Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2023. № 9.

DOI: http://doi.org/10.32702/2307-2156.2023.9.25
УДК 351

В. О. Новіков,
здобувач, ННВЦ НУЦЗУ, м. Харків, Україна
ORCID ID: https://orcid.org/0009-0002-6494-3975

АНАЛІЗ СУЧАСНОЇ КОНЦЕПЦІЇ ІНФОРМАЦІЙНО-ГІБРИДНОЇ ВІЙНИ

V. Novikov,
Graduate student, TRPC NUCDU, Kharkiv, Ukraine

ANALYSIS OF THE MODERN CONCEPT OF INFORMATION-HYBRID WARFARE

У даній статті здійснюється аналіз та доктринальний синтез концептуальних засад сутністного розуміння сучасної концепції інформаційно-гібридної війни.

В результаті проведеного дослідження констатовано, що розбудова демократичних та правових ідей є основоположним елементом сучасної державної політики України. Водночас, сьогодні процес державотворення в інформаційно-цифрових умовах набуває все більшого значення у процесі інформатизації та появи гібридних загроз. Активний розвиток передових технологій та інноваційно-новаторських ідей, які набули міжнародного значення, створюють все більшої загрози державному суверенітету будь-якої держави, правам і свободам людини і громадянина та суспільства в цілому.

Лише протягом останнього десятиліття вітчизняне законодавство було доповнено численними правовими нормами направленими на захист національних інтересів України у сфері інформаційної безпеки, де головна увага була приділена, як правило, питанням впливу інформації на суспільну думку та свідомість громадян. Внаслідок чого, проблеми реалізації державної політики у сфері інформаційної безпеки набувають особливого значення при визначенні суспільних відносин у сфері забезпечення національної безпеки як головний об'єкт посягання при інформаційно-гібридних загрозах. Акцентовано увагу на тому, що зростання ролі інформації у світі призвело до зростання можливостей інформаційних протиборств. Для політиків та військових стало очевидним, що сучасне суспільство перебуває у великій залежності від інформаційно-телекомунікаційних систем, і цей факт не може бути не врахований при розробці технологій впливу на свідомість людей шляхом маніпуляцій. Інформаційне протиборство завжди використовувалося у війнах держав за допомогою розвідки та контррозвідки, дезінформації та пропаганди та інших заходів впливу.

Доведено, що наразі ще не розроблено кардинальних заходів щодо протидії інформаційним атакам, а це означає, що в інформаційних війнах успіх забезпечуватиметься за рахунок дедалі більшого вдосконалення інформаційних технологій. Як показує практика, недостатня увага до питань парирування інформаційних загроз може завдати значної шкоди політичній системі будь-якої держави аж до руйнування самої держави, відтак питання інформаційно-гібридних загроз постає надзвичайно актуальним.

This article provides an analysis and doctrinal synthesis of the conceptual foundations of the essential understanding of the modern concept of information-hybrid warfare.

As a result of the research, it was established that the development of democratic and legal ideas is a fundamental element of the modern state policy of Ukraine. At the same time, today the process of state formation in information and digital conditions is gaining more and more importance in the process of informatization and the emergence of hybrid threats. The active development of advanced technologies and innovative and innovative ideas that have gained international significance create an ever-increasing threat to the state sovereignty of any state, the rights and freedoms of a person and citizen, and society. Only during

the last decade, the national legislation was supplemented by numerous legal norms aimed at protecting the national interests of Ukraine in the field of information security, where the main attention was paid, as a rule, to the issue of the influence of information on public opinion and the consciousness of citizens. As a result, the problems of implementation of state policy in the field of information security acquire special importance when determining social relations in the field of ensuring national security as the main object of encroachment in the case of information-hybrid threats. Attention is focused on the fact that the growth of the role of information in the world has led to the growth of opportunities for information conflicts. For politicians and the military, it became obvious that modern society is highly dependent on information and telecommunication systems, and this fact cannot be ignored when developing technologies for influencing people's consciousness through manipulation. Information warfare has always been used in state wars through intelligence and counterintelligence, disinformation and propaganda, and other influence measures.

