

УДК 316.772.5:004.738.5](043.2)

## АНАЛІЗ НЕФОРМАЛЬНИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**ЮРКОВА Ольга,**

аспірантка, email: [olga.urkova@gmail.com](mailto:olga.urkova@gmail.com)

**СМОЛА Лідія,**

д-р політ. наук, проф., email: [lidsm2010@gmail.com](mailto:lidsm2010@gmail.com)

КІП ім. Ігоря Сікорського, Видавничо-поліграфічний інститут, вул. Академіка Янгеля, 1/37, м. Київ, 03056, Україна.

*У статті розглянуто інформаційно-психологічний компонент російсько-української гібридної війни та стійкість українського суспільства до неформальних комунікацій як складової зовнішніх інформаційних впливів. Виконано стислий огляд досліджень феномена гібридної війни та його особливостей у контексті дій і воєнної думки Російської Федерації. Проаналізовано приклади використання неформальних комунікацій як інструмента інформаційної війни. Результати дослідження підтверджують, що канали неформальної комунікації за певних умов можуть бути використані для нагнітання паніки та провокації загрозливих для державної безпеки наслідків. Зазначається, що необхідно підвищувати стійкість суспільства до цієї категорії гібридних впливів.*

**Ключові слова:** неформальні комунікації, соціальні медіа, гібридна війна, державна безпека, фейкові новини.

### ANALYSIS OF INFORMAL COMMUNICATIONS IN CONDITIONS OF HYBRID WAR

*The article considers the information-psychological component of the Russian-Ukrainian hybrid war and the resilience of Ukrainian society in relation to external information influences, in particular informal communications as their component.*

*A brief overview of the most important research in the study of the phenomenon of hybrid warfare and its features in the context of the actions and military thought of the Russian Federation. Examples of the use of informal communications as a tool of the Russian information war against Ukraine are analyzed.*

*The results of the study confirm that the channels of informal communication under certain conditions can be used to inject panic and provoke threatening consequences for national security. The need to increase society's resilience to this category of hybrid influences is pointed out.*

**Key words:** informal communications, social media, hybrid war, state security, fake news.

**Вступ.** Російська агресія в Криму й на Донбасі та її формальний і неформальний інформаційний супровід підвищили актуальність вивчення науковцями та фахівцями з державної безпеки нетрадиційних, «гібридних» методів ведення збройної агресії. Серед таких методів – здійснення інформаційно-психологічного впливу на суспільство у процесі соціальної комунікації.

Такий вплив включає поширення дезінформації, маніпулювання суспільним та політичним дискурсом, маніпулювання фактами (замовчування одних фактів та підкреслення інших), свідомістю громадян через емоції, натяки, чутки та ін. Засоби неформальної комунікації відіграють особливо небезпечну роль у таких впливах, адже їхня дія є прихованою і її складно проконтролювати на державному рівні або системно відреагувати. Усе це впливає на необхідність дослідження ролі неформальної комунікації у таких впливах, яка наразі є не досить вивченими.

*Актуальність статті* обумовлена необхідністю виявлення та дослідження факторів, що загрожують національній інформаційній безпеці під час гібридної війни,

© Юркова О., Смола Л., 2021

і недостатньою дослідженістю використання неформальних комунікацій як компонента такої війни.

Посилення ролі інформаційних впливів у війнах прогнозував у минулому столітті Є. Месснер, який заявляв, що майбутні війни будуть не за нові землі і ресурси, а за «душу ворожого народу» [1, с. 64].

П. Норд ще 1971 р. зауважив, що внесення ідеології до складу психологічної війни та використання психологічних операцій у мирний час було новацією радянської влади: «Мирного часу ніколи не існує для уряду в Москві» [2].

Ролі інформації у веденні війни торкалися Е. Тоффлер, Ф. Фукуяма, Г. Ласуел та інші [3–6]. Термін «інформаційна війна» застосував А. Даллес 1967 р. [7], згодом – Т. Рона [8]. Останній вважав інформаційну структуру найважливішою частиною економіки й водночас найуразливішою мішенню. Класичними для розуміння концепту гібридної війни є праці Ф. Хоффмана, Дж. Меттіса, М. Калдор, Р. Гленна та ін. [9–15].

