

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

МОНОГРАФІЯ

Інформаційна війна:
поняття, зміст, види та засоби

Вплив інформаційних війн
на економіко-політичні, соціальні
процеси у світі та окремій країні

Інформаційна боротьба:
особливості та структурні елементи

Культура, наука, право, освіта
на захисті людини від деструктивного
впливу інформаційної зброї

Спеціальні
інформаційно-психологічні
операції: сутність,
етапи, методи проведення

Інформаційна безпека
та контрпропаганда
в умовах російсько-
української війни

АНАЛІТИЧНИЙ ЦЕНТР СУЧАСНОЇ ГУМАНІТАРИСТИКИ

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

Монографія

Харків
«Право»
2026

Авторський колектив:

Л. М. Алексеєнко, доктор економічних наук, професор; *О. М. Іванченко*, доктор юридичних наук, доцент; *У. В. Ільницька*, кандидат політичних наук, доцент; *О. В. Квасниця*, кандидат економічних наук, доцент; *Н. О. Коннова*, кандидат філософських наук, доцент; *О. С. Копитова*, доктор юридичних наук, старший дослідник; *О. В. Кравченко*, доктор історичних наук, доцент; *К. В. Настояща*, доктор соціологічних наук, доцент; *М. П. Требін*, доктор філософських наук, професор; *Н. В. Федіна*, кандидат юридичних наук, доцент; *Т. О. Чернишова*, кандидат філологічних наук, доцент; *Л. В. Чупрій*, доктор політичних наук, професор

Рецензенти:

Г. М. Куц – доктор політичних наук, професор (Харківський національний педагогічний університет імені Г. С. Сковороди);

В. І. Палагута – доктор філософських наук, професор (Національний технічний університет «Дніпровська політехніка»);

І. В. Процюк – доктор юридичних наук, професор (Національний юридичний університет імені Ярослава Мудрого)

*Рекомендовано до видання вченою радою
ГО «Аналітичний центр сучасної гуманітаристики»
(протокол № 4 від 17 липня 2026 р.)*

Інформаційна війна та її вплив на суспільство : монографія /
I-74 [Л. М. Алексеєнко, О. М. Іванченко, У. В. Ільницька та ін.] ; Аналіт.
центр сучас. гуманітаристики. – Харків : Право, 2026. – 506 с. – DOI:
<https://doi.org/10.31359/9786178852085>.

ISBN 978-617-8852-08-5

Колективну монографію присвячено дослідженню теоретичних, методологічних і практичних основ феномену інформаційної війни, розкрито її поняття, сутність, зміст. Особливу увагу приділено розумінню сутності та специфіки когнітивної війни як концепту сучасного гуманітарного протистояння. Проаналізовано види та засоби ведення інформаційної війни, особливості та структурні елементи інформаційної боротьби, сутність, етапи, методи проведення спеціальних інформаційно-психологічних операцій. Розглянуто вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремі країни. Особливу увагу приділено інформаційній безпеці, контрпропаганді, захисту людини від деструктивного впливу інформаційної зброї в умовах російсько-української війни.

УДК 14+316+32+33+34+35

© Алексеєнко Л. М., Іванченко О. М.,
Ільницька У. В. та ін., 2026

© ГО «Аналітичний центр сучасної
гуманітаристики», 2026

© ТОВ «Видавничий дім «Право», 2026

ISBN 978-617-8852-08-5

Зміст

Розділ 1

Інформаційна війна: поняття, зміст, види та засоби

1.1. Інформаційна війна в турбулентному світі: теоретико-методологічні засади (Требін М. П., Коннова Н. О.).....	5
Список використаних джерел.	41
1.2. Трансформація змісту інформаційної боротьби: генезис, форми та методи (Требін М. П., Коннова Н. О.)..	47
Список використаних джерел.	79
1.3. Сутність та специфіка когнітивної війни як концепту сучасного гуманітарного протиборства (Требін М. П., Коннова Н. О.)	84
Список використаних джерел.	120
1.4. Феномен когнітивної війни в доктринальному дискурсі НАТО (Чернишова Т. О.).....	124
Список використаних джерел.	154

Розділ 2

Спеціальні інформаційно-психологічні операції: сутність, етапи, методи проведення

2.1. Теоретико-методологічні засади та сутність спеціальних інформаційно-психологічних операцій (ІПсО) у контурі гібридних конфліктів (Требін М. П., Коннова Н. О.).....	158
Список використаних джерел.	191
2.2. Архітектура, етапи проєктування та методи реалізації сучасних ІПсО в цифровому медіасередовищі (Требін М. П., Коннова Н. О.).....	195
Список використаних джерел.	230
2.3. Північнокорейська тематика в спеціальних інформаційно-психологічних операціях російсько-української війни (Чупрій Л. В., Настояща К. В.).....	234
Список використаних джерел.	247

Розділ 3

Вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремі країни

3.1. Інформаційна війна як фактор трансформації права (Копитова О. С.)..	250
Список використаних джерел.	292

3.2. Інформаційно-безпекові імперативи цифрових і фондових інновацій у сфері публічного управління, фінансів, банків і страхування: міжнародні та національні бізнес-комунікації (Алексєєнко Л. М.)	297
Список використаних джерел.	323
3.3. Інформаційно-комунікаційні механізми політики згуртованості економічного розвитку територіально-господарських систем: пріоритети поведінкових фінансів та масштабування фінансової грамотності в умовах євроінтеграції (Квасниця О. В.)	334
Список використаних джерел.	366

Розділ 4

Інформаційна безпека та контрпропаганда в умовах російсько-української війни

4.1. Культура, наука, право, освіта на захисті людини від деструктивного впливу інформаційної зброї (Іванченко О. М.)	369
Список використаних джерел.	407
4.2. Стратегічні комунікації як механізм формування системи інформаційної безпеки та протидії інформаційним викликам і загрозам (Ільницька У. В.)	411
Список використаних джерел.	432
4.3. Особливості забезпечення інформаційної безпеки органами державного адміністрування в умовах правового режиму воєнного стану (Федіна Н. В.)	438
Список використаних джерел.	469
4.4. Інформаційна безпека та контрпропаганда в умовах російсько-української війни: стратегії та досвід України і Польщі (Кравченко О. В.)	474
Список використаних джерел.	498
Авторський колектив.	503

Розділ 1

ІНФОРМАЦІЙНА ВІЙНА: ПОНЯТТЯ, ЗМІСТ, ВИДИ ТА ЗАСОБИ

1.1. Інформаційна війна в турбулентному світі: теоретико- методологічні засади

Требін Михайло Петрович

доктор філософських наук, професор

професор кафедри міжнародних відносин і політичної філософії

Харківський національний економічний університет імені Семена Кузнеця

Коннова Ніна Олексіївна

кандидат філософських наук, доцент

доцент кафедри міжнародних відносин і політичної філософії

Харківський національний економічний університет імені Семена Кузнеця

Сучасна цивілізація вступила в якісно новий етап свого існування, який має багато назв, але головне, що притаманне цьому етапу, – це велике значення інформації в житті сучасного суспільства. Інформація сьогодні – це не просто якісь відомості про окремі речі, події, явища тощо. Інформація сьогодні – засіб впливу на людину, суспільство, державу, світове співтовариство, вона стає міцною зброєю в сучасному світі¹. Недарма кажуть: «Той, хто володіє інформацією, – володіє світом», а раз так, то і таке явище, як інформаційні війни, стає реальністю сьогодення.

Проблемам вивчення феномену «інформаційна війна» сучасні дослідники приділяють чимало уваги. Певні аспекти феномену інформаційних війн, механізмів їх зародження та розвитку вивчали такі

¹ Див.: Требін М. П. Інформація як зброя у «гібридній» війні. *Політичні та правові дисонанси в сучасних українських реаліях*: зб. матеріалів XXX Харківських політологічних читань (м. Харків, 16 червня 2017 р.). Харків: «Право», 2017. С. 70–75.

відомі західні науковці, як М. Амбіндер, К. Вайт, Дж. Велберн, Дж. Генріхсен, К. Голинська, Ф. Гранеллі, М. Грізе, А. Демус, Д. Джаммона, Б. Дженсен, Д. Зайдл, М. Кеппе, А. Кріг, С. Куомо, Б. Ліллі, П. Маллік, К. Пол, К. Розаті, Дж. Форест, О. Фрідман, М. Чаппл, М. Швілле, Ю. Шох та ін.¹ Серед українських фахівців назвемо Є. Борисенко,

¹ Див.: Chapple M., Seidl D. *Cyberwarfare: information operations in a connected world*. 2nd ed. Burlington, Massachusetts: Jones & Bartlett Learning, 2023. xxiii, 428 p.; Demus A. *Operationalizing U. S. Air Force information warfare*. Santa Monica, Calif.: RAND Project Air Force, 2024. xiii, 156 p.; Forest J. J. F. *Digital influence mercenaries: profits and power through information warfare*. Annapolis, Maryland: Naval Institute Press, 2022. xiii, 245 p.; Giammona D. J., Anderson T. *The military guide to disarming deception: battlefield tactics to expose the enemy's lies and triumph in truth*. Minneapolis, Minnesota: Chosen Books, 2022. 233 p.; Grisé M., Demus A., Shokh Y., Kepe M., Welburn J. W., Holynska K. *Rivalry in the information sphere: Russian conceptions of information confrontation*. Santa Monica, CA: RAND Corporation, 2022. xvi, 138 p.; Info ops: from World War I to the Twitter era / edited by Ofer Fridman, Vitaly Kabernik and Francesca Granelli. Boulder, Colorado: Lynne Rienner Publishers, Inc, 2022. vii, 287 p.; Jensen B. M., Whyte C., Cuomo S. *Information in war: military innovation, battle networks, and the future of artificial intelligence*. Washington, DC: Georgetown University Press, 2022. xiii, 252 p.; Krieg A. *Subversion : the strategic weaponization of narratives*. Washington, D. C.: Georgetown University Press, 2023. x, 241 p.; Lilly B. *Russian information warfare: assault on democracies in the cyber wild west*. Annapolis, Maryland: Naval Institute Press, 2022. xviii, 291 p.; Mallick P. K. *Mind wars: the new battlefield of information warfare / foreword by Lt Gen NS Raja Subramani*. New Delhi, India: Pentagon Press LLP, 2025. xxii, 277 p.; National security, journalism, and law in an age of information warfare / Marc Ambinder, Jennifer R. Henrichsen, Connie Rosati (Eds.). New York: Oxford University Press, 2024. xxxii, 329 p.; Olejnik L. *Propaganda: from disinformation and influence to operations and information warfare*. Boca Raton, FL: CRC Press, 2025. xvi, 268 p.; Paul C., Schwill M., Webber S., Demus A., Van Hegewald E. *Organizing for information warfare at the geographic combatant commands: lessons from the United States Central Command joint effects process*. Santa Monica, CA: RAND National Defense Research Institute, 2024. xi, 77 p.; Schwill M., Welch J., Fisher S., Whittaker T. M., Paul C. *Handbook for tactical operations in the information environment*. Santa Monica, Calif.: RAND Corporation, 2021. xi, 85 p.; Seib P. *Information at war: journalism, disinformation, and modern warfare*. Cambridge, UK: Medford, MA: Polity Press, 2021. x, 226 p.; Singh S. S., Venkatanarayanan A. *The art of conjuring alternate realities: how information warfare shapes your world*. Noida, Uttar Pradesh, India: HarperCollins Publishers India, 2021. xi, 283 p.; Sloss D. L. *Tyrants on Twitter: protecting democracies from information warfare*. Stanford, California: Stanford University Press, 2022. xvii, 330 p.; *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* / Alan D. Campen, contributing editor. Fairfax, Va.: AFCEA International Press, 1992. xxi, 195 p.; *The world information war: western resilience, campaigning and cognitive effects / edited by Timothy Clack and Robert Johnson*. Abingdon, Oxon; New York, NY: Routledge, 2021. xv, 300 p. та ін.

