

## Features of Modern Information Wars

UDC: 340.12

DOI: <https://doi.org/10.15421/172419>**Larioncheva Nataliia**Ph.D. Student, <https://orcid.org/0009-0000-3605-0163>, [larionchevanatalia@gmail.com](mailto:larionchevanatalia@gmail.com)*Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)*

### Abstract

**Relevance.** The article examines the current issues of modern information warfare, which is an important aspect of political and military conflicts in the modern world. Modern information wars have become an important element of political and military conflicts taking place in the world. The speed of information transmission due to the development of technology and mass communication allows for extensive manipulation of public opinion and influence on domestic and international relations. It is important to have strategies to protect against disinformation and manipulation and to actively resist information interference.

**The purpose** of the study was to reveal current trends in information warfare.

**Results.** Focusing on the use of mass communication technologies, in particular social media, by governmental and atypical groups to spread disinformation and propaganda, the article analyzes strategies for manipulating public opinion and their impact on international relations. The study demonstrates the need to develop effective strategies to protect against information threats and counteract information interference.

**Conclusions.** The role of media and social networks in spreading different narratives and legends that influence the perception of the conflict in Ukraine was discussed. In conclusion, it was noted that protection against information threats requires a comprehensive approach. In addition to technical cybersecurity measures, it is important to develop media literacy, support an independent journalistic environment, and promote transparency in government. International cooperation in the field of cybersecurity is crucial to countering information threats. Common standards, information exchange and cooperation between countries can increase the effectiveness of measures to counter disinformation and cyberattacks.

**Keywords:** information warfare, hybrid warfare, international politics, Ukraine, elections, cyberattacks, social media, propaganda

## Особливості сучасних інформаційних воєн

**Ларіончева Наталія***Київський національний університет імені Тараса Шевченка (Київ, Україна)*

### Анотація

**Актуальність.** Стаття розглядає актуальну проблематику сучасних інформаційних воєн, що є важливим аспектом політичних та військових конфліктів у сучасному світі. Сучасні інформаційні війни стали важливим елементом політичних та військових конфліктів, які відбуваються у світі. Швидкість передачі інформації завдяки розвитку технологій і засобів масової комунікації дозволяє широко маніпулювати громадською думкою та впливати на внутрішні та міжнародні відносини.

**Метою дослідження** стало розкриття сучасних тенденцій прояву інформаційних воєн.

**Результати.** Аналізуючи технологічні нововведення, політичні стратегії та соціокультурні впливи, стаття висвітлює ключові аспекти сучасних інформаційних воєн і розробляє рекомендації щодо збереження демократичних цінностей в епоху цифрової трансформації. Виокремлено значення критичного мислення та перевірки інформації в сучасному медійному середовищі, а також підкреслено важливість відстоювання демократичних цінностей, включаючи свободу слова та доступ до правдивої інформації.

**Висновки.** У висновку було зазначено, що захист від інформаційних загроз потребує комплексного підходу. Крім технічних заходів кібербезпеки, важливо розвивати медійну грамотність, підтримувати незалежне журналістське середовище та сприяти прозорості у владі. Міжнародний співробітництво в області кібербезпеки є вирішальним для протидії інформаційним загрозам. Спільні стандарти, обмін інформацією та співпраця між країнами можуть підвищити ефективність заходів протидії дезінформації та кібератак. Дослідження демонструє необхідність розробки ефективних стратегій захисту від інформаційних загроз та протидії інформаційним втручанням. У висновку було зазначено, що захист від інформаційних загроз потребує комплексного підходу. Крім технічних заходів кібербезпеки, важливо розвивати медійну грамотність, підтримувати незалежне журналістське середовище та сприяти прозорості у владі.

**Ключові слова:** інформаційна війна, гібридна війна, міжнародна політика, Україна, вибори, кібератаки, соціальні мережі, пропаганда