Нинішня російська агресія в Україні створює дедалі більші труднощі у визначенні війни. В українському контексті гібридну війну називають об'єднанням у реальному часі численних військових та невійськових урядових засобів у конфлікті. Але ефективне їх використання, аргументує Б. Перрі, врешті залежить від вдалих інформаційних операцій, які супроводжуються організованими спеціальними операціями, що провадять нетрадиційну війну. Він також зазначає, що російські інформаційні операції відіграли ключову роль для забезпечення окупації Криму та стрімкого просування на Донбас [16, с. 8].

Погляди на гібридну війну в сучасній російській військовій думці окреслені в статті начальника генштабу ЗС РФ В. Герасимова, відомий як «доктрина Герасимова» [17]. С. Чекінов та С. Богданов розширили його думку про важливість у ній інформаційних операцій [18]. І. Панарін постулював, що останні є вкрай вагомими для геополітичних кампаній, особливо для Росії, яка постійно зазнає нападів США та Заходу в інформаційній сфері, відтак «потребує захисту» [19]. Його бачення було широко підтримане іншими російськими стратегічними аналітиками. Зокрема, А. Дугін, підсилюючи тези І. Панаріна, радить Кремлю створити «євразійську мережу», аби «перевернути» західні інформаційні операції [20–21]. У цьому контексті РФ активно розвиває концепцію «рефлексивного контролю», вперше розроблену В. Лефевром у 1960-х рр., яка надалі постійно вдосконалюється [22].

Особливості гібридної війни Росії проти України активно вивчають як західні (Т. Томас, М. Галеотті, П. Померанцев і М. Вейс, Й. Дарчевська та ін.), так і українські (Г. Почепцов, В. Горбулін, С. Магда, О. Сальнікова, М. Белесков, О. Сищук та ін.) дослідники [22–31].

Низка досліджень сфокусовані на ролі соціальних медіа в гібридній війні (С. Светока, Дж. Вітер, К. Чівіс, А. Хунтінен і Дж. Рантапелконен та ін.) [32–35].

Попри окремі спроби, невирішеною частиною загальної проблеми залишається розробка дієвих рекомендацій, що забезпечать від шкідливих інформаційних впливів через посередництво соціальних медіа.

*Метою статті* є доведення тези про те, що інформаційні впливи, здійснені через сучасні канали неформальної комунікації, потенційно несуть шкідливі для державної безпеки наслідки.

*Завдання дослідження:* узагальнити результати наукових та практичних розвідок щодо ролі неформальних комунікацій серед інших засобів інформаційно-психологічного впливу в контексті гібридної війни, вказати на основні їхні форми, проаналізувати їхнє практичне застосування на прикладі, оцінити спроможність України протистояти таким впливам, використовуючи метод експертних оцінок, й окреслити перспективи подальшого вивчення порушеної проблеми.

*Об'єктом дослідження* є соціальні комунікації у контексті російсько-української гібридної війни. *Предмет наукового пошуку* – неформальні комунікації як чинни-

ки шкідливих інформаційних впливів, які здійснюються через посередництво таких сучасних каналів комунікації, як соціальні мережі та месенджери.

**Методи дослідження.** Для досягнення цілей дослідження використано комплекс взаємопов’язаних методів наукових досліджень. Основні теоретичні методи, що використовуються в розвідці, – критичний аналіз поточних наукових праць з обраної теми та синтез основних висновків у комплексне системне бачення.

Додатковими теоретичними методами, які були використані в дослідженні, є термінологічний аналіз для визначення ключових понять гібридної війни, інформаційно-психологічних впливів та неформальних комунікацій як їх частини; метод case study – для вивчення одного з останніх випадків використання неформальних комунікацій як засобу гібридної війни.

Емпіричний метод, використаний у дослідженні, – це якісний аналіз інтерв’ю з 6 українськими медіаекспертами. Дані, отримані під час інтерв’ю, ґрунтуються на особистій оцінці експерта. Критерієм відбору учасників був їхній дослідницький досвід у сфері протидії дезінформації.

**Результати й обговорення.** Як зазначає Р. Гленн, «конфлікт ХХІ ст. характеризується... гібридними війнами». Гібридна війна, на думку дослідника, – це військова стратегія, яка використовує політичне протистояння та поєднує звичайну, нерегулярну та кібервійну з іншими методами впливу, такими як фейкові новини, дипломатія, війни за допомогою законів та іноземне втручання у вибори [14, с. 73].

