УДК 351:347.132.15

Колодка Андрій

ORCID iD 0000-0002-9319-331X
e-mail: edjbar2909 @gmail.com

КРИЗОВЕ УПРАВЛІННЯ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

https://doi.org/10.33269/2618-0065-2022-2(12)-75-86

Анотація. Стійке функціонування суспільства в умовах інформаційних викликів під час повномасштабної російсько-української війни є ключовою умовою забезпечення громадянської безпеки. Проведення методичних та наукових досліджень з цього питання дає змогу отримати передовий досвід антикризового менеджменту. Відповідно науковим завданням є теоретичне обґрунтування складових розвитку кризового менеджменту від гібридного протистояння до повномасштабної війни та їх характеристики. В основу аналізу механізму державного антикризового управління покладено інформаційну протидію як його основний важіль та обґрунтовано його суттєві характеристики. Можна стверджувати, що проблема управління кризою внаслідок повномасштабної війни недостатньо досліджена вітчизняними та зарубіжними вченими. Основний акцент було зроблено на антикризовому управлінні в умовах гібридної війни як складовій заходів реагування на виникнення кризи. Методами дослідження були контент-аналіз, гіпотетичний та загальнонауковий. На підґрунті аналізу попередніх наукових розвідок визначено проблемні питання державного управління у сфері інформаційної протидії, зокрема елементи антикризового менеджменту. Опрацьовано питання щодо організації інформаційної взаємодії органів державного управління під час повномасштабної війни, врегулювання кризових ситуацій в умовах повномасштабної війни, вжиття відповідних заходів для своєчасного реагування. Проведене дослідження є теоретичним підтвердженням гіпотези про те, що інформація є основою ухвалення антикризових управлінських рішень і ключовим фактором безпеки держави. Аналіз системи антикризового управління показує, що одна зі складових діяльності органів управління спрямована на організацію та підтримку важливих систем життєзабезпечення. Значну увагу приділено також системі методичних та організаційних проблем протидії у сфері інформаційного забезпечення.

Ключові слова: російсько-українська війна, кризове управління, державне управління, інформаційна безпека.

Проблема дослідження. Сучасні війни, які ведуться через європейські кордони, підривають звичний статус безперервного миру та безпеки континенту. Війна в Україні не лише породжує

класичні загрози безпеці сусідніх держав, уважний спостерігач помітить нову, нетрадиційну, діяльність залучених сторін, яка вказує на іншу природу ворога, виклик загальносвітовій архітектурі безпеки, зокрема в Європі.

У цій статті визначаються окремі елементи передумов війни від гібридного конфлікту до повномасштабної війни, а також специфічні характеристики, які пов'язують з цим явищем.

Сучасні загрози та виклики істотно відрізняються від тих, що мали місце у недалекому минулому. Розпад біполярного світу часів холодної війни та прогресуюча глобалізація змінили природу глобального середовища безпеки. Сучасним арміям доводиться стикатися з новими ризиками. Також стає все більш реальним той факт, що величезні армії (навіть професійні), попри перевагу в озброєнні та навченому особовому складі, не спроможні впоратися з поставленими перед ними завданнями.

Аналіз останніх досліджень і публікацій. Під час дослідження проблемних питань публічного управління у сфері інформаційної протидії надавалась перевага, зокрема, елементам кризового управління.

Автори [1] провели комплексний аналіз методологічних і організаційних проблем протидії у сфері інформаційного забезпечення.

На думку авторів [2], у сфері публічного управління не приділялася належна увага саме проблемі реформування системи публічного управління під час інформаційних загроз.

Дослідники А. Баровська, Д. Дубов, В. Королько, В. Крутько, Г. Почепцов, Г. Дж. Ларкін у своїх працях розглянули публічне управління у сфері інформаційної протидії та вказали на теоретичні аспекти й проблемні питання в зазначеній сфері.

Незважаючи на широке коло досліджень науковців і практиків з питань публічного управління в інформаційній сфері, залишаються не повною мірою висвітленими, зокрема, питання кризового управління.

