УДК 330:351:29
DOI: https://doi.org/10.54929/2786-5746-2023-9-02-05

ПАРАДИГМИ ГІБРИДНОГО ВПЛИВУ В ІНФОРМАЦІЙНІЙ СФЕРІ НА ПРИКЛАДІ ДЕРЖАВНО-УПРАВЛІНСЬКИХ ЗАСАД

PARADIGMS OF HYBRID INFLUENCE IN THE INFORMATION SPHERE ON THE EXAMPLE OF STATE-MANAGEMENT FOUNDATIONS

Хряпинський А. П.
Кандидат юридичних наук,
Директор ТОВ «Хряпинський і КО»
м. Харків, Україна
ORCID: 0000-0002-4899-3326

Хмиров І. М.
Доктор наук з державного управління, доцент,
старший науковий співробітник наукового відділу
з проблем цивільного захисту
та техногенно-екологічної безпеки науково-дослідного центру,
Національний університет цивільного захисту України,
м. Харків, Україна
ORCID: 0000-0002-7958-463X

Anton Khriapynskyi
PhD in Law,
Director LTD «Khriapynskyi and Partners»,
Kharkiv, Ukraine

Ihor Khmyrov
Doctor of Science in Public Administration, Associate Professor,
Senior Researcher Scientific Department of Problems
of Civil Protection and Technogenic
and Ecological Safety of the Scientific and Research Center,
National University of Civil Protection of Ukraine,
Kharkiv, Ukraine

У статті здійснено комплексне наукове обґрунтування та дослідження проблематики визначення сутності та особливостей парадигм гібридного впливу в інформаційній сфері на прикладі державно-управлінських засад. Встановлено, що під час розробки заходів з протидії гібридним загрозам в інформаційній сфері надзвичайно корисним може бути метод аналізу витрат і вигод. Хоча його застосування до цілей опонента може не поставити основні публічні організації та координаційні безпекові центри на перше місце в списку, але дійсно, вигода від їх зриву була б великою, адже вони, швидше за все, також підготовлені та мають навички запобігання загрозам у зоні своєї відповідальності, позитивний результат стає невизначеним, а ризик швидкого викриття – великим. Натомість цей аналіз може принести користь сферам, які перебувають між відповідальністю публічних організацій, є «сліпими плямами», де загрози можуть виявлятися повільно, а реагування потребує певного часу. Аргументовано показано, що надзвичайно важливо розробити систему виявлення, яка одночасно розпізнає хибнопозитивні та хибнонегативні результати. Існує потреба в прагматичності, гнучкості та інклюзивності акторів, секторів і рівнів – усередині та між країнами. Гібридний захід не прийде туди, де його очікують, принаймні не завжди. Коли контрзаходи будуть успішними, супротивник змінить схему атаки. Тому необхідно залучати всіх акторів і враховувати як короткострокові, так і довгострокові перспективи. Тобто важливо співпрацювати між секторами та рівнями та не допускати, щоб традиційні кордони перешкоджали співпраці. Це ніколи не є таким важливим, як під час протидії гібридним загрозам, оскільки вразливі місця, як правило, існують саме в прикордонних сферах між секторами та рівнями, і це те, на що опонент буде цілитися. Це вимагає співпраці насамперед в інформаційній сфері, яка повинна розвиватися в публічному та приватному секторах, а також від місцевого та регіонального рівнів до національного та міжнародного.
Ключові слова: *управління; гібридні загрози; протидія та превенція; інноваційний розвиток; протидія загрозам; превенція загрозам; гібридні загрози в управлінні.*

In the article, a comprehensive scientific substantiation and study of the issues of determining the essence and features of the paradigm of hybrid influence in the information sphere, using the example of state-management foundations, is carried out. It was established that during the development of measures to counter hybrid threats in the information field, the cost-benefit analysis method can be extremely useful. Although applying it to an entire adversary may not put major public organizations and security coordination centers at the top of the list, but indeed, the benefit of disrupting them has been great, as they are likely also trained and have threat prevention skills in their zone responsibility, the positive result becomes uncertain, and the risk of quick exposure is great. Instead, this analysis can be applied to areas that are within the responsibilities of public organizations, which are "blind spots" where threats can be fully revealed, and responses take some time. It is argued that it is extremely important to develop a detection system that simultaneously recognizes false-positive and false-negative results. There is a need for pragmatism, flexibility and inclusiveness of actors, sectors, and levels – within and between countries. The hybrid event will not go where it is expected, at least not always. If the countermeasures are successful, the adversary will change the pattern of attack. Therefore, it is necessary to involve all players and obtain both short-term and long-term prospects. It is therefore important to collaborate across sectors and levels and not allow traditional boundaries to stand in the way of collaboration. This is never more so than when countering hybrid threats, after the vulnerabilities are usually precisely in the border areas between sectors and tiers, and this is where the opponent will target. This requires cooperation primarily in the information field, which must develop in the public and private sectors, as well as from local and regional levels to national and international. Proved that fact that at the current stage of the formation of scientific doctrine and the development of the information environment, information as a public property has a huge potential for use in malicious actions, therefore, a long historical-state chronological period attracts the attention of a huge number of specialists in the field of hybrid threats and hybrid war.
Key words: *management; hybrid threats; countermeasures and prevention; innovative development; countermeasures against threats; threat prevention; hybrid threats in management.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. На сучасному етапі становлення наукової доктрини та розвитку інформаційного середовища, інформація як суспільне надбання має величезний потенціал для використання у зловмисних діях, тому вже тривалий історико-державний хронологічний відрізок часу привертає увагу величезної кількості фахівців у сфері гібридних загроз та гібридної війни.

