DOI: https://doi.org/10.26565/1992-2337-2022-2-06
УДК 351.88::327.7::341.11

Хряпинський Антон Петрович,
кандидат юридичних наук,
директор ТОВ "ХРЯПИНСЬКИЙ І КО",
вул. Ахсарова, 4/6 А, м. Харків, 61022, Україна
e-mail: Khryapynskyy@meta.ua https://orcid.org/0000-0002-2492-051X

СФЕРИ ВПЛИВУ ТА ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ ГІБРИДНИХ ЗАГРОЗ: МОДЕЛІ ТА МЕХАНІЗМИ

Анотація. У статті наведено розв'язання актуальної наукової проблеми обґрунтування та виокремлення сфер впливу та інструментів реалізації гібридних загроз в контексті визначення моделей та відповідних механізмів. Комплексно аргументовано, що гібридні загрози націлені на зміну станів і створення необхідних ситуацій у кількох сферах шляхом застосування комбінацій інструментів. Кожен інструмент націлений на одну або кілька сфер або взаємодію між ними, створюючи або використовуючи вразливість або використовуючи можливість. Ось чому важливо визначити сфери можливого впливу або критичні функції, яким держава повинна забезпечити стійкість проти гібридних загроз, оскільки вони сильно пов'язані з національною безпекою та здатністю держави приймати рішення.

За результатами аналізу літературних джерел з питань гібридних загроз виокремлено тринадцять сфер впливу: політична, економічна, інфраструктурна, правова, соціальна, культурна, військова, інформаційна, кібернетична, публічного управління, дипломатична, розвідувальна, комунікаційна. Доведено, що у кожній сфері існують специфічні моделі та механізми, якими актор гібридної загрози може викликати бажаний для нього ефект, більше того, цей ефект може охоплювати різні сфери, оскільки вони тісно пов'язані один з одним.

Встановлено, що до появи і поширення концепції гібридних загроз основний підхід завжди включав військове втручання та фізичну окупацію як передумову для захоплення незалежної країни. Але в сучасних умовах суттєвий контроль актора над певним об'єктом може бути досягнутий без обов'язкової участі у відкритих військових діях. Крім того, актори можуть використовувати стратегію гібридної загрози, щоб послабити цільовий стан без жодного наміру фізичного контролю. Це означає, що військово-орієнтований підхід може не дати точної картини всього спектру поточних загроз і викликів. Показано, що у будь-якій концептуальній роботі важливо знайти баланс між детальністю та аналітичною цінністю узагальнення. Можливо, варто зазначити, що все ще існує кілька субсфер, і деякі наведені нижче приклади демонструють комбінації різних сфер, тому можуть бути альтернативні підходи як до консолідації, так і до розширення списку доменів.

Ключові слова: управління, гібридні загрози, протидія та превенція, інноваційний розвиток, протидія загрозам, превенція загрозам, гібридні загрози в управлінні.

Як цитувати: Хряпинський А. П. Сфери впливу та інструменти реалізації гібридних загроз: моделі та механізми. *Державне будівництво.* 2022. № 2 (32). С. 60–67. DOI: https://doi.org/10.26565/1992-2337-2022-2-06

In cites: Khriapynskyi, A.P. (2022). Spheres of influence and tools for implementing hybrid threats: models and mechanisms. *State Formation, 2 (32), 60–67.* DOI: https://doi.org/10.26565/1992-2337-2022-2-06 [in Ukrainian].