Сьогодні військові дії широкомасштабного характеру вирізняються складністю всіх задіяних засобів. У війнах останнього десятиліття чітко простежується взаємне

накладання й поєднання методів ведення регулярної та нерегулярної війни. Спільна стратегія полягає у створенні економічної незалежності від агресора. Іншою відмінною ознакою війни є використання засобів масової інформації та дипломатичних зусиль для впливу на суспільство, національні, етнічні чи релігійні групи, військовослужбовців і цивільних.

Метою статті є дослідження питання щодо організації інформаційної взаємодії між органами публічного управління під час повномасштабної війни.

Методи дослідження. Методологічною основою цієї наукової розвідки були загальнонаукові та спеціальні методи – ідеалізація, узагальнення. Досягнення визначеної мети та отримання обґрунтованих результатів здійснювалося завдяки застосуванню комплексу таких методів наукового пізнання, як: аналіз та синтез огляду понять у наукових статтях та джерелах. Абстрактно-логічний, індукційний, прогностичний методи було використано для теоретичного узагальнення дослідження і формулювання висновків.

Виклад основного матеріалу. Етимологія терміна «гібридність» походить від латинського слова «hybrida», що означає гібрид, створений внаслідок схрещування двох генетично різних особин, що належать до різних видів [3]. Гібрид – дуже широке поняття, яке зустрічається майже в усіх науках, включаючи біологію та техніку. Дія гібриду відбувається завдяки властивостям схрещування чи змішування або елементам, що належать до різних об'єктів чи станів, часто різних структурно віддалених генетично та протилежних. Метою цього процесу є створення кращої моделі з погляду посилених адаптаційних можливостей [4].

Таким чином, гібридна війна поєднує стратегію і тактику з нерегулярними операціями, а також кібервійну та інформаційні операції. Війна характеризується співіснуванням різних сторін конфлікту (держав і зовнішніх суб'єктів, військових і цивільних) та різними видами як симетричних, так і асиметричних збройних операцій [5].

Що ж до сучасних збройних конфліктів, гібридизацію можна розуміти як співіснування старих і нових війн, класичних збройних конфліктів та останніх війн, зіткнень

національних армій та асиметричних конфліктів, найсучасніших військових технологій і примітивного озброєння, боротьбу за території та ресурси, а також суперечки про ідентичність і цінності та протистояння локального характеру [6].

Гібридизація може стосуватися як ворогуючих сторін (держава, зовнішній учасник, нерегулярне збройне формування), так і простору конфлікту (поле бою), його походження та природи (конфліктна екосистема) [7].

Це є результатом співіснування в часі та просторі декількох різних поколінь війн, які перетинаються та взаємно проникають на поле бою. Для стороннього спостерігача, з одного боку, війна – це простір, де ведуть бойові дії регулярні підрозділи збройних сил держави, поділені на певні типи:

– слабо організовані й погано озброєні місцеві підрозділи;

– військові формування, оснащені найсучаснішою військовою технікою, і водночас атака розлюченого натовпу на армію загарбників, застосування технологій та засобів кібербитви, а з іншого боку, засідки, які влаштовуються під час бойових дій [7].

Дослідження доводять, що війна породжує чотири типи загроз: традиційні, незаконні, терористичні та деструктивні.

Характерною особливістю сучасної війни повномасштабного типу є те, що воєнні дії повинні супроводжуватися невоєнними компонентами. Вони також є у фазах стабілізації після завершення війни. Така діяльність потребує визначення колаборантів серед місцевої громади через те, що вони здебільшого продовжують співпрацювати з ворогом або ж залишають місця окупації разом із ворогом, який відступає. Згідно з досвідом повномасштабної війни воєнні дії здебільшого гарантують перемогу над ворогом, який використовує традиційні методи та засоби бою [8].

Війна підриває чіткі міркування щодо майбутнього середовища глобальної безпеки [9].

Характерною особливістю в сучасній війні є співіснування двох планів – територіального та віртуального.

Територіальна площина означає у класичному розумінні

національні, державні та традиційні етнічні спільноти, клани, які постійно населяють певну територію.