І. Вівчар, О. Данильяна, О. Дзьобаня, І. Жаровську, Д. Короткова, Я. Короход, О. Крет, О. Кузя, О. Кундеус, Н. Ортинську, О. Панфілова, Г. Петришин, М. Поправку, І. Пронозу, Г. Почепцова, Л. Стрільчук, П. Ткачука, К. Федотенко, І. Фещенка, М. Фролову, А. Худолія, С. Цимбала, О. Яцюк та ін.¹ Але залишаються питання, на які й досі не зна-

¹ Див.: Борисенко Є. Інформаційна війна крізь призму комунікативної теорії: спроба аналізу. *Філософська думка*. 2023. № 4. С. 21–38; Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2022. № 3. С. 11–29; Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка»*. Серія : *Юридичні науки*. 2020. Т. 7, № 2. С. 56–61; Інформаційна війна і національна безпека: [колект.] монографія / П. П. Ткачук [та ін.]. Львів : Акад. сухопут. військ, 2015. 264 с.; Короход Я. Інформаційна війна як основна загроза інформаційній безпеці держави: поняття, форми і методи ведення. *Evropský politický a právní diskurz*. 2017. Sv. 4, Vyd. 3. С. 222–227; Кундеус О. М., Вівчар І. В., Крет О. В. Інформаційна війна: сутність та особливості (кінець ХХ – початок ХХІ століття). *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2024. № 3. С. 212–223; Петришин Г. Інформаційна війна Росії проти України: еволюція основних засобів, методів та динаміка наративів. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. Вип. 1. С. 117–128; Поправка М. О. Інформаційна війна в контексті гібридного конфлікту. *Міжнародні та політичні дослідження*. 2024. Вип. 38. С. 267–274; Проноза І. І., Цимбал С. Ю. Інформаційна війна в сучасних інтернет-комунікаціях: українсько-європейські практики та виклики. *Політикус*. 2025. Вип. 3. С. 97–102; Стрільчук Л. Інформаційна війна як складова сучасних гібридних воєн (на прикладі Грузії та України). *Літопис Волині*. 2023. Чис. 28. С. 235–239; Требін М. П. Информационная война в современном мире. *Новый хозяин*. 2000. № 7. С. 26–29; Требін М. П. Феномен інформаційної війни у світі, що глобалізується. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. Серія : *Філософія, філософія права, політологія, соціологія*. 2013. № 2. С. 188–198; Требін М. П. Інформаційний континуум як поле бою. *Сучасна війна: гуманітарний аспект* : збірник матеріалів VIII Міжнародної наукової конференції Харківського національного університету Повітряних Сил імені Івана Кожедуба, 24–25 травня 2024 р. Харків: ХНУПС ім. І. Кожедуба, 2024. С. 30–36; Федотенко К. А. «Інформаційна війна» та «інформаційний фронт»: наукове осмислення понять. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2023. № 3. С. 157–170; Фещенко І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021. Т. 13, № 1. С. 96–103; Фролова М. Е., Козел В. М. Інформаційна війна в цифрову епоху: виклики та загрози для студентської аудиторії. *Вчені записки Таврійського національного університету імені В. І. Вернадського*.

йдено відповіді, насамперед ідеться про сутнісне осмислення цього явища. Інформаційна війна в турбулентному світі має аналізуватися з обґрунтуванням законів, закономірностей і принципів організації та ведення інформаційної війни як соціокультурного феномену.

Першим автором, який ще 1976 р. застосував термін «інформаційна війна» і сформулював основні положення її концепції, вважається американський учений Томас Рона¹. Сам термін «інформаційна війна» став широко застосовуватися американськими військовими фахівцями після завершення операції «Буря в пустелі», де інформаційна зброя показала свою високу ефективність і поступово набула популярності.

У грудні 1992 року Міністерство оборони США (Пентагон) затвердило цілком таємну директиву DoDD TS-3600.1 «Information Warfare»², у якій було окреслено ключові завдання з підготовки збройних сил до протиборства в інформаційній сфері. Згідно з документом, інформаційна війна визначалася як дії, що вживаються для досягнення інформаційної переваги на підтримку національної воєнної стратегії шляхом впливу на інформацію та інформаційні системи противника з одночасним захистом власної інформації та інформаційних систем. У межах цієї концепції інформаційна війна розглядалася

Серія : Психологія. 2025. Т. 36(75), №2. С. 126–132; Худолій А. Інформаційна війна 2014–2022 рр.: [монографія] / Нац. ун-т «Остроз. акад.», Ф-т романо-герман. мов, Каф. англ. філології. Острог: Вид-во Нац. ун-ту «Острозька академія», 2022. 207 с.; Яцюк О. С. Інформаційна війна як складова частина гібридної війни: метод. посіб. / Центр перепідгот. та підвищ. кваліфікації працівників орг. держ. влади, орг. місц. самоврядування, держ. підприємств, установ і орг. Вінниц. обл. Вінниця : Нілан, 2016. 51 с.; Plazova T., Kuz O., Konnova N., Korotkov D., Galushchenko O. Information Warfare as an Instrument of Geopolitical Influence on Ukraine: Main Aspects and The State's Response. *International Journal of Religion*. 2024. Vol. 5, No. 2. P. 121–130. DOI: <https://doi.org/10.61707/0g2yt516> та ін.

¹ Див.: Rona T. P. *Weapon Systems and Information War*. Seattle, WA: Boeing Aerospace Company, 1976. vi, 71 p. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

² Див.: DoD Directive TS-3600.1. «Information Warfare (U)». December 21, 1992 / U. S. Department of Defense. Washington, D. C., 1992. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_02_Directive_S-3600-1.pdf

як всеосяжна, цілісна стратегія, спрямована на визначення важливості та цінності інформації в процесах командування, управління та керівництва збройними силами, а також під час реалізації національної політики. Вона використовує операційні можливості та націлена на вразливості, які неминуче виникають в умовах зростаючої інформаційної залежності. Об'єктом впливу стають інформаційні системи (зокрема, відповідні лінії передачі, центри обробки даних та людський чинник цих систем), а також інформаційні технології, що використовуються в комплексах озброєння. Стратеги Пентагону наголошували, що інформаційна війна має наступальну та оборонну складові, але починається з цільового проектування та розробки власної «архітектури» командування, управління, комунікацій, комп'ютерів та розвідки (C4I), що забезпечує особам, які приймають рішення, вирішальну інформаційну перевагу в будь-якому конфлікті.

Узагальнення концепцій інформаційного протиборства за видами збройних сил дозволило Об'єднаному комітету начальників штабів США у липні 1996 року ухвалити стратегічний документ «Загальні погляди на період до 2010 року» (Joint Vision 2010)¹. У ньому було впроваджено та нормативно закріплено фундаментальну концепцію «інформаційної переваги» (Information Superiority) як спроможності збирати, обробляти та поширювати безперервний потік інформації, одночасно заважаючи противнику робити те саме.

На прикладному рівні та в суміжних доктринальних джерелах США того періоду (зокрема, у польовому статуті FM 100–6 «Information Operations»², ухваленому 27 серпня 1996 року) підсистему інформаційного протиборства було деталізовано. До її ключових елементів американські фахівці віднесли: добування розвідувальної інформації, дезінформування, психологічні операції, фізичне руйнування інформаційних ресурсів супротивника (у тому числі з використанням електромагнітного впливу), напади (фізичні та електронні) на його інфор-

¹ Див.: Joint Vision 2010. America's Military: Preparing for Tomorrow / Joint Chiefs of Staff. Washington, D. C., 1996. 36 p. URL: <https://apps.dtic.mil/sti/tr/pdf/ADA311168.pdf>

² Див.: FM 100–6. Information Operations / Headquarters, Department of the Army. Washington, DC, 1996. vi, 155 p. URL: <https://irp.fas.org/doddir/army/fm100-6/index.html>.

маційну інфраструктуру, застосування програмно-технічного впливу (зокрема, комп'ютерних вірусів) на обчислювальні мережі та системи, несанкціоноване проникнення в інформаційні мережі, а також комплексні заходи протидії для захисту власних інформаційних ресурсів.

Поряд з тими, хто вважає правомірним застосування поняття «інформаційна війна» для характеристики воєн нового тисячоліття, є дослідники, які не поділяють таку точку зору і стверджують, що це поняття не повною мірою характеризує війну як суспільно-політичне явище. Дефініцію війни, яку вони використовують, досить ясно сформульовано як в енциклопедичних словниках радянського періоду (наприклад, у «Військовому енциклопедичному словнику» дано таке визначення війни: «Війна – суспільно-політичне явище, продовження політики насильницькими засобами»¹), так і у виданнях незалежної України, де зберігається її основний сутнісний зміст, а саме акцент на збройне насильство². Основу такого підходу було закладено німецьким військовим теоретиком та істориком, генерал-майором пруської армії Карлом фон Клаузевицем (1780–1831) у його найвідомішій книзі «Про війну»³. У поясненні (передмові) до цієї книги він писав: «Війна є не що інше, як продовження державної політики іншими засобами»⁴ і акцентував увагу саме на насильницьких засобах. «Війна, – зазначав Клаузевиц, – це акт насильства, що має на меті змусити супротивника виконати нашу волю»⁵. У заголовку одного з підрозділів своєї праці він наводить інше визначення війни: «Війна є акт людських стосунків». І далі: «Війна... належить... до галузі громадського життя. Війна є зіткнення значних інтересів, що розв'язується кровопролиттям, і тільки цим вона відрізняється від інших суспільних

¹ Военный энциклопедический словарь. Москва: Воениздат, 1983. С. 151.

² Див.: Політична енциклопедія / Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ: Парламентське видавництво, 2011. С. 105; Політологія: енциклопедичний словник / [В. М. Денисенко, Л. Я. Угрин, Н. М. Хома]; за ред. д-ра філос. наук, проф. В. П. Мельника. Львів : ЛНУ імені Івана Франка, 2014. С. 48; Соціологія права: енциклопедичний словник / Л. М. Герасіна, О. Ю. Панфілов, В. Л. Погрібна та ін.; за ред. М. П. Требіна. Харків : Право, 2020. С. 146.

³ Див.: Клаузевиц К. О войне: в 2 т. Москва: ООО «Изд-во АСТ»; Санкт-Петербург : Terra Fantastica, 2002. Т. 1. 558 с. Т. 2. 574 с.

⁴ Там само. Т. 1. С. 11.

⁵ Там само. С. 23.

конфліктів»¹. І все ж таки Клаузевіц не вважав кровопролиття і застосування збройної сили обов'язковими ознаками війни. Слушно зазначаючи, що «війна є зброєю політики; вона неминуче повинна відбивати характер останньої»², Клаузевіц припускав, що «доведеться хоч-не-хоч дійти до визнання таких воєн, які полягають тільки в погрозі супротивнику»³, і що їх ведення припускає використання тільки політичних та інших невоєнних засобів. У цьому він виявився солідарним з відомим китайським полководцем і військовим теоретиком Сунь-Цзи, який ще в VI–V ст. до н. е. писав: «Найкраща війна – розбити задуми супротивника; на наступному місці – розбити його союзи; на наступному місці – розбити його війська»⁴.

Проблема логічної коректності дефініції «інформаційна війна» залишається досить гострою і на сьогодні. У США, наприклад, існують декілька підходів до тлумачення цього явища. У доктринальній праці «Наріжні камені інформаційної війни» (1995) міністр ВПС США Шейла Відналл та начальник штабу ВПС США Рональд Фоглмен запропонували лаконічне військове визначення, згідно з яким «інформаційна війна – це будь-яка дія з метою заборони, використання, викривлення або знищення інформації противника та її функцій; захист нас самих від таких дій; та використання наших власних військових інформаційних функцій»⁵.

Водночас на загальнодержавному та міжвідомчому рівнях Міністерства оборони США було сформовано уніфікований стратегічний підхід. У перших офіційних нормативних актах Об'єднаного комітету начальників штабів США (зокрема, в директиві CJCSI 3210.01 «Joint Information Warfare Policy» від 2 січня 1996 р.) інформаційна війна тлумачилася як «дії, спрямовані на досягнення інформаційної переваги на підтримку національної воєнної стратегії шляхом впливу

¹ Клаузевиц К. О войне: в 2 т. Т. 1. С. 163.

² Там само. Т. 2. С. 438.

³ Там само. С. 429.

⁴ Сунь-Цзы. У-Цзы. Трактаты о военном искусстве / пер. с кит., предисл. и коммент. Н. И. Конрада. Москва: ООО «Изд-во АСТ» ; Санкт-Петербург: Terra Fantastica, 2002. С. 40.

⁵ Cornerstones of Information Warfare / Department of the Air Force ; [S. E. Widnall, R. R. Fogleman]. Washington, D. C., 1995. P. 3.

на інформацію та інформаційні системи противника з одночасним посиленням ефективності використання і захисту власної інформації та інформаційних систем»¹. Таким чином, це визначення відображало спільну (міжвидову) доктрину Пентагону, на відміну від суто видового (авіаційного) підходу Ш. Відналл та Р. Фоглмена.

Аналіз доктринальних трансформацій свідчить, що розуміння сутності інформаційного протиборства наприкінці ХХ століття та в сучасний період кардинально відрізняється. Північноатлантичний альянс повністю відійшов від концепції суто технічної «інформаційної війни» (Information Warfare), зосередженої на радіоелектронній боротьбі чи захисті систем зв'язку. Замість цього НАТО перейшло до комплексного концепту Стратегічних комунікацій (StratCom), де головним полем битви стає когнітивний простір.

Цей концептуальний зсув було започатковано у Військовій концепції стратегічних комунікацій НАТО (MCM-0085-2010²) та остаточно закріплено у чинній Політиці стратегічних комунікацій НАТО та Стратегічній концепції НАТО. Відповідно до цих документів, StratCom визначається як інтегроване й скоординоване використання всіх комунікаційних можливостей та інформаційних спроможностей Альянсу (включаючи публічну дипломатію, зв'язки з громадськістю, військові зв'язки з медіа, інформаційні та психологічні операції) задля впливу на сприйняття, ставлення та поведінку цільових аудиторій.