Постановка проблеми. Сьогодні світ стрімко змінюється під впливом сучасних технологій, які багато в чому зближують людей усієї земної кулі. Справді, за допомогою мережі Інтернет ми можемо спілкуватися з будь-якою людиною в будь-якій точці світла, обмінюючись миттєвими повідомленнями. З одного боку, це робить наше життя більш вільним та зручним. З іншого боку, розмиваються національні кордони і, що значно важливіше, традиції держав. Глобалізація дуже широко обговорюється в сучасній науковій літературі в різних аспектах. Однак у цій статті ми пропонуємо звернутися до дослідження наслідків глобалізації та масового поширення сучасних технологій для безпеки держав. Насамперед йдеться про формування єдиного світового інформаційного простору, який кардинально змінює духовне життя суспільства та виступає одним із ключових факторів формування нової національної самосвідомості. Сучасні ЗМІ та соціальні мережі дозволяють створювати та передавати на будь-які відстані інформаційних продуктів. У результаті відбувається інтенсивний процес міжкультурних комунікацій, та слід визнати, що наша держава не так пропонує світові свої культурні цінності, що споживає запропоновані ціннісні зразки, які вже досить міцно вкоренилися в національній свідомості. Ці інструменти включають різні способи іноземного впливу на громадянське суспільство, інформаційно-комунікаційні та соціальні системи держав. На вирішення військових, політичних, економічних конфліктів у міжнародних відносини все активніше впливають інформаційні прийоми формування громадської думки, фінансово-економічні технології впровадження масових стандартів, просування культурно-історичних оцінок моделей національного розвитку, рейтингові оцінки фінансової та соціальної стабільності тощо.

Аналіз останніх досліджень і публікацій. Теоретико-прикладні аспекти дослідження внутрішніх загроз знайшли своє відображення у наукових працях багатьох вчених, зокрема таких як: Л. Акімова, С. Лазаренко, В. Ліпкан, Н. Словацька. Водночас, питання пов’язані із комплексним науковим обґрунтуванням та дослідженням сфер впливу та інструментів реалізації гібридних загроз в контексті розкриття моделей та механізмів ще не отримали належного теоретико-прикладного обґрунтування та аналізу.

Метою даної статті є наукове обґрунтування та дослідження сфер впливу та інструментів реалізації гібридних загроз в контексті розкриття моделей та механізмів.

Виклад основного матеріалу. Як відомо, гібридні загрози націлена на зміну станів і створення необхідних ситуацій у кількох сферах шляхом застосування комбінацій інструментів. Кожен інструмент націлений на одну або кілька сфер або взаємодію між ними, створюючи або використовуючи вразливість або використовуючи можливість. Ось чому важливо визначити сфери можливого впливу або критичні функції, яким держава повинна забезпечити стійкість проти гібридних загроз, оскільки вони сильно пов’язані з національною безпекою та здатністю держави приймати рішення.

За результатами аналізу літературних джерел з питань гібридних загроз нами було визначено тринадцять таких сфер: політична, економічна, інфраструктурна, правова, соціальна, культурна, військова, інформаційна, кібернетична, публічного управління, дипломатична, розвідувальна, комунікаційна. Тут ми використовували підхід, запропонований у широко відомій праці «The landscape of hybrid threats: A conceptual model» [1, с. 18], а також при визначені сфер впливу гібридних загроз враховувалися такі основні аспекти.

По-перше, у всіх абревіатурах, які позначають інструменти національної безпеки, основною завжди була військова компонента. До появи і поширення концепції гібридних загроз основний підхід завжди включав військове втручання та фізичну окупацію як передумову для захоплення незалежної країни. Але в сучасних умовах суттєвий контроль актора над певним об'єктом може бути досягнутий без обов'язкової участі у відкритих військових діях. Крім того, актори можуть використовувати стратегію гібридної загрози, щоб послабити цільовий стан без жодного наміру фізичного контролю. Це означає, що військово-орієнтований підхід може не дати точної картини всього спектру поточних загроз і викликів. По-друге, у будь-якій концептуальній роботі важливо знайти баланс між детальністю та аналітичною цінністю узагальнення. Можливо, варто зазначити, що все ще існує кілька субсфер, і деякі наведені нижче приклади демонструють комбінації різних сфер, тому можуть бути альтернативні підходи як до консолідації, так і до розширення списку доменів. По-третє, наразі не існує загального чи універсального підходу до структурування гібридних інструментів. Тому немає вагомих причин вибирати будь-які існуючі концепції з безлічі підходів, які використовуються паралельно і які не повністю відповідають вимогам опису гібридних загроз. По-четверте, переліки сфер та інструментів залишаються відкритими і ні в якому разі не остаточними. Дослідники або практики можуть обмежити кількість сфер, об'єднавши деякі, або збільшити їхню кількість шляхом подальшого уточнення деталей. Точне розуміння кожної конкретної ситуації стане наріжним камнем адекватної реакції та подолання прогалин у стійкості.