На відміну від цього, віртуальна площина має територіальну, транскордонну мережеву структуру, яка дає змогу спілкуватися в межах цієї мережі, та глобальне просування цінностей, ідей і принципів, включаючи підтримку та відновлення власної структури.

Війна на територіальній площині покликана поширювати та підтримувати юрисдикцію та адміністративний контроль над певною територією, охороняти кордони, що визначають межі юрисдикції, дотримуватись конституційних принципів та правових норм щодо населення, яке проживає на цій території, і забезпечувати громадський порядок, управління природними ресурсами та господарську діяльність [10].

Російська ідея «війни нового покоління» базується на таких елементах: політична диверсія, створення допоміжної інфраструктури, повномасштабне вторгнення, маніпулювання переговорами [11].

Війна в Україні довела, що політичний саботаж можна здійснювати через ЗМІ, на основі пропаганди та агітації, торкаючись водночас соціально чутливих питань, таких як соціальні, мовні та культурні відмінності.

Операції ЗМІ покликані поглибити розбіжності та двобічність між соціальними групами, створити корупцію та агітувати впливових чиновників. Втручання у допоміжну інфраструктуру означає захоплення ключових компонентів національної інфраструктури, тобто аеропортів, вокзалів, складів.

Досвід війни в Україні показав, що вона може мати форму раптової імпровізованої організації польових навчань на кордоні зі значною кількістю розгорнутих військ та техніки до повномасштабного вторгнення. Водночас здійснюється незаконна співпраця з перекиданням техніки, підготовкою сепаратистів та створенням баз матеріально-технічного забезпечення. Загроза полягає в небезпеці застосування ядерної зброї, організації маневрів й агресивної діяльності сухопутних і повітряних сил, щоб сусідні держави були обережними, не втручалися в конфлікт.

Про російський підхід до концепції ведення війни заявив герасімов під час виступу 26 січня 2013 р. перед членами російської академії військових наук. Промова була передусім виразом поглядів командування росії щодо того, як розпочати війну нового типу, конфлікт, у якому зникають усі відмінності між війною та миром, а також особливості переходу до повномасштабної війни. На його думку, таке поєднання особливе, коли війни не оголошуються, а найважливіше те, що вона може перетворити цілком стабільну країну на арену найінтенсивнішого збройного конфлікту протягом декількох днів. До того ж, як він зазначив, нові конфлікти тягнуть за собою принципову зміну законів війни. За його словами, ці заходи можуть бути значно ефективнішими за звичайні військові методи, оскільки використання асиметричних дій зменшує перевагу противника в бою. Як приклади таких методів, він навів використання спецпідрозділу та внутрішньої опозиції з метою створення постійно зростаючого фронту на всій території ворожої держави, а також інформаційні операції (форми та засоби яких постійно змінюються). Крім того, герасімов заявив, що нинішні військові дії стають все більш динамічними, активними та ефективними. Також зникають тактичні та оперативні інтервали, які можуть бути використані іншою стороною [10].

З огляду на аналіз звернення герасімова та початок повномасштабного вторгнення стає зрозуміло, що російська концепція ведення сучасного конфлікту передбачає дотримання схеми, наведеної нижче.

Фаза 1. Підготовка: розгортання психологічних операцій через відродження сепаратистського і здебільшого агресивного мислення та риторики. Створення атмосфери неминучості війни в поєднанні з дипломатичними зусиллями на міжнародній арені.

Фаза 2. Дезінформація: здійснення дезінформаційної діяльності (на всіх рівнях, починаючи від стратегічних комунікацій і закінчуючи локальними повідомленнями) усіма доступними засобами комунікації, відповідальними за передавання інформації в запланованій зоні бойових дій та в міжнародному середовищі. У дипломатичному аспекті – для

досягнення бажаної реакції, у тому числі й агресор для внутрішніх потреб отримує повідомлення, спрямоване на пом'якшення чи загострення реальної картини ситуації. Він має бути адаптований до індивідуальних особливостей країни, її міжнародного та внутрішнього становища. У військовому аспекті — протягом усього періоду операції проведення агресором значної кількості навчань та перестановки тактичних бойових груп під виглядом проведення навчального циклу військових підрозділів з метою сприяння прихованню розгортання військ, призначених для дій у районі прогнозованих бойових дій.