Узагальнюючи еволюцію доктринальних підходів провідних країн світу та зважаючи на всеохопний характер сучасних соціокомунікаційних процесів, ми пропонуємо трактувати інформаційну війну як складне соціальне явище. У такому контексті вона є однією з деструктивних форм розв'язання наявних інтерсуб'єктивних суперечностей в усіх сферах суспільного життя – між державами, націями, народами чи соціальними групами, – що реалізується інструментами та засобами інформаційного насильства. Таке розуміння дозволяє

¹ CJCSI 3210.01. Joint Information Warfare Policy / Chairman of the Joint Chiefs of Staff Instruction. Washington, D. C. : Joint Chiefs of Staff, 1996. URL: <https://irp.fas.org/doddir/army/fm100-6/ref.htm>.

² Див.: MCM-0085-2010. Military Concept for NATO Strategic Communications / Military Committee Memorandum. Brussels : NATO Headquarters, 2010. 13 p. URL: <https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf>.

вийти за межі вузькотехнічного або виключно мілітарного дискурсу й розглядати інформаційну війну як тривалий соціокультурний процес, спрямований на деформацію смислового поля, цінностей та ідентичності суспільства – об'єкта впливу.

Доцільність інтерпретації інформаційної війни через призму соціального явища та інформаційного насильства підтверджується декількома деструктивними наслідками для ментальної безпеки та життєвості суспільства.

1. Когнітивна деформація індивідуальної та масової свідомості. Інформаційне насильство спрямоване не на руйнування технічної інфраструктури, а на примусову зміну базисних елементів психіки людини. Через механізми семантичного маніпулювання, поширення сконструйованих симулякрів та штучних наративів відбувається підірив ментальної безпеки. Унаслідок цього об'єкт впливу втрачає здатність до об'єктивного сприйняття дійсності, а його мислення та поведінка починають підпорядковуватися інтересам агресора.

2. Ерозія соціального капіталу та інституційної довіри. Ця форма насильства штучно актуалізує, консервує та поглиблює наявні в суспільстві лінії розлому, зокрема етнічні, релігійні, мовні, майнові чи політичні. Шляхом цілеспрямованої радикалізації суспільного дискурсу руйнується горизонтальна солідарність між соціальними групами та нищиться вертикальна довіра до базових державних інституцій, що призводить до системного внутрішнього розколу й паралічу суспільної системи без застосування військової сили.

3. Атака на історичну пам'ять та соціокультурну ідентичність. Інформаційне насильство завжди має ціннісно-символічний характер. Об'єктом експансії стають національні міфи, культурні коди, історична пам'ять та мовне середовище. Через агресивне нав'язування деструктивних світоглядних конструктів відбувається ментальна дезорієнтація суспільства, що позбавляє його внутрішніх орієнтирів та волі до опору.

Таким чином, інформаційне насильство є не просто формою передачі даних, а латентним інструментом соціальної інженерії, який трансформує ментальний простір соціуму, роблячи його вразливим до зовнішнього управління.

Отже, дослідження генезису понятійно-категоріального апарату інформаційного протиборства дало змогу простежити його тривалу еволюцію від вузькоспеціалізованих військово-технічних концептів до всеохопних стратегій безпеки. Аналіз першоджерел унаочнив, що початковий етап інституціоналізації цієї сфери у США (зокрема, Директива Пентагону DoDD TS-3600.1 1992 року та видова доктрина ВПС «Cornerstones of Information Warfare» 1995 року) спирався на мілітарне розуміння інформаційної війни (Information Warfare) як інструменту впливу на інформаційні системи ворога за одночасного захисту власних технологічних ресурсів та архітектури С4І.

Встановлено, що на межі XX–XXI століть під егідою Об'єднаного комітету начальників штабів США (документ «Joint Vision 2010») та військових статутів (зокрема, FM 100–6 «Information Operations») відбувся якісний перехід до концепцій «інформаційної переваги» та «інформаційних операцій». Цей вектор отримав свій логічний розвиток у доктринах Північноатлантичного альянсу 2010–2020-х років (насамперед у Військовій концепції стратегічних комунікацій НАТО MCM-0085-2010). Сучасний підхід НАТО демонструє повну відмову від ізолюваного сприйняття інформаційної війни на користь людиноцентричної системи Стратегічних комунікацій (StratCom), яка інтегрує політичні, дипломатичні та військові спроможності задля контролю над наративами й когнітивним простором.

На основі критичного переосмислення західного доктринального досвіду та врахування специфіки сучасних гібридних загроз обґрунтовано авторське бачення досліджуваного феномену. Запропоновано трактувати інформаційну війну як складне соціальне явище, що виходить далеко за межі суто армійських операцій і стає деструктивною формою розв'язання міждержавних, міжнаціональних та внутрішньосупільних суперечностей. Ключовим інструментом цього процесу визначено інформаційне насильство, спрямоване на когнітивну деформацію масової свідомості, ерозію соціального капіталу й руйнування соціокультурної ідентичності суспільства – об'єкта атаки. Таке соціокультурне розширення дефініції дозволяє розробляти більш ефективні, комплексні стратегії захисту ментальної та національної безпеки в умовах сучасного глобалізованого інформаційного простору.

Організація і ведення інформаційної війни базуються на відповідних законах, закономірностях і принципах. Категорії «закон» і «закономірність» тісно пов'язані і мають схожі ознаки. Закон інформаційної війни визначається як істотне, необхідне, стійко повторюване відношення, що характеризує впорядкованість устрою і функціонування, тенденції зміни і розвитку тих чи інших явищ у ході її ведення. Під закономірністю інформаційної війни розуміється підпорядкованість закону або вказівка на те, що основу пізнання будь-якого її явища становлять один або декілька законів. Поняття «закономірність» є доцільнішим у тих випадках, коли зв'язки, відносини інформаційної війни, що повторюються, недостатньо виражені кількісно. Особливістю законів і закономірностей інформаційної війни є те, що, на відміну від законів і закономірностей природи, вони виявляються лише через діяльність людей, мають очевидний відбиток суб'єктивного чинника. Закони інформаційної війни являють собою більш-менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, що існують і діють в інформаційному просторі. Їх виявлення і пізнання тільки починаються. Уже пізнані, відображені в нашій свідомості й описані, вони стануть основою для практичної діяльності щодо підготовки і ведення інформаційної війни.

До основних законів інформаційної війни можна віднести: закон визначальної ролі її політичних цілей; закони залежності її перебігу і результату від економічних, соціально-політичних, науково-технічних та військових можливостей протиборчих сторін; закон випереджального когнітивного домінування; закон асиметрії інформаційного впливу.

Провідним законом інформаційної війни є *закон визначальної ролі політичних цілей*. Інформаційне насильство ніколи не є самоціллю, воно завжди підпорядковане конкретному політичному чи геополітичному замислу суб'єкта. Аналіз інформаційного протиборства держав та інших суспільних структур свідчить, що саме політичні цілі визначають ступінь залучення сил і засобів інфосфери, масштаби та запеклість ведення інформаційної війни, вибір головного та інших противників, а також кінцеву стратегічну мету конфлікту й заходи для зміцнення союзницьких відносин усередині коаліції воюючих сторін.

При цьому форми і способи ведення інформаційної війни, її перебіг і результат обумовлюються економічними, соціально-політичними, науково-технічними та військовими можливостями протидіючих сторін. Рівень стійкості суспільства та ефективність наступальних інформаційних спроможностей прямо пропорційні загальному потенціалу держави. Економічно могутніші актори здатні розгортати та фінансувати інформаційні операції стратегічного масштабу. Ця тенденція чітко простежується на прикладі США, де фінансування інформаційно-технологічного сектору та оборонних кіберпрограм демонструє стрімке експоненціальне зростання. Якщо на етапі зародження концепцій інформаційної війни у 1980 році витрати США на інформаційні технології становили близько 8 млрд дол., а у 1996 році – понад 30 млрд дол., то в сучасний період (середина 2020-х років) сукупні державні та приватні інвестиції США суто у сфері штучного інтелекту, квантових обчислень та кібербезпеки оцінюються сотнями мільярдів доларів щорічно. Як зазначав один із провідних американських теоретиків у галузі інформаційного протидіюства Уінн Швартау¹, саме фінансово-технологічна перевага дозволяє державі не лише створювати передовий військовий інструментарій, а й утримувати монополію на глобальному ринку програмного забезпечення та цифрових платформ, конвертуючи економічний потенціал у стратегічне домінування в інфосфері.

Закон випереджального когнітивного домінування виявляється в тому, що успіх у сучасних конфліктах визначається не моментом початку кінетичних (фізичних) дій, а спроможністю суб'єкта заздалегідь сформуванню деструктивний інформаційний контекст у полі противника. Перемагає той суб'єкт, який першим нав'язує базові інтерпретаційні рамки (фрейми) та стратегічні наративи, змушуючи іншу сторону постійно перебувати в позиції виправдання чи реакції. Ефективність дії цього закону спирається на закладену Е. Гоффманом соціологічну теорію фреймінгу², а також на концепцію метафорично-

¹ Див.: Schwartz W. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994. 432 p.

² Див.: Goffman E. Frame Analysis: An Essay on the Organization of Experience. Cambridge : Harvard University Press, 1974. ix, 586 p.

го моделювання Дж. Лакоффа¹, які доводять: той, хто першим формує ментальні рамки сприйняття ситуації, повністю контролює подальшу логіку мислення об'єкта. В умовах інформаційного насильства ви-переджальне структурування смислового поля позбавляє противника можливості сформулювати власний альтернативний порядок денний, оскільки будь-які його контраргументи автоматично інтерпретуються всередині вже створеної агресором смислової матриці.

Закон асиметрії інформаційного впливу доводить, що ефективність та руйнівна сила інформаційного насильства не пропорційні фінансовим чи технічним витратам на його реалізацію. Мінімальні ресурси (наприклад, точковий когнітивний удар за допомогою алгоритмів штучного інтелекту чи вірусний дезінформаційний наратив) за умови точного потрапляння в соціальні лінії розлому здатні викликати каскадний обвал критичних державних та суспільних інститутів. Механізм дії цього закону тісно пов'язаний із положеннями синергетики про нелінійні системи та теорією «керованого хаосу» С. Манна². В умовах латентної соціальної напруги та низького рівня інституційної довіри інформаційний удар стає тригером (точкою біфуркації), який запускає некеровані процеси саморуйнування системи. Таким чином, асиметрія полягає в тому, що агресор використовує внутрішню енергію та суперечності самого суспільства-об'єкта, конвертуючи мінімальні інформаційні інвестиції у масштабну дестабілізацію національної безпеки противника.

Поряд із фундаментальними законами, праксеологічний вимір досліджуваного феномену визначається системою об'єктивних закономірностей. На основі узагальнення специфіки сучасного інформаційного простору ми вважаємо за доцільне розподілити ці закономірності на дві взаємопов'язані групи: закономірності перебігу та безпосереднього ведення інформаційної війни та закономірності розбудови й розвитку національних сил і засобів інформаційної війни.

¹ Див.: Lakoff G. Don't think of an elephant! : know your values and frame the debate : the essential guide for progressives / foreword by Howard Dean; introduction by Don Hazen. White River Junction, Vt.: Chelsea Green Pub. Co., 2004. xvi, 124 p.

² Див.: Mann S. R. Chaos Theory and Strategic Thought. *Parameters*. 1992. Vol. 22, No. 1. P. 54–68. DOI: 10.55540/0031–1723.1634.

До першої групи належать такі закономірності.

1. Залежність форм, способів та загальної ефективності інформаційного протиборства від кількісних і якісних параметрів засобів інформаційного впливу, а також від рівня підготовки та професіоналізму залученого особового складу. Універсальний характер цієї закономірності виявляється в тому, що винахід новітніх технологічних засобів та їх впровадження у військову практику неминує трансформують архітектуру бойових дій та породжують нові форми стратегічного планування. Пошук у цьому напрямку безупинно активізується. Ілюстрацією дії цієї закономірності є ретроспективний аналіз мілітаризації кіберпростору США на зламі XX і XXI століть. Так, ще в середині 1990-х років у США з 22 критичних технологій стратегічного рівня понад половину (12 напрямків) стосувалися безпосередньо інформатики. Якщо у 1995 році Міністерство оборони США використовувало близько 800 тис. обчислювальних машин, то вже на початку 2000-х років цей показник перевищив 2,5 млн комп'ютерів, об'єднаних у понад 10 000 локальних та 100 магістральних мереж. Цей стрімкий технологічний стрибок зумовив виникнення закономірної вразливості: значна частина військового трафіка почала циркулювати через цивільні мережі загального користування (глобальну мережу інтернет). Унаслідок цього за останні десятиліття сукупна частка витрат провідних держав світу на інформатику, кібербезпеку та підготовку до ведення інформаційних операцій зросла в рази, перетворивши інформаційне забезпечення на один із найбільш капіталомістких елементів оборонних бюджетів.

