якості, оскільки починають працювати як частини єдиного механізму. Інформаційна кампанія пояснює економічний тиск.

Економічний тиск підсилює соціальне невдоволення. Соціальне невдоволення використовується для політичної дестабілізації. Політична дестабілізація створює умови для силового втручання або міжнародного тиску. Наведена взаємозалежність інструментів формує системну природу гібридного впливу.

Психологічний вимір не завжди подають як окрему групу інструментів, фактично він пронизує всі інші форми впливу. Інформаційні операції працюють із масовими емоціями. Кібератаки створюють відчуття незахищеності. Економічний тиск породжує страх перед погіршенням рівня життя. Інфраструктурні порушення викликають втому, роздратування і недовіру. Силові провокації підтримують постійне очікування небезпеки. У результаті суспільство може перейти у стан хронічної напруги, коли будь-яка подія сприймається не раціонально, а через емоції. Для агресора це вигідно, оскільки емоційно виснажене суспільство легше піддається маніпуляціям.

Зовнішньополітичний вимір гібридного впливу спрямований як на державу-мішень, так і на її союзників, міжнародні організації та зовнішню аудиторію. Агресор може прагнути представити конфлікт як внутрішню кризу, громадянське протистояння, регіональну суперечку або наслідок помилкової політики самої держави-мішені. Така стратегія дозволяє послаблювати міжнародну підтримку жертви агресії, затягувати ухвалення рішень, створювати сумніви серед партнерів і розмивати відповідальність. У цьому разі дипломатичні та інформаційні інструменти працюють разом: дипломатія формально подає позицію агресора, а інформаційні кампанії створюють для неї потрібне пояснювальне середовище.

З огляду на це класифікація інструментів гібридного впливу не може бути лише переліком окремих груп. Вона повинна показувати, яку функцію виконує кожен інструмент у загальній стратегії. Інформаційні інструменти формують сприйняття, політико-інституційні - розхитують управлінську систему, економічні - створюють залежність і матеріальний тиск, кібернетичні - порушують цифрову та управлінську стабільність, силові - забезпечують примус і демонстрацію загрози,

інфраструктурні - впливають на повсякденне життя населення, комбіновані - поєднують ці напрями у цілісну систему. Тільки за такого підходу можна зрозуміти, чому гібридна стратегія є настільки складною для протидії.

Часовий вимір має принципове значення, адже частина інструментів забезпечує швидкий ефект, інша працює у довгостроковій перспективі[47]. Їх поєднання дозволяє одночасно досягати оперативних і стратегічних цілей. Саме ця комбінація створює стійкість гібридного впливу і ускладнює протидію.

Отже, класифікація інструментів гібридного впливу повинна враховувати їх функціональне призначення, взаємодію та часову динаміку. У сукупності вони формують складну систему, у якій інформаційні, кібернетичні, економічні та силові компоненти взаємно підсилюють один одного[48]. Така інтегрованість забезпечує ефективність гібридної стратегії та визначає її значення у сучасному міжнародному середовищі[49].

[47] Berthelsen E. Hybrid times: War and peace in military innovation studies. Journal of Strategic Studies. 2025. DOI: https://doi.org/10.1080/01402390.2025.2512238.
[48] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. Defence Studies. 2024. Vol. 24, No. 3. P. 449
[49] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. 2023. Vol. 8, No. 2. P. 192

РОЗДІЛ 2. ГІБРИДНИЙ ІНСТРУМЕНТАРІЙ ЗОВНІШНЬОЇ ПОЛІТИКИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

2.1. Інформаційно-комунікаційні та пропагандистські інструменти формування і просування зовнішньополітичних наративів російської федерації

Якщо розглядати гібридний інструментарій російської федерації не декларативно, а на рівні реальних механік впливу, то інформаційно-комунікаційний сегмент постає як базове середовище, у якому формується початкова конфігурація будь-якої подальшої дії – від економічного тиску до військового втручання[50]. Йдеться не про супровід подій, а про їх попереднє моделювання через наративи, які задають рамки сприйняття ще до виникнення самих фактів[51]. У цьому вимірі інформаційний простір використовується як інструмент конструювання реальності, де інтерпретація часто передує події і визначає її подальше розуміння.

Російська інформаційна стратегія демонструє суттєву відмінність від класичних моделей пропаганди, характерних для XX століття[52]. Якщо раніше центральним було завдання переконання через відносно узгоджений ідеологічний дискурс, то сучасна модель функціонує через перевантаження, фрагментацію і конкурентність повідомлень[53]. Вона не прагне до логічної завершеності або внутрішньої узгодженості. Навпаки, суперечливість стає інструментом, що ускладнює перевірку і знижує довіру до будь-якої інформації як такої. Це дозволяє

---

[50] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449

[51] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192

[52] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 135

[53] Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. *Santa Monica: RAND Corporation.* 2016. URL: https://www.rand.org/pubs/perspectives/PE198.html

досягати стану, коли встановлення істини стає менш важливим, ніж створення сумніву.

У практичному вимірі така модель проявляється через одночасне поширення кількох версій однієї події. У випадку міжнародних криз фіксується паралельна присутність взаємовиключних наративів: заперечення факту події, альтернативне пояснення причин, перекладання відповідальності на іншу сторону, а також емоційно насичені конспірологічні інтерпретації[54]. Важливо, що жодна з цих версій не є домінуючою, їх функція полягає у створенні інформаційного поля, де встановлення достовірності стає практично неможливим[55].

Цей ефект підсилюється швидкістю поширення інформації. Повідомлення з'являються практично миттєво після події або навіть випереджають її, формуючи первинну інтерпретацію[56]. У подальшому навіть спростовані дані продовжують функціонувати, оскільки вони вже інтегровані у когнітивні схеми аудиторії. Повторюваність виступає ключовим фактором впливу, адже вона формує відчуття правдивості незалежно від фактичного змісту[57].

Технологічна основа цього процесу базується на використанні цифрових платформ, передусім соціальних мереж, які забезпечують масштабування і швидкість поширення інформації[58]. Значна частина активності у цих мережах має штучний характер. Використання бот-мереж створює ілюзію масової підтримки певних позицій, а алгоритми платформ, орієнтовані на залучення користувачів, підсилюють видимість такого контенту[59]. У результаті формується ситуація, коли

---

[54] Ibid.
[55] Ibid.
[56] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 450
[57] Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. *Santa Monica: RAND Corporation.* 2016.
[58] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021. Vol. 18, No. 4. P. 1720
[59] Topor L., Tabachnik A. Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies.* 2021. Vol. 12, No. 1. P. 112

популярність повідомлення не є показником його достовірності, а лише відображає рівень його технічного просування.

Паралельно функціонують координовані групи акаунтів, які виконують більш складну функцію – поширення інформації, що супроводжується зміною структури дискурсу[60]. Тобто вони можуть втручатися у коментарі, ініціювати конфлікти, змінювати тон обговорення, переводити увагу з фактів на емоційні оцінки[61]. У результаті таких дій навіть нейтральні теми трансформуються у поляризовані дискусії, що підсилює загальний ефект дестабілізації.

Для систематизації механіки такого впливу доцільно звернутися до узагальненої моделі поширення дезінформації, яка демонструє логіку трансформації повідомлення від джерела до аудиторії.

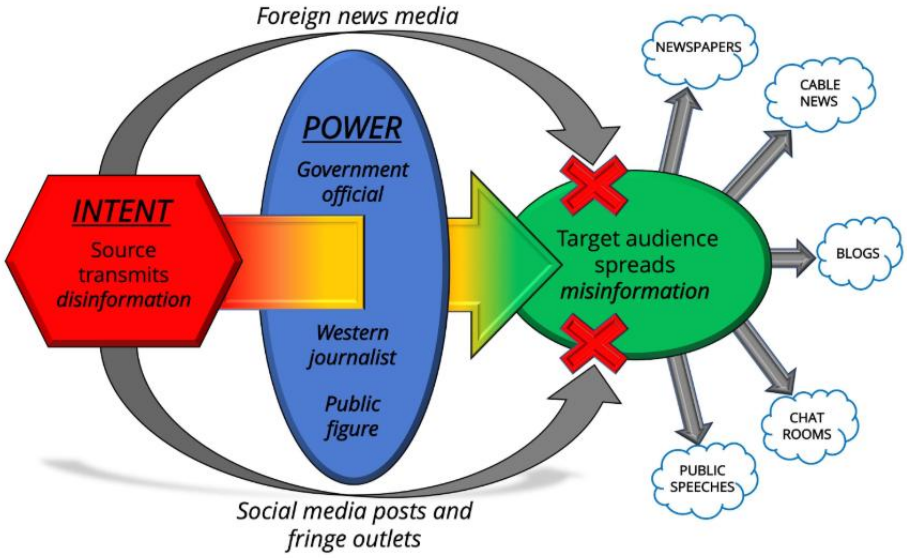

Рисунок 2.1 – Модель трансформації та поширення дезінформації у гібридному інформаційному середовищі

[60] Ibid.
[61] Ibid.

Джерело: Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. Santa Monica: RAND Corporation. 2016. URL: https://www.rand.org/pubs/perspectives/PE198.html (date of access: 19.04.2026).

Представлена схема ілюструє ключову особливість інформаційного впливу – його проходження через посередницькі ланки, які трансформують початкове повідомлення[62]. На першому етапі формується намір і створюється дезінформаційний контент. Далі він проходить через різні канали – офіційні структури, медіа, публічні фігури, що надає йому додаткової легітимності[63]. На фінальному етапі аудиторія сприймає інформацію і сама починає її поширювати, перетворюючись на активний елемент системи. Така циркуляція створює замкнений цикл, у якому дезінформація відтворюється і посилюється.

Зовнішньополітичні наративи російської федерації не зводяться лише до поширення окремих дезінформаційних повідомлень, їх доцільно розглядати як стійкі смислові конструкції, які формують для аудиторії певний спосіб пояснення міжнародних подій, причин конфліктів, ролі росії, позиції Заходу та статусу держави-мішені. Якщо окреме повідомлення може бути спростоване фактологічно, то наратив діє глибше: він задає загальну рамку мислення, у межах якої навіть нові факти інтерпретуються відповідно до вже сформованої схеми[64]. Саме тому інформаційно-комунікаційні інструменти у гібридній стратегії мають не лише оперативне, а й довгострокове значення.

Для кращої візуалізації доцільно виокремити основні російські зовнішньополітичні наративи, які повторюються у різних інформаційних кампаніях.

Таблиця 2.1

[62] Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. *Santa Monica: RAND Corporation.* 2016. URL: https://www.rand.org/pubs/perspectives/PE198.html (date of access: 19.04.2026).
[63] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449–471. DOI: https://doi.org/10.1080/14702436.2024.2365214.
[64] Ibid.

Основні зовнішньополітичні наративи російської федерації у гібридному інформаційному впливі

Основний наратив	Зміст наративу	Функціональне призначення
«росія лише реагує на зовнішні загрози»	Дії російської федерації подаються як вимушені, оборонні або відповідні на нібито агресивну поведінку Заходу, НАТО чи України	Зміщення відповідальності з агресора на зовнішнє середовище
«Україна є несамостійною державою»	Україна зображується як залежна від зовнішніх центрів ухвалення рішень, внутрішньо нестабільна або неспроможна до ефективного управління	Делегітимація української державності та підрив довіри до інституцій
«конфлікт має внутрішній характер»	Зовнішня агресія маскується під внутрішню політичну або громадянську кризу	Ускладнення міжнародної кваліфікації агресії та зниження рівня зовнішньої підтримки України
«Захід перебуває у кризі»	Демократія, санкції, міжнародне право, євроінтеграція та колективна безпека подаються як неефективні або лицемірні	Дискредитація західних інституцій і послаблення довіри до союзників
«санкції не працюють»	Обмежувальні заходи подаються як безрезультатні або	Формування сумнівів щодо доцільності тиску на російську федерацію

	шкідливі передусім для самих західних держав	
«необхідний прагматичний компроміс»	Поступки агресору подаються як раціональний шлях до миру або стабільності	Перенесення дискусії з питання відповідальності на питання «втоми» й «реалізму»
«росія є альтернативним центром сили»	Російська федерація представляється як опонент західної гегемонії та захисник багатополярного світу	Залучення аудиторій поза євроатлантичним простором

Джерело: узагальнено на основі [17], [18], [23], [36], [41].

Одним із центральних напрямів інформаційної стратегії є формування образу росії як держави, що нібито не здійснює агресивної політики, а лише реагує на зовнішні загрози. Такий наратив дозволяє змістити відповідальність із суб'єкта агресії на міжнародне середовище, Захід, НАТО, Україну або інші держави, які подаються як джерело нестабільності. У межах цієї логіки будь-які дії російської федерації можуть бути представлені як «вимушені», «оборонні» або «відповідні». Така підміна має принципове значення, оскільки вона дозволяє агресору уникати прямого визнання власної ролі та одночасно формувати для різних аудиторій образ держави, що начебто діє у межах власних безпекових інтересів[65].