Фаза 3. Дестабілізуюча: подолання центральних і місцевих центрів влади противника, його силових структур, представників ЗМІ та бізнесу з використанням широко застосовуваних методів та інструментів, у тому числі політичних, економічних та технологічних (наприклад, кібератаки).

Фаза 4. Військові операції: створення місцевих підрозділів сепаратистів, до складу яких входять, наприклад, національні меншини, які діють за підтримки збройних сил і підрозділів найманців агресора як із розпізнавальними знаками, так і без будь-яких, оснащені спеціалізованою технікою та озброєнням, основними завданнями яких є окупація територій та утримання її військовим шляхом.

Фаза 5. Колаборація: створення залежних від агресора центральних та місцевих органів влади, які підтримуватимуть процес формального включення сфери діяльності до державних структур агресора.

Аналіз елементів сучасної війни виявляє такі суттєві загрози [10; 12]**:**

- економічні загрози сприймаються як загроза безпеці національної економіки, якщо економіка не може розвиватися, генерувати прибутки та заощадження для інвестицій, або якщо зовнішні загрози призводять до збоїв у її функціонуванні;
- військові загрози – це ситуація, коли існує загроза державі та її суверенітету чи територіальній цілісності внаслідок застосування збройних сил агресора;
- соціальні загрози стосуються всього, що загрожує

втратою національної та етнічної ідентичності окремих спільнот;

- загрози для критичної інфраструктури. Критична інфраструктура – це системи та взаємопов'язані функціональні об'єкти, у тому числі будівлі, технічні споруди та служби, критичні для безпеки держави та її громадян, які забезпечують належне функціонування органів публічного управління;

- інформаційні загрози. Це сфера безпеки, зміст якої (цілі, умови, методи, зміст) стосується інформаційного середовища (включаючи кіберпростір) держави, наприклад:

- пропагандистсько-інформаційні операції;

- маніпулювання інформацією;

- розгортання агітаційних кампаній та психологічних операцій з використанням послуг Інтернету та мережі мобільного зв'язку;

- операції проти критичної інфраструктури держави, включаючи злом систем безпеки;

- несанкціонований доступ або зловживання інформацією або несанкціонована зміна інформації;

- кібертероризм, кіберзлочинність, хакерство.

Інформаційна війна розвивається непомітно, потім настає стадія швидкого розвитку, що призводить до враження різних органів публічного управління. Інформаційна війна може тривати роками. За систематичної тривалості це може мати незворотні наслідки.

Проте війна повинна мати значний військово-політичний результат, тоді як інформаційна війна покликана ініціювати та діяти як каталізатор цього успіху.

Також у Західній Європі та в самій росії проводилася інтенсивна інформаційна кампанія для росіян з метою підтримки сепаратистів в Україні. Внутрішня діяльність полягала в інформуванні та мобілізації суспільства стосовно іміджу НАТО та Західної Європи як постійного противника росії. Тим часом вони створили міцний імідж України як націоналістичної держави з новим упередженим урядом, діяльність якого спрямована на обмеження прав російської меншини. Крім того, поширювалася теза про історичну передумову приналежності певних територій України до росії.

Такі пропагандистські дії, спрямовані на суспільство росії, здійснюються, аби викликати відчуття несправедливості, ізоляції та несправедливого ставлення з боку решти світу.

З одного боку, суспільство відчуває власну унікальність і переконане у доцільності дій росії. З іншого боку, суспільство переживає несправедливе відчуження, воно стикається з поглибленням антагонізму між цінностями Сходу і Заходу. Таким суспільством легше маніпулювати, яке своєю чергою може полегшити труднощі та незручності, які виникають внаслідок ведення збройного конфлікту протягом тривалого періоду часу (наприклад, нестача їжі через санкції Заходу або скорочення видатків на соціальні виплати та зарплати).