Не кожен інструмент і діяльність, націлені на сфери впливу, можна класифікувати як гібридну загрозу. Подібним чином, не всі активи в межах сфери однаково важливі для ворожого суб'єкта. Вплив гібридної загрози, націлений на сфери та використання сфер як середовища, описане нижче, буде кваліфікована як така шляхом одночасного використання кількох інструментів у скоординованій кампанії, спрямованій на використання вразливостей або можливостей і, як наслідок, на підрив процесу прийняття рішень опонентом, зберігаючи певний ступінь правдоподібного заперечення.

Сфери не слід досліджувати ізольовано, оскільки вплив на одну сферу може викликати каскадні ефекти в інших. Це особливо важливо, коли розглядається вплив гібридної загрози на ту чи іншу сферу. В одній з праць зазначається, що «серія синхронізованих, слабо спостережуваних або

неспостережуваних подій… зазвичай стає очевидною лише тоді, коли починають проявлятися їхні кумулятивні та нелінійні ефекти» [1, с. 53]. У цій же праці дії, спрямовані на одну сферу, додатково аналізуються, щоб відобразити впливи першого та другого порядку на інші сфери. Нижче коротко описана кожна сфера з наголосом на компоненти сфери, на які може націлитися гібридна загроза, а також на зв'язки між сферами.

1. *Політична сфера*. У контексті гібридних загроз політична сфера охоплює акторів, які здійснюють владу чи правлять на певній території шляхом застосування різних форм політичної влади та впливу. У сучасних демократичних державах посадовці або обираються народом чи його представниками, або призначаються обраними особами. При цьому очікується, що політична система буде репрезентувати культурні, історичні, демографічні та іноді релігійні фактори, які формують ідентичність суспільства. Права громадян, вибори та підзвітність посадовців зазвичай є характерними ознаками демократії [1, с. 103].

2. *Економічна сфера*. Економіка як сфера гібридних загроз визначається як виробництво, розподіл і споживання всіх товарів і послуг для країни, і включає її економічний розвиток і розподіл багатства. Державне регулювання економіки або досягнення цілей зовнішньої політики шляхом використання зовнішніх факторів безпеки економічних взаємодій завжди було традиційним джерелом державної влади та впливу. У цьому сенсі Блеквілл і Гарріс запропонували використовувати термін «геоекономіка» як адаптацію терміну «геополітика» [2, с. 89-90].

3. *Інфраструктурна сфера.* Хоча немає загальноприйнятого визначення критичної інфраструктури (КІ), усі визначення підкреслюють роль КІ, що сприяє життєзабезпеченню суспільства, або робить виснажливий ефект на нього у разі збою [3, с. 26]. Європейське визначення розглядає «критичну інфраструктуру» як: «Актив, система або її частина, розташована в державах-членах, яка є важливою для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, безпеки, економічного чи соціального добробуту людей, і порушення або знищення якої матиме значний вплив на державу-член в результаті нездатності підтримувати ці функції» [4, с. 182].