2. Залежність стратегічних цілей інформаційної війни від наявного операційного потенціалу сил і засобів та визначених способів їх практичного застосування. Дія цієї закономірності полягає в тому, що якісна еволюція технологічного інструментарію не просто вдосконалює старі методи, а радикально масштабує та трансформує самі цілі, які суб'єкт планує досягти у конфлікті. Наочною ілюстрацією цієї закономірності в сучасний період (середина 2020-х років) є інтеграція у простір інформаційного протиборства технологій генеративного штучного інтелекту (ГШІ) та автоматизованих систем аналізу великих даних (Big Data). До появи цих спроможностей цілі

інформаційних операцій мали переважно локальний, дискретний характер і обмежувалися дезорганізацією конкретних вузлів зв'язку або точковою дискредитацією окремих військово-політичних лідерів противника, оскільки створення та поширення контенту вимагало значного людського ресурсу та часу. Натомість сучасний операційний потенціал, що базується на нейромережових алгоритмах, дозволяє агресору ставити принципово нові, раніше недосяжні стратегічні цілі: тотальне переформатування ментального поля цілих націй, довгострокова зміна електоральної поведінки та деструкція системи ухвалення рішень на державному рівні. Автоматизована генерація мільярдів персоналізованих психологічних профілів користувачів у соціальних мережах, миттєве створення гіперреалістичного аудіо-та відеоконтенту (дипфейків) у промислових масштабах перетворили інформаційне насильство з інструменту підтримки класичних бойових дій на самостійну стратегічну силу, здатну паралізувати волю держави до опору ще до моменту залучення кінетичних сил.

3. Залежність досягнення кінцевої мети від синхронізації, єдності та узгодженості дій різних суб'єктів інформаційної діяльності в часі та просторі (координація між відомствами, союзниками та громадянським суспільством).

Прояв цієї закономірності полягає в тому, що монополія держави на ведення інформаційного протидіювання в епоху децентралізованих цифрових платформ остаточно втрачена. Жодна офіційна інституція чи військова структура не здатна самостійно протидіяти масштабному інформаційному насильству без інтеграції недержавних акторів у єдиний контур оборони. Наочним історичним підтвердженням дії цієї закономірності є досвід відбиття повномасштабної інформаційно-психологічної агресії Російської Федерації проти України. Ефективність українського когнітивного опору та збереження ментальної безпеки суспільства стали можливими саме завдяки унікальному мережевому механізму координації трьох ключових суб'єктів: 1) державно-відомчого апарату (Центр протидії дезінформації при РНБО, Центр стратегічних комунікацій та інформаційної безпеки, Сили оборони); 2) міжнародних союзників (моніторингові та аналітичні структури НАТО і ЄС, які синхронізували викриття ворожих наративів

на глобальному рівні); 3) ресурсів громадянського суспільства (волонтерські OSINT-спільноти, незалежні журналісти-фактчекери, IT-армія та мільйони цифрових активістів). Синхронізація дій цих різних сил у часі та просторі забезпечила високу швидкість реакції на інформаційні загрози, нейтралізувала спроби деструктивного впливу противника на систему державного управління та дозволила утримати стратегічну ініціативу в медіапросторі. Натомість порушення цієї закономірності – десинхронізація дій або відомча ізольованість – неминуче призводить до утворення «інформаційного вакууму», який миттєво заповнюється семантичними операціями агресора.

4. *Нерівномірність розподілу сил і засобів по всій інфосфері (зосередження ключових ресурсів на критичних напрямках впливу та вразливості системи).* Сутність цієї закономірності полягає в тому, що інформаційний простір за своєю архітектурою є глибоко асиметричним та неоднорідним, а отже, розпилення сил по всьому семантичному чи технологічному полю є стратегічно неефективним. Суб'єкти інформаційного протиборства завжди діють за принципом фокусної концентрації, зосереджуючи інтелектуальні, фінансові та програмно-технічні ресурси в точках найвищої капіталізації уваги – так званих «вузлах глобальної інфосфери». У сучасний період дія цієї закономірності чітко простежується у двох ключових вимірах: а) технологічно-платформений вимір (основні наступальні та оборонні ресурси концентруються навколо екосистем кількох транснаціональних медіагігантів (Big Tech, таких як Meta, Alphabet, Microsoft, Apple, ByteDance, X); сама архітектура цих платформ, їхні алгоритми рекомендацій та модерації контенту є тими критичними ділянками, де ведеться безперервна боротьба за контроль над цифровими потоками) і б) соціокогнітивний вимір (інформаційне насильство спрямовується не на суспільство загалом, а на конкретні цільові групи, які виконують роль провідників впливу (лідери думок, журналісти, політичні еліти) або є найбільш вразливими до маніпуляцій через психологічні особливості (радикалізовані спільноти, маргіналізовані верстви). У результаті, відносно невелика за обсягом, але прецизійно сфокусована атака на ці «вузли уразливості» інфосфери здатна дестабілізувати всю національну систему безпеки про-

тивника, що підтверджує об'єктивний характер нерівномірного розподілу сил у сучасних конфліктах.

5. *Нерівнозначність і нелінійність впливу різних інструментів на інформаційну інфраструктуру та когнітивну сферу протиборчої сторони.* Прояв цієї закономірності полягає в тому, що ефект від застосування засобів інформаційного насильства має нелінійний характер: результат не пропорційний масштабу чи інтенсивності зусиль, а визначається семантичною та психологічною точністю удару. Прямолінійне масове поширення офіційних пропагандистських наративів часто викликає ефект психологічного відторгнення (реактивності) в аудиторії противника, демонструючи нульову або навіть деструктивну ефективність попри колосальні фінансові витрати. Натомість асиметричні, точкові інструменти впливу демонструють надвисоку нелінійну результативність у двох головних площинах:

у когнітивній сфері – використання прецизійних психологічних тригерів, когнітивної зброї та віральних смислових конструктів (наприклад, стратегічно сконструйованих інтернет-мемів, які маскуються під низовий гумор). Завдяки механізмам самореплікації та віральності (швидкого самопоширення користувачами), такі мікроінструменти здатні за лічені дні проникнути крізь будь-які державні фільтри, латентно переформатувати емоційне тло суспільства й посіяти паніку чи нігілізм;

у технологічній сфері – керовані витоки реальної або частково сфальсифікованої критично важливої інформації (leaking), автентичність якої важко спростувати. Публікація одного верифікованого документа у правильний операційний момент здатна миттєво зруйнувати міжнародні коаліції, обнулити політичні рейтинги лідерів чи паралізувати роботу військових штабів. Таким чином, нелінійність доводить: в інформаційній війні якість, контекст і своєчасність смислового імпульсу повністю домінують над кількістю каналів його поширення.

6. *Закономірність технологічно-соціального десинхронозу.* Швидкість розвитку інформаційно-комунікаційних технологій та методів інформаційного насильства завжди суттєво випереджає швидкість адаптації правових, соціальних та психологічних механізмів захисту

суспільства. Це створює постійні «вікна вразливості» ментальної безпеки, які агресор використовує до моменту створення державою ефективних контрзаходів. Яскравішим проявом дії цієї закономірності в сучасний період є стрімка експансія інструментів ГШІ та технологій створення дипфейків (deepfakes). Здатність алгоритмів за лічені секунди генерувати фото-, аудіо- та відеоматеріали будь-якого ступеня складності, які неможливо відрізнити від реальності, миттєво перетворилася на високоефективну інформаційну зброю. За допомогою цих інструментів агресор здійснює прецизійні атаки, фальсифікуючи заяви вищих посадових осіб, накази військового командування чи створюючи панічні повідомлення в масштабах цілої країни. Водночас десинхроноз виявляється в тому, що нормативно-правова база (як національне законодавство, так і міжнародне гуманітарне право) та технічні системи верифікації контенту відстають від технологічного прогресу на роки. Поки міжнародні інституції розробляють регуляторні акти (наприклад, Акт про штучний інтелект або профільні конвенції), а соціальні інститути намагаються адаптувати програми з медіаграмотності, суспільство залишається беззахисним перед когнітивним насильством нового типу. Це підтверджує об'єктивну природу десинхронозу як постійного джерела системних загроз для національної безпеки.

7. *Закономірність тотальної медіатизації конфлікту.* У сучасних умовах факт події має менше значення, ніж те, як цю подію репрезентовано та інтерпретовано в медіапросторі. Подія, яка не отримала інформаційного супроводу, фактично виключається із політичного та воєнного процесу, тоді як штучно згенерований симулякр може призвести до реальних геополітичних наслідків. Теоретичним підґрунтям цієї закономірності є концепція соціології медіа та філософська теорія симулякрів Ж. Бодріяра, яка в умовах інформаційного насильства набуває прикладного мілітарного змісту. Військові дії середини 2020-х років доводять: медіатизація перетворила інформаційний простір із джерела новин на первинний театр воєнних дій. Ефективне утримання територій або успішне проведення кінетичної операції на полі бою втрачають свій стратегічний сенс, якщо в глобальному медіапросторі вони рефреймовані (подані) противником

як поразка. Навпаки, суто інформаційні операції (наприклад, віртуальна демонстрація сили, прецизійно змонтовані ролики ударів БПЛА, скоординовані тренди у TikTok та X) здатні деморалізувати армію противника та змусити уряди третіх країн припинити фінансову чи оборонну підтримку. Факт реальності повністю заміщується медійною картинкою, яка й стає основою для ухвалення рішень міжнародними лідерами та суспільством, що остаточно закріплює тотальну медіатизацію як панівну закономірність сучасних воєн.

До другої групи закономірностей належать такі.

1. Обумовленість масштабів і спрямованості інституційної побудови характером актуальної воєнно-політичної та економічної обстановки, а також довгостроковими цілями політики національної безпеки держави чи суміжних суспільних структур. Сутність цієї закономірності полягає в тому, що архітектура, штатна структура та завдання органів, відповідальних за інформаційну безпеку, ніколи не є статичними чи випадковими. Держава розбудовує та фінансує ці спроможності лише як пряму інституційну відповідь на критичні зміни у зовнішньому безпековому середовищі та відповідно до своїх геополітичних пріоритетів. Наочним та історично близьким прикладом дії цієї закономірності є еволюція сектору інформаційної безпеки України. До 2014 року, за умов відносно стабільної (хоч і латентно загрозливої) воєнно-політичної обстановки, у державі не існувало спеціалізованих інституцій для відбиття масштабних когнітивних атак, а інформаційна безпека розглядалася переважно через вузьку технічну функцію захисту державних таємниць. Проте різке загострення обстановки внаслідок російської гібридної агресії та визначення євроатлантичної інтеграції як довгострокової політичної мети актуалізували радикальну розбудову абсолютно нової інфраструктури. На виконання Стратегії інформаційної безпеки України було створено спеціалізовані міжвідомчі органи стратегічного рівня: Центр протидії дезінформації при РНБО України та Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики. Схожі процеси відбулися і в країнах НАТО (зокрема, створення Передового центру НАТО з питань стратегічних комунікацій у Ризі – NATO StratCom COE та Європейського центру

з протидії гібридним загрозам у Гельсінкі). Ці приклади доводять: масштаби та вектор інституційного будівництва у сфері інфосфери завжди жорстко детерміновані гостротою воєнно-політичного моменту та національними інтересами держави.

2. *Відповідність змісту, архітектури та масштабів засобів інформаційного впливу характеру й унікальним особливостям суспільного та державного устрою.* Прояв цієї закономірності полягає в тому, що політико-правова природа держави та соціокультурні особливості суспільства безпосередньо детермінують характер інструментів, які ця держава здатна розробляти та застосовувати в інфосфері. Держава не може створити інфраструктуру інформаційного протиборства, яка суперечить її базовим конституційним принципам та суспільним цінностям. Яскравим виявом цієї закономірності є ментально-інституційна асиметрія між двома типами державного устрою: а) авторитарні та тоталітарні режими (на прикладі РФ чи КНР) будують архітектуру інформаційного впливу за принципом жорсткої вертикальної централізації та монополізму. Їхні засоби базуються на тотальному державному контролі, створенні закритих суверенних сегментів мережі (проекти типу «Золотий щит»), тотальній цензурі та використанні промислових державних «фабрик тролів» для агресивної дезінформації. Такий зміст засобів прямо відповідає їхній внутрішній командно-адміністративній суті; б) ліберально-демократичні системи (країни НАТО та Україна) через необхідність дотримання фундаментальних прав людини, свободи слова та преси принципово не можуть використовувати інструменти тотального блокування чи створення державної монополії на правду. Тому архітектура їхніх засобів захисту є децентралізованою, мережевою та відкритою. Вона базується на концепціях підвищення суспільної резистентності (медіаграмотності), розвитку незалежного фактчекінгу, прозорості алгоритмів Big Tech та функціонуванні гнучких Стратегічних комунікацій (StratCom), які діють не через примус, а через відновлення довіри між суспільством і владою. Таким чином, державний устрій є природним рамковим фільтром, який визначає межі допустимого та ефективного інструментарію в ході ведення інформаційного протиборства.