Пропаганда, спрямована на сусідні країни є попередженням, спрямованим на те, щоб зумовити побоювання ескалації конфлікту та втрати свободи. Цей метод застосовується для Грузії та Молдови. Інший вид пропаганди безпосередньо адресований країнам Балтії. Вся міжнародна пропаганда – це фактично інформаційний хаос, дезінформація, вигадування реальності та маніпуляції, спрямовані на руйнування єдності Західної Європи.

Інше питання, пов'язане з веденням війни, – це гуманітарна інтервенція або її правильне використання. Гуманітарна допомога, наявна в міжнародному праві, починає використовуватися не за призначенням. Крім того, реалії довели, що гуманітарна інтервенція може бути здійснена проти волі країни, населенню якої надається, а гуманітарна допомога слугує інтересам держави, з якої вона надійшла.

Висновки та напрями подальших досліджень. Підсумовуючи, слід підкреслити, що характер сучасних війн свідчить: противник, який використовує асиметричні методи ведення бою, не буде дотримуватися принципів гуманітарних законів збройних конфліктів. Буде продовжувати напади на осіб і об'єкти, які захищені міжнародним правом, здійснювати експлуатацію цивільних осіб у своїх інтересах.

Цілком імовірно, що агресор і надалі буде використовувати уніформу чи розпізнавальні знаки українських військових формувань. Це було видно через діяльність російської федерації в Криму та під час повномасштабної війни

на території України. З одного боку, можна виділити гібридність цих видів діяльності, які пов'язують старі та нові методи ведення бою, зокрема свідому агресію.

З іншого боку, ми можемо спостерігати поєднання військових дій з інформаційною війною (на всіх рівнях, від стратегічної до локальної комунікації).

У предметній літературі немає чіткого і загальноприйнятого визначення поняття гібридна війна. Його також немає в жодній доступній класифікації війн у теорії військового мистецтва. Треба припустити, що гібридність у сучасних війнах також стала ознакою нашого часу, її існування є відчутно очевидним.

Список використаних джерел

1. Шорохова Г. М. Деякі проблеми інформаційно-аналітичного забезпечення діяльності Національної поліції. *Юридична наука України : історія, сучасність, майбутнє* : матеріали Міжнародної науково-практичної конференції, м. Харків, 1–2 листопада 2019. Харків : Східноукраїнська наукова юридична організація, 2019. С. 142–143.
2. Tsybulenko E., Kajander A. The Hybrid Arsenal of Russia's War Against the Democratic World. *Springer Nature*. 2022. Switzerland. P. 173–194.
3. Witold S., Bartholomew Z. Asymetria i hybrydowość – stare armie wobec nowych konfliktów 2012. The National Security Agency, Polish Society of International Studies-nation Kielce, Warszawa. 2012. 250 p.
4. Ciekanowski Z. Działania asymetryczne jako źródło zagrożeń bezpieczeństwa. Higher School of Management and Law of Helena Chodkowska. 2019. Warsaw. P. 47–72.
5. Czaputowicz J. Bezpieczeństwo międzynarodowe. Współczesne koncepcje. 2012. Warszawa. 262 p.
6. Kaldor M. New and Old Wars : Organized Violence in a Global Era. 2011. Stanford University Press. 216 p.
7. Міністерство національної оборони НАТО, щодо оперативних можливостей у сфері гібридності сучасної війни / Центр навчання та підготовки Збройних Сил Польщі. Бидгощ. 2015. 156 с.
8. NATO's response is Hybrid Threads. Foreword to General Philip M. Breedlove Supreme Allied Commander Europe, NATO Defense College. 2015. Rome. Italy. 478 p.
9. Gentile G. P. The imperative for an American general purpose army that can fight, 2009. Philadelphia, USA. 374 p.
10. Analityczny model dla oceny hybrydowości współczesnych konfliktów / Центр навчання та підготовки Збройних Сил Польщі. Бидгощ. 2015. 156 с.

11. Antczak-Barzan, A. Dynamika wojny hybrydowej na Ukrainie. Kwartalnik Bellona. 1.2016. P. 44–52.
12. Krystiana J.; Robb J. Brave New War. The Next Stage of Terrorism and the End of Globalization. Wiley. 2012. Hoboken. 208 p.