Як відомо, саме використання операцій впливу як державними, так і недержавними інституціями та спільнотами постає все більш очевидним як для тих, хто приймає рішення, так і для пересічного громадянина. Науково-технічна революція та інноваційно-корпоративний розвиток, що впливає на розповсюдження інформації та соціальний обмін у наших суспільствах і спільнотах, а також посилення зв'язаності ключових суспільних систем та інфраструктури відкрило не лише нові можливості, а також й вразливі місця. Більше того, саме зміни ціннісних орієнтирів та соціально-державного ладу, парадигм щодо сутності державного управління та держави в цілому, розширили можливості та горизонти для частини суспільства, але залишили інших невпевненими у своєму місці чи представленості їхніх інтересів в усталених державно-суспільних відносинах, а також у політичній сфері, що набуває особливого значення на сучасному етапі українського державотворення.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор. Теоретико-прикладні аспекти дослідження проблем гібридного впливу, його етимологічний зміст та сутність суб'єктивних та об'єктивних детермінантів, їх парадигмальні та догматичні аспекти ставали предметом наукових пошуків численних авторів, зокрема С. Зубченка (щодо націоналістичних та ідеологічних засад) [1], Є. Магди (щодо теоретичних аспектів сутності гібридного впливу та гібридної війни) [2], О. Курбана (щодо протидії загрозам в умовах інформаційного впливу) [3], О. Литвиненка (щодо еволюції сутністних уявлень щодо гібридного впливу на тлі українського державотворення) [4], І. Валюшко (щодо еволюції гібридного впливу крізь призму інформаційних війн) [5], В. Кравченко (щодо теоретичних вимірів гібридної війни на тлі сучасних загроз) [6] та інші.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Водночас, питання пов'язані із дослідженням проблематики визначення сутності та особливостей парадигм гібридного впливу в інформаційній сфері на прикладі державно-управлінських засад ще не отримали належного теоретико-прикладного обґрунтування та аналізу.

Формулювання цілей статті (постановка завдання). Внаслідок чого метою даної статті є повне, всебічне та доктринальне дослідження сутності та особливостей парадигм гібридного впливу в інформаційній сфері на прикладі державно-управлінських засад.

Виклад основного матеріалу дослідження. В сучасних державно-управлінських реаліях постає очевидним той факт, що дійсно існує низка викликів, що виникають у сучасному нестабільному безпековому середовищі, яке характеризу-

ється, перш за все, дедалі більш розмитою відмінністю між війною та миром, що впливає на всі сфери державної політики, у тому числі й на державну інформаційну політику. У цьому природно складному та дедалі неоднозначному середовищі концепції гібридних загроз і гібридної війни (надалі – «ГЗ і ГВ») допомагають як у структуруванні розуміння природи загроз, з якими ми стикаємося, так і в стратегії та методах потенційних супротивників. Таким чином, слід використовувати комплексний погляд на загрози, а також на існуючі інструменти та засоби протидії їм [7, с. 103].

Такий комплексний погляд акцентує увагу на природі загроз і супротивників, а також викликах, які вони створюють для демократичних країн. При цьому стає все більш важливим питання спроможності демократій та демократичних державних інституцій безпеки протистояти ГЗ і ГВ, розуміючи конкретні вразливі місця в демократичних суспільствах і ліквідуючи їх, а також розробляючи відповіді на ворожі заходи з боку зовнішніх акторів. Особлива вразливість і обмеження, а також переваги демократій вимагають особливих підходів у цьому середовищі [1, с. 3]. Відкриті суспільства, побудовані на нормативних засадах верховенства права, прав людини та демократії, обов'язково захищаючи свободу слова, об'єднань і преси, повинні розробити рішення, які не тільки зберігають ці основні свободи, але й спираються на їхні сильні сторони. Як показує досвід багатьох країн, ця робота йде повним ходом, для чого залучаються численні організації, яким доручено аналізувати та вирішувати проблему протидії гібридним загрозам, у тому числі (а часто і переважно) в інформаційній сфері [8, с. 330-331].