3. *Пряма залежність масштабів та якості формування спроможностей від матеріальних, технологічних і духовних (ціннісних, інтелектуальних) можливостей держави.* Ця закономірність фіксує інтегральний характер розбудови інформаційного потенціалу, доводячи, що спроможність держави захищати свій семантичний суверенітет детермінована двома взаємозалежними векторами – матеріально-технічним підґрунтям та духовним (когнітивно-ціннісним) станом соціуму. Дія цієї закономірності розгортається у двох паралельних площинах: а) матеріально-технологічний сектор (масштаби розгортання сил кіберзахисту, фінансування інноваційних оборонних розробок, інтеграція алгоритмів ІІІ для моніторингу дезінформації прямо пов'язані з економічною могутністю актора. Держава з високим науково-технічним потенціалом здатна інституціоналізувати високотехнологічні підрозділи інформаційних операцій, створювати закриті супутникові контури зв'язку та прецизійні системи аналізу великих даних, що забезпечує структурну перевагу над технологічно слабшим противником); б) духовний (ціннісно-інтелектуальний) сектор (якість та стійкість сформованих спроможностей безпосередньо залежать від рівня інтелектуального розвитку суспільства та міцності його ціннісного каркаса. У площині інформаційного протиборства цей потенціал виявляється у високому рівні критичного мислення громадян, розвиненій медіакulturі та наявності монолітної соціокультурної ідентичності. Навіть за умов тотальної економічної та технологічної переваги агресора, його спроби інформаційного насильства зазнають краху, якщо вони стикаються із високою духовною резистентністю нації, яка має стійкі ціннісні орієнтири, консолідовану історичну пам'ять та високий рівень патріотичної свідомості). Таким чином, матеріальні ресурси забезпечують інструментальну сторону інформаційної безпеки («панцир»), тоді як духовні та інтелектуальні можливості суспільства формують її змістовне ядро («імунітет»), що в синергії визначає остаточний рівень захищеності національного інформаційного простору.

На основі знання законів і закономірностей, а також набуття досвіду в результаті практичної діяльності виробляються принципи ведення інформаційної війни, тобто загальні науково обґрунтовані

положення, правила, рекомендації щодо її підготовки і ведення, а також керівництва її силами і засобами. Поняття «принцип» є близьким за змістом до понять «закон» і «закономірність». Їх спільність полягає в тому, що всі вони відображають істотні, об'єктивні, повторювані зв'язки, відносини дійсності. Однак принцип не тільки відбиває об'єктивний зв'язок, а й пропонує, як слід діяти в конкретних умовах для досягнення тієї або іншої мети. У ньому виражається єдність об'єктивного і суб'єктивного.

Зміст і масштаби завдань інформаційної війни зумовлюють наявність розгалуженої системи принципів її ведення. Основний принцип інформаційної війни – *відповідність (підпорядкованість) її цілей і завдань політичним цілям* – безпосередньо впливає із закону визначальної ролі політики та її вирішального впливу на характер конфлікту. Історично дія цього принципу чітко виявилася під час проведення коаліційних операцій у зоні Перської затоки («Буря в пустелі»), операції НАТО в Косові, а також військових кампаній в Афганістані та Іраку. Увесь інформаційний супровід, який став обов'язковою та невіддільною складовою дій багатонаціональних сил, був прецизійно спрямований на легітимізацію та обґрунтування доцільності цих кампаній для світового співтовариства через акцентування на порушеннях противником прав людини, норм міжнародного права чи підтримці тероризму. При цьому важливо констатувати, що інформаційний вплив на світову спільноту, окремі країни та регіони розпочинався задовго до перших кінетичних ударів. Якщо у Перській затоці інформаційні заходи активізувалися за п'ять місяців, а в Гренаді – за три роки до військового втручання, то в сучасному контексті російської гібридної агресії проти України когнітивна та семантична підготовка до війни (через нав'язування псевдоісторичних наративів, інформаційне насильство та спроби розколу українського соціуму) тривала десятиліттями, що остаточно підтверджує перманентний і випереджальний характер реалізації цього базового принципу.

Наступний принцип інформаційної війни – *необхідність зосередження сил і засобів на критичних напрямках (у вирішальному місці) та у вирішальний момент* – є праксеологічним відображенням

об'єктивної закономірності нерівномірного розподілу сил в інфосфері. У сучасних умовах зміст цього принципу став набагато об'ємнішим, а його практична реалізація – складною та інтегрованою. Ретроспективний аналіз локальних конфліктів кінця XX століття наочно демонструє генезу цього принципу. Так, під час операцій коаліційних сил у зоні Перської затоки («Буря в пустелі», 1991 р. та «Лис у пустелі», 1998 р.) інформаційне протиборство вперше набуло тривимірного масштабу (стратегічного, оперативного та тактичного). Концентрація сил виявилася у розгортанні безпрецедентного на той час угруповання: понад 20 розвідувальних супутників та 50 літаків-розвідників забезпечували цілодобовий моніторинг обстановки. За відсутності симетричної протидії з боку Іраку це дозволило у режимі реального часу надавати органам управління військами вичерпну та точну інформацію. Одночасно у вирішальних точках застосовувалися засоби радіоелектронного придушення (зокрема, літаки РЕБ EA-6B Prowler), що повністю заблокувало системи командування іракської армії¹. Не менш масштабна концентрація інформаційних та психологічних ресурсів спостерігалася під час 78-добової повітряної кампанії НАТО проти Югославії у 1999 році. Проте в сучасних конфліктах середини 2020-х років принцип зосередження сил зазнав докорінної трансформації. Сьогодні «вирішальне місце» перенесено з фізичних вузлів зв'язку та локальних радіостанцій у глобальний цифровий простір та архітектуру магістральних платформ (Big Tech). Замість концентрації поодиноких літаків РЕБ сучасне когнітивне домінування досягається прецизійним фокусуванням автоматизованих бот-мереж, алгоритмів штучного інтелекту та фабрик дипфейків на специфічних соціальних групах у моменти найвищої суспільно-політичної напруги (електоральні цикли, кризи, початок воєнних операцій). Це дозволяє агресору синергетично поєднувати технологічний та соціокультурний вплив, досягаючи максимального руйнівного ефекту мінімальними, але надточно сконцентрованими силами.

Одним із фундаментальних принципів інформаційної війни є *всєбічна завчасна підготовка її сил і засобів*. Цей принцип безпосередньо

¹ Див.: Conduct of the Persian Gulf War: final report to Congress. Washington, DC: Dept. of Defense, 1992. xxxi, 824 p.

відбиває об'єктивний закон залежності перебігу і результату інформаційного протистояння від співвідношення економічних, матеріально-технічних та духовних можливостей протистоячих сторін. Інформаційне насильство не може бути ефективним, якщо воно розгортається спонтанно; воно вимагає створення розгалуженої інфраструктури, розробки стратегічних наративів та підготовки когнітивних пасток задовго до початку відкритих бойових дій. У ретроспективному вимірі дія цього принципу чітко простежується в діяльності військово-політичного керівництва Ізраїлю під час Ліванської війни 1982 року. За свідченнями профільних аналітичних видань того часу (зокрема, лондонського журналу «The Middle East»), інформаційні служби ізраїльського уряду за рік до початку операції розробили детальні варіанти офіційних заяв для світової преси з ретельно сформованою версією Тель-Авіва щодо причин вторгнення. До моменту, коли перші військові підрозділи перетнули ліванський кордон, у дипломатичних представництвах Ізраїлю по всьому світу вже перебували заздалегідь підготовлені багатомовні комплекти матеріалів, покликані оперативно легітимізувати військові дії в очах міжнародної спільноти. У сучасних конфліктах середини 2020-х років цей принцип набув тотального характеру. Завчасна підготовка сьогодні передбачає не просто написання пресрелізів, а багаторічне латентне формування цифрової та семантичної інфраструктури агресії. Наочним прикладом є дії Російської Федерації, яка задовго до повномасштабного вторгнення 2022 року інвестувала колосальні ресурси у створення мереж проксі-медіа, підготовку інструментарію кібератак на критичну інфраструктуру України та країн Заходу, а також у довгострокові психологічні операції, спрямовані на розмивання національної ідентичності та волі до опору об'єкта експансії. Це доводить, що етап завчасної підготовки в інформаційній сфері часто є більш тривалим та ресурсомістким, ніж безпосередня кінетична фаза війни.

Принцип *високої активності і рішучості в ході ведення інформаційної війни* безпосередньо зумовлений її стратегічними цілями. Історія воєнного мистецтва демонструє безліч прикладів, коли непевність, коливання, пасивність або зволікання із застосуванням ефективних заходів протидії противнику призводили до катастрофічних

наслідків, аж до повної поразки. Тому зазначений принцип має про-
низувати дії кожної командної інстанції та стратегічного керівництва.
Вимоги високої активності та рішучості стосуються як захисту влас-
ного інформаційного поля, так і деструктивного впливу на когнітив-
ну сферу конфронтуючої сторони. У праксеології інформаційної війни
цей принцип часто реалізується через агресивне випереджальне по-
ширення маніпулятивних наративів, де швидкість та емоційний ре-
зонанс домінують над фактологічною верифікацією. Хрестоматійним
прикладом є інформаційна кампанія США та Кувейту напередодні
війни у Перській затоці в 1990 році. Для дискредитації іракського
режиму американське PR-агентство «Hill & Knowlton» (отримавши
за роботу близько 10,8 млн дол.) сфабрикувало та організувало виступ
перед Конгресом США нібито кувейтської дівчинки-очевидця, яка
заявила, що іракські солдати вбивали немовлят, викидаючи їх з куве-
зів у лікарнях¹. Цей емоційний медійний наратив, миттєво тиражова-
ний світовою пресою, радикально змінив громадську думку в США
на користь військового втручання, хоча згодом факт фальсифікації
було повністю доведено. Схожий алгоритм рішучого інформаційного
наступу було застосовано у 2002–2003 роках щодо наявності в Іраку
зброї масового ураження (ЗМУ). Завдяки постійній та динамічній
зміні тез у медіапросторі (від оцінок у два роки до кількох місяців
щодо готовності створення ядерного потенціалу), США сформували
міжнародну легітимність для вторгнення 2003 року, попри те, що зго-
дом ЗМУ на території країни так і не було знайдено².

Принцип рішучості виявляється і в гіперболізації власних військо-
вих успіхів за умов монополізації глобального інформаційного про-
стору (на прикладі трансляцій телекомпанії CNN у 1991 р.). Так,
Пентагон офіційно звітував про 96% успішних перехоплень ракет
«Скад» комплексами «Петріот» (45 із 47 пусків). Лише через роки,
у ході детальних незалежних розслідувань, ця цифра в офіційних

¹ Див.: Knightley P. The Disinformation Campaign. *The Center for Public Integrity*. October 14, 2001. URL: <https://publicintegrity.org/accountability/the-disinformation-campaign/>.

² Див.: Iraq and Weapons of Mass Destruction : National Security Archive Electronic Briefing Book No. 80 / ed. by J. Richelson. *The National Security Archive*. February 11, 2004. URL: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB80/index.htm>

звітах знизилася спочатку до 52%, а згодом – до реальних 9%¹. Наведена практика доводить цинічну, але об’єктивну закономірність інформаційного протиборства: стратегічний успіх досягається за рахунок операційної сміливості та швидкості первинного когнітивного удару. Оскільки ретроспективна верифікація та викриття дезінформації відбуваються через місяці чи роки, на момент оприлюднення правди ключові політичні та геополітичні цілі агресора вже виявляються повністю досягнутими.

Принцип *узгодженого спільного застосування різних видів і типів сил та засобів ведення інформаційної війни* є визначальним, оскільки розв’язання абсолютної більшості стратегічних та оперативних-тактичних завдань вимагає синхронного залучення гетерогенних (різномірних) за своїми характеристиками ресурсів та чіткої координації їхніх дій. Імперативом реалізації цього принципу є побудова інтегрованої вертикалі управління, що забезпечує безперервну взаємодію між різними суб’єктами оборонного та цивільного секторів. Під час обрання способів спільного застосування різномірних сил органи управління повинні ретельно і всебічно враховувати специфіку кожного конкретного завдання, умови операційного середовища, а також сильні сторони, вразливості та лімітації кожного залученого інструменту ведення інформаційного протиборства. У сучасній військовій практиці цей принцип знайшов своє найвище втілення у концепції міжвідомчої інтеграції сил і спроможностей (інформаційних, психологічних, кібернетичних та радіоелектронних операцій). Наочним прикладом є сучасна архітектура Стратегічних комунікацій НАТО, яка вимагає, щоб кібератаки на критичну інфраструктуру противника, радіоелектронне придушення його систем зв’язку та психологічні операції в когнітивній сфері не проводилися ізольовано². Вони мають бути поєднані в єдиний смисловий і часовий контур, де технологічний

¹ Див.: Почепцов Г. Как ведутся тайные войны: психологические операции в современном мире. Харьков: Консум, 2000. С. 97.