It has been proven that no drastic measures have yet been developed to counter information attacks, which means that success in information wars will be ensured by the ever-increasing improvement of information technologies. As practice shows, insufficient attention to the issues of countering informational threats can cause significant damage to the political system of any state up to the destruction of the state itself, therefore the issue of informational-hybrid threats becomes extremely relevant.

Ключові слова: *управління, гібридні загрози, протидія та превенція, інформаційна війна, гібридна війна, протидія загрозам, превенція загрозам, гібридні загрози в управлінні.*

Keywords: *management, hybrid threats, countermeasures and prevention, information warfare, hybrid warfare, threat countermeasures, threat prevention, hybrid threats in management.*

Постановка проблеми. Розбудова демократичних та правових ідей є основоположним елементом сучасної державної політики України. Водночас, сьогодні процес державотворення в інформаційно-цифрових умовах набуває все більшого значення у процесі інформатизації та появи гібридних загроз.

Активний розвиток передових технологій та інноваційно-новаторських ідей, які набули міжнародного значення, створюють все більшої загрози державному суверенітету будь-якої держави, правам і свободам людини і громадянина та суспільства в цілому. Лише протягом останнього десятиліття вітчизняне законодавство було доповнено численними правовими нормами направленими на захист національних інтересів України у сфері інформаційної безпеки, де головна увага була приділена, як правило, питанням впливу інформації на суспільну думку та свідомість громадян. Внаслідок чого, проблеми реалізації державної політики у сфері інформаційної безпеки набувають особливого значення при визначенні суспільних відносин у сфері забезпечення національної безпеки як головний об’єкт посягання при інформаційно-гібридних загрозах.

Теоретико-прикладні аспекти дослідження сутності гібридної війни знайшли своє відображення у наукових працях багатьох вчених: соціологів Д. Альбертса, О. Бардіна, Бжезінського, М. Гарєєва, О. Данильяна, О. Дзьобаня, П. І. Круть, В. Мандрагеля, Є. Мануйлова, І. Панаріна, О. Панфілова, А. Папікяна, В. Сліпченка, А. Смелянцева, М. Требіна, Дж. Фрідмена, Ф. Фукуями, С. Хантінгтон, причому саме з позицій якісно-нової форми загроз даний інститут висвітлювали М. Кревельд, М. Калдор, М. Хардт й А. Негрі. В той же час, не дивлячись на сталий науковий інтерес чимало аспектів залишаються невирішеними.

Внаслідок чого **метою** даної статті є наукове обґрунтування та дослідження проблематики концептуальних засад сутністного розуміння сучасної концепції інформаційно-гібридної війни.

Виклад основного матеріалу. Як відомо, поняття – «гібридні» війни у військово-політичному дискурсі з'явився не так давно, під яким стали вважати загрози нового типу. Під гібридною війною (від лат. «hibrida», «hybrida» – поміс) розуміють сучасний спосіб ведення військових дій, що є поєднанням класичних методів військових операцій з партизанською війною, тероризмом, інформаційною війною (кібервійною), біологічною і т.д.

Поняття «гібридна війна»(«hybrid warfare») та «гібридна загроза»(«hybrid warfare threats») вжевведені до офіційної термінології західної військової політики. Так, у підсумковому документі, прийнятому на саміті НАТО у вересні 2014 року в Уельсі, Англія, у п.13 йдеться про необхідність підготовки Північноатлантичного військового альянсу до того, «щоб НАТО була здатна ефективно долати конкретні виклики, що виникають у зв'язку з загрозами гібридної війни, під час якої застосовується широкий ряд тісно взаємопов'язаних відкритих і прихованих військових, воєнізованих та цивільних заходів» [1, с. 22]. Учасники альянсу розглядають гібридні війни як широкий набір бойових дій, таємних операцій, що здійснюються партизанськими формуваннями, із залученням цивільних компонентів, а також як боротьбу з пропагандистськими кампаніями, кібератаками та місцевим сепаратизмом.