Стаття надійшла / Article arrived: 01.02.2024

Схвалено до друку / Accepted: 29.02.2024

### Вступ.

Сучасні інформаційні війни стали важливим елементом політичних та військових конфліктів, які відбуваються у світі. Швидкість передачі інформації завдяки розвитку технологій і засобів масової комунікації дозволяє широко маніпулювати громадською думкою та впливати на внутрішні та міжнародні відносини. Засоби соціальних мереж, такі як Facebook, Twitter, YouTube, стають ареною для поширення дезінформації та пропаганди. Часто різноманітні урядові та нетипові групи використовують фейкові акаунти та групи, щоб розповсюджувати свої наративи та впливати на громадську думку. Поширення маніпулятивної інформації викликає сумніви та підозри серед громадськості, особливо у тих випадках, коли правдивість інформації стає під сумнів. Важливо мати стратегії захисту від дезінформації та маніпуляцій та активно протистояти інформаційним втручанням. Дослідження сучасних інформаційних воєн допомагає розкрити та розуміти такі аспекти, як технологічні нововведення, політичні стратегії та соціокультурні впливи. Розширення знань у цій області дозволить розробити більш ефективні стратегії протидії інформаційним загрозам та зберегти демократичні цінності в епоху цифрової трансформації.

**Мета дослідження** є розкриття та характеристика сучасних тенденцій прояву інформаційних воєн.

### Аналіз попередніх публікацій.

Слід зауважити, що багато вітчизняних дослідників внесли свій внесок у вивчення даної проблематики. Однак у їхніх дослідженнях не враховано в повній мірі тенденцію стрімкого розвитку цього явища, що призвело до недостатнього вивчення нових явищ, таких як медіа-тероризм. За думкою Георгія Почепцова (Почепцов, 2000), інформаційна цивілізація не зосереджується на діях у фізичному просторі, вона вважає перемогу зафіксованою в інформаційних і віртуальних просторах. М. Лібікі (Libicki, 1995) однією із форм інформаційної війни він називає психологічну. Їх дослідження свідчать про актуалізацію дослідження інформаційних воєн в сучасному світі інформації. М. Маклюен засоби масової комунікації самі називав новими «природними ресурсами», а Т. Рона (Rona, 1976) вважав, що інформаційна інфраструктура є ключовим аспектом економіки, але в той же час вона стає вразливою метою як у військовій, так і в мирній час.

### Результати дослідження.

Сучасна держава стикається з викликом відсутності єдиного централізованого органу, який би мав повний спектр інструментів для ведення ефективного протистояння у сучасних військових конфліктах. Така ситуація значно підвищує важливість вчасного та адекватного аналізу військово-політичної обстановки, розпізнавання військових загроз та вимагає від держави підвищення стандартів

управління та координації дій між державними структурами. У зв'язку з тим, що характер сучасних військових конфліктів постійно змінюється, методи та підходи до аналізу військово-політичної обстановки також повинні еволюціонувати. Зміна характеристик сучасних військових конфліктів та військово-політичних відносин накладає нові вимоги до аналізу, зосереджуючи увагу на нових аспектах та елементах, які необхідно ретельно вивчити для отримання об'єктивних результатів оцінки ситуації. (Бочарніков, & Свешніков, 2017).

Нещодавно науковці відзначають, що сучасні військові конфлікти відрізняються від минулих, оскільки вони набули нових рис і характеристик, що вимагають ретельного аналізу та розуміння. У минулому, стратегія ведення війни базувалася в основному на силовому примусі та прямому військово-політичному протистоянню між сторонами конфлікту. Однак сучасні військові конфлікти виявляють складніші та більш різноманітні характеристики. Виокремлення цих нових рис конфліктів породило такі терміни, як "проксі-війна", "гібридна війна", "мережева війна" (Горбулін, 2014).

Класичні війни в історії відрізнялися від сучасних військових конфліктів, оскільки перед винайденням ядерної зброї вони відбувалися переважно між державами або коаліціями держав із чіткими політичними цілями. Такі конфлікти використовували значні військові формування, наприклад, армії, і політичні цілі формулювалися правлячою елітою кожної держави. Вони в основному зосереджувалися на військових діях, діях з використанням сили.

Поняття проксі-війни описує ситуації, коли конфлікт між двома чи більше сторонами відбувається через підтримку, фінансування або збройну допомогу з боку інших суб'єктів, які не прямо беруть участь у війні. Проксі-війни, з'явилися на тлі розвитку технологій та методів збройної боротьби. Впливові держави ведуть конфлікти не прямо, а через дії своїх "сателітів" - політично підпорядкованих держав або різних внутрішніх збройних формувань, в яких самі держави-домінанти здебільшого надають економічну, інформаційну та іншу підтримку.