Наративи, спрямовані на делегітимацію України як суб'єкта міжнародної політики у російській стратегії гібридного впливу займають ключове місце. У таких повідомленнях Україна подається як держава з обмеженою самостійністю, внутрішньо нестабільна, залежна від зовнішніх центрів ухвалення рішень або

[65] Eggen K.A. A strategy for the weak: The role of information confrontation in Russia's grand strategy. Defence Studies. 2025. DOI: https://doi.org/10.1080/14702436.2025.2561639.

неспроможна ефективно виконувати базові функції державного управління[66]. Цей тип наративів має подвійну функцію. По-перше, він покликаний підірвати довіру до українських інституцій усередині країни. По-друге, він орієнтований на зовнішню аудиторію, для якої Україна має постати не як жертва агресії, а як проблемний політичний простір, де конфлікт нібито має внутрішню природу. У цьому полягає основна маніпуляція російської інформаційної стратегії: зовнішній вплив маскується під внутрішню кризу[67].

Історичні наративи в цій стратегії ґрунтуються на вибірковому використанні минулого, застосуванні історичних аналогій, символічних елементів, пам'ятних дат і колективних уявлень. Їхня мета полягає не у відтворенні історичної складності, а у створенні політично зручної картини минулого, яка виправдовує сучасні зовнішньополітичні дії[68]. Такий підхід дозволяє російській пропаганді представляти агресивну політику не як порушення міжнародного права, а як нібито «відновлення справедливості», «захист історичної пам'яті» або «повернення до природного порядку». Унаслідок цього історія перетворюється на інструмент політичної легітимації, а не на сферу критичного осмислення.

Не менш значущими є наративи, спрямовані на дискредитацію західних інституцій. У них демократія, міжнародне право, санкційні механізми, європейська інтеграція та колективна безпека подаються як неефективні, лицемірні або кризові явища. Наведена риторика має не лише антизахідне спрямування. Вона виконує ширшу функцію – зменшує довіру до тих інституцій, які можуть обмежувати дії російської федерації або підтримувати державу-мішень. Якщо аудиторія починає сумніватися у спроможності міжнародних організацій чи західних демократій діяти

---

[66] Bachmann S.-D. D., Gunneriusson H. Russia's hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. Georgetown Journal of International Affairs. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198

[67] Ibid.

[68] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. Small Wars & Insurgencies. 2026. Vol. 37, No. 1. P. 135

послідовно, тоді російська позиція отримує додатковий простір для маневру. Через це теми «кризи демократії», «втоми Заходу», «неефективності санкцій» або «розколу союзників» регулярно відтворюються у різних інформаційних кампаніях[69].

Наведені наративи адаптуються до різних аудиторій. Для внутрішньої російської аудиторії вони переважно виконують мобілізаційну функцію: пояснюють дії влади, виправдовують обмеження, підтримують образ зовнішньої загрози та знижують критичність щодо державної політики[70]. Для української аудиторії акцент переноситься на деморалізацію, втому, недовіру до влади, сумнів у підтримці союзників і відчуття невизначеності. Для західної аудиторії на перший план виходять теми економічних витрат, ризиків ескалації, неефективності допомоги та необхідності «прагматичного компромісу». Для аудиторій поза євроатлантичним простором можуть активізуватися антизахідні або антиколоніальні мотиви, через які росія намагається представити себе як альтернативний центр сили.

Така адаптивність показує, що російська інформаційна стратегія не потребує єдиного ідеологічного повідомлення для всіх. Навпаки, вона може використовувати різні, іноді суперечливі аргументи, якщо вони ведуть до одного політичного результату[71]. Для однієї аудиторії росія може позиціонуватися як «захисник традиційних цінностей», для іншої – як «антизахідний полюс», для третьої – як «жертва зовнішнього тиску», для четвертої – як «раціональний геополітичний гравець». На перший погляд ці образи не завжди сумісні. Проте їх об’єднує спільна функція: послабити довіру до держави-мішені, розмити відповідальність агресора і ускладнити формування консолідованої міжнародної реакції[72].

---

[69] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. DIIS Report No. 2017:06. Copenhagen: Danish Institute for International Studies. 2017.
[70] Ibid.
[71] Paul C., Matthews M. The Russian “firehose of falsehood” propaganda model: Why it might work and options to counter it
[72] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023

Окремої уваги заслуговує механізм емоційного кодування повідомлень. Російські інформаційні кампанії часто апелюють не до складної аргументації, а до страху, образи, ностальгії, почуття несправедливості, тривоги або втоми. Це дозволяє знижувати рівень критичного аналізу аудиторії, оскільки емоційно забарвлене повідомлення сприймається швидше, ніж раціонально структурований доказ[73]. Значна частина пропагандистських матеріалів має не аналітичну, а мобілізаційно-психологічну природу. Це означає, що їхньою метою є не стільки пояснення події, скільки формування реакції на них. Коли аудиторія реагує через страх або обурення, вона менш схильна перевіряти джерела, зіставляти факти чи аналізувати логічну послідовність тверджень[74].

У цифровому середовищі цей механізм посилюється завдяки алгоритмам платформ і діяльності координованих мереж акаунтів. Повідомлення, що викликають сильну емоційну реакцію, мають більшу ймовірність поширення, а тому пропагандистські структури використовують конфліктні, провокативні або поляризувальні формулювання[75]. Бот-мережі та скоординовані акаунти не лише збільшують видимість потрібного контенту, а й створюють ілюзію суспільної підтримки певних позицій[76]. Унаслідок цього аудиторія може сприймати штучно створену активність як органічну громадську думку. Це особливо небезпечно в умовах криз, коли суспільство шукає швидкі пояснення і гостро реагує на інформаційні сигнали.

До цього додається механізм перехресного підкріплення. Йдеться про ситуацію, коли однаковий або близький за змістом наратив з’являється одночасно у різних каналах: офіційних заявах, медіа, експертних коментарях, соціальних

---

[73] Ibid.
[74] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. 2017
[75] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations
[76] Topor L., Tabachnik A. Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies.* 2021. P.112.

мережах, відеоконтенті, Telegram-каналах або коментарях користувачів[77]. Для аудиторії така повторюваність створює враження підтвердження з різних джерел. Насправді ж ці джерела можуть бути пов'язані спільною інформаційною логікою або координованою кампанією. У цьому полягає важлива риса сучасної пропаганди: вона прагне не лише поширити повідомлення, а створити ефект його всюдисущості.

Наративи виконують також функцію попередньої підготовки аудиторії до майбутніх дій. Інформаційна кампанія може передувати економічному тиску, кібероперації, дипломатичному шантажу або військовій ескалації[78]. Наприклад, перед посиленням тиску може формуватися образ держави-мішені як винної сторони, перед силовими діями – образ загрози, перед дипломатичним ультиматумом – уявлення про нібито безальтернативність поступок. У такому випадку інформаційний вплив не просто пояснює подію після її настання, а створює рамку, у якій ця подія буде сприйнята[79].

Інформаційні наративи можуть підсилюватися кібернетичним компонентом, який включає злами, витоки даних, або імітації витоків. У таких випадках атаки на інформаційні ресурси створюють приводи, що згодом вбудовуються у пропагандистську рамку[80]. Наведені кібер-операції виконують не лише технічну, а й комунікативну функцію. Вона створює матеріал для подальшого інформаційного використання. Навіть якщо дані є неповними, спотвореними або сфальсифікованими, сам факт їх появи може бути використаний як доказ у межах уже підготовленого наративу.

---

[77] Ibid.

[78] Eggen K.A. A strategy for the weak: The role of information confrontation in Russia's grand strategy. *Defence Studies.* 2025

[79] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024.

[80] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025. Vol. 6, No. 2. DOI: https://doi.org/10.37458/ssj.6.2.3.

Ще одним аспектом є стратегія нормалізації агресії. Вона полягає у поступовому привчанні аудиторії до порушення міжнародного права, втручання у справи інших держав, окупації, шантажу або застосування сили. Якщо такі дії постійно пояснюються як «вимушені», «захисні», «історично обґрунтовані» або «неминучі», вони поступово втрачають ознаки надзвичайності. У цьому полягає небезпека тривалих пропагандистських кампаній, адже вони змінюють загальні межі прийнятного у політичному мисленні[81].

Інформаційно-комунікаційні інструменти російської федерації мають не лише зовнішню, а й внутрішню функцію. Усередині російського суспільства вони забезпечують легітимацію зовнішньої політики, створюють образ постійної загрози, знижують чутливість до наслідків агресивних дій і формують терпимість до обмеження прав або зростання витрат, пов'язаних із зовнішньополітичним курсом. Назовні ці самі або адаптовані наративи використовуються для розмивання відповідальності, послаблення міжнародної підтримки України, стимулювання сумнівів серед союзників і перенесення дискусії з питання агресії на питання «втоми», «компромісу» чи «геополітичного балансу»[82].

Тому інформаційно-комунікаційні та пропагандистські інструменти російської федерації слід оцінювати не тільки за критерієм правдивості або неправдивості окремих повідомлень. Значно важливішим є функціональний аналіз: яку поведінку вони стимулюють, яку довіру руйнують, які політичні рішення ускладнюють, яку відповідальність маскують і які конфлікти загострюють. Такий підхід дозволяє побачити, що наратив є не другорядним елементом гібридної стратегії, а одним із її центральних механізмів[83]. Через наративи інформаційний

---

[81] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 195

[82] Ibid.

[83] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021

вплив перетворюється на політичну дію, а пропаганда стає інструментом стратегічного управління сприйняттям.

У ширшому вимірі інформаційно-комунікаційні інструменти виконують зв'язкову функцію у структурі гібридної стратегії[84]. Вони забезпечують координацію інших інструментів і дозволяють досягати синергетичного ефекту. Їхня роль не обмежується окремими кампаніями, а визначає загальну логіку гібридного впливу.

У підсумку, інформаційний вимір гібридної стратегії виконує кілька взаємопов'язаних функцій. Він формує інтерпретаційні рамки подій, забезпечує масштабування наративів і створює умови для реалізації інших інструментів впливу[85]. Функціональна універсальність інформаційно-комунікаційного інструментарію визначає його центральне місце у сучасних моделях гібридної агресії.

2.2. Економічний та енергетичний вимір гібридної війни російської федерації

Економічний та енергетичний сегмент гібридної стратегії російської федерації функціонує не як допоміжний елемент, а як один із базових каналів реалізації зовнішньополітичного впливу. Його специфіка полягає у тому, що економічні відносини цілеспрямовано трансформуються у механізм формування залежності, яка в подальшому використовується як інструмент політичного тиску. При цьому вплив не має різкого або відкритого характеру – він реалізується поступово, через зміну параметрів взаємодії.

---

[84] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192

[85] Ibid.

Ключовим інструментом у цій системі виступає енергетичний сектор, у контексті енергетичного сектору російської федерації це насамперед постачання природного газу[86]. Важливим є не сам факт експорту, а конфігурація контрактних і інфраструктурних зв'язків, які формують довготривалі залежності. Умови можуть включати довгострокові угоди з фіксованими обсягами постачання, складні формули ціноутворення, залежність від конкретних маршрутів транспортування, що створюють ситуацію, у якій держава-споживач обмежена у можливостях швидкої диверсифікації[87]. Відмова від таких умов потребує значних витрат, що фактично перетворює економічну взаємодію на форму структурної залежності. У цьому сенсі енергетика виступає не лише економічною сферою, а інструментом стратегічного впливу, інтегрованим у ширшу систему гібридної політики.

Ця залежність не є статичною. Вона використовується як регульований інструмент впливу через зміну обсягів постачання, коригування цін або перегляд контрактних умов[88]. Важливо, що такі дії формально подаються як економічно обґрунтовані рішення, що дозволяє уникати прямої політичної кваліфікації. Однак їх синхронізація з політичними процесами свідчить про іншу логіку застосування, де економічні параметри виступають змінними, що можуть коригуватися залежно від зовнішньополітичних цілей[89]. У результаті формується гнучкий механізм впливу, який дозволяє адаптувати інтенсивність тиску без порушення формальних норм.

У цьому контексті енергетичні проєкти виконують подвійну функцію. З одного боку, вони забезпечують економічну взаємодію, з іншого – формують

---

[86] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus.
[87] Ibid.
[88] Ibid.
[89] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449

політичні зв'язки, які можуть бути використані для впливу на прийняття рішень[90]. Реалізація великих інфраструктурних ініціатив часто супроводжується формуванням груп інтересів у державах-учасниках, що створює додаткові канали впливу[91]. Такі групи зацікавлені у збереженні співпраці, що обмежує можливості держави-споживача змінювати політику у відповідь на зовнішній тиск.