Враховуючи складний характер наявних загроз, реагування має бути організованим відповідно спільних принципів, інтегруючи різні сектори суспільства, а також різні держави [2, с. 14]. Ще один важливий висновок, який випливає з розглянутого вище, це важливість знання свого противника. У той час як ідентифікація та приписування загроз створює реактивні відповіді, проактивне усунення наявних вразливостей для підвищення стійкості вимагає усвідомлення не лише того, що робить супротивник, але й чому [4, с. 95]. У зв'язку з цим актуальним стає погляд на світ очима супротивника, щоб визначити стратегічні цілі та шляхи їх досягнення, а також уразливі місця супротивника.

Сучасні дослідження також включають (принаймні більшість з них) успішні приклади протидії гібридній війні. Результатом багатьох досліджень стало комплексне уявлення про те, що можна назвати «гібридністю», яке замість статичної картини дій і реакцій забезпечує крос-секційне та міжчасове розуміння взаємодії між акторами, загрозами, відповідями та результатами [3, с. 10]. До цього гібридність була певним «ярликом», який використовувався в соціальних науках «для позначення процесів, у яких окремі соціальні практики або структури, що існували різними способами, поєднуються, створюючи нові структури, об'єкти та практики, у яких змішуються попередні елементи» [5, с. 101]. Запропонована нами нижче модель гібридного впливу в інформаційній сфері дає картину того, як поточні або потенційні ворожі гібридні заходи та відповіді на них динамічно впливають на довгострокову суспільну вразливість і стійкість [9, с. 199].

Безумовно, повне розуміння та протидія ГЗ і ГВ є складним, але водночас дуже важливим завданням державної інформаційної політики. Далі ми наведемо схематичну модель того, як зрозуміти ГЗ і ГВ в інформаційній сфері. Дану модель можна представити в трьох версіях, перша з яких представляє спрощену картину динаміки ГЗ і ГВ та, а також відповіді на них і контрзаходів [6, с. 13]. Друга версія додає часовий вимір до цього зв'язку, демонструючи, як короткострокові дії та відповіді пов'язані з довгостроковою вразливістю та стійкістю. Третя версія, навпаки, спрямована на надання точнішої картини складної ситуації в реальному світі. Метою моделі є надання можливості не тільки краще зрозуміти саму динаміку, але й те, як ідентифікувати, зрозуміти та протидіяти ГЗ і ГВ. Спрощена модель описує схематичну модель динаміки взаємопов'язаних відносин між захисником і нападником у короткостроковій і довгостроковій перспективі, а також те, як взаємодіють різні параметри, пов'язані з часом та акторами.

Спрощена модель гібридного впливу в інформаційній сфері включає виміри часу та акторів. Обидва вони важливі, оскільки ГЗ і ГВ не є ані одноразовою подією, ані її неможливо тимчасово відокремити від певного контексту [10, с. 12]. У цій моделі включено два актори, захисник та нападника, разом із двома часовими вимірами, «короткий термін» і «тривалий термін». У короткостроковій перспективі битва складається з безперервного взаємного процесу між ГЗ і ГВ, який здійснює нападник, і різними відповідями та контрзаходами захисника. Це безперервний і постійний процес без заздалегідь визначеного початку чи кінця.

У довгостроковій перспективі конкуренція відбувається між вразливими сторонами захисника та стійкістю, створеною для їх усунення. Очікується, що нападник виявить вразливі місця, щоб використати їх. Вразливі місця, виявлені захисником, – «виявлення власних вразливостей», – допомагають підвищити стійкість захисника. Зусилля щодо підвищення стійкості логічно означатимуть зміну вразливостей. Але навіть якщо

вразливості зменшаться, зміни на стороні захисника теоретично можуть відкрити нові вразливості, які зловмисник виявить і використає – «збільшення або зменшення вразливостей» [11, с. 193].

З боку захисника також існує взаємозв'язок між короткостроковими реакціями та контрзаходами з одного боку та формуванням довгострокової стійкості з іншого боку. Існуюча стійкість впливає на здатність захисника реагувати та вживати контрзаходів проти атак і загроз («збільшення або зменшення здатності до відповіді»). У свою чергу відповіді та контрзаходи підвищують або зменшують стійкість захисника. Коротше кажучи, між довгостроковою та короткостроковою перспективами з обох сторін відбувається зворотний процес.