Більшість науковців, що досліджували гібридні війни, базують свої роботи на досвіді Ліванської війни 2006 р. [9; 14; 33], тому розглядають гібридну війну насамперед як таку, яку провадять недержавні суб’єкти [9; 14; 25; 33], наприклад, «Хезболла» в контексті війни з Ізраїлем. Ф. Хоффман зазначає, що гібридна війна може вестись як державними, так і недержавними акторами і включає звичайні можливості, нерегулярні тактику та формування, терористичні акти, зокрема «невибіркове насильство» та примус, «злочинні заворушення» [9]. Б. Перрі називає агресію Росії в Україні першим прикладом такої війни, що ведеться саме державою [16].

Ф. Карбер пропонує схему гібридної війни, яка складається з чотирьох компонентів, що розташовані в порядку від малоінтенсивних і прихованих до високоінтенсивних і таких, які держава-агресор провадить відкрито: «політична диверсія», «Проху Sanctum», «втручання» та «примусове стримування». Інформаційні операції у цій системі належать до «політичної диверсії», яка розташована на початку цього спектра і є прихованим впливом держави-агресора. Сюди ж відносять саботаж, тероризм, замах на життя, засилання агентів та захоплення урядових будівель. Під «Проху Sanctum» мається на увазі залучення підрозділів Сил спеціальних операцій (ССО) до нетрадиційної війни. Втручання включає в себе кібератаки, погрози й підготовку до вторгнення, вогневу та ресурсну підтримку, напади на ізольовані урядові сили тощо. До засобів примусового стримування відносять публічні розмови про ядерну потужність, низькі польоти літаків та демонстрацію сили, розгортання потужних ракет «земля-земля», натяки на ескалацію конфлікту тощо [36, с. 4].

Ключову роль у розумінні позиції РФ відіграє «доктрина Герасимова». Начальник Генерального штабу Збройних сил Російської Федерації В. Герасимов говорить про зростання ролі невоєнних засобів, які «в багатьох випадках перевищували силу зброї за ефективністю» [17]. С. Чекінов та С. Богданов постулюють, що інформаційна війна поряд з ООС та скоординованою ескалацією буде ключовою в майбутніх конфліктах і «значною мірою створить основу для перемоги. Жодної мети не буде досягнуто..., якщо один із тих, хто воює, не отримає інформаційну перевагу над іншим» [18, с. 17].

І. Панарін перелічує вісім компонентів інформаційних операцій: «соціальний контроль», «соціальне маневрування», «дезінформація», «вигадування інформації» та «маніпулювання інформацією», «лобіювання», «шантаж» та «вимагання бажанної інформації» [19].

Рефлексивний контроль А.Дугін окреслює як передачу партнеру або опоненту навмисне підготовлених даних, які схиляють його до ухвалення потрібного ініціатору рішення. Серед методів він називає заохочення, шантаж силою, маскування та дезінформацію [20–21].

Б. Перрі поділяє російські інформаційні операції в Україні, що сприяли окупації Криму та Донбасу, на три групи: 1) попередня російська „гуманітарна” зовнішня політика, 2) проросійські ЗМІ в Україні та 3) глобальні проросійські ЗМІ, спрямовані на Захід. Він зазначає, що такі операції діяли узгоджено з Силами спеціальних операцій (ССО). Багато країн давно практикували пропаганду, ССО, економічну війну та інші елементи гібридної війни. А втім, Росія одна з перших застосовує їх одночасно й скоординовано проти іншої держави. По суті, такі операції приховують воєнний характер російської агресії [16].

Інформаційно-психологічний вплив на суспільство включає стратегічну розробку, а також тактичне й оперативне виконання комунікаційних планів, що допомагають країні-агресору досягти цілей. Серед них – радикалізація, зменшення рівня довіри в суспільстві, зневіра громадян і, як наслідок, низька критичність у сприйнятті ворожих наративів. Це допомагає створити бажану для агресора громадську думку та обмежити суспільні уявлення про вибір варіантів допустимих дій набором опцій, вигідних агресору.

Для такого впливу характерні висока емоційність, вірусний потенціал інформації, підвищена конфліктність і відсутність етичних та ціннісних рамок [31].