² Див.: AJP-3.10. Allied Joint Doctrine for Information Operations. Edition A, Version 1. December 2015 / NATO Standardization Office (NSO). URL: <https://mppsotc.army.gr/wp-content/uploads/2024/03/2.-AJP-3.10-EDA-V1-E.pdf>

удар (наприклад, блокування мережі) миттєво посилюється когнітивним впливом (поширенням віральних наративів паніки серед населення противника), що синергетично помножує підсумкову ефективність операції.

Особливого значення в інформаційній війні набуває вміле використання принципу *раптовості дій*. Несподівані за часом, місцем, масштабом, інтенсивністю та інструментами інформаційно-технічні удари й когнітивні операції проти інформаційного середовища противника дозволяють захопити його зненацька, посіяти паніку, дезорганізувати систему державного й військового управління, а також повністю скувати волю до опору. При цьому постійно зростаючі можливості інформаційної зброї визначають стійку тенденцію до реалізації саме раптового та асиметричного нападу. Ефективне досягнення раптовості охоплює комплекс взаємопов'язаних заходів: збереження в суворій таємниці задумів, концепцій та планів майбутніх операцій; латентну підготовку до розгортання сил і спроможностей ведення інформаційного протиборства; здійснення експансії в інформаційному середовищі противника на тих напрямках, де він є найменш захищеним (використання «вузлів уразливості»); застосування невідомих противнику видів інформаційно-когнітивної зброї та інноваційних способів розв'язання завдань; уміле оперативне маскування (маскування за стандартами НАТО) і дезінформування. У сучасній практиці конфліктів середини 2020-х років принцип раптовості вийшов на принципово новий рівень технологічної реалізації. У кіберпросторі він виявляється у формі масованих, скоординованих атак із використанням раніше невідомих експлойтів і вразливостей «нульового дня» (0-day), що дозволяє миттєво паралізувати державні реєстри та критичну інфраструктуру ще до моменту активації систем протидії. У когнітивній площині раптовість досягається за рахунок тривалого прихованого зміщення меж суспільної норми через механізми «вікна Овертона» та смислові диверсії, які трансформуються в агресивний, відкритий психологічний тиск безпосередньо у момент початку кінетичної фази конфлікту. У межах політичної та воєнної соціології ця закономірність спирається на теоретичну модель

Дж. Овертона¹, яка описує рамки допустимості ідей у суспільному дискурсі. В умовах інформаційного насильства агресор латентно трансформує сприйняття суспільством певних деструктивних смислів: від категорії «мислимого» чи «прийнятного» до повної капітуляції перед наративами ворога. Завдяки тривалій підготовці фінальний когнітивний удар у момент переходу конфлікту у відкриту фазу виявляється для суспільства-об'єкта абсолютно раптовим, оскільки внутрішні психологічні механізми масового опору та розрізнення ворожих сенсів були завчасно еродовані та паралізовані. Як наслідок, об'єкт атаки втрачає здатність до системного захисту свого смислового суверенітету, що призводить до деструкції національної ідентичності та паралічу волі до опору.

До інших основних принципів інформаційної війни належить принцип *постійної готовності сил і засобів до захисту власного інформаційного простору та здійснення деструктивного впливу на інформаційне середовище противника*. Специфіка дії цього принципу зумовлена тим, що інфосфера є простором перманентного протиборства, яке не припиняється під час підписання мирних угод чи затишшя на полі бою. Тому сили інформаційно-психологічних операцій, кіберзахисту та стратегічних комунікацій повинні перебувати в стані постійної операційної готовності. У сучасному безпековому вимірі цей принцип трансформувався у вимогу побудови цифрової та когнітивної резистентності держави. Захисний аспект принципу передбачає безперервний, цілодобовий моніторинг національного медіапростору, виявлення латентних ворожих наративів на ранніх стадіях їхнього зародження та миттєве блокування кіберзагроз для критичної інфраструктури. Наступальний (або контрнаступальний) аспект вимагає наявності завчасно розгорнутих, високотехнологічних спроможностей для здійснення миттєвого симетричного чи асиметричного впливу на когнітивну сферу та технічні вузли управління противника у разі ескалації конфлікту. Постійна готовність унеможливорює утворення «інформаційного вакууму» чи технологічних пауз, які

¹ Див.: Russell N. J. An Introduction to the Overton Window of Political Possibility. Mackinac Center for Public Policy. January 4, 2006. URL: <https://www.mackinac.org/7504>

противник міг би використати для перехоплення стратегічної ініціативи, що робить цей принцип основою життєздатності сучасної системи національної безпеки і повністю відповідає сучасній американській концепції безперервного операційного залучення (*Persistent Engagement*)¹.

Дуже важливим є *принцип безперервності ведення інформаційної війни*. Сутність цього принципу випливає з об'єктивного закону тотальності інфосфери та полягає в тому, що інформаційне протиборство є перманентним процесом, який не має фіксованих хронологічних меж, не розпочинається з офіційного оголошення війни і не припиняється після укладання мирних договорів чи припинення вогню на кінетичному театрі воєнних дій. Якщо класична гаряча війна є дискретною (має чіткі фази початку, перебігу та завершення), то інформаційне насильство здійснюється безперервно. У сучасному воєнно-політичному дискурсі цей принцип є фундаментальною основою доктрин ведення війн у «сірій зоні» (Gray Zone Warfare) та реалізації стратегій гібридної експансії². У мирний час безперервність виявляється у формі латентного психологічного тиску, ведення постійного розвідувального моніторингу, підриву інституційної довіри та довгострокового ідеологічного перекодування суспільства противника. Під час відкритої фази конфлікту цей вплив лише масштабується та синхронізується з кінетичними ударами. Нехтування цим принципом, тобто згортання інформаційних чи оборонних спроможностей у так званий «мирний час», неминуче призводить до втрати стратегічної ініціативи, когнітивного роззброєння держави та створення критичних вразливостей у системі національної безпеки, які противник гарантовано використає для підготовки майбутньої гарячої фази конфлікту.

Треба також згадати про *принцип ведення інформаційної війни з напругою, необхідною для виконання поставлених завдань*. Сутність

¹ Див.: Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command / U. S. Cyber Command. Fort Meade, MD, 2018. 12 p. URL: <https://www.cybercom.mil/portals/56/documents/uscycercom%20vision%20april%202018.pdf>

² Див.: Clark B., Gunzinger M., Sloman J. Winning in the gray zone: using electromagnetic warfare to regain escalation. Washington, DC: Center for Strategic and Budgetary Assessments, 2017. 72 p.

цього принципу полягає в раціональному дозуванні та точному калібруванні інтенсивності інформаційно-психологічного та технічного впливу. Рівень операційної напруги має бути прямо пропорційним масштабу визначеної мети і не призводити до перевитрати інтелектуальних, технологічних чи фінансових ресурсів держави. Праксеологічний аспект цього принципу виявляється в запобіганні ефекту так званого «перенасичення» інформаційного поля. Надмірно інтенсивне, агресивне та прямолінійне поширення дезінформації або пропагандистських наративів з боку суб'єкта може викликати у суспільстві противника зворотну реакцію – психологічне відторгнення (реактивність) та підвищення рівня когнітивної пильності, що повністю нівелює результати операції. У технологічному ж вимірі (наприклад, у кіберпросторі або РЕБ) цей принцип вимагає дозованого застосування спроможностей, оскільки передчасна або занадто масштабна демонстрація новітніх алгоритмів чи експлойтів дозволяє противнику завчасно розгадати задум, адаптувати свої системи захисту та закрити наявні «вікна вразливості». Отже, оптимальна напруга забезпечує прихованість дій, раціональне використання сил та максимальний коефіцієнт корисної дії кожного точкового інформаційного імпульсу.

Треба нагадати й про принцип *когнітивної прецизійності (високої точності) та релевантності*. Цей принцип впливає із закону асиметрії інформаційного впливу та закономірності нерівнозначності інструментів інфосфери. Згідно з його вимогами, будь-який інформаційно-психологічний імпульс або контрзахід має розроблятися з урахуванням унікальних психологічних, етнокультурних, соціальних та релігійних характеристик конкретної цільової аудиторії противника. Ефективність сучасного інформаційного насильства визначається не масовістю чи валовим обсягом поширення інформації, а точністю її потрапляння у наявні внутрішні соціокультурні лінії розлому суспільства – об'єкта атаки. Прецизійне калібрування контенту під ментальні особливості конкретної групи дозволяє мінімальними ресурсами викликати масштабні каскадні процеси дестабілізації.

Дуже важливим є принцип *проактивності та формування когнітивного імунітету (резистентності)*. Цей принцип пропонує алгоритм дій в умовах закономірності технологічно-соціального десинхронозу. Перевагу в інформаційній сфері отримує той суб'єкт, який діє на випередження: не просто реагує на вже здійснені атаки противника (що змушує постійно перебувати в позиції виправдання), а проактивно формує первинний порядок денний, завчасно розкриває латентні загрози та вибудовує системну стійкість власного соціуму. У практичній площині цей принцип вимагає безперервного розвитку критичного мислення громадян, медіаграмотності та консолідації національної ідентичності як головного захисного «імунітету» проти зовнішніх деструктивних смислових диверсій.

Окрему групу складають *практико-логічні принципи командно-ресурсного забезпечення*, які регламентують безпосередній процес управління інструментарієм інформаційного протистояння. До них належать: *принцип своєчасного маневру силами і засобами* (спроможність оперативно перекидати технологічні, інтелектуальні та медійні ресурси на нові, критично важливі або раптово виявлені операційні напрямки інфосфери); *принцип урахування духовного чинника в інтересах виконання поставлених завдань* (прецизійний аналіз морально-психологічного стану, національної ідентичності та соціокультурних цінностей як власного суспільства, так і соціуму противника); *принцип всебічного забезпечення, підтримки життєздатності та своєчасного відновлення сил* (неперервне логістичне, фінансове, технічне й кадрове підживлення інфраструктури безпеки, захист її від кібердеструкції); *принцип рішучості й безперервності управління* (побудова стійкої, захищеної та централізованої вертикалі координації між різними відомствами й суб'єктами інформаційної діяльності); *принцип непохитності у досягненні намічених цілей, виконанні ухвалених рішень і реалізації поставлених стратегічних завдань*.

Усі зазначені принципи знаходять своє практичне втілення в конкретних формах і способах ведення інформаційної війни. При цьому методологічно важливо враховувати, що наведена система принципів

не є статичною, вічною чи сталою. Вони є динамічною категорією воєнно-політичної науки, яка безперервно еволюціонує, трансформується та уточнюється в синергії із експоненціальним розвитком технологічних засобів і методів інформаційного насильства.

Переходячи до безпосереднього аналізу інструментарію інформаційного протистояння, необхідно чітко диференціювати форми та способи його реалізації. У сучасній військовій науці та спільних доктринах НАТО (зокрема, у базовому стандарті AJP-3.10 «Allied Joint Doctrine for Information Operations») ці категорії піддаються суворому розмежуванню¹: форма – визначає організаційно-стратегічні рамки, просторово-часові межі, масштаб, хронологію та архітектуру, у межах яких розгортається протистояння (наприклад, операція, кампанія); спосіб (метод) – відображає прикладний вимір, тобто конкретні дії, технологічні алгоритми та інструменти, за допомогою яких безпосередньо здійснюється деструктивний вплив (наприклад, дезінформація, РЕБ, кібератака)².

Зважаючи на масштаб, кінцеві цілі, тривалість та склад залучених суб'єктів, організаційна структура дій в інфосфері поділяється на три панівні форми.

1. *Стратегічна інформаційна кампанія* (Strategic Information Campaign) – найвища форма інформаційного протистояння, яка має перманентний характер і безперервно триває роками (як у мирний час, так і в умовах відкритого збройного конфлікту). Вона координується вищим військово-політичним керівництвом держави та спрямована на фундаментальну, довгострокову зміну геополітичної орієнтації, ціннісного каркаса, ментальних установок чи соціокультурної ідентичності суспільства – об'єкта експансії³.

¹ Див.: Cline L. E. Planning for Strategic Information Operations. *Contemporary Military Challenges*. 2024. Vol. 26, No. 2. P. 9–20. DOI: <https://doi.org/10.2478/cmc-2024-0010>

² Див.: Information Operations vs Information Warfare: What is the Difference? *OSavul*. URL: <https://www.osavul.cloud/blog/information-operations-vs-information-warfare>

³ Див.: Vuletić D., Milenković M. R. Information Warfare as an Introduction to Russia-Ukraine Armed Conflict. *Strategic Intersections : The New Architecture of International Security* / Editors Milovan Subotić, Šerban Cioculescu. Belgrade : Vojna štamparija, 2023. P. 185–197.

2. *Інформаційна операція* (Information Operation) – інтегрована сукупність узгоджених за метою, завданнями, часом та місцем дій (як технічного, так і психологічного характеру), які плануються та реалізуються у межах конкретного конфлікту або розгортаються для безпосереднього забезпечення і підтримки кінетичної (фізичної) компоненти воєнної кампанії¹.