Паралельно з енергетичним сектором використовується ширший спектр економічних інструментів. До них належать торговельні обмеження, вибіркові санкційні заходи, зміни митних процедур, обмеження доступу до ринків. Характерною рисою є їх точковість, що дозволяє мінімізувати втрати для власної економіки[92]. Вплив спрямовується на конкретні галузі або компанії, що створює дисбаланс у внутрішній економічній структурі держави-цілі[93]. Такий підхід відповідає загальній логіці гібридної стратегії, де пріоритет надається селективним, а не тотальним заходам[94].

Суттєвим елементом економічного впливу є використання фінансових інструментів. Під фінансовими інструментами мається на увазі перш за все інвестиції, кредитні програми, участь у банківських структурах, а також непряме фінансування окремих економічних або політичних акторів. Ці механізми дозволяють впливати на внутрішні процеси у державах-цілях, формуючи сприятливе середовище для реалізації зовнішньополітичних інтересів[95]. При цьому їх застосування часто залишається поза публічним контролем, що ускладнює ідентифікацію та оцінку масштабу впливу[96]. Така прихованість підсилює

---

[90] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus
[91] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.
[92] Brown J. An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state. *Journal of Global Faultlines.* 2018. Vol. 5, No. 1-2. P. 58
[93] Ibid.
[94] Ibid.
[95] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.
[96] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192

ефективність фінансових інструментів і робить їх важливою складовою гібридної стратегії.

Окрему роль відіграє здатність використовувати кризові ситуації. Енергетичні дефіцити, коливання цін або економічна нестабільність створюють умови, у яких залежність від зовнішніх ресурсів зростає[97]. У таких обставинах навіть незначні зміни параметрів постачання можуть мати суттєвий вплив на економіку держави. Це дозволяє посилювати політичний тиск без прямого втручання, використовуючи вже існуючі структурні вразливості[98].

Економічні інструменти не функціонують ізольовано. Вони інтегруються у ширшу систему гібридного впливу, де поєднуються з інформаційними та кібернетичними механізмами. Економічні рішення супроводжуються інформаційним обґрунтуванням, яке формує відповідне сприйняття у суспільстві[99]. Наприклад, обмеження постачання може пояснюватися технічними причинами або ринковими умовами, що знижує ймовірність політичної реакції. Така комбінація інструментів підсилює ефект і забезпечує більш стійкий результат.

У ширшому контексті економічний вимір гібридної війни відповідає концепції непрямого впливу, де досягнення політичних цілей відбувається без відкритого застосування сили[100]. Як зазначається у сучасних дослідженнях, подібні підходи є характерними для нових форм конфліктів, у яких межа між економічною та політичною діяльністю фактично стирається[101]. У результаті економічні інструменти стають не лише допоміжним елементом, а центральною складовою

---

[97] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus.
[98] Ibid.
[99] Ibid.
[100] Arifin J. D. Unraveling current trends in hybrid warfare 3.0: A literature study on modern non-conventional threats. *Proceedings of the International Conference on Economics, Technology, Management, Accounting, Education (ICETEA).* 2025. Vol. 1. URL: https://conference.unita.ac.id/index.php/icetea/article/view/378
[101] Ibid.

гібридної стратегії, що визначає її ефективність у сучасному міжнародному середовищі.

Таким чином, економічний та енергетичний інструментарій російської федерації формує складну систему впливу, у якій поєднуються інфраструктурні, фінансові та регуляторні механізми. Його ефективність визначається здатністю створювати і підтримувати залежності, які можуть бути активовані у необхідний момент для досягнення зовнішньополітичних цілей.

У структурному вимірі цей процес можна представити як взаємодію трьох рівнів: формування залежності, управління параметрами взаємодії та інтеграція з іншими інструментами гібридного впливу. Саме така багаторівнева організація забезпечує стійкість і адаптивність економічної складової гібридної стратегії.

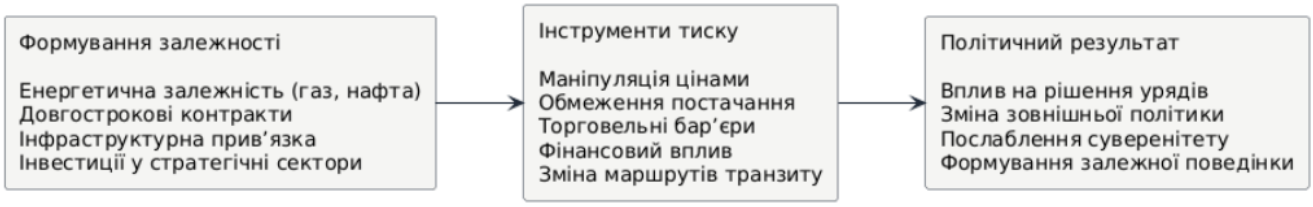

Рисунок 2.2 – Структура економічного та енергетичного впливу російської федерації в умовах гібридної війни

У відносинах із європейськими державами довгий час формувалася модель, за якої російський газ займав домінуючу частку в енергетичному балансі окремих країн[102]. Це досягалося не лише за рахунок цінових пропозицій, але й через інтеграцію у внутрішні енергетичні ринки – участь у спільних підприємствах, контроль над сегментами транспортування, інвестиції в інфраструктуру. У результаті виникала ситуація, коли економічна доцільність співпраці поєднувалася

[102] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus.

з політичною вразливістю, оскільки залежність від постачання перетворювалася на фактор впливу.

Подальший етап – використання цієї залежності у кризових ситуаціях. Зменшення обсягів постачання або їх перерозподіл між ринками створює дефіцит, який відразу відображається на цінах[103]. Навіть короткострокові обмеження можуть призводити до значних коливань, що впливає на промисловість, енергетику та соціальну сферу держави. Важливо, що такі дії не потребують формального порушення контрактів – достатньо змінити технічні або комерційні параметри, що дозволяє зберігати формальну правомірність дій[104].

Окремий механізм – використання транзитного фактору. Держави, через територію яких проходять енергетичні потоки, опиняються у подвійній позиції. З одного боку, вони отримують економічні вигоди від транзиту, з іншого – стають вразливими до змін маршрутів постачання. Будівництво альтернативних трубопроводів дозволяє обходити такі держави, знижуючи їх стратегічне значення і, відповідно, політичні можливості[105]. У цьому випадку інфраструктурне рішення фактично змінює геополітичну конфігурацію, створюючи новий баланс сил у регіоні[106].

У відносинах з Україною економічний та енергетичний тиск набуває ще більш виразного характеру. Тут поєднуються кілька рівнів впливу: маніпуляції з цінами на газ, перегляд умов постачання, обмеження транзиту, а також використання торговельних бар'єрів[107]. У різні періоди ці інструменти застосовувалися

---

[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023
[107] Bachmann S.-D. D., Gunneriusson H. Russia's hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. *Georgetown Journal of International Affairs*. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198.

комплексно, що дозволяло досягати значного впливу на економічну ситуацію в країні та формувати залежність у стратегічних секторах.

При цьому економічний тиск часто супроводжується інформаційним оформленням. Зміни у постачанні або цінах подаються як наслідок «ринкових процесів» або «порушень з боку партнера»[108]. Така інтерпретація знижує рівень міжнародної реакції і створює простір для подальших дій, оскільки переводить проблему у площину економічних відносин. У результаті економічний інструмент набуває подвійного ефекту – матеріального і когнітивного, що значно підвищує його результативність[109].

Варто звернути увагу і на менш очевидні механізми впливу. Один із них – створення умов для економічної присутності через інвестиції у стратегічні галузі. Йдеться про енергетику, транспорт, фінансовий сектор, де навіть частковий контроль відкриває можливості для впливу на прийняття рішень[110]. Контроль або співконтроль над такими активами дозволяє інтегрувати економічні інтереси у політичні процеси, створюючи складні залежності[111].

Ще одним аспектом варто вказати використання торговельних обмежень як інструменту сигналу. Введення або скасування обмежень щодо окремих товарів дозволяє демонструвати готовність до ескалації або, навпаки, до нормалізації відносин[112]. Такі дії мають не лише економічний, але й символічний характер, оскільки вони впливають на очікування учасників ринку та формують поведінкові стратегії держав. У результаті економічний інструментарій гібридної агресії

---

[108] Göransson M. B. Russia’s thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024.
[109] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation.
[110] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.

[111] Ibid.
[112] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future “energy-resources-climate” security nexus. 2024

виступає не лише засобом тиску, а й механізмом довгострокового впливу на структуру міжнародних відносин[113].

У сучасних умовах економічний вплив дедалі частіше поєднується з кібернетичними інструментами. Атаки на енергетичну інфраструктуру або інформаційні системи компаній можуть створювати додаткові ризики, які підсилюють ефект економічного тиску. Наприклад, порушення роботи енергетичних об’єктів може збігатися у часі з обмеженням постачання ресурсів, що значно ускладнює ситуацію для держави-цілі[114].

Крім того, кіберпростір використовується для збору інформації про економічні процеси, що дозволяє більш точно визначати вразливі точки. Отримані дані можуть застосовуватися для планування подальших дій або коригування вже існуючих стратегій. Така інтеграція різних інструментів відповідає загальній логіці гібридної війни, де ефективність досягається через поєднання різних форм впливу.

Системний характер економічного впливу підтверджується і його узгодженістю з іншими напрямами зовнішньої політики. Економічні заходи можуть передувати політичним рішенням або, навпаки, закріплювати їх результати. Наприклад, після досягнення певних домовленостей можуть змінюватися умови співпраці, що створює додаткові стимули для їх дотримання.

У цьому контексті економічний інструментарій виконує не лише функцію тиску, але й функцію управління поведінкою. Він дозволяє формувати стимули і обмеження, які впливають на прийняття рішень іншими державами. Такий підхід є більш гнучким порівняно з прямим застосуванням сили, оскільки він допускає різні рівні інтенсивності впливу.

Історична перспектива показує, що подібні практики не є новими, однак їх масштаб і технологічна складність значно зросли. Сучасні інструменти дозволяють

---

[113] Ibid.
[114] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025. Vol. 6, No. 2.

більш точно налаштовувати параметри впливу, враховуючи економічні, політичні та соціальні фактори. Це підвищує ефективність і знижує ризики для сторони, яка застосовує такі методи[115].

Отже економічний та енергетичний вимір гібридної війни російської федерації можна охарактеризувати як систему керованих залежностей, які активуються у потрібний момент і комбінуються з іншими інструментами впливу. Його сила полягає не у масштабі окремих дій, а у здатності поступово змінювати умови взаємодії, формуючи довгострокові переваги у зовнішньополітичній.

2.3. Військові та кібернетичні інструменти реалізації гібридного впливу у зовнішній політиці російської федерації

Військовий компонент у структурі гібридного впливу російської федерації не зникає, але змінює форму. Замість відкритого застосування регулярних сил використовується комбінація обмежених, часто непрямих дій, які складно однозначно ідентифікувати як акт агресії[116]. Це дозволяє одночасно досягати тактичних результатів і мінімізувати політичні наслідки на міжнародному рівні. Однією з характерних рис є використання так званої «невизначеності суб'єкта», що передбачає свідоме розмивання відповідальності за військові дії[117]. У практичному вимірі це означає залучення формувань, які формально не входять до складу збройних сил держави: нерегулярні підрозділи, місцеві збройні групи, приватні військові компанії. Їх присутність дозволяє створити ситуацію, у якій відповідальність за військові дії залишається розмитою, що ускладнює застосування механізмів міжнародного права і знижує ймовірність прямої ескалації.

---

[115] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 135.
[116] Ibid.
[117] Ibid.

Паралельно використовується принцип обмеженого втручання[118]. Йдеться про застосування сили у таких масштабах, які не провокують негайної колективної відповіді, але достатні для зміни ситуації на місці. Це може включати контроль над окремими територіями, підтримку певних сторін у конфлікті або створення «зон нестабільності», які ускладнюють функціонування державних інституцій[119]. Такий формат дозволяє поступово змінювати баланс сил без переходу до відкритого конфлікту, зберігаючи можливість маневру у міжнародному середовищі.

Важливо, що військові дії у гібридній моделі майже завжди передуються підготовчим етапом. Інформаційні кампанії формують відповідне сприйняття подій, економічні інструменти послаблюють державу-ціль, політичні процеси створюють внутрішні суперечності[120]. У результаті військове втручання відбувається у середовищі, де опір є неповним і, як наслідок, менш ефективним. Така послідовність дій свідчить про системний характер гібридної стратегії, де військовий компонент виступає завершальним етапом більш широкого процесу впливу.

На тактичному рівні використовуються методи, що поєднують класичні військові дії з нестандартними підходами[121]. Операції можуть включати одночасне застосування регулярних підрозділів, диверсійних груп і місцевих формувань, що створює складну структуру взаємодії[122]. Така багаторівнева конфігурація ускладнює координацію відповіді з боку держави-цілі і створює додаткові труднощі для ідентифікації джерела загрози. Важливо, що ці елементи не функціонують ізольовано, а взаємодіють у межах єдиної операційної логіки.