Однією з проблем спрощеної моделі є те, що, хоча вона надає схематичну картину гібридних конфліктів, вона не враховує аспекти хаосу, обману та заперечення ГЗ і ГВ у реальному світі, вона просто не повністю враховує безлад, що там існує [12, с. 55]. Щоб забезпечити додаткове та точніше уявлення про складне середовище безпеки, ми пропонуємо більш складну версію моделі гібридного впливу в інформаційній сфері. Дана модель особливо корисна для зображення ситуації, коли ціль ГЗ і ГВ постійно буде наосліп атакована з усіх можливих кутів незліченними невеликими атаками, які неможливо відокремити одна від одної чи локалізувати, що робить захисника нездатним адекватно відповісти та протидіяти. Більше того, ГЗ і ГВ можуть бути неідентифіковані (це властиво обману та запереченню гібридності), якщо джерело або анонімне, або прикрите через використання проксі-серверів.

Наразі безсумнівно, що ГЗ і ГВ в інформаційній сфері потрібно вирішувати за допомогою комплексного всеохоплюючого підходу [13,с. 59]. Немає жодної загрози, немає правильної відповіді на те, як протидіяти ГЗ і ГВ і реагувати на них, ані як створити стійкість. Також немає жодного актора чи структури, які можуть досягти успіху як сьогодні, так і завтра. Необхідно адаптуватися та адаптуватися заново, коли опонент і загроза постійно змінюються. Як зазначив Сунь Цзи: «Найбільша перемога – це та, яка не потребує битви». Тому найкраще рішення у гібридній війні – не шукати битви, а знайти способи досягти такої перемоги. Один із способів досягти цього — думати про ГЗ і ГВ так само, як Лао-Цзи думав про воду. Вода текуча, м'яка, податлива. Але вода буде зношувати камінь, який твердий. Як правило, те, що текуче, м'яке і податливе, переможе те, що жорстке і жорстке. Це ще один парадокс: те, що м'яке, є сильним.

Парадокс «м'який як сильний» є хорошим орієнтиром, якщо розглядати ГЗ і ГВ і відповіді та контрзаходи на них, а також стійкість і вразливість [14, с. 144]. Щоб досягти успіху, не можна зосереджуватися лише на жорсткій обороні чи жорсткій безпеці, а також шукати битви. Це може призвести до виснаження супротивника в результаті гібридної війни, гібридні заходи, якщо вони є плавними, м'якими та поступливими, то подолають усе, що є жорстким та твердим. Противник виявлятиме м'які цілі, працюватиме за сприятливих умов, щоб націлитися на виявлені вразливі місця, шукаючи способи уникнути або обійти механізм виявлення, нейтралізуючи здатність реагувати та протидіяти [15, с. 95]. Загрози можуть бути навіть невизначеними або невідомими, коли можна не знати, що хтось є ціллю або що існує загроза. Так будуть подолані жорсткість і твердість. Подібним чином захист також має бути плавним, м'яким і гнучким. Тільки так можна добитися перемоги над супротивником, використовуючи повний спектр гібридних засобів.

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, можна зробити висновок, що під час розробки заходів з протидії гібридним загрозам в інформаційній сфері надзвичайно корисним може бути метод аналізу витрат і вигод. Хоча його застосування до цілей опонента може не поставити основні публічні організації та координаційні безпекові центри на перше місце в списку, але дійсно, вигода від їх зриву була б великою, але оскільки вони, швидше за все, також підготовлені та мають навички запобігання загрозам у зоні своєї відповідальності, позитивний результат стає невизначеним, а ризик швидкого викриття – великим. Натомість цей аналіз може принести користь сферам, які перебувають між відповідальністю публічних організацій, є «сліпими плямами», де загрози можуть виявлятися повільно, а реагування потребує певного часу.

Окрім того, надзвичайно важливо розробити систему виявлення, яка одночасно розпізнає хибнопозитивні та хибнонегативні результати. Існує потреба в прагматичності, гнучкості та інклюзивності акторів, секторів і рівнів – усередині та між країнами. Гібридний захід не прийде туди, де його очікують, принаймні не завжди. Коли контрзаходи будуть успішними, супротивник змінить схему атаки. Тому необхідно залучати всіх акторів і враховувати як короткострокові, так і довгострокові перспективи. Тобто важливо співпрацювати між секторами та рівнями та не допускати, щоб традиційні кордони перешкоджали співпраці. Це ніколи не є таким важливим, як під час протидії ГЗ і ГВ, оскільки вразливі місця, як правило, існують саме в прикордонних сферах між секторами та рівнями, і це те, на що опонент буде цілитися. Це вимагає співпраці насамперед в інформаційній сфері, яка повинна розвиватися в публічному та приватному секторах, а також від місцевого та регіонального рівнів до національного та міжнародного.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Zubchenko, S. (2018). Vijna Putina proty Ukrajiny. Revoljucija, nacionalizm i kryminalitet [Putin's war against Ukraine. Revolution, nationalism and criminality]. Kyiv, Duh i Litera [in Ukrainian].