4. *Правова сфера.* З точки зору нашого дослідження правова сфера відноситься до сукупності правових норм, дій, процесів та інститутів, включаючи як їх нормативний, так і фізичний прояв, які використовуються або можуть бути використані для досягнення правових або неправових наслідків у контексті гібридних загроз [5, с. 107]. По-перше, суб'єкти, які хочуть підірвати демократичні держави або держави, що демократизуються, використовують право з метою подолання конкретних вразливих місць у демократичних суспільствах. Наприклад, покладання на право на свободу слова створює простір для кампаній з дезінформації. По-друге, право використовується для досягнення руйнівних, підривних чи інших зловмисних ефектів у цільовій нації чи проти неї. По-третє, у багатьох випадках право використовується у спосіб,

який є образливим або іншим чином руйнує верховенство права. По-четверте, право часто використовується для досягнення ефекту в інших сферах, зокрема (але не тільки) в інформаційному просторі, тоді як діяльність в інших сферах може бути розроблена або використана для досягнення ефекту в правовій сфері.

5. *Соціальна сфера*. Соціальна сфера зазвичай використовується для створення, поглиблення або використання соціокультурних розколів, які породжують соціальні потрясіння, необхідні для продовження чи успіху впливу гібридної загрози. Спірні питання, такі як безробіття, бідність і освіта, завжди є предметом дебатів у західних суспільствах, і тому є легкою мішенню. Однак питання, які можуть створити або підтримувати кризу, є особливо привабливими. Як приклад можна зазначити недавній економічний спад, нелегальну імміграцію та терористичні атаки (інциденти з активною стрілянино, кібератаки, тощо). Кінцевою метою гібридних атак у цій сфері є вплив на те, як функціонує суспільство в цільовій державі, щоб створити сприятливі умови для реалізації гібридних загроз в різних сферах.

6. *Культурна сфера*. Ця сфера передбачає використання агресором культурної державної експансії для підтримки ворожих цілей за допомогою гібридної діяльності. Сфера державного управління культурою може бути внутрішньою або зовнішньою. Внутрішнє управління культурою передбачає використання культурних і цивілізаційних тем для визначення фундаментальних елементів національної ідентичності», тоді як стратегія зовнішньої культурної політики намагається просувати культуру як засіб створення привабливого іміджу за кордоном [6, с. 18–19].

7. *Військова сфера.* У військових операціях основним завданням є збереження незалежності, а також недоторканності та єдності території рідної країни, зокрема для підтримки та захисту суверенітету.

У мирний час військові приєднуються до цивільних органів влади для навчань і надання допомоги. Для того, щоб мати можливість швидко реагувати на терористичні атаки, на запити цивільної влади про допомогу (у разі пошкодження повенями, лавинами тощо), а також на зміни в безпосередній близькості від рідної країни, військові сили повинні підтримувати постійну присутність на певних територіях. Порушення військової та оборонної спроможності країни може бути дуже ефективним засобом посилення впливу, здійснення тиску та, у деяких випадках, підготовки ґрунту для майбутніх військових операцій. Порушення військової обороноздатності країни викликає реакцію постраждалої країни, що призводить до збільшення витрат на оборону та виснаження різноманітних ресурсів. Це також неявний спосіб здійснення економічного тиску. Вплив у військовій сфері також може підштовхнути ціль до ескалації, реагуючи на дії, які вважаються ворожими, і це може бути метою гібридної акції.

8. *Інформаційна сфера*. Використання інформації як зброї залишається характерною рисою гібридних загроз і нелінійних стратегій. Інформацію використовують, щоб підірвати уявлення про безпеку людей, протиставляючи

політичні, соціальні та культурні ідентичності одна одній. Мета інформаційного впливу часто полягає в тому, щоб використати у власних інтересах політику ідентичності та лояльності, розділивши впливові групи інтересів і політичні альянси [7, с. 4].