Для досягнення цієї мети використовуються як формальні, так і неформальні канали поширення інформації, що надає комунікації відповідного характеру. Формальна комунікація має форму текстів або сюжетів і передається за посередництва певного технічного каналу поширення інформації на зразок засобів масової інформації, політичних заяв, документів тощо. Неформальна – здебільшого усна комунікація, наприклад, чутки, плітки, анекдоти, пісні, інколи записані, але які поширюються поза офіційними дискусіями. У сучасних умовах, коли соціальні медіа стали одним з основних каналів комунікації, до неофіційної комунікації додалися чутки в соцмережах та месенджерах, відео, меми тощо. Їх активно застосовують для впливу на погляди та настрої цільових аудиторій і підштовхування їх до бажаних дій [32–35].

Яскравим прикладом неформального гібридного впливу є провокації громадських заворушень на початку пандемії COVID-19. 20 лютого 2020 р. 94 людини, евакуйовані з китайського Уханя, поселили на обсервацію в селищі Нові Санжари Полтавської області. Місцеві жителі зі страху заразитися влаштували акцію протесту, зокрема заблокували дорогу й чинили опір правоохоронцям. Постраждали дев'ять поліцейських та одна цивільна особа. 13 учасників отримали підозри у скоєнні злочинів, пов'язаних із груповим порушенням громадського порядку. Усі евакуйовані згодом виявилися здоровими.

Про ситуацію написали світові медіа. Також вона спричинила інформаційну хвилю – багато користувачів Facebook написали, що їм соромно за жителів Нових Санжар. Цей наратив «сорому» поширювали також російські й проросійські медіа та блогери.

Журналістське розслідування виявило, що центром нагнітання паніки стали соціальні медіа. Зокрема, провокативні дописи було поширено через соціальну мережу «Facebook» та групи в месенджері «Viber». Уперше про приїзд евакуйованих повідомив о 10.00 19 лютого у Facebook колишній депутат, відомий проросійськими поглядами. Потім інформацію синхронно поширили на місцевих Facebook-сторінках та в Instagram-акаунтах. Після 19.00 у Viber почали створюватися спільноти, до яких долучилися тисячі жителів Полтавської області. В одному з таких чатів кожні 10–20 хв поширювали неправдиві чутки та заклики до агресивного спротиву: пе-

регороджувати дороги, залізницю, робити коктейлі молотова, спалити госпіталь та атакувати місцеві адміністрації. Поступово чутки набували емоційних подробиць, що мали провокувати страх. Найактивнішими були 20 користувачів, які також закликали дивитися проросійські телеканали «112», «NewsOne», «ZIK» і «НАШ». Журналісти встановили, що адміністратори не є місцевими жителями і, можливо, за припущеннями авторів, пов’язані зі спецслужбами РФ, що дозволило їм отримати номери телефонів жителів селища (адже в чат за день було додано 6 тис. людей при тому, що в селищі живе понад 8 тис.).

Спільнота радила підписуватись на анонімні проросійські канали в Telegram, які поширювали подібні панічні меседжі, що свідчить про можливу координацію [37]. Згодом журналісти простежили вплив цих Telegram-каналів на рішення депутатів партії «Слуга народу», яка має більшість у парламенті [38].

Таких спільнот було створено декілька, і вони охопили суттєву частину населення Нових Санжар.

Офіційної інформації про вибір Нових Санжар для евакуації 19 лютого не було. Голова селищної ради та інші представники влади заявили, що дізналися про це із чуток в інтернеті. Фактично, шкідливі чутки заповнили вакуум достовірної інформації. Прем’єр-міністр згодом пояснив відсутність офіційної комунікації турботою про безпеку евакуйованих.

Експертні оцінки, надані фахівцями з інформаційної безпеки, зокрема Р.Шутовим, Н.Лігачовою, свідчать, що Росія у своїй інформаційній політиці працює на поляризацію й розкол цільових суспільств, добираючи інструменти тиску, розбрату й ті болючі теми, які є в кожній конкретній державі або цільовій групі.

Ситуація в Нових Санжарах показала, що держава не готова реагувати на інформаційні виклики, що зумовлені не лише зовнішнім впливом, а й низькою якістю комунікації всередині країни.

Будь-які стратегії, спрямовані на протидію дезінформації, є обмеженими, адже гібридна війна, яку Кремль веде проти України, передбачає широкий спектр інструментів. Дезінформація є лише маленькою їх частиною. Найнебезпечнішими є інструменти, що не передбачають дезінформацію як таку:

- маніпулювання суспільним та політичним дискурсом;
- маніпулювання свідомістю реципієнтів через натяжки та емоції;
- маніпулювання з правдою – поширення вибіркової правди, коли якісь факти замовчують, натомість інші підкреслюються. При цьому інформація є правдивою, але подана так, щоб призводити до хибних висновків.