2. Maghda, E. (2017). Ghibrydna aghresija Rosiji: uroky dlja Jevropy [Russia's Hybrid Aggression: Lessons for Europe]. Kyjiv, Kalamar [in Ukrainian].

3. Kurban, O. V. (2016). Suchasni informacijni vijny v merezhevomu on-lajn prostori [Modern information wars in the online network space]. Kyjiv: VIKNU. Retrieved from http://www.mil.univ.kiev.ua/files/222_1044284240.pdf [in Ukrainian].

4. Lytvynenko, O. (2017). Evoljucija ghibrydnoji vijny Rosijsjkoji Federaciji proty Ukrajiny [The evolution of the hybrid war of the Russian Federation against Ukraine]. *Nauka i oborona – Science and defense*, 2. 11-16 [in Ukrainian].

5. Valjushko, I. O. (2015). Evoljucija informacijnykh vijn: mynule i suchasnistj [Evolution of information wars: past and present]. *Istoryko-politychni studiji – Historical and political studies*, 2. 127-134 [in Ukrainian].

6. Kravchenko, V. (2015). Teorija «ghibrydnoji vijny»: ukrajinsjkyj vymir [The theory of «hybrid war»: the Ukrainian dimension]. *Visnyk Dnipropetrovsjkogho universytetu – Bulletin of Dnipropetrovsk University*, 2. 144-148 [in Ukrainian].

7. Nyzhnyk, N. R. & Mosov, S. P. (2011). Teoretychni aspekty derzhavnoho upravlinnia [Theoretical aspects of public administration]. Chernivtsi: Tekhnodruk [in Ukrainian].

8. Ielahin, V. P. (2010). Sotsialna polityka: teoretyko-metodolohichni ta kontseptualni pidkhody [Social policy: theoretical, methodological and conceptual approaches]. Kharkiv [in Ukrainian].

9. Skurativskyi, V. (2011). Sotsialna bezpeka ukrainskoho suspilstva ta shliakhy yii zabezpechennia [Social security of Ukrainian society and ways of ensuring it]. *Visnyk NADU – Bulletin of the National Academy of Public Administration Under the President of Ukraine*, 3. 194-204 [in Ukrainian].

10. Averianov, V. B. (1998). Derzhavne upravlinnia: teoriia i praktyka [Public administration: theory and practice], Kyiv: Yurinkom Inter [in Ukrainian].

11. Panchenko, O. A. (2011). Informacijna bezpeka osobystosti: monoghrafija [Personal information security: monograph], Kyiv: KIT [in Ukrainian].

12. Bakumenko, V. D. (2003). Teoretychni ta orhanizatsiini zasady derzhavnoho upravlinnia [Theoretical and organizational principles of state administration]. Kyiv: Vydavnytstvo NADU [in Ukrainian].

13. Hrabar, N. S. & Khmyrov, I. M. (2021). Stanovlennia ta transformatsiia mekhanizmiv derzhavnoho upravlinnia (na prykladi upravlinnia intelektualno-innovatsiinymy resursamy ekonomiky v Ukraini) [Formation and transformation of state management mechanisms (on the example of management of intellectual and innovative resources of the economy in Ukraine).]. *Visnyk NUTZU. Seriia «Derzhavne upravlinnia» – Bulletin of the National University of Civil Defense of Ukraine. «Public administration»*, 1(14), 58-65. DOI: https://doi.org/10.52363/2414-5866-2021-1-8 [in Ukrainian].

14. Nadobko, S. V. (2020). Intelektualna vlasnist yak obiekt administratyvno-pravovoi okhorony [Intellectual property as an object of administrative and legal protection]. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia – Expert: Paradigm of Legal Sciences and Public Administration*, 3(9), 141-149. DOI: https://doi.org/10.32689/2617-9660-2020-3(9)-141-149 [in Ukrainian].

15. Hoshovska, V. A. (2003). Sotsialna dominanta natsionalnoi bezpeky [Social dominance of national security]. *Stratehichna panorama − Strategic panorama*, 2, 94-99 [in Ukrainian].