Гібридна війна включає в себе поєднання військових, політичних, економічних, інформаційних та інших методів впливу з метою досягнення військових та політичних цілей. Мережева війна описує ситуації, коли конфлікт розгортається у віртуальному просторі, включаючи інформаційні атаки, кібератаки та маніпуляції в мережі Інтернет. Гібридні війни стали типовим явищем у світі глобалізації, де військові дії поступово відступають на другий план перед іншими засобами впливу, такими як економічний тиск, інформаційна пропаганда та спеціальні операції. Головна мета гібридних воєн полягає в досягненні політичних цілей через різноманітні засоби впливу.

Концепція гібридних воєн свідчить про зміну стратегій і тактик у сучасних міжнародних відносинах, де гнучкість та інновації стають ключовими факторами успіху. Термін "гібридна війна" підкреслює поєднання різноманітних воєнних та невоєнних інструментів, адже всі воєнні конфлікти у сучасному світі можна вважати гібридними, оскільки вони використовують весь спектр доступних інструментів. Мережеві війни виникли в епоху широкого доступу до інформаційних технологій, що відкрило нові можливості використання інформаційних засобів для досягнення воєнно-політичних цілей. Ці війни, іноді відомі як мережецентричні, відрізняються від звичайних воєн тим, що вони характеризуються застосуванням нових технологій та методів ведення війни у кібернетичному просторі. (Савин, 2011).

Аналітики Джон Арквіля та Девід Ронфелдт із корпорації "RAND" впровадили цей термін, натхненні ідеями та методами кібернетичної війни, щоб застосувати їх у вирішенні завдань, що раніше вирішувалися виключно за допомогою збройних сил. Вони використали цей термін, щоб визначити новий підхід до розв'язання проблем, який базується на використанні технологій та інформаційних засобів для досягнення стратегічних цілей. (Arquilla, & Ronfeldt, 2001).

Останнім часом науковці та військові експерти активно відзначають еволюцію сучасних військових конфліктів, які різко відрізняються від традиційних. Ця еволюція обумовлена новими рисами і характеристиками, які виникли в контексті глобалізації, технологічного прогресу та соціальних змін. Сучасні конфлікти відзначаються не лише відкритою військовою агресією між державами, але й використанням нових методів та стратегій, спрямованих на досягнення політичних та геополітичних цілей через різноманітні засоби впливу. Однією з таких нових стратегій ведення війни є мережева війна, яка зосереджена на дезорієнтації та зміні уявлень населення противника. У цьому виді війни основний акцент робиться на впливі на психологічний та інформаційний фронт, замість прямої військової агресії. Відмінність мережевої війни полягає в тому, що вона не передбачає примусового підпорядкування, але ставить за мету зміну уявлень та переконань населення, що може призвести до дезорієнтації та ослаблення внутрішньої стійкості противника. Ця концепція передбачає застосування різноманітних інструментів, зокрема інформаційно-психологічних, для формування враження про необхідність або доцільність певних дій чи переконань. Важливо зазначити, що мережева війна може мати як ненасильницький, так і насильницький характер, залежно від мети і цілей, що ставляться перед агресором. У сучасній мережевій війні держава-агресор залучає внутрішні суб'єкти, такі як партії, недержавні організації та інші, а також

може користуватися зовнішніми суб'єктами, такими як держави-сателіти та міжнародні терористичні організації. Враховуючи комплексність цієї стратегії та її великий потенціал впливу на сучасні конфлікти, мережева війна стала об'єктом пильного дослідження як військових експертів, так і політичних аналітиків. (Glenn, 1989).

Інформаційна війна є складним процесом, який включає широкий спектр стратегічних та тактичних дій з метою маніпулювання інформацією та впливу на цільову аудиторію. Основна мета цього виду війни полягає в тому, щоб спонукати цільову аудиторію приймати рішення, що користуються інтересам ініціатора інформаційної кампанії. Інформаційна війна може виникати як міждержавний конфлікт, так і між різними суб'єктами у межах однієї держави чи конфліктуючих сторін. Цей вид війни включає в себе різноманітні стратегії та тактики, такі як збір і аналіз інформації, її подальше поширення через різні канали засобів масової інформації, соціальні мережі та інші канали зв'язку. До цього також можуть відноситися створення та поширення пропагандистських матеріалів, дезінформація, психологічний тиск на цільову аудиторію та інші методи впливу на громадську думку. Важливим аспектом інформаційної війни є розуміння того, що вона може мати далекосяжні наслідки, які важко передбачити. Її вплив може сягати політичної, економічної, соціальної та культурної сфер життя суспільства. Тому аналіз і вивчення методів та тенденцій інформаційної війни стають надзвичайно важливими для розуміння сучасних міжнародних конфліктів та розвитку стратегій безпеки та оборони. (Hong, & Hung, 2022).