Що кращими є урядові комунікації, то менше залишається місця для маніпуляцій та інформаційних спецоперацій. Важливу роль у стійкості до таких впливів відіграє також рівень медіаграмотності населення.

Висновки та перспективи. Каналом для поширення дезінформації щораз більше стають не лише класичні медіа, а й соціальні мережі та месенджери, де немає регулювання й законодавчих обмежень, а інформація поширюється блискавично. При цьому вона часто не є неправдивою, але її подання впливає на формування потрібної агресору реакції, а відтак – на ухвалення рішень, вигідних для маніпуляторів. Тому розуміння можливих наслідків поширення чуток часто є так само важливим, як і оцінка їхньої достовірності.

Тож варто розвивати прямі засоби протидії дезінформації й окремим фейкам і наративам (наприклад, шляхом законодавчих обмежень або санкцій), але не зупинятися на цьому. Необхідно також просувати власні наративи й налагоджувати урядові стратегічні комунікації, що включають політику «єдиного голосу». Третій важливий напрямок роботи – просвіта й популяризація медіаграмотності, а також запровадження її в освітні програми. За цими напрямками необхідно працювати комплексно. Жоден окремо не здатен повністю розв’язати проблему.

Питання щодо використання неформальних комунікацій як інформаційної зброї в умовах гібридної війни не є достатньо розробленим. Відтак видається перспективним подальше вивчення цього явища з метою покращення його розуміння та впровадження політик, спрямованих на комплексну протидію цьому різновиду інформаційних впливів.

1. Хочешь мира, победы мятежевойну! Творческое наследие Е. Э. Месснера. Москва : Военный университет, 2005. 696 с.
2. Nord P. L'intoxication: Arme Absolue De La Guerre Subversive. Paris : FeniXX, 1971. 456 p.
3. Toffler A. The Third Wave. Vol. 484. New York : Bantam books, 1980. 544 p.
4. Toffler A., Toffler H. War and anti-war: Survival at the dawn of the 21st century. Boston : Little Brown&Co, 1993. 302 p.
5. Fukuyama F. The Great Disruption: Human Nature and the Reconstitution of Social Order. New York : The Free Press, 1999. 354 p.
6. Lasswell H. D. Propaganda technique in world war I. Vol. 170. Cambridge, MA : MIT Press, 1971. 268 p.
7. Dulles A. The secret surrender. New York : Harper&Row, 1966. 268 p.
8. Rona T. P. Weapon Systems and Information War. Seattle, WA : Boeing Aerospace Co., 1976. 86 p.
9. Hoffman F. G. Conflict in the 21st century: The rise of hybrid wars. Arlington, WA : Potomac Institute for Policy Studies, 2007. 72 p.
10. Hoffman F. G. Hybrid warfare and challenges. Joint Force Quarterly. Washington, DC, 2009. Vol.52. Pp. 34–48.
11. Hoffman F. G. Further Thoughts on Hybrid Threats. Small Wars Journal. 2009. March, 3. Pp.1–4. URL: <https://smallwarsjournal.com/blog/journal/docs-temp/189-hoffman.pdf> (дата звернення 13.09.2021).
12. Kaldor M. In Defence of New Wars. Stability: International Journal of Security and Development. Bradford, 2013. Vol. 2, No. 1: 4. Pp.1–16.
13. Mattis J. N., Hoffman F. Future warfare: The rise of hybrid wars. Proceedings -United States Naval Institute. 2005. Vol. 131 (11), No.18. Pp.1–2. URL: <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf> (дата звернення:13.09.2021).
14. Glenn R. W. All glory is fleeting: Insights from the Second Lebanon War. Santa Monica, CA : RAND National Defense Research Institute, 2012. 122 p.
15. Maigre M. Nothing new in hybrid warfare: the Estonian experience and recommendations for NATO. Washington, DC : German Marshall Fund of the United States, 2015. 8 p.
16. Perry B. Non-linear warfare in Ukraine: The critical role of information operations and special operations. Small Wars Journal. McLean, VA, 2015. No. 14. Pp.1–30.
17. Герасимов В. Ценность науки в предвидении. Военно-промышленный курьер. 2015. № 8 (476). URL: <https://vpk-news.ru/articles/14632> (дата звернення: 13.09.2021).
18. Чекинов С. Г., Богданов С. А. О характере и содержании войны нового поколения. Военная мысль. 2013. № 10. С.13–24.
19. Панарин И. Н. Информационная война за будущее России. Москва : Горячая линия-Телеком, 2008. 256 с.
20. Дугин А. Г. Четвертая политическая теория. СПб : Амфора, 2009. 343 с.
21. Дугин А. Г. Геополитика постмодерна. Времена новых империй. Очерки геополитики XXI века. СПб : Амфора, 2007. 382 с.
22. Thomas T. Russia's reflexive control theory and the military. Journal of Slavic Military Studies. Philadelphia, PA, 2004. No. 17(2). Pp. 237–256.
23. Galeotti M. "Hybrid war" and "little green men": How it works, and how it doesn't". Ukraine and Russia: People, politics, propaganda and perspectives. Bristol, 2015. Pp.160–167.
24. Pomerantsev P., Weiss M. The menace of unreality: How the Kremlin weaponizes information, culture and money. New York : Institute of Modern Russia, 2014. 41 p.
25. Darczewska J. The anatomy of Russian information warfare. The Crimean operation, a case study, Warsaw : Ośrodek Studiów Wschodnich im. Marka Karpia, 2014. 37 p.
26. Почепцов Г. Информационные войны. Новый инструмент политики. Киев : Litres, 2018. 256 с.