Вчені-фахівці включають у поняття загроз гібридної війни всі засоби, що сприяють можливості завдати шкоди противнику, – і традиційні, класичні, і нові, такі як війни в інформаційному просторі, використання та розробку сценаріїв конфліктів низької інтенсивності на території противника, міжнародний тероризм, міграцію, розпалювання етнічних та релігійних конфліктів, транснаціональну злочинність, демографічні ризики, глобалізаційні виклики та ін. [2, с. 177]. Ставиться завдання адаптувати у гібридній війні і традиційні методи, і нетрадиційні. Завданням нашої державності з метою забезпечення своєї безпеки є врахування можливості використання потенційним противником згаданих загроз для досягнення своїх довготривалих політичних цілей. Таким противником може бути і якась держава, і союз держав, і організація [3, с. 105].

Існує ще одна назва для технологій, що використовуються у гібридних війнах, – це технології керованого хаосу, коли в країні створюється політична та економічна нестабільність, що сприятиме захопленню влади спеціальними підготовленими групами. Ці технології використовувалися в підготовці та здійсненні «кольорових» революцій у низці країн у 2003–2004 роках (Грузії –

«Революція троянд», Киргизії – «Революція тюльпанів»). На думку окремих науковців, у даних державах були запровадженні технології здійснення державних переворотів та зовнішнього управління політичною ситуацією в країні в умовах штучно створеної політичної нестабільності, в яких тиск на владу здійснюється у формі політичного шантажу з використанням як інструмент шантажу молодіжного протестного руху» [4, с. 12]. Політичний шантаж переходить у силову фазу з подальшим розв'язуванням громадянської війни в країні та втручанням зовнішніх «миротворчих» сил.

Зростання ролі інформації у світі призвело до зростання можливостей інформаційних протиборств. Для політиків та військових стало очевидним, що сучасне суспільство перебуває у великій залежності від інформаційно-телекомунікаційних систем, і цей факт не може бути не врахований при розробці технологій впливу на свідомість людей шляхом маніпуляцій. Інформаційне протиборство завжди використовувалося у війнах держав за допомогою розвідки та контррозвідки, дезінформації та пропаганди та ін.

Термін «інформаційна війна» використав одним із перших Т. Рон в аналітичному звіті для компанії Боїнг «Системи зброї та інформаційна війна» у 1976 р. [5, с. 166]. Власне, з того моменту починає формуватися розуміння того, що інформація може бути зброєю. А з урахуванням того, що розвиток економік країн Європи та США ґрунтується на прориві в інформаційно-телекомунікаційних технологіях, цей сектор стає особливо вразливим як у військовий, так і у мирний час [6, с. 184]. Тут необхідна деталізація напрямків впливу інформаційної зброї, адже її застосування відбувається за двома напрямками щодо об'єктів впливу: вплив на інформаційні засоби та системи супротивника та вплив на свідомість людей. Перший напрямок отримав ще назву кібервійн, коли атакам піддається технічне обладнання та системи його програмного забезпечення. У світі існують цілі наукові інститути, які розробляють нові і нові комп'ютерні віруси, вірусні програми та інші засоби виведення з ладу комп'ютерів або крадіжки інформації.

Другий напрямок – це старі способи пропаганди та агітації,

контрпропаганди та контрагітації, які досягли небувалих за своєю силою висот за витонченістю та масовістю впливу на свідомість людей та суспільства. Використовується відверта брехня і підробка інформації (набув поширення термін «фейкова» війна, від англ. «fake» – підроблений). Якщо метою першого напряму є завдання шкоди життєзабезпечуючим системам держави-противника (в галузі енергетики, оборони, управління та ін.), то другий спрямований на досягнення масованої психологічної обробки людей з метою дестабілізації політичної ситуації в країні.

Найбільш відомим визначенням інформаційних воєн стало таке: «… це вид конфлікту, при якому завданнями протиборчих сторін є захист власної інформації та інформаційних систем, маніпулювання інформацією противника або її спотворення, а також обмеження можливостей протиборчої сторони у доступі та обробці інформації» [5, с. 3].

Світ не відмовився від колишніх форм ведення війни. Зброя, як і раніше, стріляє, завдаючи руйнувань і людських втрат, тоді як величезною ж перевагою інформаційної війни є те, що без єдиного пострілу можна опанувати ресурси держави, якщо перепрограмувати поведінку противника, переконавши, наприклад, суспільство в єдино-вірних цінностях. Розроблено технологію такого перепрограмування, першими об'єктами якої є владна еліта та молодь. Поряд з багатьма можна дати таке визначення інформаційної війни: це активні дії в інформаційному просторі, які мають на меті дестабілізацію інформаційної системи супротивника та захист власного інформаційного середовища. Пропонуються й інші синонімічні визначення воєн в інформаційному просторі: мережева війна, кібервійна [6, с. 184].