---

[118] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023.
[119] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 451
[120] Ibid.
[121] Ibid.
[122] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 451

Окремо варто відзначити роль кіберінструментів, які стали невід'ємною частиною військового впливу. Кібероперації дозволяють досягати ефекту, співставного з традиційними військовими діями, без фізичного втручання. Йдеться про атаки на енергетичну інфраструктуру, транспортні системи, державні інформаційні ресурси, що можуть призводити до порушення критично важливих процесів[123]. У результаті вплив охоплює не лише військову сферу, а й економіку, управління та соціальну стабільність держави.

Технічно такі операції реалізуються через проникнення у інформаційні системи, використання вразливостей програмного забезпечення, а також застосування шкідливого коду[124]. Важливо, що кібероперації можуть бути як точковими, так і масштабними. У першому випадку вони спрямовані на конкретні об'єкти, у другому – на створення системних збоїв, які охоплюють ширші сегменти інфраструктури[125]. Така гнучкість дозволяє адаптувати характер впливу до конкретної ситуації.

Крім безпосереднього впливу, кіберінструменти виконують розвідувальну функцію. Отримання доступу до внутрішніх систем дозволяє збирати інформацію про структуру управління, економічні процеси та військові можливості[126]. Ці дані використовуються для планування подальших дій і підвищення їх ефективності, що підкреслює стратегічний характер кібероперацій.

Суттєвою перевагою кібероперацій є можливість заперечення причетності. Навіть у випадку виявлення атаки встановлення її джерела потребує часу і не завжди є однозначним[127]. Це створює додаткові труднощі для міжнародної реакції і дозволяє уникати прямої відповідальності[128]. У результаті кібернетичний компонент стає

---

[123] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025.
[124] Ibid.
[125] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021.
[126] Ibid.
[127] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.
[128] Ibid.

одним із найбільш ефективних інструментів гібридної стратегії, оскільки поєднує високий рівень впливу з відносно низькими ризиками для суб'єкта дії.

У підсумку військовий компонент гібридного впливу не зникає, а трансформується, інтегруючись із іншими інструментами і набуваючи нових форм реалізації. Його ефективність визначається не масштабом застосування сили, а здатністю поєднувати різні механізми впливу, створюючи комплексний ефект, який важко нейтралізувати традиційними засобами.

У структурі гібридного впливу кіберінструменти часто виконують роль «підсилювача». Вони можуть супроводжувати військові дії, створюючи додатковий тиск, або використовуватися самостійно для досягнення певних цілей. Наприклад, атаки на інформаційні ресурси можуть поєднуватися з поширенням дезінформації, що підсилює їх ефект.

Важливим аспектом є синхронізація різних інструментів. Військові та кібернетичні дії рідко здійснюються ізольовано. Вони інтегруються у загальну стратегію, де кожен елемент виконує свою функцію. Така координація забезпечує комплексний вплив, який складно нейтралізувати окремими заходами.

У ширшому контексті це відповідає концепції гібридної війни як багатовимірного процесу, де межі між різними формами конфлікту стають розмитими. Військові та кібернетичні інструменти виступають частиною єдиної системи, яка спрямована на досягнення політичних результатів через комбінування різних методів впливу[129].

Для розуміння практичної дії військових і кібернетичних інструментів доцільно розкласти їх на послідовність операційних кроків, які повторюються у різних конфліктах із незначними варіаціями. Початковий етап не має відкрито військового характеру. Він включає розвідку – як традиційну, так і кібернетичну.

[129] Arifin J. D. Unraveling current trends in hybrid warfare 3.0: A literature study on modern non-conventional threats. *Proceedings of the International Conference on Economics, Technology, Management, Accounting, Education (ICETEA).* 2025

Проникнення в інформаційні системи державних установ, енергетичних компаній, телекомунікаційних операторів дозволяє отримати дані про структуру управління, вразливості інфраструктури, канали комунікації. Ця інформація не є самоціллю. Вона використовується для точного налаштування наступних дій.

Після цього формується фаза дестабілізації. На цьому етапі кібероперації спрямовуються на створення збоїв у функціонуванні ключових систем. Йдеться не обов'язково про повне виведення їх з ладу. Часто достатньо короткострокових порушень, які підривають довіру до інституцій. Наприклад, тимчасове відключення енергопостачання або збої у роботі державних сервісів створюють ефект нестабільності, який має як практичні, так і психологічні наслідки[130].

У цей же період активізується військовий компонент, але у непрямій формі. Замість масштабних операцій використовуються локальні дії, спрямовані на зміну балансу сил у конкретних точках. Це можуть бути операції із захоплення стратегічних об'єктів, підтримка певних груп або створення умов для їх посилення. Важливо, що такі дії не супроводжуються офіційним визнанням, що дозволяє зберігати простір для політичних маневрів і уникати формалізованої відповідальності[131].

Особливістю є синхронізація цих процесів. Кіберзбої, інформаційні кампанії і військові дії відбуваються у взаємозв'язку, формуючи єдину логіку впливу. Наприклад, порушення роботи комунікаційних систем може збігатися з активізацією збройних дій, що ускладнює координацію відповіді. Одночасно у медійному просторі поширюються інтерпретації, які пояснюють події у вигідному для російської федерації ключі[132]. Така дія створює ефект перевантаження, коли

---

[130] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025. Vol. 6, No. 2.

[131] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 135

[132] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449

держава-ціль змушена реагувати одразу на кілька типів загроз, що знижує ефективність кожної окремої відповіді.

У випадку України ця логіка проявлялася у поєднанні кібероперацій проти енергетичної інфраструктури з військовими діями на сході країни [8, с. 198]. Порушення роботи енергосистеми не лише створювало практичні труднощі, але й підсилювало відчуття вразливості. У таких умовах навіть локальні військові операції отримують більший резонанс і вплив на загальну ситуацію, оскільки вони накладаються на вже дестабілізоване середовище.

Кіберінструменти використовуються і для маніпуляції інформаційними потоками. Злам медіа-ресурсів або їх імітація дозволяє поширювати повідомлення від імені легітимних джерел. Це ускладнює перевірку інформації і підвищує рівень довіри до неправдивих повідомлень. У результаті інформаційний і кібернетичний компоненти фактично зливаються в єдиний механізм впливу.

Військові дії у такій системі виконують функцію фіксації результату. Після створення сприятливого середовища вони закріплюють зміни, досягнуті на попередніх етапах. Це може бути контроль над територією, зміна політичної конфігурації або формування нових центрів впливу. Важливо, що ці дії часто мають обмежений масштаб, але їх ефект підсилюється попередніми операціями, що робить їх стратегічно значущими.

Окремо варто розглянути питання керованості ескалації. Гібридна модель дозволяє змінювати інтенсивність впливу залежно від реакції міжнародної спільноти[133]. Якщо відповідь є слабкою, тиск може посилюватися. У разі ризику прямого конфлікту – навпаки, знижуватися або переводитися у інші форми. Така гнучкість забезпечує стратегічну перевагу, оскільки дозволяє уникати ситуацій, у яких противник має чіткі підстави для колективної відповіді.

---

[133] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026.

Ще один аспект – використання часу як ресурсу. Гібридні операції не орієнтовані на швидкий результат. Вони можуть тривати роками, поступово змінюючи ситуацію[134]. Кібероперації забезпечують постійний доступ до інформації, військові дії підтримують напруженість, а інформаційні кампанії формують відповідне сприйняття. У сукупності це створює довготривалий вплив, який складно нейтралізувати навіть за умов активної протидії.

У ширшому вимірі військові та кібернетичні інструменти виконують роль силового каркасу гібридної стратегії. Вони забезпечують можливість переходу від непрямих форм впливу до більш жорстких дій у разі необхідності. При цьому межа між цими формами залишається розмитою, що ускладнює визначення моменту, коли конфлікт переходить у відкриту фазу[135].

З урахуванням цього можна говорити про формування нової моделі застосування сили, де військові та кібернетичні інструменти інтегруються у єдину систему разом із економічними та інформаційними засобами. Їх ефективність визначається не окремими операціями, а здатністю діяти синхронно, створюючи комплексний тиск на державу-ціль. У підсумку військовий і кібернетичний компоненти гібридного впливу російської федерації характеризуються адаптивністю, прихованістю та високим рівнем координації з іншими інструментами. Саме ця комбінація дозволяє досягати значних результатів без переходу до повномасштабної війни, зберігаючи при цьому можливість подальшої ескалації або деескалації залежно від ситуації.

---

[134] Göransson M. B. Russia’s thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024.

[135] Bachmann S.-D. D., Gunneriusson H. Russia’s hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. *Georgetown Journal of International Affairs*. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198.

РОЗДІЛ 3. ПРАКТИКА ГІБРИДНОЇ АГРЕСІЇ РФ І МІЖНАРОДНІ МЕХАНІЗМИ ПРОТИДІЇ ЗАГРОЗАМ

3.1. Україна як ключовий об'єкт гібридної агресії російської федерації

Позиція України у сучасній системі міжнародних відносин формується під впливом як геополітичного розташування, так і глибших структурних факторів, пов'язаних із перетином економічних потоків, енергетичних маршрутів, безпекових інтересів і політичних орієнтацій. Україна є державою, через яку проходить лінія зіткнення між різними моделями регіонального порядку: євроатлантичною, що спирається на принципи суверенітету, інституційної демократії та правової визначеності, і російською, орієнтованою на збереження сфер впливу, контроль над сусідніми державами та обмеження їхньої зовнішньополітичної автономії. Через це український простір став не випадковою ареною конфлікту, а одним із головних напрямів реалізації гібридної стратегії російської федерації.

На рівні наукового осмислення Україна розглядається як простір, де відбувалася апробація сучасних моделей гібридної війни. М. Магда (M. Mahda) пов'язує початкову фазу цієї трансформації з подіями 2014 року, коли поєднання інформаційних, політичних і силових дій набуло рис узгодженої стратегії[136]. Це поєднання не мало випадкового характеру. Воно відображало прагнення сформувати нову логіку впливу, у якій військовий тиск не відокремлюється від інформаційної обробки суспільства, економічного примусу та політичної дестабілізації.

Український кейс показує, що гібридна агресія розгортається не миттєво. Її практична логіка полягає у поступовій зміні середовища, у якому функціонує держава. Спершу формується інформаційне тло, що підриває довіру до влади, армії, міжнародних партнерів і власної державності. Далі активізуються політичні й

[136] Mahda Y. The start of RF's hybrid aggression against Ukraine: The point of bifurcation. *European Political and Law Discourse*. 2018. Vol. 5, No. 2. P. 41–47.

соціальні розломи, посилюється економічний тиск, створюються контрольовані осередки нестабільності. Британський аналітик Кір Джайлз (K. Giles) звертає увагу на те, що інформаційний простір у російській стратегії виступає не допоміжним каналом, а середовищем формування сприйняття реальності[137]. Для України це мало принципове значення, оскільки ще до відкритих силових дій російська федерація працювала над тим, щоб подати українську державність як нестійку, залежну і внутрішньо конфліктну.

Першим практичним прикладом, який демонструє дію гібридних механізмів, стала анексія Криму у 2014 році. У цьому випадку російська федерація поєднала військову присутність без офіційного визнання, інформаційну кампанію про «захист населення», політичне конструювання псевдолегітимних процедур і швидке адміністративне закріплення контролю над територією. С.-Д. Д. Бахманн і Х. Гуннеріуссон (S.-D. D. Bachmann, H. Gunneriusson) підкреслюють, що інформаційна сфера була інтегральною частиною російської гібридної війни на сході Європи[138]. У випадку Криму це проявилося у тому, що силова операція супроводжувалася комунікативною рамкою, яка мала створити враження внутрішнього політичного процесу, а не зовнішнього втручання.

Другим показовим прикладом став конфлікт на Донбасі. Тут гібридна агресія реалізовувалася через підтримку нерегулярних формувань, формування так званих «народних республік», інформаційне заперечення зовнішньої участі та поступове перетворення локальної нестабільності на довготривалий інструмент тиску на Україну. Р. Аллегрі (R. Allegri) зазначає, що використання непрямих форм військового впливу дозволяє державі-агресору мінімізувати політичні ризики та

---

[137] Giles K. The next phase of Russian information warfare. *Riga: NATO Strategic Communications Centre of Excellence*. 2016.

[138] Bachmann S.-D. D., Gunneriusson H. Russia's hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. *Georgetown Journal of International Affairs*. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198.

зберігати простір для заперечення відповідальності[139]. Для України це означало появу ситуації, коли військовий конфлікт фактично існував, однак його міжнародно-правова кваліфікація ускладнювалася через навмисне розмивання суб'єкта агресії.

З метою узагальнення практичної логіки гібридного впливу доцільно представити ескалаційну структуру застосування інструментів російської федерації щодо України.

Таблиця 3.1

Ескалаційні рівні гібридної агресії російської федерації щодо України

Рівень впливу	Характер дій	Основні механізми	Практичний прояв	Очікуваний ефект
Початковий	Прихований	Інформаційні кампанії, політична дестабілізація	Поширення наративів про «кризу державності», «внутрішній конфлікт», «зовнішнє управління»	Формування недовіри до інституцій
Проміжний	Змішаний	Проксі-структури, економічний тиск, локальна дестабілізація	Підтримка контрольованих груп, тиск через енергетичні й торговельні механізми	Ослаблення державної спроможності

[139] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 135.