27. Горбулін В. П. Світова гібридна війна: український фронт : монограф. / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.
28. Магда Є. В. Виклики гібридної війни: інформаційний вимір. Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine, 2014. № 5. С. 138–142.
29. Сальнікова О. Ф., Іващенко, А. М., Сівоха, І. М. Застосування рефлексивного управління в стратегічних комунікаціях для протидії загрозам гібридного характеру. Social development & Security. Т. 9, № 5. С. 16–22.
30. Белесков М. М. Сучасний російський спосіб ведення війни: теоретичні основи і практичне наповнення : аналіт. доп. Київ : НІСД, 2021. 29 с.
31. Сищук О. А. Інформаційно-психологічний компонент «гібридної війни». Україна в системі змін парадигми світопорядку ХХ–ХХІ століть. Київ : Ун-т ім. Б. Грінченка, 2015. С.143–147.
32. Svetoka S. Social media as a tool of hybrid warfare. Riga : NATO Strategic Communications Centre of Excellence, 2016. 49 p.
33. Wither J. K. Making sense of hybrid warfare. Connections QJ. 2016. Vol.15, No. 2. Pp. 73–87. URL: <http://connections-qj.org/article/making-sense-hybrid-warfare> (дата звернення 13.09.2021).
34. Chivvis C. S. Understanding Russian “Hybrid Warfare”. Santa Monica, CA : Rand Corporation, 2017. 12 p.
35. Huhtinen A. M., Rantapelkonen, J. Disinformation in hybrid warfare: The rhizomatic spread of social media in the spamosphere. Journal of Information Warfare. Luray, VA, 2016. Vol.15, No. 4. Pp. 50–67.
36. Karber P. A. Russian Style Hybrid Warfare. McLean, VA : The Potomac Foundation, 2015. 8 p.
37. Величко Л. Майстри паніки. Як проросійська мережа в Україні організувала бунт в Нових Санжарах. URL: <https://texty.org.ua/articles/100356/specoperaciya-imeni-portnovata-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-hto-za-cum-stoyit/> (дата звернення: 13.09.2021).
38. Величко Л. “Телега” для Слуги. Як Телеграм-канали, що ймовірно ведуться з Росії, впливають на роботу Ради. URL: <https://texty.org.ua/articles/101438/tyelyeha-dlya-sluhy-yak-telegram-kanaly-sho-jmovirno-vedutsya-z-rosiyi-vplyvayut-na-robotu-rady/> (дата звернення: 13.09.2021).
1. Want pease? Defeat the mutiny war: the creative heritage of E.E.Messner (2005), Voennyi Universitet, Moscow, 696 p.
2. Nord, P. (1971), L’intoxication: Arme Absolue De La Guerre Subversive. FeniXX, Paris, 456 p.
3. Toffler, A. (1980), The Third Wave (Vol. 484), Bantam books, New York, 544 p.
4. Toffler, A., & Toffler, H. (1993), War and anti-war: Survival at the dawn of the 21st century, Little Brown&Co, Boston, 302 p.
5. Fukuyama, F. (1999), The Great Disruption: Human Nature and the Reconstitution of Social Order, The Free Press, New York, 354 p.
6. Lasswell, H.D. (1971), Propaganda technique in world war I (Vol. 170), MIT Press, 268 p.
7. Dulles, A. (1966), The secret surrender, Harper&Row, New York, 268 p.
8. Rona, T.P. (1976), Weapon Systems and Information War, Boeing Aerospace Co., Seattle, WA, 86 p.
9. Hoffman, F.G. (2007), Conflict in the 21st century: The rise of hybrid wars, Potomac Institute for Policy Studies, Arlington, 72 p.
10. Hoffman, F.G. (2009), “Hybrid warfare and challenges”, Joint Force Quarterly, vol. 52, pp. 34–48.
11. Hoffman, F.G. (2009), “Further Thoughts on Hybrid Threats”, Small Wars Journal, March, 3, available at: <https://smallwarsjournal.com/blog/journal/docs-temp/189-hoffman.pdf> (accessed 13 September 2021).
12. Kaldor, M. (2013), “In Defence of New Wars”, Stability: International Journal of Security and Development, vol. 2, no. 1: 4, pp.1–16.
13. Mattis, J., & Hoffman, F. (2005), ”Future warfare: The rise of hybrid wars”, Proceedings-United States Naval Institute, vol. 131(11), no.18, available at: <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf> (accessed 13 September 2021).