Аналіз теоретичних досліджень та прикладних даних дозволяє сформулювати основні цілі та завдання, яких можна досягти за допомогою нового типу війни – інформаційної [7, с. 4]. Це: дезінформація світової спільноти шляхом розміщення у засобах масової інформації, переважно електронних, свідомо неправдивої та провокаційної інформації; поширення своєї ідеології шляхом масованих атак на свідомість громадян інших держав,

маніпулювання їхньою свідомістю; вербування прихильників, де пріоритетне середовище: владна еліта, молодь, наука та освіта; доступ до інформаційних ресурсів (архівів, банків даних, музеїв, бібліотек та ін.) з подальшим їх спотворенням або знищенням; зниження впливу держави у міжнародних відносинах, на ухвалення важливих політичних рішень; впровадження у суспільну свідомість принципів споживацтва, користолюбства, атмосфери аморальності, негативного ставлення до своєї історії та культури; дестабілізація політичної та економічної системи держави; поширення ганебних та наклепницьких відомостей про керівництво країни; створення стану конфронтації між провідними політичними силами держави; шантаж впливових політичних діячів; розпалювання націоналізму, ксенофобії, расової та релігійної ненависті; організація масових заворушень, протестних виступів, екстремістських виявів.

На теперішньому етапі української та міжнародної державності стало очевидним фактом, що якщо ще нещодавно інтернет-простір мав переважно інформаційну складову, то тепер у ньому все більше набирає сили сектор агітаційний, пропагандистський аспект, що відрізняється яскраво вираженою агресивністю [8]. Традиційні засоби масової інформації дедалі більше працюють із інтернет-ресурсами як джерелами інформації та засобом впливу на уми громадян. Інформація в мережі стає все більш масово затребуваною, швидко поширюваною та суспільно значущою. Вітчизняне суспільство зіштовхнулося зі зростаючою загрозою в інформаційно-комунікаційному середовищі. Метою інформаційної війни є управління процесом зміни свідомості людей, їх світогляду, ставлення до суспільства та держави; небезпекою для людей є втрата ними власної волі, а для держави – її суверенітету. Це завжди було метою будь-якого завойовника, але тепер того ж можна домогтися «м'яким» способом (навіть термін з'явився: «soft power» – м'яка сила, введена у вжиток американським політологом Дж. Найєм) [9]. Але «м'які» зусилля в деяких випадках можуть бути небезпечнішими за «жорсткі», тому що жертва м'якого примусу може і не усвідомлювати обману, може

побачити результат тільки тоді, коли вже є відчутними результати, при цьому така зброя має масовий характер поразки [10, с. 268]. Зі зрозумілих причин вільне та важко контрольоване розповсюдження інформації в Інтернеті створює чимало проблем спецслужбам усіх держав. Лавиноподібний потік інформації (і дезінформації) здатний завдати шкоди будь-якій державі (аж до революційного вибуху та повалення влади).

Висновки і пропозиції. Таким чином, в результаті проведеного дослідження стає очевидним, що наразі ще не розроблено кардинальних заходів щодо протидії інформаційним атакам, а це означає, що в інформаційних війнах успіх забезпечуватиметься за рахунок дедалі більшого вдосконалення інформаційних технологій. Як показує практика, недостатня увага до питань парирування інформаційних загроз може завдати значної шкоди політичній системі будь-якої держави аж до руйнування самої держави, відтак питання інформаційно-гібридних загроз постає надзвичайно актуальним.

Перспективи подальших розвідок у даному напрямі стосуються формуванню та розробленню пропозицій методологічного інструментарію методів протидії інформаційно-гібридних загроз.

Література

1. Ахновська, І. О. (2016). Забезпечення інноваційної безпеки національної економіки. *Економіка і організація управління*. Vol. 2(22), 17-27. URL: https://jeou.donnu.edu.ua/article/view/47914.