References

1. Shorokhova, H. M. (2019). Deiaki problemy informatsiino-analitychnoho zabezpechennia diialnosti Natsionalnoi politsii [Some problems of information and analytical support for the activities of the National Police], Yurydychna nauka Ukrainy: istoriia, suchasnist, maibutnie materialy Mizhnarodnoi naukovo-praktychnoi konferentsii [Legal science of Ukraine: history, modernity, future: materials of the International Scientific and Practical Conference]. Kharkiv [in Ukrainian].
2. Tsybulenko, E., Kajander, A. (2022). The Hybrid Arsenal of Russia's War Against the Democratic World. *Springer Nature*, Switzerland, 173–194. [in English].
3. Witold, S., Bartholomew, Z. (2012). Asymetria i hybrydowość – stare armie wobec nowych konfliktów 2012. The National Security Agency, Polish Society of International Studies-nation Kielce. Warszawa [in English].
4. Ciekanowski, Z. (2019). Działania asymetryczne jako źródło zagrożeń bezpieczeństwa. Higher School of Management and Law of Helena Chodkowska. Warsaw. P. 47–72. [in English].
5. Czaputowicz, J. (2012). Bezpieczeństwo międzynarodowe. Współczesne koncepcje. Warszawa [in English].
6. Kaldor, M. (2011). New and Old Wars: Organized Violence in a Global Era. Stanford University Press [in English].
7. Tsentr navchannia ta pidhotovky Zbroinykh Syl Polshchi. (2015). Ministerstvo natsionalnoi oborony NATO, shchodo operatyvnykh mozhlyvostei u sferi hibrydnosti suchasnoi viiny [Ministry of National Defense of NATO, regarding operational capabilities in the field of hybridity of modern warfare]. Bydhoshch [in Ukrainian].
8. NATO Defense College. (2015). NATO's response is Hybrid Threads. Foreword to General Philip M. Breedlove Supreme Allied Commander Europe. Rome. Italy [in English].
9. Gentile, G. P. (2009). The imperative for an American general purpose army that can fight. Philadelphia USA [in English].
10. Training and Training Center of the Armed Forces of Poland. (2015). Analityczny model dla oceny hybrydowości współczesnych konfliktów. Bydhoshch [in English].
11. Antczak-Barzan, A. (2016). Dynamika wojny hybrydowej na Ukrainie. Kwartalnik Bellona, 1, 44–52. [in English].
12. Krystiana, J., Robb, J. (2012). Brave New War. The Next Stage of Terrorism and the End of Globalization. Wiley. Hoboken [in English].

CRISIS MANAGEMENT DURING OF FULL-SCALE WAR

Kolodka Andrii

Abstract. The sustainable functioning of society in the conditions of information challenges during the full-scale Russian-Ukrainian war is a key condition for ensuring civil security, conducting methodological and scientific research on this issue makes it possible to prepare the best practices of crisis management. Accordingly, the scientific task is the theoretical substantiation of the components of the development of crisis management from a hybrid confrontation to a full-scale war and their characteristics. In the basis of the analysis of the mechanism of public crisis management, information countermeasures are defined as its main lever, and its significant characteristics are substantiated. It can be argued that the problem of crisis management as a result of a full-scale war has not been sufficiently studied by domestic and foreign scientists. The main emphasis was on anti-crisis management in the conditions of hybrid war, as a component of measures to respond to the emergence of a crisis. The research methods were content analysis, hypothetical and general scientific. On the basis of the analysis of previous scientific studies, problematic issues of public management in the field of information countermeasures, in particular elements of crisis management, have been identified. The issue of dissemination regarding the organization of information interaction between public administration bodies during a full-scale war was investigated. Issues of crisis management in conditions of full-scale war, taking appropriate measures for timely response. The conducted research is a theoretical confirmation of the hypothesis that information is the basis of making crisis management decisions and is a key factor of state security. The analysis of the crisis management system shows that one of the components of the activities of management bodies is aimed at the organization and support of important life support systems. Considerable attention is also paid to the system of methodological and organizational problems of countermeasures in the field of information provision.

Keywords: Russian-Ukrainian war, crisis management, public administration, information security.