Активний	Обмежено відкритий	Локальні військові дії, кібератаки, інформаційний супровід	Донбас, атаки на критичну інфраструктуру, дезінформація про перебіг бойових дій	Зміна балансу сил
Ескалаційний	Відкритий	Масштабне застосування сили, стратегічний тиск	Повномасштабне вторгнення, ракетні удари, тиск на цивільну інфраструктуру	Політичне примушення

Джерело: узагальнено на основі [8], [35], [23].

Подана таблиця показує, що гібридна агресія проти України не зводиться до одного інструменту або одного періоду. Її особливість полягає у переході між рівнями впливу залежно від політичної ситуації, стану міжнародної реакції та внутрішньої стійкості України. Початкові приховані дії не зникають після переходу до відкритої фази. Навпаки, інформаційні кампанії, економічний тиск і кібероперації продовжують діяти паралельно з військовим компонентом, що забезпечує тривалість і складність агресії.

На концептуальному рівні цей процес відображає поступове нарощування інтенсивності при збереженні можливості заперечення відповідальності. Нижче подано узагальнену модель, яка ілюструє перехід від прихованого до відкритого гібридного впливу.

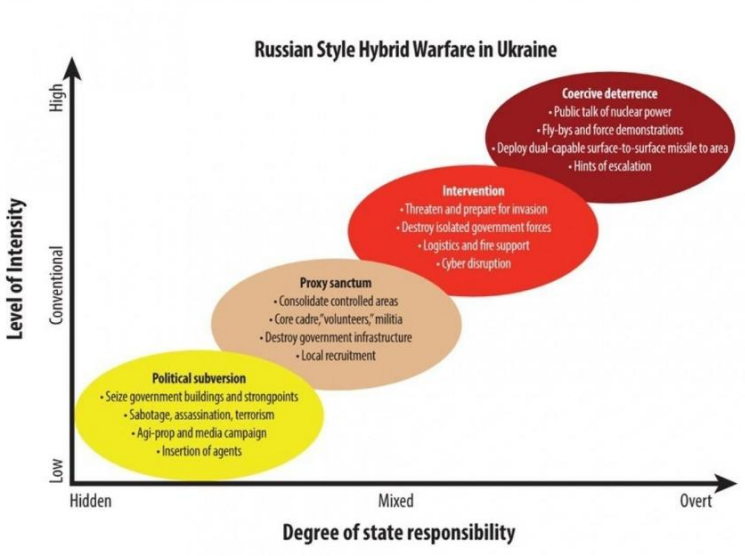

Рисунок 3.1 – Динаміка переходу від прихованого до відкритого гібридного впливу (за інтенсивністю та рівнем державної відповідальності)

Джерело: [14]

Представлена схема демонструє, що збільшення інтенсивності впливу супроводжується поступовим переходом від непрямих форм дії до відкритих інструментів примусу. На ранніх етапах переважають інформаційні кампанії, політичні операції, економічний тиск і кібернетичні втручання. Їхня функція полягає у підготовці середовища, де подальші дії виглядатимуть менш несподіваними або навіть нібито виправданими. На наступних етапах активізуються проксі-структури, локальні силові дії, демонстрація військової присутності. У фазі відкритої ескалації військовий компонент стає домінантним, однак не витісняє попередні інструменти. Вони продовжують працювати як засоби супроводу, легітимації та дезорієнтації аудиторій.

Практичний зміст цієї моделі добре простежується у випадку України. У Криму російська федерація діяла через комбінацію військової присутності без офіційного визнання, інформаційної кампанії та швидкого політико-правового оформлення контролю. На Донбасі переважала модель проксі-конфлікту, де ключовим було створення видимості місцевої ініціативи. У подальшому, після 2022

року, відбулося різке зростання рівня відкритості агресії, проте гібридні інструменти не втратили значення. Вони були інтегровані у ширшу військово-політичну стратегію.

У випадку України важливу роль відіграє економічний вимір впливу. Енергетичний сектор виступав одним із ключових каналів формування залежності, особливо до переорієнтації української енергетичної політики. М. Джері (M. Geri) підкреслює, що використання енергетичних ресурсів як інструменту політичного впливу дозволяє досягати стратегічних цілей без прямого військового втручання[140]. Для України це проявлялося у маніпуляціях умовами постачання, цінових конфліктах, використанні транзитного фактору та спробах зберегти енергетичну вразливість як інструмент зовнішнього тиску.

Окремий практичний кейс пов'язаний із кіберопераціями проти України. Їх застосування дозволяло впливати на критичну інфраструктуру, інформаційні системи, комунікаційні канали та державні ресурси. Н. Махмуд (N. Mahmood) зазначає, що кібероперації виконують не лише деструктивну функцію, а й розвідувальну, оскільки забезпечують доступ до інформації, яка може використовуватися для подальшого планування[141]. Е. Капсоколі (E. Kapsokoli) розглядає кіберпростір як один із напрямів російсько-української війни, де цифрові атаки стають частиною ширшої стратегії тиску[142]. Практично це означає, що кібератаки не лише порушують роботу систем, а й формують психологічний ефект вразливості держави.

У цьому контексті показовими є атаки на енергетичну та цифрову інфраструктуру. Їхній ефект виходить за межі технічного збою. Порушення

---

[140] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. *Journal of Strategic Security*. 2024. Vol. 17, No. 3. Article 2.
[141] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021. Vol. 18, No. 4. P. 1720.
[142] Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025. Vol. 6, No. 2.

електропостачання, роботи державних сервісів або комунікаційних систем створює відчуття нестабільності, підриває довіру до державних інституцій і посилює соціальну напругу. У гібридній логіці такий вплив працює не самостійно, а у поєднанні з інформаційними повідомленнями, які пояснюють події у вигідному для агресора ключі.

Військовий компонент у гібридній моделі набуває специфічної форми. Замість прямого і повного застосування регулярної сили на початкових етапах використовуються локальні дії, підтримка нерегулярних формувань, створення зон нестабільності. Р. Аллегрі (R. Allegri) зазначає, що такий підхід дозволяє поєднувати досягнення тактичних результатів із мінімізацією політичних ризиків[143]. Це формує ситуацію, у якій конфлікт може тривалий час не переходити у класичну відкриту фазу, але зберігати високий рівень напруженості та впливати на всю систему державного управління.

Ще один практичний вимір пов'язаний із медичною та гуманітарною сферою. М. С. Бейкер, Дж. Бейкер і Ф. М. Беркл (M. S. Baker, J. Baker, F. M. Burkle) наголошують, що російська гібридна війна проти України створює загрози не лише для військової безпеки, а й для охорони здоров'я та гуманітарного захисту[144]. У практичному плані це проявляється через атаки на медичні заклади, руйнування гуманітарної інфраструктури, дезінформацію щодо гуманітарних операцій і спроби використати страждання цивільного населення як елемент політичного тиску.

Адаптивність стратегії залишається визначальною рисою. М. Йоранссон (M. Göransson) підкреслює, що інструменти впливу постійно коригуються залежно від реакції держави-цілі та міжнародного середовища[145]. У випадку України це означає,

---

[143] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 138

[144] Baker M. S., Baker J., Burkle F. M. Russia's hybrid warfare in Ukraine threatens both healthcare & health protections provided by international law. *Annals of Global Health.* 2023. Vol. 89, No. 1. Article 3.

[145] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449

що російська федерація змінювала акценти: від заперечення участі у конфлікті до відкритого військового тиску, від енергетичного примусу до руйнування інфраструктури, від наративів про «внутрішній конфлікт» до ширших тез про протистояння із Заходом.

Важливим елементом є також правова невизначеність. Частина дій не підпадає під класичні визначення агресії або потребує складного доказування. А. Полякова і М. Булег (A. Polyakova, M. Boulègue) звертають увагу на те, що така невизначеність дозволяє уникати консолідованих дій з боку інших держав[146]. В українському випадку ця проблема була особливо помітною на початкових етапах агресії, коли використання нерегулярних формувань і заперечення участі російської федерації ускладнювали швидке формування міжнародної відповіді.

Соціальний вимір проявляється через зміну поведінки суспільства. Інформаційні кампанії формують нові інтерпретації подій, підвищують рівень поляризації, знижують довіру до інституцій і створюють умови для внутрішньої напруги. Ф. Сплідсбоель Гансен (F. Splidsboel Hansen) наголошує, що інформаційні операції здатні змінювати соціальну динаміку навіть без прямого застосування сили[147]. Для України це означало постійний тиск на суспільну єдність, спроби посіяти недовіру між громадянами і владою, між державою та міжнародними партнерами, між різними регіонами країни.

У ширшому вимірі Україна виступає не лише об’єктом впливу, а й елементом геополітичної стратегії. А. Мамфорд і П. Карлуччі (A. Mumford, P. Carlucci) розглядають гібридну війну як інструмент трансформації міжнародних відносин, який дозволяє змінювати баланс сил без прямого зіткнення великих держав[148]. Український кейс надає цьому підходу практичного наповнення, оскільки

---

[146] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.
[147] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. *DIIS Report No. 2017:06. Copenhagen: Danish Institute for International Studies.* 2017.
[148] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192

демонструє, як локалізований на перший погляд конфлікт впливає на регіональну безпеку, енергетичну політику Європи, санкційні режими, оборонне планування НАТО і загальне розуміння міжнародної відповідальності.

У підсумку Україна постає як центральний об’єкт гібридної агресії російської федерації, де поєднуються різні інструменти впливу і відпрацьовуються нові моделі конфлікту. Практичний аспект демонструє, що гібридна агресія проти України має комплексний характер. Її роль визначається не лише географічним положенням, а й функцією у формуванні сучасних стратегій протистояння. Гібридна агресія, спрямована на Україну, показує здатність до адаптації, координації та тривалого впливу, що робить її одним із ключових викликів для міжнародної безпеки.

3.2. Практика застосування гібридних інструментів російської федерації у міжнародному середовищі

Аналіз сучасних міжнародних процесів демонструє, що гібридні інструменти російської федерації не обмежуються регіональними рамками, а поступово інтегруються у ширший простір глобальної політики. Йдеться не про ізольовані епізоди впливу, а про системну практику, яка формує нову конфігурацію взаємодії між державами. Така практика проявляється у різних регіонах, але зберігає спільну логіку: поєднання інформаційних кампаній, економічного тиску, політичного втручання, кібероперацій і обмеженого силового компонента. У цьому полягає одна з ключових відмінностей гібридної стратегії від класичного військово-політичного примусу, адже вплив здійснюється не через один домінантний канал, а через послідовне накладання кількох механізмів на вразливі ділянки держави або регіону.

У наукових дослідженнях дедалі частіше підкреслюється, що гібридний вплив функціонує як адаптивна стратегія, здатна змінювати форму залежно від політичного середовища. Дж. Д. Аріфін (J. D. Arifin) зазначає, що сучасні конфлікти характеризуються переходом від прямих форм протистояння до непрямих методів,

які дозволяють досягати стратегічних цілей без відкритої ескалації[149]. Це означає, що гібридні інструменти можуть застосовуватися у різних політичних і культурних умовах: у державах із нестабільними інститутами, у країнах із високою енергетичною залежністю, у суспільствах із глибокою політичною поляризацією, а також у просторах затяжних регіональних конфліктів.

У міжнародному середовищі така стратегія реалізується через створення умов, за яких внутрішні процеси держав поступово піддаються зовнішньому коригуванню. Інформаційний вплив формує інтерпретаційні рамки, економічні інструменти створюють залежності, політичні механізми змінюють конфігурацію влади, а кібероперації підривають довіру до інституційної спроможності держави. К. Джайлз (K. Giles) підкреслює, що інформаційні операції відіграють центральну роль у цьому процесі, оскільки вони визначають спосіб сприйняття реальності та впливають на прийняття рішень[150]. Через це практичне застосування гібридних інструментів доцільно аналізувати не лише за типом дій, а й за тим, яку політичну функцію вони виконують.

Особливу увагу привертає здатність російської федерації поєднувати різні інструменти у межах єдиної логіки впливу. У міжнародній практиці це проявляється через синхронізацію дій, коли інформаційні кампанії супроводжують економічні рішення, політичні процеси підсилюються кібероперaціями, а військова активність подається як реакція на нібито зовнішні загрози. А. Мамфорд і П. Карлуччі (A. Mumford, P. Carlucci) наголошують, що така невизначеність і гнучкість дозволяють формувати ситуації, у яких складно ідентифікувати джерело впливу та своєчасно реагувати на нього[151]. На практиці це означає, що держава-ціль часто стикається не

[149] Arifin J. D. Unraveling current trends in hybrid warfare 3.0: A literature study on modern non-conventional threats. *Proceedings of the International Conference on Economics, Technology, Management, Accounting, Education (ICETEA).* 2025.
[150] Giles K. The next phase of Russian information warfare. *Riga: NATO Strategic Communications Centre of Excellence*. 2016.
[151] Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. 2023. P. 192.