14. Glenn, R.W. (2012), *All glory is fleeting: Insights from the Second Lebanon War*, RAND National Defense Research Institute, Santa Monica, CA, 122 p.
15. Maigre, M. (2015), *Nothing new in hybrid warfare: the Estonian experience and recommendations for NATO*, German Marshall Fund of the United States, Washington, DC, 8 p.
16. Perry, B. (2015), "Non-linear warfare in Ukraine: The critical role of information operations and special operations", *Small Wars Journal*, no. 14, pp. 1–30.
17. Gerasimov, V. (2013), "The value of science in prediction". *Voyenno-promyshlennyy kuryer [Military-Industrial Kurier]*, no. 27, available at: <https://vpk-news.ru/articles/14632> (accessed 13 September 2021).
18. Chekinov, S.G. & Bogdanov, S.A. (2013), "The nature and content of a new-generation war", *Voyennaya mysl [Military thought]*, no. 4, pp.13–24.
19. Panarin, I.N. (2008), *Information war for russia's future*, Goryachaya liniya-Telekom, Moscow, 256 p.
20. Dugin, A.G. (2009), *Fourth Political Theory. Russia and Political Ideas of the 20th Century*, St. Petersburg, Amfora, 343 p.
21. Dugin, A.G. (2007), *Postmodern Geopolitics*, St. Petersburg, Amfora, 382 p.
22. Thomas, T. (2004), "Russia's reflexive control theory and the military", *Journal of Slavic Military Studies*, no. 17(2), pp.237–256.
23. Galeotti, M. (2015), "Hybrid war" and "little green men": How it works, and how it doesn't". *Ukraine and Russia: People, politics, propaganda and perspectives*, pp.160–167.
24. Pomerantsev, P. & Weiss, M. (2014), *The menace of unreality: How the Kremlin weaponizes information, culture and money*, Institute of Modern Russia, New York, 41 p.
25. Darczewska, J. (2014), *The anatomy of Russian information warfare. The Crimean operation, a case study*, Ósrodek Studiów Wschodnich im. Marka Karpia, Warsaw, 37 p.
26. Pocheptsov, G. (2018), *Information wars. New policy tool*, Litres, Kyiv, 256 p.
27. Gorbulin, V.P. (2017), *World hybrid war: Ukrainian front: monograph*, NISD, Kyiv, 496 p.
28. Magda, Y.V. (2014). "Challenges of hybrid warfare: information dimension", *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*, vol. 5, pp.138–142.
29. Salnikova, O.V., Ivashchenko, A.M., & Sivokha, I.M. (2019), "Application of reflexive control in strategic communications for counteraction to threats of hybrid character", *Social development & Security*, vol. 9, no. 5, pp. 133–142.
30. Bielestov, M.M. (2021), *Modern Russian way of waging war: theoretical foundations and practical content: an analytical report*, NISS, Kyiv, 29 p.
31. Syshchuk, O.A. (2015), *Information and psychological component of the «hybrid war», Ukraine in the system of paradigm changes of the world order of the XX-XXI centuries*, Un-t im. B. Grinchenka, Kyiv, pp.143–147.
32. Svetoka, S. (2016), *Social media as a tool of hybrid warfare*, NATO Strategic Communications Centre of Excellence, Riga, 49 p.
33. Wither, J.K. (2016), "Making sense of hybrid warfare", *Connections*, vol. 15, no. 2, pp.73–87.
34. Chivvis, C.S. (2017), *Understanding Russian "Hybrid Warfare"*, Rand Corporation, Santa Monica, CA, 12 p.
35. Huhtinen, A.M., & Rantapelkonen, J. (2016). "Disinformation in hybrid warfare: The rhizomatic speed of social media in the spamosphere", *Journal of Information Warfare*, vol. 15 no. 4, pp. 50–67.
36. Karber, P.A. (2015), *Russian Style Hybrid Warfare*, The Potomac Foundation, McLean, VA. 8 p.
37. Velychko, L., «Masters of panic. This is how the pro-Russian network in Ukraine organized a riot in Novi Sanzhary» [in Ukrainian], available at: <https://texty.org.ua/articles/100356/specoperaciya-imeni-portnova-ta-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-hto-zachym-stoyit/> (accessed 13 September 2021).
38. Velychko, L., «Telega» for the Servant. This is how Telegram channels, presumably from Russia, affect the work of the parliament» [in Ukrainian], available at: <https://texty.org.ua/articles/101438/tyelyeha-dlya-sluhy-yak-telehram-kanaly-sho-jmovirno-vedutsya-z-rosiyi-vplyvayut-na-robotu-rady/> (accessed 13 September 2021).