2. Краснощокова, Ю. В. (2011). Інноваційна безпека підприємства як запорука конкурентоспроможності в умовах європейської інтеграції. *Управління розвитком*. Vol. 4 (101),177-178.

3. Неустроєв, Ю. Г. (2021). Роль інновацій у забезпеченні економічної безпеки. *Агросвіт*. 2021. Vol. 7-8, 103-108. DOI: 10.32702/2306-6792.2021.7-8.103

4. Башинська І. О., Шерстньова А. В. (2018). Інноваційна безпека: загрози та шляхи зниження. *Сучасні інформаційні технології та*

телекомунікаційні мережі: тези доповідей 53-ої наукової конференції молодих дослідників ОНПУ. (м. Одеса, ОНПУ, 2018р.), Vol. Одеса, 11-13.

5. Еляшевська, Н. (2015). Вразливість України до інформаційної війни. Теле- та радіожурналістика, Vol. 14, 165-169.

6. Лубкович, І. М. (2014). Місце українських медій в інформаційній війні 2013–2014 рр. Наукові записки інституту журналістики, Vol. 56, 182-187.

7. Сенченко, М. (2014). Запорука національної безпеки в умовах інформаційної війни. Вісник Книжкової палати, Vol. 6, 3-9.

8. Dibb, P. (2016). Why Russia is a threat to the international order. Access: https://www.aspi. org.au/publications/why-russia-is-a-threat-to-the-internationalorder/Russia.pdf.

9. Kofman, M., Rojansky, M. (2015). A Closer look at Russia's «Hybrid War». Access: https://www.wilsoncenter.org/sites/default/files/7KENNAN%20CABLEROJANSKY%20KOFMAN.pdf

10. Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. In War in the information age: new challenges for U. S. security policy(ed. by Robert L Pfaltzgraff; Richard H Shultz). Washington: D. C.: Brassey's, 256–268.

References

1. Akhnovska, I.O. (2016), "Ensuring innovative security of the national economy", *Ekonomika i orhanizatsiia upravlinnia*, vol. 2(22), pp. 17–27.

2. Krasnoshchokova, Yu.V. (2011), "Innovative enterprise security as a guarantee of competitiveness in the conditions of European integration", *Upravlinnia rozvytkom* vol. 4, pp. 177-178.

3. Neustroiev, Y. (2021), "The role of innovation in ensuring economic security", *Agrosvit*, vol. 7-8, pp. 103–108.

4. Bashynska, I. O. and Sherstnyova, A. V. (2018), " Innovative security: threats and ways of reduction", Suchasni informatsiini tekhnolohii ta

telekomunikatsiini merezhi. Zbirka dopovidei 53-oi naukovoi konferentsii molodykh doslidnykiv ONPU-ma vyp. 53 [Modern information technologies and telecommunication networks. Collection of reports of the 53rd scientific conference of young researchers of the ONPU-ma issue 53], ONPU, Odesa, Ukraine, pp. 11–13

5. Eliashevska, N. (2015), "Vulnerability of Ukraine to information warfare", *Tele-ta radizhurnalistyka*, Vol. 14, 165–169.

6. Lubkovitch, I. M. (2014), "The role of Ukrainian media in the information war of 2013–2014", *Naukovi zapysky instytutu zhurnalistyky*, Vol. 56, 186–187.

7. Senchenko, M. (2014), "A guarantee of national security in the conditions of information warfare", *Visnyk Knyzhkovoi palaty*, Vol. 6, 3–9.

8. Dibb, P. (2016), "Why Russia is a threat to the international order", available at: https://www.aspi.org.au/publications/why-russia-is-a-threat-to-the-internationalorder/Russia.pdf (Accessed 10 Aug 2023).

9. Kofman, M. and Rojansky, M. (2015), "A Closer look at Russia's "Hybrid War", available at: https://www.wilsoncenter.org/sites/default/files/7KENNAN%20CABLEROJANSKY%20KOFMAN.pdf (Accessed 10 Aug 2023).

10. Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. In War in the information age: new challenges for U. S. security policy, Brassey's, Washington: D. C., pp. 256–268.

Стаття надійшла до редакції 03.09.2023 р.