з одним викликом, а з кількома паралельними кризами, які виглядають автономними, хоча працюють на один політичний результат.

Найбільш показовим практичним прикладом залишається Україна. Тут російська федерація застосувала майже повний набір гібридних інструментів: інформаційне заперечення факту зовнішньої агресії, політичну делегітимацію українських інститутів, підтримку контрольованих збройних формувань, економічний тиск, кібератаки та військове втручання. С. Д. Д. Бахманн і Х. Гуннеріуссон (S.-D. D. Bachmann, H. Gunneriusson) розглядають інформаційну сферу як невід'ємний елемент російської гібридної війни на сході Європи[152]. У практичному плані це проявлялося у формуванні наративу про «внутрішній конфлікт», який мав знизити міжнародну відповідальність російської федерації та ускладнити консолідацію зовнішньої підтримки України.

Другий практичний напрям пов'язаний із європейським енергетичним простором. Упродовж тривалого часу російська федерація використовувала постачання газу, інфраструктурні проєкти та цінову політику як засоби формування залежності окремих європейських держав. М. Джері (M. Geri) зазначає, що енергетичний сектор став одним із ключових напрямів російської гібридної стратегії щодо Європи[153]. Практичний ефект полягав у тому, що економічна доцільність співпраці поступово поєднувалася з політичною вразливістю. Держава, яка значною мірою залежить від одного постачальника енергоресурсів, обмежена у свободі зовнішньополітичних рішень, особливо під час криз.

У європейському кейсі гібридний характер впливу проявляється не лише у використанні газу як товару, а у перетворенні енергетичної інфраструктури на політичний інструмент. Трубопроводи, довгострокові контракти, спільні

[152] Bachmann S.-D. D., Gunneriusson H. Russia's hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. 2015

[153] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. 2024

підприємства та інвестиції в енергетичні активи формують мережу залежності, яку можна активувати в потрібний момент. При цьому економічні рішення часто супроводжуються інформаційним поясненням, яке подає обмеження постачання або зміну цін як наслідок «ринкової логіки». Такий формат знижує ймовірність негайної політичної реакції, адже зовнішній тиск маскується під комерційні процеси.

Окремим прикладом застосування гібридних інструментів є іранський напрям. У цьому випадку йдеться не про класичну модель впливу на державу-ціль, а про використання гібридних інструментів для формування антизахідної координації в умовах санкційного тиску. Взаємодія російської федерації з Іраном демонструє інший бік гібридної практики: інструменти використовуються не лише для послаблення опонентів, а й для створення альтернативних каналів політичної, економічної та військово-технічної взаємодії. У цьому проявляється прагнення знизити ефективність західних санкцій, розширити простір дипломатичного маневру і сформувати наратив про протистояння «західній гегемонії». Така логіка корелює із ширшим розумінням гібридної війни як гнучкої системи впливу, що діє не тільки через конфлікт, але й через створення ситуативних партнерств[154].

Іранський приклад важливий для практичного аналізу, оскільки він показує, як економічні, інформаційні та військово-технологічні елементи можуть поєднуватися не у форматі прямої агресії, а у форматі стратегічного зближення. Інформаційний рівень такої взаємодії спирається на спільні наративи про «багатополярний світ», «несправедливість санкцій» і «кризу західного порядку». Економічний рівень пов’язаний із пошуком альтернативних маршрутів торгівлі, фінансових каналів і механізмів обходу обмежень. Безпековий рівень охоплює координацію позицій у регіональних конфліктах. У підсумку іранський кейс демонструє, що гібридна практика може бути спрямована не лише на деструкцію, а й на побудову паралельних мереж впливу.

[154] Arifin J. D. Unraveling current trends in hybrid warfare 3.0: A literature study on modern non-conventional threats. 2025.

Ще один практичний приклад пов’язаний із Сирією. У сирійському конфлікті російська федерація поєднала військову підтримку режиму Башара Асада з дипломатичною активністю, інформаційним супроводом і використанням обмежених силових інструментів. Р. Аллегрі (R. Allegri) звертає увагу на історичну тяглість російського використання гібридних підходів, де військовий компонент поєднується з політичним і інформаційним впливом[155]. У сирійському випадку військова присутність подавалася як участь у боротьбі з тероризмом, тоді як фактично вона дозволила російській федерації зміцнити позиції на Близькому Сході, забезпечити військово-морську присутність у Середземномор’ї та посилити роль у переговорах щодо регіональної безпеки.

Сирійський кейс показує, що гібридні інструменти можуть використовуватися для закріплення геополітичної присутності за межами пострадянського простору. Військова активність у цьому випадку супроводжувалася інформаційними повідомленнями про «стабілізаційну місію», дипломатичними контактами з регіональними акторами та демонстрацією здатності впливати на перебіг конфлікту. Така комбінація дозволила російській федерації виступати не лише як сторона конфлікту, а як посередник і силовий гарант. Це підвищило її переговорну вагу в міжнародному середовищі.

У випадку західних держав демонструється інша практика застосування гібридних інструментів. Тут на перший план виходять інформаційні операції, вплив на суспільні настрої, підтримка поляризації та використання кібернетичних засобів. Ф. Сплідсбоель Гансен (F. Splidsboel Hansen) підкреслює, що російські дезінформаційні практики спрямовані не лише на переконання аудиторії, а й на підрив довіри до демократичних інститутів[156]. У практичному вимірі це

[155] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. 2026. P. 139
[156] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. *DIIS Report No. 2017:06. Copenhagen: Danish Institute for International Studies.* 2017.

проявляється у поширенні суперечливих повідомлень, підсиленні радикальних позицій, використанні соціальних мереж і створенні враження суспільного розколу.

Кібернетичний компонент у міжнародному середовищі доповнює інформаційні кампанії. Н. Махмуд, А. І. Малік і М. Н. Мірза (N. Mahmood, A. I. Malik, M. N. Mirza) зазначають, що кібероперації у гібридній війні можуть виконувати як деструктивну, так і розвідувальну функцію[157]. На практиці це означає, що кібератаки не обмежуються пошкодженням систем. Вони можуть використовуватися для отримання даних, створення інформаційних приводів, поширення викрадених матеріалів або імітації витоків. У поєднанні з інформаційними кампаніями такі дії здатні впливати на політичний порядок денний інших держав.

Для систематизації практичних випадків доцільно подати узагальнену таблицю, яка відображає регіональну специфіку застосування.

Таблиця 3.2

Практичні кейси застосування гібридних інструментів російської федерації у міжнародному середовищі

Практичний кейс	Провідні інструменти	Механізм застосування	Очікуваний або досягнутий ефект
Україна	Інформаційні, військові, кібернетичні, економічні	Делегітимація державних інститутів, підтримка контрольованих збройних структур,	Дестабілізація держави, ускладнення міжнародної реакції, зміна безпекового середовища

[157] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021.

		кібератаки, економічний тиск	
Європейський енергетичний простір	Економічні, енергетичні, інформаційні	Формування залежності від постачання газу, використання контрактів та інфраструктури як важелів впливу	Політичний тиск, обмеження свободи зовнішньополітичних рішень окремих держав
Іранський напрям	Економічні, політичні, інформаційні, військово-технологічні	Координація в умовах санкційного тиску, формування антизахідних наративів, пошук альтернативних каналів взаємодії	Послаблення ефекту санкцій, формування паралельних мереж впливу
Сирія	Військові, дипломатичні, інформаційні	Підтримка режиму, військова присутність, інформаційна легітимація дій	Закріплення геополітичної присутності, посилення переговорної ролі
Західні держави	Інформаційні, кібернетичні, політичні	Поширення дезінформації, підтримка поляризації, втручання у цифровий простір	Зниження довіри до демократичних інститутів, вплив на суспільні настрої

Джерело: узагальнено на основі аналізу гібридних інструментів у межах дослідження.

Представлена таблиця показує, що практичний аспект застосування гібридних інструментів російської федерації має не одну, а кілька моделей реалізації. В Україні переважає комплексна модель, де одночасно застосовуються військові, інформаційні, економічні та кібернетичні засоби. У Європі більш помітним є економічно-енергетичний вимір. В Ірані простежується модель стратегічної координації і формування альтернативних каналів взаємодії. У Сирії домінує поєднання військового впливу, дипломатії та інформаційної легітимації. У західних державах особливо виразними є інформаційні та кібернетичні методи.

Практика застосування гібридних інструментів демонструє, що економічний вимір відіграє ключову роль у формуванні довгострокових залежностей. М. Джері (M. Geri) підкреслює, що використання енергетичних ресурсів як інструменту впливу дозволяє змінювати політичні рішення без прямого втручання[158]. У міжнародному середовищі це проявляється через формування енергетичних зв'язків, які обмежують можливості держав щодо самостійної політики. Водночас економічний тиск майже завжди супроводжується інформаційним поясненням, що переводить політичний вплив у площину нібито ринкових процесів.

Військовий компонент у міжнародній практиці зберігає допоміжну, але важливу роль. Його застосування відбувається у формі локальних дій, які не провокують негайної ескалації, але дозволяють змінювати ситуацію на місці. Р. Аллегрі (R. Allegri) звертає увагу на те, що такі дії поєднуються з іншими інструментами, формуючи комплексний вплив[159]. У практичному вимірі це особливо помітно там, де російська федерація прагне не стільки повного контролю, скільки створення залежності або постійної нестабільності.

Адаптивність залишається ключовою характеристикою цієї практики. М. Йоранссон (M. Göransson) підкреслює, що стратегія постійно змінюється залежно

[158] Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. 2024

[159] Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. 2026. P. 135..

від реакції міжнародної спільноти[160]. Якщо один інструмент втрачає ефективність, акцент переноситься на інший. Це дозволяє підтримувати тиск навіть тоді, коли прямі методи стають менш результативними або надто ризикованими.

Важливим аспектом є також використання правової невизначеності. Частина дій не підпадає під класичні визначення агресії, що ускладнює формування міжнародної відповіді. А. Полякова і М. Булег (A. Polyakova, M. Boulègue) наголошують, що це дозволяє уникати консолідованих дій з боку інших держав[161]. У практичному плані це означає, що гібридний вплив часто реалізується у проміжній зоні між політичним тиском, економічним примусом і безпековою загрозою.

Соціальний вимір проявляється через зміну поведінки суспільства у різних країнах. Інформаційні кампанії формують нові інтерпретації подій, підвищують рівень поляризації, знижують довіру до інституцій. Ф. Сплідсбоель Гансен (F. Splidsboel Hansen) підкреслює, що такі процеси здатні впливати на політичні рішення навіть без прямого втручання[162]. У міжнародному середовищі це дозволяє російській федерації працювати не лише з урядами, а й із суспільними настроями, групами невдоволення, інформаційними розломами та кризами довіри.

У ширшому вимірі практика застосування гібридних інструментів формує нову модель міжнародних відносин, у якій межі між війною і миром стають менш визначеними. М. Калдор (M. Kaldor) пов’язує цей процес із трансформацією природи конфліктів, де традиційні підходи поступаються місцем більш гнучким формам впливу[163]. Через це гібридна практика російської федерації у міжнародному середовищі має не лише регіональне, а й системне значення, оскільки вона змінює уявлення про безпеку, відповідальність і механізми протидії.

---

[160] Göransson M. B. Russia’s thinking on new wars and its full-scale invasion of Ukraine. 2024.
[161] Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.
[162] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. 2017.
[163] Kaldor M. In defence of new wars. 2013.

У підсумку можна констатувати, що гібридні інструменти російської федерації у міжнародному середовищі формують складну систему впливу, яка поєднує різні механізми та забезпечує довгостроковий ефект. Їх ефективність визначається здатністю адаптуватися до змін середовища, інтегрувати різні інструменти та використовувати слабкі місця у функціонуванні держав. Практичні кейси України, європейського енергетичного простору, Ірану, Сирії та західних держав демонструють, що гібридний вплив реалізується не за єдиним шаблоном, а через зміну конфігурації інструментів відповідно до конкретного політичного середовища. Саме ця гнучкість робить його одним із ключових викликів для сучасної міжнародної безпеки.

3.3. Міжнародні механізми реагування та протидії гібридним загрозам

Сучасна практика міжнародної безпеки демонструє, що гібридні загрози створюють якісно новий тип викликів, які не можуть бути ефективно нейтралізовані в межах традиційних підходів до колективної оборони. Їхня специфіка полягає у поєднанні різних форм впливу, які реалізуються з різною інтенсивністю, часто нижче порогу відкритого конфлікту. Це ускладнює як ідентифікацію джерела загрози, так і вибір адекватних механізмів реагування.