UDC 316.772.5:004.738.5](043.2)

## **ANALYSIS OF INFORMAL COMMUNICATIONS IN CONDITIONS OF HYBRID WAR**

**Yurkova Olga**, PhD student, e-mail: olga.urkova@gmail.com

ORCID: <https://orcid.org/0000-0002-9282-866X>

**Smola Lydiya**, D. Sc. (Political Science), Professor, e-mail: lidsm2010@gmail.com

ORCID: <https://orcid.org/0000-0001-8145-1046>.

Igor Sikorsky Kyiv Polytechnic Institute, the Publishing and Printing Institute, 1/37, Akademika Yangelya St., Kyiv, 03056, Ukraine.

**Introduction.** Informal communication means play a dangerous role in psychological influences conducted as a part of hybrid warfare as it is covert and difficult to identify. This raises the problem of counteracting them. The paper attracts attention to the peculiarities of using informal communications in a context of Russian-Ukrainian information war.

**Relevance and purpose.** The purpose of the study is to summarize the results of research on the role of informal communication as the mean for hybrid war and to analyze their practical application by example. The relevance is due to the need to identify and explore the factors threatening the national information security during the hybrid war.

**Methodology.** The main methods used in the study are critical analysis and synthesis. The additional methods are the terminological analysis; the case study method and the qualitative analysis of interviews with 6 Ukrainian media experts.

**Results.** As a result of the study is established that the purpose of information influence on society includes, first of all, radicalization, a decrease in the level of trust, and, as a consequence, low criticism in the perception of hostile narratives. To achieve this goal, both formal and informal information channels are used. To informal ones rumors on social networks and messengers have been added in modern conditions. A striking example of informal hybrid influence is the provocation of public unrest at the beginning of the COVID-19 pandemic in the town of Novi Sanzhary, Poltava region, on February 20, 2020. One of the main reasons for the situation was the lack of quality official communication.

**Conclusions.** The work has led us to conclude that not only classic media, but also social networks and messengers are becoming more and more a channel for spreading disinformation. There are no regulations and legal restrictions, and information is spread in a real time there. In this case, it is often not untrue, but its presentation shapes the reaction desired by the aggressor, and, hence, leads to the decisions that are beneficial to the manipulators. So, understanding the possible consequences of spreading rumors is often as important as assessing their veracity.

**Key words:** *informal communications, social media, hybrid war, state security, fake news.*

Стаття надійшла до редакції 14.09.2021.