3. *Інформаційний (когнітивний) удар* (Information Strike) – одноразова, раптова, високоточна та скоординована акція, розрахована на миттєвий ефект. Прикладами реалізації такої форми є масований керований витік критично важливих таємних документів (leaking) або синхронна публікація високотехнологічних дипфейків у світовому медіапросторі. Головна мета удару полягає в тому, щоб викликати шок, когнітивний дисонанс, паніку та параліч системи ухвалення рішень противника у критично важливий (переломний) операційний момент².

Практична реалізація інформаційного насильства на прикладному рівні розгортається у двох взаємозалежних площинах: технологічній та когнітивній. Інформаційно-технічні методи спрямовані на деструктивний вплив, блокування, викривлення або повне знищення матеріальних і програмних елементів інформаційної інфраструктури противника, його систем командування, управління, комунікацій, комп'ютерів та розвідки (C4I).

У сучасних технологічних умовах (середина 2020-х років) до північних інформаційно-технічних методів належать³:

кібернетичні атаки (Cyber Attacks) та *операції в комп'ютерних мережах*. Цей метод передбачає несанкціоноване проникнення в обчислювальні системи противника, використання раніше невідомих вразливостей «нульового дня» (0-day vulnerabilities) та застосування

¹ Див.: Information Operations. RAND. URL: <https://www.rand.org/topics/information-operations.html>

² Див.: Information Warfare and the Future of Conflict. URL: https://threatcasting.asu.edu/sites/g/files/litvpz1036/files/2020-07/threatcasting-2020-The%20Future%20of%20Information%20Warfare-WEB_1.pdf

³ Див.: Bakirov A., Suleimenov I. Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare. *Computers*. 2025. Vol. 14, Issue 10. Art. 410. DOI: <https://doi.org/10.3390/computers14100410>

шкідливого програмного забезпечення (зокрема, програм-вимагачів та вірусів-вайперів, що безповоротно знищують дані). Об'єктом впливу стають державні реєстри, хмарні сховища даних, системи військового зв'язку, а також автоматизовані системи управління технологічними процесами (АСУ ТП) об'єктів критичної інфраструктури (енергетика, логістика, банкінг);

радіоелектронне придушення та боротьба в електромагнітному спектрі (Electronic Warfare / РЕБ). Метод базується на генеруванні навмисних електромагнітних завад для повного блокування, перехоплення або викривлення каналів радіозв'язку, супутникової навігації (GPS/ГЛОНАСС), радарів та ліній телеметрії безпілотних систем противника. Сучасна закономірність РЕБ полягає в переспрямуванні зусиль з ізолюваного тактичного глушіння рацій на стратегічне придушення мережецентричних систем бойового управління та супутникових інтернет-угруповань;

фізичне (кінетичне) руйнування елементів інфосфери. Цей спосіб доводить інтегрований характер сучасної війни, де фізичне насильство застосовується для досягнення інформаційних цілей. Він реалізується шляхом завдання високоточних ударів (ракетами, артилерією, БПЛА-камікадзе) по матеріальних вузлах інформаційної інфраструктури: телевізійних та радіовежах, наземних станціях супутникового зв'язку, серверних центрах (дата-центрах), магістральних вузлах інтернет-комунікацій та лініях електропередачі, що живлять ці об'єкти.

Слід наголосити, що інформаційно-технічні методи сьогодні діють у синергетичному контурі. Наприклад, фізичне знищення підстанцій живлення чи веж зв'язку синхронізується із кібератаками на резервні сервери та радіоелектронним придушенням резервних частот, що призводить до повного ізолювання та інформаційного колапсу системи управління противника.

На відміну від інфраструктурного впливу, інформаційно-когнітивні (психологічні) методи спрямовані на індивідуальну, групову та масову свідомість. Їхньою метою є примусова деформація смислового поля суспільства-об'єкта, руйнування його системи ціннісних орієн-

тирів та параліч волі до опору. У такій системі об'єктом експансії стає ментальна безпека та людський чинник інформаційних систем противника.

У сучасній практиці гібридних конфліктів до ключових інформаційно-когнітивних методів належать:

рефлексивне управління (Reflexive Control). Специфічний метод, що полягає в цілеспрямованій передачі противнику такої спеціально підготовленої інформації (вихідних даних), яка спонукає його «самостійно» та «добровільно» ухвалити рішення, наперед вигідне для агресора, але згубне для самого противника. Цей спосіб базується на прецизійному моделюванні психологічних особливостей та алгоритмів мислення осіб, які приймають стратегічні рішення;

масштабована (промислова) дезінформація та фабрикація смислів. Метод передбачає не просто поширення неправдивих новин (фейків), а конструювання альтернативної віртуальної реальності за допомогою алгоритмів генеративного штучного інтелекту та великих мовних моделей. Завдяки автоматизованій персоналізації контенту, агресор здійснює точкові інформаційні удари по наявних внутрішніх соціальних лініях розлому (етнічних, релігійних, майнових чи політичних) об'єкта атаки, викликаючи каскадні процеси суспільної дестабілізації;

семантичні диверсії та історичний ревізіонізм. Спосіб довгострокового стратегічного впливу, спрямований на ерозію історичної пам'яті, національних міфів, мовного середовища та культурних кодів соціуму. Через агресивне нав'язування псевдоісторичних концепцій та рефреймінг національних цінностей противник намагається зруйнувати соціокультурну ідентичність суспільства, позбавляючи його внутрішніх орієнтирів та ідеологічного фундаменту для когнітивного опору;

керовані, прецизійні витoki інформації (Leaking). Метод компрометації та дезорганізації, який полягає в дозованому оприлюдненні у правильний операційний момент реальних, чутливих або частково сфальсифікованих конфіденційних даних (державних таємниць, за-

критих листувань, військових планів). Цей інструмент використовується для миттєвої дискредитації вищого військово-політичного керівництва держави, підриву інституційної довіри громадян до державних органів та штучного провокування конфліктів всередині міжнародних оборонних коаліцій.

Таким чином, інформаційно-когнітивні підходи трансформують інформаційне середовище з каналу передачі даних на латентний простір соціальної інженерії, де кінцева перемога досягається не фізичним знищенням армії противника, а повним підпорядкуванням та переформатуванням ментальної матриці його суспільства.

У підрозділі здійснено комплексний теоретико-методологічний аналіз сутності, законів, закономірностей, принципів і методів інформаційної війни в умовах сучасного турбулентного світу.

Психологічний та технологічний складники інформаційної війни, маючи спільну основу (інформаційну сферу), суттєво відрізняються за характером і об'єктами впливу. Інформаційно-психологічний чинник спрямований на духовну сферу (свідомість та підсвідомість соціуму) через відкриті вербально-маніпулятивні засоби. Натомість інформаційно-технологічний складник є латентним і деструктивно впливає на матеріальні об'єкти – бази даних, канали зв'язку та інформаційні системи. Незалежно від специфіки застосованих засобів, кінцевий результат інформаційного протиборства завжди має матеріальний вимір. Він виражається у віддаленому за часом деструктивному впливі на критичну інформаційну інфраструктуру держави та її політичну систему в цілому.

Стрімке зростання ролі інформаційного чинника нівелює традиційні межі між мирним і воєнним часом, військовими та цивільними сферами, а також методами політичної та збройної боротьби. Унаслідок цього інформаційна війна трансформується у глобальний, перманентний та потенційно тотальний процес, який охоплює всі сфери життєдіяльності держави. Ключовим суб'єктом інформаційної війни є держава; об'єкти охоплюють діапазон від індивідуальної свідомості до державної інфраструктури; засоби варіюються від пропаганди до кібератак на мережі передачі даних, а просторово-часові характеристики є необ-

меженими. Фінальна мета інформаційної війни завжди має радикальний політичний характер і спрямована на підриг суверенітету, зміну політичного курсу або повне підпорядкування об'єкта впливу.

Таким чином, сформований теоретико-методологічний базис підтверджує, що захист національного інформаційного простору в епоху турбулентності вимагає переходу від пасивної фільтрації контенту до проактивного стратегічного наративу та розбудови когнітивної стійкості суспільства. Окреслена динаміка та різноплановість засобів впливу зумовлюють необхідність детального дослідження історичного генезису та еволюції інструментарію інформаційного протистояння, що становить зміст наступного підрозділу.

==== Список використаних джерел

1. Борисенко Є. Інформаційна війна крізь призму комунікативної теорії: спроба аналізу. *Філософська думка*. 2023. №4. С. 21–38.
2. Военный энциклопедический словарь. Москва: Воениздат, 1983. 863 с.
3. Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2022. №3. С. 11–29.
4. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки*. 2020. Т. 7, №2. С. 56–61.
5. Інформаційна війна і національна безпека: [колект.] монографія / П. П. Ткачук [та ін.]. Львів : Акад. сухопут. військ, 2015. 264 с.
6. Клаузевиц К. О войне: в 2 т. Москва: ООО «Изд-во АСТ»; Санкт-Петербург : Terra Fantastica, 2002. Т. 1. 558 с. Т. 2. 574 с.
7. Короход Я. Інформаційна війна як основна загроза інформаційній безпеці держави: поняття, форми і методи ведення. *Evropský politický a právní diskurz*. 2017. Sv. 4, Vyd. 3. С. 222–227.
8. Кундеус О. М., Вівчар І. В., Крет О. В. Інформаційна війна: сутність та особливості (кінець ХХ – початок ХХІ століття). *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2024. №3. С. 212–223.

9. Петришин Г. Інформаційна війна Росії проти України: еволюція основних засобів, методів та динаміка наративів. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. Вип. 1. С. 117–128.
10. Політична енциклопедія / Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ: Парламентське видавництво, 2011. 808 с.
11. Політологія: енциклопедичний словник / [В. М. Денисенко, Л. Я. Угрин, Н. М. Хома]; за ред. д-ра філос. наук, проф. В. П. Мельника. Львів : ЛНУ імені Івана Франка, 2014. 406 с.
12. Поправка М. О. Інформаційна війна в контексті гібридного конфлікту. *Міжнародні та політичні дослідження*. 2024. Вип. 38. С. 267–274.
13. Почепцов Г. Как ведутся тайные войны: психологические операции в современном мире. Харьков : Консум, 2000. 280 с.
14. Проноза І. І., Цимбал С. Ю. Інформаційна війна в сучасних інтернет-комунікаціях: українсько-європейські практики та виклики. *Політикус*. 2025. Вип. 3. С. 97–102.
15. Соціологія права: енциклопедичний словник / Л. М. Герасіна, О. Ю. Панфілов, В. Л. Погрібна та ін.; за ред. М. П. Требіна. Харків : Право, 2020. 984 с.
16. Стрільчук Л. Інформаційна війна як складова сучасних гібридних воєн (на прикладі Грузії та України). *Літопис Волині*. 2023. Чис. 28. С. 235–239.
17. Сунь-Цзы. У-Цзы. Трактати о военном искусстве / пер. с кит., предисл. и коммент. Н. И. Конрада. Москва: ООО «Изд-во АСТ» ; Санкт-Петербург: Terra Fantastica, 2002. 558 с.
18. Требин М. П. Информационная война в современном мире. *Новый хозяин*. 2000. № 7. С. 26–29.
19. Требин М. П. Феномен інформаційної війни у світі, що глобалізується. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. Серія : Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 188–198.
20. Требин М. П. Інформація як зброя у «гібридній» війні. *Політичні та правові дисонанси в сучасних українських реаліях*: зб. матеріалів XXX Харківських політологічних читань (м. Харків, 16 червня 2017 р.). Харків: «Право», 2017. С. 70–75.
21. Требин М. П. Інформаційний континуум як поле бою. *Сучасна війна: гуманітарний аспект* : збірник матеріалів VIII Міжнародної наукової конференції Харківського національного університету Повітряних Сил

- імені Івана Кожедуба, 24–25 травня 2024 р. Харків: ХНУПС ім. І. Кожедуба, 2024. С. 30–36.
22. Федотенко К. А. «Інформаційна війна» та «інформаційний фронт»: наукове осмислення понять. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2023. № 3. С. 157–170.
23. Фещенко І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021. Т. 13, № 1. С. 96–103.
24. Фролова М. Е., Козел В. М. Інформаційна війна в цифрову епоху: виклики та загрози для студентської аудиторії. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Психологія*. 2025. Т. 36(75), № 2. С. 126–132.
25. Худолій А. Інформаційна війна 2014–2022 рр.: [монографія] / Нац. ун-т «Остроз. акад.», Ф-т романо-герман. мов, Каф. англ. філології. Острог: Вид-во Нац. ун-ту «Острозька академія», 2022. 207 с.
26. Яцюк О. С. Інформаційна війна як складова частина гібридної війни: метод. посіб. / Центр перепідгот. та підвищ. кваліфікації працівників орг. держ. влади, орг. місц. самоврядування, держ. підприємств, установ і орг. Вінниц. обл. Вінниця : Нілан, 2016. 51 с.
27. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command / U. S. Cyber Command. Fort Meade, MD, 2018. 12 p. URL: <https://www.cybercom.mil/portals/56/documents/uscybercom%20vision%20april%202018.pdf>
28. AJP-3.10. Allied Joint Doctrine for Information Operations. Edition A, Version 1. December 2015 / NATO Standardization Office (NSO). URL: <https://mpsotc.army.gr/wp-content/uploads/2024/03/2.-AJP-3.10-EDA-V1-E.pdf>
29. Bakirov A.; Suleimenov I. Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare. *Computers*. 2025. Vol. 14, Issue 10. Art. 410. DOI: <https://doi.org/10.3390/computers14100410>
30. Chapple M., Seidl D. Cyberwarfare: information operations in a connected world. 2nd ed. Burlington, Massachusetts: Jones & Bartlett Learning, 2023. xxiii, 428 p.
31. CJCSI 3210.01. Joint Information Warfare Policy / Chairman of the Joint Chiefs of Staff Instruction. Washington, D. C. : Joint Chiefs of Staff, 1996. URL: <https://irp.fas.org/doddir/army/fm100-6/ref.htm>.