Термін "інформаційна війна", що вперше використав Збройні Сили Сполучених Штатів, на сьогодні охоплює широкий спектр технологічних аспектів, що стосуються не лише електронної та кібернетичної сфер, а й управління інформацією та діяльності в комп'ютерних мережах. Він також обіймає заходи з атаки та захисту в цих контекстах. Варіант "інформаційні операції", як використовують його інші військові формування, більш широкий, оскільки, крім технологічних аспектів, акцентує увагу на людських факторах використання інформації. Це охоплює аналіз соціальних мереж, оцінку рішень та аспекти управління й контролю, що включають роль людини в цьому процесі. У цілому, інформаційна війна має на увазі не лише технічні аспекти, але й вплив на поведінку, рішення та перспективи управління. (Stein, 2022).

Згідно з концепцією НАТО, ця війна спрямована на досягнення інформаційної переваги над опонентом, що є ключовим аспектом сучасної воєнної стратегії.

Інформаційна війна, що є одним із ключових аспектів сучасних конфліктів, проявляється у широкому спектрі форм та методів, спрямованих

на маніпуляцію інформацією та вплив на громадську думку. Приглушення телевізійних, інтернет- та радіопередач відбувається з метою порушення зв'язку та поширення дезінформації серед населення. Відключення логістичних мереж створює ускладнення в комунікаціях та обмежує доступ до інформації. Підроблення або перешкоджання ворожих комунікаційних мереж, зокрема в соціальних медіа, відбувається для впливу на громадську думку та створення негативного образу ворога. Операції на фондовій біржі можуть бути саботовані шляхом електронного втручання, витоку конфіденційної інформації або розміщення дезінформації з метою спричинення фінансових турбулентностей. Використання дронів та інших роботизованих систем для спостереження дає можливість здійснювати розвідувальні дії та збирати інформацію з найвіддаленіших територій. Комунікаційний менеджмент включає в себе контроль за розповсюдженням інформації, підтримкою певного іміджу та формуванням позитивного ставлення до власної сторони. Використання синтетичних носіїв інформації дозволяє створювати та поширювати інформаційні продукти, що відповідають конкретним потребам та завданням. Усі ці форми та методи інформаційної війни свідчать про складний характер сучасних конфліктів та необхідність розробки комплексних стратегій захисту та контрзаходів у сфері інформаційної безпеки. (Tyson, & Broad, & Tristan, 2022).

У сфері кіберпростору важливо розглядати два основні аспекти зброї: мережевоцентричну війну та C4ISR, яка включає інтегроване управління, контроль, зв'язок, комп'ютери, розвідку, спостереження та розвідку. Ці концепції стають все більш важливими в умовах постійного розвитку технологій та зміни характеру війни. Мережевоцентрична війна передбачає використання мережевих технологій для координації військових дій та забезпечення комунікації між військовими одиницями. З іншого боку, концепція C4ISR відображає інтеграцію систем управління, зв'язку та розвідки для забезпечення керівництва та контролю в умовах військових операцій.

Поширення дезінформації також відіграє важливу роль у цих інформаційних битвах. Більшість росіян, згідно з проведеними дослідженнями (Hedenskog, & Hjelms, 2020), віддають перевагу отриманню інформації з телебачення, що часто є основним джерелом новин в країні. Проте, серед молодшого покоління спостерігається тенденція користуватися онлайн-джерелами для отримання інформації. Зазначено, що багато молодих росіян звертаються до використання віртуальних приватних мереж (VPN), щоб отримати доступ до незалежних джерел інформації, оскільки вони втратили довіру до державно контрольованих ЗМІ та їхньої спроможності надавати об'єктивну інформацію про події в країні (Nell, 2022).

Пропаганда не обмежується лише російськими кордонами, але і впливає на інші країни. Китайські дипломати, урядові органи та контрольовані державою ЗМІ використовують ситуацію українського конфлікту для поширення пропагандистських ідей та антиамериканських тез. Крім того, вони активно розповсюджують теорії змови, спрямовані на дискредитацію американської політики та внутрішньої ситуації у США, що підштовхується російськими пропагандистськими нарративами (Wong, 2022).