У наукових дослідженнях підкреслюється, що ефективна протидія гібридним загрозам потребує не лише військових інструментів, а комплексного підходу, який охоплює політичні, економічні, інформаційні та кібернетичні компоненти. Ф. Хоффман (F. Hoffman) зазначає, що сучасні конфлікти характеризуються зміщенням від прямого застосування сили до комбінованих форм впливу, що вимагає відповідної трансформації систем безпеки[164]. Це означає, що міжнародні механізми реагування повинні враховувати не лише характер загроз, але й їхню динаміку.

[164] Hoffman F., Neumeyer M., Jensen B. The future of hybrid warfare.

Ключовим елементом протидії виступає концепція стримування, яка в умовах гібридних загроз набуває подвійного змісту. З одного боку, йдеться про підвищення вартості агресивних дій для суб'єкта впливу, з іншого – про зниження ефективності цих дій через посилення стійкості держав. Такий підхід відображає зміну парадигми безпеки, де акцент переноситься з реагування на попередження.

Для систематизації міжнародних механізмів протидії доцільно узагальнити їх основні напрями.

Таблиця 3.3

Міжнародні механізми реагування на гібридні загрози

Напрям реагування	Зміст механізму	Інструменти	Очікуваний ефект
Політичний	Координація дій держав	Міжнародні угоди, санкційна політика	Консолідація позицій
Економічний	Обмеження ресурсів агресора	Санкції, контроль ринків	Зниження можливостей впливу
Інформаційний	Протидія дезінформації	Моніторинг, фактчекінг, медіаполітика	Формування стійкості суспільства
Кібернетичний	Захист інфраструктури	Кібербезпека, обмін даними	Зменшення вразливостей
Військовий	Демонстрація готовності	Колективна оборона, навчання	Стримування ескалації

Джерело: узагальнено на основі [15; 25; 35]

Представлена таблиця відображає, що ефективність реагування визначається не окремими інструментами, а їх узгодженим застосуванням. У цьому зв'язку особливого значення набуває координація дій між державами та міжнародними організаціями.

Аналітичне осмислення механізмів протидії доцільно доповнити візуалізацією логіки стримування гібридних загроз.

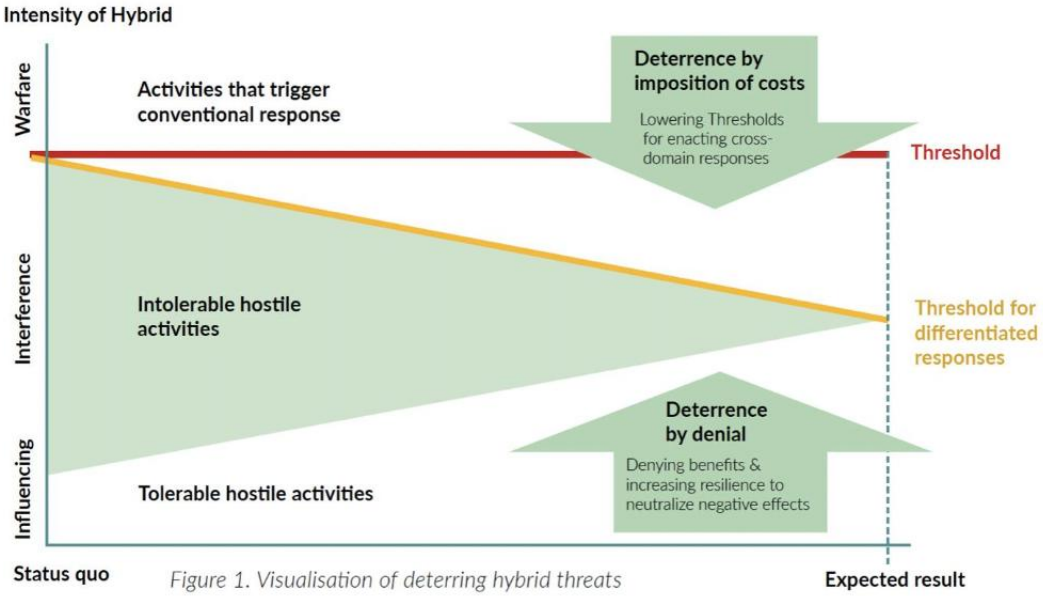

Figure 1. Visualisation of deterring hybrid threats

Рисунок 3.2 – Модель стримування гібридних загроз через підвищення вартості дій та посилення стійкості держав

Джерело: [26]

Зазначена модель демонструє, що ефективна протидія ґрунтується на поєднанні двох взаємодоповнюючих підходів. Перший передбачає підвищення витрат для суб'єкта агресії через санкційні та політичні механізми. Другий спрямований на зміцнення внутрішньої стійкості держав, що знижує ефективність зовнішнього впливу. Поєднання цих підходів дозволяє зміщувати поріг, після якого гібридні дії стають економічно або політично невигідними.

Важливою характеристикою міжнародних механізмів реагування є їхня адаптивність. М. Йоранссон (M. Göransson) підкреслює, що гібридні загрози

постійно змінюються, що змушує системи безпеки коригувати свої підходи[165]. Це означає, що статичні моделі протидії втрачають ефективність, поступаючись місцем більш гнучким рішенням.

Значну роль відіграє і правовий вимір. Відсутність чітких критеріїв визначення гібридної агресії у міжнародному праві ускладнює застосування колективних механізмів реагування, оскільки більшість дій, що входять до її структури, не підпадають під класичні визначення збройного нападу або агресії у традиційному розумінні[166]. Це стосується як інформаційних операцій, так і кібернетичних атак, економічного тиску чи втручання у політичні процеси, які розглядаються окремо, але не завжди визнаються як частини єдиного агресивного акту[167]. У результаті виникає ситуація, коли держави можуть системно впливати на інші країни, не порушуючи формальних юридичних норм, що значно ускладнює формування адекватної міжнародної відповіді.

А. Полякова (A. Polyakova) і М. Булег (M. Boulègue) підкреслюють, що така невизначеність створює простір для маневру, який активно використовується у сучасних конфліктах[168]. Йдеться про можливість варіювати інтенсивність і форми впливу, зберігаючи їх у межах, які не провокують негайної колективної реакції. У відповідь на це у міжнародній практиці формується тенденція до розширеного тлумачення загроз, коли окремі дії починають розглядатися не ізольовано, а як елементи комплексної стратегії[169]. Такий підхід дозволяє адаптувати існуючі правові механізми до нових умов, хоча і не усуває повністю проблеми невизначеності.

---

[165] Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. P. 449

[166] olyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion.

[167] Ibid.

[168] Ibid.

[169] Ibid.

Важливо зазначити, що правовий вимір гібридних загроз пов'язаний не лише з їх кваліфікацією, а й з механізмами відповідальності. У багатьох випадках складно встановити суб'єкта впливу, що створює додаткові труднощі для застосування санкцій чи інших заходів реагування[170]. Це особливо характерно для кібероперацій та інформаційних кампаній, де ідентифікація джерела потребує складних технічних і аналітичних процедур. Таким чином, правова невизначеність поєднується з технічною складністю, що додатково підсилює ефективність гібридних інструментів.

Окрему увагу привертає роль міжнародних організацій, які виступають ключовими акторами у формуванні системи протидії гібридним загрозам. НАТО розглядає такі загрози як комплексне явище, що потребує інтегрованого підходу до реагування[171]. Це означає, що протидія не може обмежуватися військовими заходами, а повинна включати політичні, економічні, інформаційні та кібернетичні інструменти[172]. У межах цієї логіки формується концепція колективної стійкості, яка передбачає підвищення здатності держав до протидії різним формам впливу.

Практична реалізація такого підходу передбачає розвиток механізмів координації між державами, зокрема у сфері обміну інформацією та спільного аналізу загроз[173]. Важливу роль відіграють спеціалізовані центри, які займаються моніторингом гібридних загроз і розробкою рекомендацій щодо їх нейтралізації. Така інституційна структура дозволяє забезпечити більш швидке реагування і підвищити ефективність колективних дій.

Інформаційний вимір протидії набуває особливого значення у зв'язку з поширенням дезінформації як одного з ключових інструментів гібридної агресії. Ф. Сплідсбоель Гансен (F. Splidsboel Hansen) наголошує, що інформаційні операції

---

[170] Ibid.
[171] Countering hybrid threats. *North Atlantic Treaty Organization*
[172] Ibid.
[173] Ibid.

здатні впливати на поведінку суспільства, формуючи умови для прийняття політичних рішень[174]. Це означає, що інформаційний вплив не обмежується сферою комунікації, а має безпосередні наслідки для функціонування держави[175]. У зв'язку з цим зростає значення систем моніторингу інформаційного простору, які дозволяють своєчасно виявляти дезінформаційні кампанії[176].

Розвиток аналітичних інструментів стає важливою складовою протидії. Йдеться про використання технологій аналізу великих даних, які дозволяють відстежувати поширення інформації, виявляти мережі ботів і визначати джерела впливу[177]. Такі інструменти дозволяють не лише реагувати на загрози, а й прогнозувати їх розвиток. Паралельно формується система стратегічних комунікацій, яка спрямована на формування альтернативних наративів і підвищення рівня довіри до офіційних джерел інформації[178].

Кібернетичний компонент також займає ключове місце у системі протидії гібридним загрозам. Н. Махмуд (N. Mahmood) підкреслює, що кібероперації можуть мати значний вплив на функціонування держав, що вимагає посилення захисту критичної інфраструктури[179]. Йдеться не лише про технічні заходи, а й про формування комплексної системи кібербезпеки, яка включає нормативно-правове регулювання, розвиток кадрового потенціалу та міжнародну співпрацю. У міжнародному вимірі це проявляється через створення спільних платформ обміну інформацією, що дозволяє швидко реагувати на кіберзагрози .

Особливого значення набуває взаємодія між державами у сфері кібербезпеки. Обмін даними про кіберінциденти, координація дій та спільні навчання дозволяють

---

[174] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. 2017.
[175] Ibid.
[176] Ibid.
[177] Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021.
[178] Ibid.
[179] Ibid.

підвищити рівень готовності до можливих атак[180]. У цьому контексті кіберпростір розглядається як один із ключових напрямів сучасної безпеки, де формується новий тип міжнародної взаємодії.

У підсумку міжнародні механізми реагування на гібридні загрози формують комплексну систему, яка поєднує різні інструменти та підходи. Їх ефективність визначається здатністю адаптуватися до змін середовища, координувати дії між державами та забезпечувати баланс між стримуванням і стійкістю[181]. Важливим є також поєднання реактивних і превентивних заходів, що дозволяє не лише відповідати на вже існуючі загрози, а й знижувати ймовірність їх виникнення[182]. Такий підхід формує нову модель міжнародної безпеки, у якій гнучкість і координація виступають ключовими факторами ефективності.

[180] Ibid.
[181] Countering hybrid threats. *North Atlantic Treaty Organization*.
[182] Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. 2017.

ВИСНОВКИ

Проведене дослідження дало змогу комплексно осмислити природу гібридної агресії російської федерації, визначити її ключові характеристики, інструменти реалізації та особливості прояву у сучасному міжнародному середовищі. Узагальнення теоретичних підходів і практичного досвіду дозволяє сформулювати низку системних висновків, що відображають як сутність досліджуваного явища, так і напрями його подальшого вивчення.

Насамперед встановлено, що гібридна війна є результатом трансформації традиційних форм конфлікту, у межах яких відбувається зміщення акценту з відкритого силового протистояння на комбіновані форми впливу. Така модель базується на поєднанні військових і невійськових інструментів, що функціонують у взаємозв'язку і спрямовані на досягнення стратегічних цілей без формального переходу до повномасштабної війни. Визначальною рисою цієї форми протистояння є розмитість меж між війною і миром, що ускладнює її своєчасне розпізнавання та знижує ефективність традиційних механізмів реагування.

Дослідження інструментального виміру гібридної агресії показало, що вона реалізується через інтегровану систему впливу, де кожен компонент виконує окрему функцію, водночас підсилюючи інші. Інформаційний компонент формує необхідні інтерпретації подій і впливає на суспільну свідомість, створюючи сприятливі умови для подальших дій. Економічні інструменти забезпечують формування залежностей, які можуть використовуватися як важелі політичного тиску. Кібернетичний вплив спрямований на дестабілізацію функціонування інфраструктури та інформаційних систем, а військовий компонент виконує роль фіксації результатів і зміни балансу сил. Встановлено, що ефективність гібридної стратегії визначається не окремими інструментами, а їх узгодженим і синхронізованим застосуванням.

Особливу увагу у роботі приділено ролі України як ключового об’єкта гібридної агресії. З’ясовано, що український кейс відображає повний спектр застосування гібридних інструментів, що дозволяє розглядати його як модель сучасного конфлікту. Вплив здійснюється поступово, через зміну внутрішнього середовища держави, що включає політичні процеси, економічні параметри та інформаційний простір. Такий підхід забезпечує довготривалий ефект і дозволяє досягати стратегічних результатів без різкої ескалації. Україна у цьому процесі виступає не лише об’єктом впливу, але й важливим елементом ширшої геополітичної стратегії.