32. Clark B., Gunzinger M., Sloman J. Winning in the gray zone: using electromagnetic warfare to regain escalation. Washington, DC: Center for Strategic and Budgetary Assessments, 2017. 72 p.
33. Cline L. E. Planning for Strategic Information Operations. *Contemporary Military Challenges*. 2024. Vol. 26, No. 2. P. 9–20. DOI: <https://doi.org/10.2478/cmc-2024-0010>
34. Conduct of the Persian Gulf War : final report to Congress. Washington, DC: Dept. of Defense, 1992. xxxi, 824 p.
35. Cornerstones of Information Warfare / Department of the Air Force ; [S. E. Widnall, R. R. Fogleman]. Washington, D. C., 1995. 11 p. URL: <https://nsarchive.gwu.edu/sites/default/files/documents/4164297/United-States-Air-Force-Cornerstones-of.pdf>
36. Demus A. Operationalizing U. S. Air Force information warfare. Santa Monica, Calif.: RAND Project Air Force, 2024. xiii, 156 p.
37. DoD Directive TS-3600.1. «Information Warfare (U)». December 21, 1992 / U. S. Department of Defense. Washington, D. C., 1992. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_02_Directive_S-3600-1.pdf
38. FM 100–6. Information Operations / Headquarters, Department of the Army. Washington, DC, 1996. vi, 155 p. URL: [https://www.bits.de/NRANEU/others/amd-us-archive/fm100-6\(96\).pdf](https://www.bits.de/NRANEU/others/amd-us-archive/fm100-6(96).pdf).
39. Forest J. J. F. Digital influence mercenaries: profits and power through information warfare. Annapolis, Maryland: Naval Institute Press, 2022. xiii, 245 p.
40. Giammona D. J., Anderson T. The military guide to disarming deception: battlefield tactics to expose the enemy's lies and triumph in truth. Minneapolis, Minnesota: Chosen Books, 2022. 233 p.
41. Goffman E. Frame Analysis: An Essay on the Organization of Experience. Cambridge : Harvard University Press, 1974. ix, 586 p.
42. Grisé M., Demus A., Shokh Y., Kepe M., Welburn J. W., Holynska K. Rivalry in the information sphere: Russian conceptions of information confrontation. Santa Monica, CA: RAND Corporation, 2022. xvi, 138 p.
43. Henschke A. Cognitive warfare: grey matters in contemporary political conflict. London; New York: Routledge Taylor & Francis Group, 2025. xi, 264 p.
44. Info ops: from World War I to the Twitter era / edited by Ofer Fridman, Vitaly Kabernik and Francesca Granelli. Boulder, Colorado: Lynne Rienner Publishers, Inc, 2022. vii, 287 p.

45. Information Operations vs Information Warfare: What is the Difference? *OSavul*. URL: <https://www.osavul.cloud/blog/information-operations-vs-information-warfare>
46. Information Operations. *RAND*. URL: <https://www.rand.org/topics/information-operations.html>
47. Information Warfare and the Future of Conflict. URL: https://threatcasting.asu.edu/sites/g/files/litvpz1036/files/2020-07/threatcasting-2020-The%20Future%20of%20Information%20Warfare-WEB_1.pdf
48. Iraq and Weapons of Mass Destruction : National Security Archive Electronic Briefing Book No. 80 / ed. by J. Richelson. *The National Security Archive*. February 11, 2004. URL: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB80/index.htm>
49. Jensen B. M., Whyte C., Cuomo S. Information in war: military innovation, battle networks, and the future of artificial intelligence. Washington, DC: Georgetown University Press, 2022. xiii, 252 p.
50. Joint Vision 2010. America's Military: Preparing for Tomorrow / Joint Chiefs of Staff. Washington, D. C., 1996. 36 p. URL: <https://apps.dtic.mil/sti/tr/pdf/ADA311168.pdf>
51. Knightley P. The Disinformation Campaign. *The Center for Public Integrity*. October 14, 2001. URL: <https://publicintegrity.org/accountability/the-disinformation-campaign/>.
52. Krieg A. Subversion : the strategic weaponization of narratives. Washington, D. C.: Georgetown University Press, 2023. x, 241 p.
53. Lakoff G. Don't think of an elephant! : know your values and frame the debate : the essential guide for progressives / foreword by Howard Dean; introduction by Don Hazen. White River Junction, Vt.: Chelsea Green Pub. Co., 2004. xvi, 124 p.
54. Lilly B. Russian information warfare: assault on democracies in the cyber wild west. Annapolis, Maryland: Naval Institute Press, 2022. xviii, 291 p.
55. Mallick P. K. Mind wars: the new battlefield of information warfare / foreword by Lt Gen NS Raja Subramani. New Delhi, India: Pentagon Press LLP, 2025. xxii, 277 p.
56. Mann S. R. Chaos Theory and Strategic Thought. *Parameters*. 1992. Vol. 22, No. 1. P. 54–68. DOI: 10.55540/0031-1723.1634.
57. MCM-0085–2010. Military Concept for NATO Strategic Communications / Military Committee Memorandum. Brussels : NATO Headquarters, 2010. 13 p. URL: <https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf>.

58. National security, journalism, and law in an age of information warfare / Marc Ambinder, Jennifer R. Henrichsen, Connie Rosati (Eds.). New York: Oxford University Press, 2024. xxxii, 329 p.
59. Olejnik L. Propaganda: from disinformation and influence to operations and information warfare. Boca Raton, FL: CRC Press, 2025. xvi, 268 p.
60. Paul C., Schwille M., Webber S., Demus A., Van Hegewald E. Organizing for information warfare at the geographic combatant commands: lessons from the United States Central Command joint effects process. Santa Monica, CA: RAND National Defense Research Institute, 2024. xi, 77 p.
61. Plazova T., Kuz O., Konnova N., Korotkov D., Galushchenko O. Information Warfare as an Instrument of Geopolitical Influence on Ukraine: Main Aspects and The State's Response. *International Journal of Religion*. 2024. Vol. 5, No. 2. P. 121–130. DOI: https://doi.org/10.61707/0_g2yt516.
62. Rona T. P. Weapon Systems and Information War. Seattle, WA: Boeing Aerospace Company, 1976. vi, 71 p. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf
63. Russell N. J. An Introduction to the Overton Window of Political Possibility. *Mackinac Center for Public Policy*. January 4, 2006. URL: <https://www.mackinac.org/7504>
64. Schwartz W. Information Warfare: Chaos on the Electronic Superhighway. New York : Thunder's Mouth Press, 1994. 432 p.
65. Schwille M., Welch J., Fisher S., Whittaker T. M., Paul C. Handbook for tactical operations in the information environment. Santa Monica, Calif.: RAND Corporation, 2021. xi, 85 p.
66. Seib P. Information at war: journalism, disinformation, and modern warfare. Cambridge, UK; Medford, MA: Polity Press, 2021. x, 226 p.
67. Singh S. S., Venkatanarayanan A. The art of conjuring alternate realities: how information warfare shapes your world. Noida, Uttar Pradesh, India: HarperCollins Publishers India, 2021. xi, 283 p.
68. Sloss D. L. Tyrants on Twitter: protecting democracies from information warfare. Stanford, California: Stanford University Press, 2022. xvii, 330 p.
69. The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War / Alan D. Campen, contributing editor. Fairfax, Va.: AFCEA International Press, 1992. xxi, 195 p.
70. The world information war: western resilience, campaigning and cognitive effects / edited by Timothy Clack and Robert Johnson. Abingdon, Oxon; New York, NY: Routledge, 2021. xv, 300 p.

71. Vuletić D., Milenković M. R. Information Warfare as an Introduction to Russia-Ukraine Armed Conflict. *Strategic Intersections : The New Architecture of International Security* / Editors Milovan Subotić, Şerban Cioculescu. Belgrade : Vojna štamparija, 2023. P. 185–197. DOI: https://doi.org/10.18485/isimod_strint.2023.ch11

===== 1.2. Трансформація змісту інформаційної боротьби: генезис, форми та методи

Требін Михайло Петрович

доктор філософських наук, професор

професор кафедри міжнародних відносин і політичної філософії

Харківський національний економічний університет імені Семена Кузнеця

Коннова Ніна Олексіївна

кандидат філософських наук, доцент

доцент кафедри міжнародних відносин і політичної філософії

Харківський національний економічний університет імені Семена Кузнеця

Інформаційна боротьба зазвичай розпочинається задовго до перших збройних актів і свідомо спрямована на руйнування духовного світу націй і народів, проти яких ведеться¹. Дослідження генезису інформаційної боротьби засвідчує, що використання інформаційного чинника як асиметричного інструменту протиборства

¹ Див.: Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2022. № 3(54). С. 11–29. DOI: <https://doi.org/10.21564/2663-5704.54.265589>; Калініченко Б. М. Інформаційна війна: чинники ескалації та засоби протидії. Черкаси: Видавець Чабаненко Ю., 2020. 350 с.; Курбан О. Історія становлення та розвитку технологій інформаційних війн. *Вісник Книжкової палати*. 2016. № 4. С. 50–52; Почепцов Г. Г. Сучасні інформаційні війни. Київ: Видавничий дім «Києво-Могилянська академія», 2016. 512 с.; Требин М. П. Информационная война. *Журналіст*. 2000. № 4–5. С. 14–19; Шпига П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326–339.

==== Авторський колектив

Алексєєнко Людмила Михайлівна, доктор економічних наук, професор, професор кафедри управління та адміністрування, Івано-Франківський навчально-науковий інститут менеджменту Західноукраїнського національного університету.

Іванченко Ольга Миколаївна, доктор юридичних наук, доцент, доцент кафедри загальної теорії права та держави, Національний університет «Одеська юридична академія».

Ільницька Уляна Вікторівна, кандидат політичних наук, доцент, доцент кафедри політології та міжнародних відносин, Національний університет «Львівська політехніка».

Квасниця Оксана Василівна, кандидат економічних наук, доцент, доцент кафедри фінансів ім. С. І. Юрія, Західноукраїнський національний університет (м. Тернопіль).

Коннова Ніна Олексіївна, кандидат філософських наук, доцент, доцент кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Копитова Олена Сергіївна, доктор юридичних наук, старший дослідник, доцент кафедри економіко-правових дисциплін Навчально-наукового інституту права і психології, Національна академія внутрішніх справ (м. Київ).

Кравченко Олена Валентинівна, доктор історичних наук, доцент, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Настояща Катерина Василівна, доктор соціологічних наук, доцент, завідувач Центру соціологічних досліджень, Інститут національної стійкості та безпеки; Науково-дослідний інститут українознавства Київського національного університету імені Тараса Шевченка.

Требін Михайло Петрович, доктор філософських наук, професор, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Федіна Наталія Василівна, кандидат юридичних наук, доцент, доцент кафедри адміністративно-правових дисциплін Навчально-наукового інституту права та правоохоронної діяльності, Львівський державний університет внутрішніх справ.

Чернишова Таїсія Олексіївна, кандидат філологічних наук, доцент, доцент кафедри гуманітарних та соціальних дисциплін, Харківський національний університет Повітряних Сил імені Івана Кожедуба.

Чупрій Леонід Васильович, доктор політичних наук, професор, завідувач кафедри політології та соціології, Київський столичний університет імені Бориса Грінченка.

Наукове видання

Алексесенко Людмила Михайлівна,
Іванченко Ольга Миколаївна,
Ільницька Уляна Вікторівна та ін.

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

Монографія

Редактор *Т. О. Чернишова*

Підписано до друку 28.07.2026. Формат 60×84/16.
Ум. друк. арк. 29,4. Обл.-вид. арк. 24. Тираж 100 пр. Зам. № 729

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20

Вебсайт: <https://pravo-izdat.com.ua>

E-mail для замовників послуг: verstka@pravo-izdat.com.ua

E-mail для покупців: sales@pravo-izdat.com.ua

Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт Плюс»,
вул. Весніна, 12, м. Харків, 61023, Україна
Тел. (097) 445-07-79

Вебсайт: <https://promart.in.ua>

Свідоцтво суб'єкта видавничої справи ДК № 8388 від 16.07.2025