9. *Кібернетична сфера.* Кібернетичний вимір відіграє виняткову та дуже специфічну роль щодо гібридних загроз сьогодні, не в останню чергу тому, що будь-що важливе, що відбувається в реальному світі, включно з кожним політичним і військовим конфліктом, також відбувається у кіберпросторі. З точки зору національної безпеки це включає кіберзлочинність, пропаганду, шпигунство, тероризм і навіть саму війну. Природа загроз національній безпеці не змінилася, але кіберпростір надає новий механізм, канали та інструменти здійснення ворожих впливів, які можуть збільшити швидкість, розповсюдження та силу атаки, а також забезпечити анонімність і невиявленість. Низька ціна входу, анонімність та асиметрія вразливості означають, що дрібніші актори мають більше можливостей для здійснення впливів у кіберпросторі, ніж у багатьох більш традиційних сферах.

10. *Сфера публічного управління.* Публічне управління тлумачиться в його найширшому розумінні як «процес перетворення державної політики на результати» [8, с. 13]. Дихотомія політика-управління визначається як фундаментальна риса європейських суспільств [9, с. 44–45]. Іншими словами, публічне управління існує для виконання закону та правил. Проте хоча ця концепція зрозуміла в теорії, вона може бути важко застосовною на практиці. По-перше, під час тлумачення закону з метою втілення його в життя публічні службовці можуть ненавмисно робити оціночні судження, які можуть мати політичний характер. По-друге, публічне управління природно сприяє формуванню політики, оцінюючи існуючу політику та організовуючи формулювання нової. Тому основною метою гібридних атак у цій сфері є вплив на осіб, що приймають рішення у системі публічного управління.

11. *Дипломатична сфера.* Тут дипломатія тлумачиться в її міжнародному вимірі як ведення міжнародних відносин. Зовнішня політика традиційно зосереджена на безпеці, і при цьому нормативні теорії міжнародних відносин виправдовують війну як оборонний захід проти спровокованої агресії з урахуванням обмежень пропорційності та захисту некомбатантів [10, с. 87].

12. *Розвідувальна сфера.* Згідно з Ловенталєм, розвідка – це процес, за допомогою якого запитуються, збираються, аналізуються та надаються політикам певні типи інформації, важливої для національної безпеки; продукти цього процесу; захист цих процесів і цієї інформації за допомогою контррозвідувальної діяльності; і проведення операцій за вимогою законних органів влади [11, с. 15]. Розвідка надає тим, хто приймає рішення, обізнаність щодо ситуації, необхідну для прийняття стратегічних рішень і рішень, пов’язаних із безпекою. Таким чином, розвідувальна діяльність повинна бути розроблена та реалізована для задоволення потреб, визначених особами, які приймають рішення, або передбачених їхніми політичними вказівками.

13. *Комунікаційна сфера.* Комунікаційні послуги включають навігацію, зв'язок, дистанційне зондування, а також науку та дослідження. Зростає занепокоєння щодо гібридних загроз у комунікаційній сфері через те, що кілька країн розробляють контркосмічні можливості за допомогою кількох державних суб'єктів, які можуть вплинути на комунікації, що здійснюються саме через супутниковий зв'язок [12, с. 8]. Вплив гібридних операцій у комунікаційній сфері впливає не лише на військову сферу, але також може мати значний вплив на цивільну комерційну діяльність, оскільки вона все більше покладається на комунікаційні можливості. Насправді, більшість інструментів, які можуть націлюватися на комунікаційну сферу, використовують зв'язок комунікаційних активів з іншими сферами, описаними в даному параграфі, і потенційні каскадні ефекти, якщо вони стають скомпрометованими, навіть тимчасово. Ця сфера тісно пов'язана із військовою, розвідувальною, економічною, інфраструктурною та інформаційною сферами.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, у кожній сфері існують специфічні моделі та механізми, якими актор гібридної загрози може викликати бажаний для нього ефект, більше того, цей ефект може охоплювати різні сфери, оскільки вони тісно пов'язані один з одним.

Стаття надійшла до редакції 16.10.2022 р.
Стаття рекомендована до друку 20.11.2022 р.