Аналогічні теорії змови та пропагандистські нарративи також виявлені у медіа Куби та Латинської Америки. Крім того, RT Actualidad, медіа-гілка російського пропагандистського агентства RT, активно використовується для поширення дезінформації та пропагандистських ідей про конфлікт в Україні (Wilner, Delgado, & Torres, 2022).

Отже, інформаційна пропаганда та маніпуляція громадською думкою стають все більш актуальними в різних країнах, де цільова аудиторія впливається пропагандистськими нарративами, що впливають на їхнє сприйняття подій в Україні та світі.

У 2022 році урядові групи, що представлялись як незалежні новинні організації, активно використовували соціальні мережі, такі як Facebook, Instagram, Twitter, YouTube, Telegram, а також російськомовні платформи "Однокласники" і "В Контакте", для поширення російських нарративів. Їхні зусилля включали створення фейкових акаунтів та груп, які використовувались для розповсюдження дезінформації та маніпулювання громадською думкою. Одним із ключових елементів цієї стратегії було створення враження про безпорадність українських сил та намагання зім'яти їхню мораль, використовуючи сфабриковані матеріали та відеозаписи.

Згідно з The Washington Post, вже в 2014 році російська військова розвідка (ГРУ) створила понад 30 псевдоукраїнських груп і акаунтів у соціальних мережах, а також 25 "провідних англомовних" видань. Ці акаунти використовувались для розповсюдження дезінформації та провокацій, спрямованих на підірив українського уряду та мобілізацію проросійськи налаштованої аудиторії. (Hedenskog, & Hjelms, 2020).

З іншого боку, на початку 2016 року українські журналісти виявили мережу десятків груп у соціальних мережах, керованих з Москви, які використовували націоналістичну риторику для підірив українського уряду та мобілізації протестувальників. Ці групи активно поширювали проросійську пропаганду та провокативний контент для стимулювання напруги та конфлікту в Україні.

Крім цього, російські оперативники інформаційної війни здійснювали спроби перехоплення повідомлень українських активістів у Facebook, штучно класифікуючи їх як порнографію чи інші порушення правил платформи, щоб дискредитувати діяльність

опозиції та активістів. В реакцію на рішення Facebook і Twitter щодо блокування російських акаунтів і контенту, Росія ухвалила кілька заходів з обмеження доступу до цих платформ на своїй території.

Окремим інструментом інформаційного протистояння стали меми. В кінці лютого 2022 року, в Генічеську, відбулося подія, яка стала символом української вольової боротьби та відданості. На відеозаписі, знятому 25 лютого, зображено літню жінку, яка відверто лає російського солдата і передає йому насіння соняшнику з проханням посадити його, щоб соняшники виростили там, де він знаходиться. Цей емоційний і символічний момент вразив глядачів своєю правдивістю та виразністю, і став своєрідним актом опору проти агресії. (Sharma, 2022).

Легенда про "Привида Києва" також стала предметом широкого обговорення. Цей персонаж, за переказами, був українським пілотом-випробувачем, який, за легендою, збив шість російських літаків. Хоча деякі деталі цієї історії були піддані сумнівам і не підтверджені фактами, вона все ж стала символом героїзму та відваги українського народу.

Не менш вражаючими були відповіді українських захисників на острові Зміїний, а також відеозаписи, де українські фермери буксирують покинуті російські танки. Ці події вразили своєю мужністю та відданістю ідеям свободи та незалежності України. Їхні вчинки стали втіленням давньої боротьби за справедливість та гідність українського народу. (Wilner, Delgado, & Torres, 2022).

#### Висновки.

Стаття висвітлює ряд ключових аспектів інформаційної війни в контексті конфлікту в Україні. Розглянуто різноманітні способи впливу на громадську думку, починаючи від медіа та соціальних мереж і закінчуючи символічними актами громадян. Показано, як пропаганда та різні наративи можуть впливати на сприйняття конфлікту, а також визначено

важливість доступу до об'єктивної інформації в умовах інформаційної війни. Визначено значення критичного мислення та перевірки інформації в сучасному медійному середовищі, а також підкреслено важливість відстоювання демократичних цінностей, включаючи свободу слова та доступ до правдивої інформації.

Ключові позиції:

Сучасні інформаційні війни відіграють ключову роль у глобальному політичному та військовому контексті. З використанням новітніх технологій масової комунікації, вони стали ефективним інструментом впливу на громадську думку, формування дискурсу та маніпулювання відносинами міжнародного співтовариства.