Аналіз практики застосування гібридних інструментів у міжнародному середовищі показав їх універсальність і здатність адаптуватися до різних умов. Встановлено, що такі інструменти використовуються у різних регіонах, але зберігають спільну логіку реалізації, яка передбачає поєднання інформаційних, економічних, політичних і силових механізмів. Це свідчить про формування нової моделі міжнародних відносин, у якій межі між внутрішніми і зовнішніми процесами стають менш визначеними. Гібридний вплив спрямовується на зміну внутрішніх процесів держав, що дозволяє досягати результатів без прямого втручання.

Важливим результатом дослідження є встановлення ролі адаптивності як ключової характеристики гібридної стратегії. Зміна інструментів і методів впливу залежно від реакції держави-цілі та міжнародної спільноти дозволяє зберігати ефективність впливу навіть за умов протидії. Це ускладнює розробку універсальних механізмів реагування і вимагає постійного вдосконалення підходів до забезпечення безпеки.

У ході дослідження також з’ясовано, що міжнародні механізми реагування на гібридні загрози перебувають у процесі трансформації. Традиційні підходи, орієнтовані на військову відповідь, доповнюються комплексними моделями, які включають політичні, економічні, інформаційні та кібернетичні інструменти.

Ефективність таких механізмів залежить від рівня координації між державами, здатності до швидкого обміну інформацією та розвитку систем колективної безпеки. Водночас встановлено, що значна частина гібридних дій залишається поза межами чітких правових визначень, що ускладнює їх кваліфікацію та застосування відповідних заходів.

Окремо варто відзначити зростання ролі превентивних механізмів протидії. Зміщення акценту з реагування на попередження передбачає підвищення стійкості держав до зовнішнього впливу, зниження вразливостей та формування ефективних систем захисту. Це включає розвиток інформаційної безпеки, зміцнення економічної незалежності, удосконалення кіберзахисту та підвищення ефективності державного управління.

Узагальнюючи результати дослідження, можна стверджувати, що гібридна агресія російської федерації є складним і динамічним явищем, яке поєднує різні інструменти впливу і реалізується через зміну середовища функціонування держави-цілі. Її ефективність зумовлена здатністю діяти приховано, адаптуватися до змін і використовувати слабкі місця у системі міжнародної безпеки. Це створює серйозні виклики для сучасної системи міжнародних відносин і вимагає формування нових підходів до забезпечення безпеки.

Отримані результати підтверджують необхідність подальшого розвитку теоретичних і практичних підходів до аналізу гібридних конфліктів. Перспективи дослідження пов’язані з поглибленням вивчення механізмів взаємодії різних інструментів впливу, удосконаленням методів їх ідентифікації та розробкою ефективних стратегій протидії. Це має важливе значення як для наукового осмислення сучасних конфліктів, так і для практики забезпечення національної та міжнародної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анатомія російсько-українського конфлікту (2014–2022 рр.) в епоху гібридних війн. *Національна бібліотека України імені В. І. Вернадського.* URL: http://www.nbuv.gov.ua/node/5937 (дата звернення: 21.04.2026).
2. Гібридна війна Росії проти України після Революції гідності / за ред. М. Дорошка, В. Балюка. Київ: Ніка-Центр, 2018. URL: https://www.hups.mil.gov.ua/assets/uploads/library/vitchizna/gibridna-viyna-rosii-proti-ukraini.pdf (дата звернення: 21.04.2026).
3. Крищенко А. В., Іващенко С. М., Ремез В. В. Гібридна війна як новий вимір сучасних конфліктів. *Питання психології.* 2025. № 4 (86). С. 85–95. DOI: https://doi.org/10.33099/2617-6858-25-86-4-85-95.
4. Смола Л. Інформаційно-психологічний складник «гібридної» війни. *Національна безпека і оборона*. 2016. URL: https://razumkov.org.ua/uploads/journal/ukr/NSD167-168_2016_ukr.pdf (дата звернення: 21.04.2026).
5. Хударковський К. І., Сідченко С. О., Залкін С. В., Белімов В. В., Ревін О. В., Шигімага Н. В. Особливості гібридної війни Російської Федерації проти України. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. № 1 (83). С. 98–105. DOI: https://doi.org/10.30748/zhups.2025.83.12.
6. Allegri R. The Russian resort to hybrid warfare: From Peter the Great to Gerasimov. *Small Wars & Insurgencies*. 2026. Vol. 37, No. 1. P. 135–168. DOI: https://doi.org/10.1080/09592318.2025.2560478.
7. Arifin J. D. Unraveling current trends in hybrid warfare 3.0: A literature study on modern non-conventional threats. *Proceedings of the International Conference on Economics, Technology, Management, Accounting, Education (ICETEA)*. 2025. Vol. 1.

URL: https://conference.unita.ac.id/index.php/icetea/article/view/378 (date of access: 11.04.2026).

8. Bachmann S.-D. D., Gunneriusson H. Russia's hybrid warfare in the East: Using the information sphere as integral to hybrid warfare. *Georgetown Journal of International Affairs*. 2015. Vol. 16 (Supplement: International Engagement on Cyber V). P. 198–211.
9. Baker M. S., Baker J., Burkle F. M. Russia's hybrid warfare in Ukraine threatens both healthcare & health protections provided by international law. *Annals of Global Health.* 2023. Vol. 89, No. 1. Article 3. DOI: https://doi.org/10.5334/aogh.4022.
10. Berger-Hrynova T. Scientific research as a weapon in Russia's hybrid war in Europe: An example of the Joint Institute for Nuclear Research in Dubna, Russia. *arXiv*. 2026. URL: https://doi.org/10.48550/arXiv.2603.21896 (date of access: 11.04.2026).
11. Berthelsen E. Hybrid times: War and peace in military innovation studies. *Journal of Strategic Studies.* 2025. DOI: https://doi.org/10.1080/01402390.2025.2512238.
12. Blasco Robledo F. J. La guerra híbrida. *Sociedad Argentina de Estudios Estratégicos y Globales*. 2022. URL: https://saeeg.org/index.php/2022/09/12/la-guerra-hibrida/ (date of access: 21.04.2026).
13. Brown J. An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state. *Journal of Global Faultlines.* 2018. Vol. 5, No. 1-2. P. 58-82. DOI: https://doi.org/10.13169/jglobfaul.5.1-2.0058.
14. Clas A. Commanding in Multi-Domain Formations. *U.S. Army*. 2018. URL: https://www.army.mil/article/201352/commanding_in_multi_domain_formations (date of access 21.04.2026).
15. Countering hybrid threats. *North Atlantic Treaty Organization*. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats/ (date of access: 03.04.2026).
16. Crowther G. A. NATO and hybrid warfare: Seeking a concept to describe the challenge from Russia. URL:

https://www.researchgate.net/publication/349496199_NATO_and_hybrid_warfare_Seeking_a_concept_to_describe_the_challenge_from_Russia (date of access: 13.04.2026).

17. Eggen K.A. A strategy for the weak: The role of information confrontation in Russia's grand strategy. *Defence Studies*. 2025. DOI: https://doi.org/10.1080/14702436.2025.2561639.
18. EUvsDisinfo. *European External Action Service*. URL: https://euvsdisinfo.eu/ (date of access: 11.04.2026).
19. Ferguson M. P. Misinformed: Implications of Foreign Influence on the Information Environment that Launched Operation Iraqi Freedom. *Marine Corps University Press*. 2023. URL: https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/Misinformed/ (date of access: 21.04.2026).
20. Geri M. Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. *Journal of Strategic Security*. 2024. Vol. 17, No. 3. Article 2. URL: https://digitalcommons.usf.edu/jss/vol17/iss3/2/ (date of access: 14.04.2026).
21. German Council on Foreign Relations. URL: https://dgap.org/en (date of access: 13.04.2026).
22. Giles K. The next phase of Russian information warfare. *Riga: NATO Strategic Communications Centre of Excellence*. 2016. URL: https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176 (date of access: 14.04.2026).
23. Göransson M. B. Russia's thinking on new wars and its full-scale invasion of Ukraine. *Defence Studies*. 2024. Vol. 24, No. 3. P. 449–471. DOI: https://doi.org/10.1080/14702436.2024.2365214.

24. Hladchenko M. Implications of Russia's full-scale invasion of Ukraine for the international mobility of Ukrainian scholars. *arXiv.* 2026. URL: https://doi.org/10.48550/arXiv.2602.06510 (date of access: 11.04.2026).
25. Hoffman F., Neumeyer M., Jensen B. The future of hybrid warfare. URL: https://www.csis.org/analysis/future-hybrid-warfare (date of access: 13.04.2026).
26. Hybrid CoE. Hybrid CoE launches a playbook on hybrid deterrence. *Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats*. 2020. URL: https://www.hybridcoe.fi/news/hybrid-coe-launches-a-playbook-on-hybrid-deterrence/ (date of access: 21.04.2026).
27. Kaldor M. In defence of new wars. *Stability: International Journal of Security and Development*. 2013. Vol. 2, No. 1. Article 4. DOI: https://doi.org/10.5334/sta.at.
28. Kapsokoli E. Weaponizing cyberspace: The Russia-Ukrainian war. *Security Science Journal.* 2025. Vol. 6, No. 2. DOI: https://doi.org/10.37458/ssj.6.2.3.
29. Laber M., Klimek P., Bruckner M., Yang L., Thurner S. Shock propagation from the Russia-Ukraine conflict on international multilayer food production network determines global food availability. *arXiv*. 2022. URL: https://doi.org/10.48550/arXiv.2210.01846 (date of access: 20.04.2026).
30. Mahda Y. The start of RF's hybrid aggression against Ukraine: The point of bifurcation. *European Political and Law Discourse*. 2018. Vol. 5, No. 2. P. 41–47. URL: https://eppd13.cz/wp-content/uploads/2018/2018-5-2/07.pdf (date of access: 21.04.2026).
31. Mahmood N., Malik A. I., Mirza M. N. Analysing hybrid warfare and information/cyber operations. *Webology*. 2021. Vol. 18, No. 4. P. 1720–1731. URL: https://shs.hal.science/halshs-03788137/document (date of access: 21.04.2026).
32. Marchandise C., McKee M. Europe in a hybrid war: Health security as strategic defence. *European Journal of Public Health.* 2025. Vol. 35, No. 6. P. 1074–1075. DOI: https://doi.org/10.1093/eurpub/ckaf210.

33. McWilliams A., Legnér M. Threat assessments and heritage in the age of hybrid warfare. *International Journal of Heritage Studies*. 2024. Vol. 30, No. 12. P. 1379–1392. DOI: https://doi.org/10.1080/13527258.2024.2393610.

34. Monaghan S. Countering Hybrid Warfare: So What for the Joint Force? *National Defense University Press.* 2019. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979787/countering-hybrid-warfare-so-what-for-the-joint-force/ (date of access: 21.04.2026).

35. Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2023. Vol. 8, No. 2. P. 192–206. DOI: https://doi.org/10.1017/eis.2022.19.

36. Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it. *Santa Monica: RAND Corporation.* 2016. URL: https://www.rand.org/pubs/perspectives/PE198.html (date of access: 19.04.2026).

37. Polyakova A., Boulègue M. The evolution of Russian hybrid warfare: Conclusion. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-conclusion/ (date of access: 13.04.2026).

38. Reuters. URL: https://www.reuters.com/ (date of access: 18.04.2026).

39. Rizalah T., Khaerudin K., Yanto S. Examining the conflict of Ukraine and Russia in terms of military strength, strategy and risks. *International Journal of Humanities Education and Social Sciences.* 2025. Vol. 5, No. 1. P. 184–189. DOI: https://doi.org/10.55227/ijhess.v5i1.1254.

40. Romandash A. Hybrid warfare: Ukraine, Russia and Western lessons. *Policy Brief No. 209. Waterloo: Centre for International Governance Innovation. 2025*. URL: https://www.cigionline.org/static/documents/PB_no.209.pdf (date of access: 20.04.2026).

41. Splidsboel Hansen F. Russian hybrid warfare: A study of disinformation. *DIIS Report No. 2017:06. Copenhagen: Danish Institute for International Studies.* 2017. URL:

https://www.econstor.eu/bitstream/10419/197644/1/896622703.pdf (date of access: 21.04.2026).

42. Strategic Studies Institute. *U.S. Army War College*. URL: https://ssi.armywarcollege.edu/ (date of access: 13.04.2026).
43. The 2022 Code of Practice on Disinformation. *European Commission*. 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (date of access: 21.04.2026).
44. The Defence Horizon Journal. URL: https://tdhj.org/ (date of access: 13.04.2026).
45. Topor L., Tabachnik A. Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies.* 2021. Vol. 12, No. 1. P. 112–127. DOI: https://doi.org/10.21140/mcuj.20211201005.
46. Voyger M. What is "hybrid warfare," really? URL: https://cepa.org/article/what-is-hybrid-warfare-really/ (date of access: 13.04.2026).