Khriapynskyi A. P.,
Candidate of Law,
director TOV "KHRYAPINSKY AND CO",
St. Akhsarova, 4/6 A, Kharkiv, 61022, Ukraine
e-mail: Khryapynskyy@meta.ua *https://orcid.org/0000-0002-2492-051X*

SPHERES OF INFLUENCE AND TOOLS FOR IMPLEMENTING HYBRID THREATS: MODELS AND MECHANISMS

Annotation. The article provides a solution to the current scientific problem of substantiating and distinguishing spheres of influence and tools for the implementation of hybrid threats in the context of defining models and relevant mechanisms. It is comprehensively argued that hybrid threats are aimed at changing states and creating necessary situations in several areas by applying combinations of tools. Each tool targets one or more areas or the interaction between them, creating or exploiting a vulnerability or exploiting an opportunity. This is why it is important to identify the areas of possible influence or critical functions that a state must ensure resilience against hybrid threats, as they are strongly related to national security and the state's decision-making capacity.

According to the results of the analysis of literary sources on hybrid threats, thirteen spheres of influence are distinguished: political, economic, infrastructural, legal, social, cultural, military, informational, cybernetic, public administration, diplomatic, intelligence, communication. It has been proven that in each sphere there are specific models and mechanisms by which a hybrid threat actor can cause the desired effect for him, moreover, this effect can cover different spheres, as they are closely related to each other.

It was established that before the emergence and spread of the concept of hybrid threats, the main approach always included military intervention and physical occupation as a prerequisite for capturing an independent country. But in modern conditions, significant control of an actor over a certain object can be achieved without mandatory participation in open military operations. In addition, actors can use a hybrid threat strategy to weaken the target state without any intention of physical control. This means that a military-oriented approach may not provide an accurate picture of the entire spectrum of current threats and challenges. It is shown that in any conceptual work it is important to find a balance between detail and analytical value of generalization. It may be worth noting that there are still multiple subfields, and some of the examples below show combinations of different fields, so there may be alternative approaches to both consolidation and expanding the domain list.

Keywords: management, hybrid threats, counteraction and prevention, innovative development, countermeasures against threats, prevention of threats, hybrid threats in management.

REFERENCES

1. Nemeth, William, J. (2002). Future War and Chechnya: A Case for Hybrid Warfare. Monterey: Naval Postgraduate School.
2. Newton, K., J. W. van Deth (2010). Foundations of Comparative Politics: Democracies of the Modern World. 2nd ed. Cambridge: Cambridge University Press.
3. Norris, William J. (2016). Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control. Ithaca: Cornell University Press.
4. Nye, Joseph S. (2013). What China and Russia Don't Get About. Soft Power. *Foreign Policy*. DOI: https://doi.org/10.2307/1148580
5. Nye, Joseph (1990). Soft Power. *Foreign Policy, 80, 153–171.* DOI: https://doi.org/10.2307/1148580
6. O'Rourke, Ronald (2018). A Shift in the International Security Environment: Potential Implications for Defense – Issues for Congress.
7. Oyserman, Daphna, Spike W. S. Lee (2008). Does Culture Influence What and How We Think? Effects of Priming Individualism and Collectivism. *Psychological Bulletin, 134 (2), 311–342.* DOI: https://doi.org/10.1037/0033-2909.134.2.311
8. Pacheco, Fernando Celaya (2009). Narcofearance: How Has Narcoterrorism Settled in Mexico? *Studies in Conflict & Terrorism, 32 (12), 1021–1048.* DOI: https://doi.org/10.1080/1057610090331979 7
9. Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman (2018). Countering Information Influence Activities. Swedish Civil Contingencies Agency.
10. Parton, Charles (2019). China-UK Relations Where to Draw the Border Between Influence and Interference? London.
11. Pindják, Peter (2014). Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together? NATO Review.
12. PSSI (2018). Europe's Preparedness to Respond to Space Hybrid Operations.

The article was received by the editors 16.10.2022.
The article is recommended for printing 20.11.2022.