Пропаганда та дезінформація стали ключовими стратегіями інформаційних воєн. Зловживання соціальними мережами та іншими медіа-платформами дозволяє режимам та нетиповим суб'єктам змінювати громадську думку, впливати на рішення та підірвати довіру до демократичних інститутів.

Захист від інформаційних загроз потребує комплексного підходу. Крім технічних заходів кібербезпеки, важливо розвивати медійну грамотність, підтримувати незалежне журналістське середовище та сприяти прозорості у владі.

Міжнародний співробітництво в області кібербезпеки є вирішальним для протидії інформаційним загрозам. Спільні стандарти, обмін інформацією та співпраця між країнами можуть підвищити ефективність заходів протидії дезінформації та кібератак.

Демократичні суспільства повинні активно захищати свободу слова та вільний доступ до інформації. Розуміння загроз інформаційних воєн та розробка стратегій протидії є важливими кроками для збереження демократичних цінностей та стабільності у світі.

## БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

- Бочарніков, В., & Свешніков, С. (2017). Погляди на характер сучасних воєнних конфліктів. *Наука і оборона*, 1, 3-8.
- Горбулін, В. (2014). *«Гібридна війна» як ключовий інструмент російської геостратегії реваншу*. Видавничий центр ЛНУ імені Івана Франка. Retrieved from [www.niss.gov.ua/public/File/2015\\_book/012315\\_Gorbulyn.pdf](http://www.niss.gov.ua/public/File/2015_book/012315_Gorbulyn.pdf)
- Почепцов, Г. (2000). *Информационные войны*. Рефл-бук. К.: Ваклер.
- Савин, Л. (2011). *Сетецентричная и сетевая война. Введение в концепцию*. Евразийское движение.
- Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars. The future of terror, crime, and militancy*. Rand Corporation.
- Glenn, J. (1989). Chapter 9 Defense, (p. 195-201). *The Mind of the Future*. Washington, DC: Acropolis Books.
- Hedenskog, J., & Hjelm, M. (2020). *Propaganda by Proxy: Ukrainian oligarchs, TV and Russia's influence*. Swedish Defense Research Agency, RUFBS Briefing, 48(A112001), 7312.
- Hong, Z.-C., & Hung, Z.-W. (2022). How cognitive warfare works in China: A frontline perspective on Taiwan's wars against disinformation. *Journal of Global Security Studies*, 7(4).
- Libicki, M. C. (1995). *What is Information Warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University. Retrieved from <http://viysko.com.ua/technologiji-voyen/martin-libicki-shho-take-informacijna-vijna/>
- Nell, C. (2022). Here's how propaganda is clouding Russians' understanding of the war in Ukraine. *NPR*. Retrieved from <https://www.npr.org/2022/03/15/1086705796/russian-propaganda-war-in-ukraine>

- Rona, T. P. (1976). Weapon Systems and Information warfare. *Office of the Secretary of Defense Washington DC*. Retrieved from [https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science\\_and\\_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf](https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf)
- Sharma, S. (2022, February). Brave Ukrainian women's tells Russian soldier: 'Put sunflower seeds in your pocket so they grow when you die'. *The Independent*. Retrieved from <https://www.independent.co.uk/news/world/europe/ukraine-russia-soldier-woman-confrontation-b2022993.html>
- Stein, G. J. (2022). *Information Warfare*. Air University (USA). Press.
- Tyson, H., E.-U., & Broad, G., & Tristan, T. H. (2022). Using social media for information divisiveness and warfare. *Proceedings of the 33rd ACM conference on Hypertext and social media, HT '22*, (p. 259-262). New York: Association for Computing Machinery.
- Wilner, M., Delgado, M. A., & Torres, G. N. (2022). Explainer: How Russia's war in Ukraine is shuffling U.S. alliances in Latin America. *Miami Herald*. Retrieved from [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihlJzM4OSEAxVowAIHHWCrCuUQFnoECBUQAQ&url=https%3A%2F%2Fwww.miamiherald.com%2Fnews%2Fnation-world%2Fworld%2Famericas%2Fvenezuela%2Farticle259261614.html&usq=AOvVaw2N\\_2hYGydS7zxBf8PNtH5L&opi=89978449](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihlJzM4OSEAxVowAIHHWCrCuUQFnoECBUQAQ&url=https%3A%2F%2Fwww.miamiherald.com%2Fnews%2Fnation-world%2Fworld%2Famericas%2Fvenezuela%2Farticle259261614.html&usq=AOvVaw2N_2hYGydS7zxBf8PNtH5L&opi=89978449)
- Wong, E. (2022). U.S. Fights Bioweapons Disinformation Pushed by Russia and China. *The New York Times*. Retrieved from <https://www.nytimes.com/2022/03/10/us/politics/russia-ukraine-china-bioweapons.html>

## REFERENCES

- Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars. The future of terror, crime, and militancy*. Rand Corporation.
- Bocharnikov, V., & Sveshnikov, S. (2017). Views on the nature of modern military conflicts. *Science and Defense*, 1, 3-8.
- Glenn, J. (1989). Chapter 9 Defense, (p. 195-201). *The Mind of the Future*. Washington, DC: Acropolis Books.
- Gorbunin, V. (2014). *"Hybrid warfare" as a key tool of the Russian geostrategy of revenge*. Publishing Center of Ivan Franko National University of Lviv. Retrieved from [www.niss.gov.ua/public/File/2015\\_book/012315\\_GorbulyN.pdf](http://www.niss.gov.ua/public/File/2015_book/012315_GorbulyN.pdf)
- Hedenskog, J., & Hjelm, M. (2020). *Propaganda by Proxy: Ukrainian oligarchs, TV and Russia's influence*. Swedish Defense Research Agency, RUFBS Briefing, 48(A112001), 7312.
- Hong, Z.-C., & Hung, Z.-W. (2022). How cognitive warfare works in China: A frontline perspective on Taiwan's wars against disinformation. *Journal of Global Security Studies*, 7(4).
- Libicki, M. C. (1995). *What is Information Warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University. Retrieved from <http://viysko.com.ua/technologiji-voyen/martin-libicki-shho-take-informacijna-vijna/>
- Nell, C. (2022). Here's how propaganda is clouding Russians' understanding of the war in Ukraine. *NPR*. Retrieved from <https://www.npr.org/2022/03/15/1086705796/russian-propaganda-war-in-ukraine>
- Pocheptsov, G. (2000) *Information Wars*. Refl-book. K.: Wackler.
- Rona, T. P. (1976). Weapon Systems and Information warfare. *Office of the Secretary of Defense Washington DC*. Retrieved from [https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science\\_and\\_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf](https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf)
- Savin, L. (2011). *Network-centered and network warfare. Introduction to the concept*. Eurasian Movement.
- Sharma, S. (2022, February). Brave Ukrainian women's tells Russian soldier: 'Put sunflower seeds in your pocket so they grow when you die'. *The Independent*. Retrieved from <https://www.independent.co.uk/news/world/europe/ukraine-russia-soldier-woman-confrontation-b2022993.html>
- Stein, G. J. (2022). *Information Warfare*. Air University (USA). Press.
- Tyson, H., E.-U., & Broad, G., & Tristan, T. H. (2022). Using social media for information divisiveness and warfare. *Proceedings of the 33rd ACM conference on Hypertext and social media, HT '22*, (p. 259-262). New York: Association for Computing Machinery.
- Wilner, M., Delgado, M. A., & Torres, G. N. (2022). Explainer: How Russia's war in Ukraine is shuffling U.S. alliances in Latin America. *Miami Herald*. Retrieved from [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihlJzM4OSEAxVowAIHHWCrCuUQFnoECBUQAQ&url=https%3A%2F%2Fwww.miamiherald.com%2Fnews%2Fnation-world%2Fworld%2Famericas%2Fvenezuela%2Farticle259261614.html&usq=AOvVaw2N\\_2hYGydS7zxBf8PNtH5L&opi=89978449](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihlJzM4OSEAxVowAIHHWCrCuUQFnoECBUQAQ&url=https%3A%2F%2Fwww.miamiherald.com%2Fnews%2Fnation-world%2Fworld%2Famericas%2Fvenezuela%2Farticle259261614.html&usq=AOvVaw2N_2hYGydS7zxBf8PNtH5L&opi=89978449)
- Wong, E. (2022). U.S. Fights Bioweapons Disinformation Pushed by Russia and China. *The New York Times*. Retrieved from <https://www.nytimes.com/2022/03/10/us/politics/russia-ukraine-china-bioweapons.html>