СОЦІАЛЬНА СТРУКТУРА, СОЦІАЛЬНІ ІНСТИТУТИ ТА ПРОЦЕСИ

УДК 316.4:355
DOI https://doi.org/10.24195/spj1561-1264.2020.2.8

Криворучко Максим Геннадійович
аспірант кафедри соціології та політології
Національного технічного університету «Харківський політехнічний інститут»
вул. Кирпичова 2, Харків, Україна

ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ: СКЛАДНОСТІ ТА ДОСВІД УКРАЇНИ

Стаття присвячена проблемі російсько-української війни, що поєднує як традиційні військові збройні заходи, так і новітні методи деструктивного впливу на державу та суспільство країни, яка є об'єктом агресії. Це утворює міждисциплінарну ситуацію. Зокрема, цивільно-військові операції досліджуються соціально-гуманітарними дисциплінами, у тому числі соціологією. Традиційне визначення війни: «конфлікт між державами або цивільними об'єднаннями, що відбувається у формі бойових дій з метою нав'язати противнику свою волю», у сучасних реаліях втрачає актуальність, адже більшість розвинених країн не можуть дозволити собі починати відкриті збройні зіткнення для досягнення своїх цілей. Поточну ситуацію добре описує концепція гібридної війни, висунута колишнім офіцером морської піхоти, а нині науковим співробітником Міністерства оборони США Френком Хоффманом. У цій статті під цим поняттям мається на увазі сучасна форма ведення війни, що відрізняється переважанням невійськових методів впливу над традиційними бойовими діями або навіть повною відмовою від них. Досвід України у протидії гібридним загрозам доцільно узагальнити з метою посилення національної безпеки та інформування союзників України щодо небезпек та ризиків гібридної війни. Метою статті є опис сучасних методів гібридної агресії, що застосовуються проти України протягом останніх років, і узагальнення досвіду протидії гібридним загрозам як з боку держави, так і силами громадянського суспільства. Для вирішення цього завдання поточні загрози розділені на 8 кластерів, що включають пропаганду і дезінформацію, збір персональних даних та стеження за громадянами, хакерські атаки, економічний тиск, упровадження в державний апарат замаскованих представників, розпалювання громадянських конфліктів, створення та підтримку сепаратистських та терористичних угруповань. Розглянуто ступінь небезпеки цих загроз, наведені відповідні приклади, описані приклади протидії гібридним загрозам з боку держави та громадського суспільства.

Ключові слова: *війна, гібридна війна, громадянський конфлікт, негативне управління громадянським конфліктом, шляхи протидії гібридним загрозам, методи ведення гібридної війни.*

Вступ. Актуальність теми статті визначається характером сучасної російсько-української війни, що сполучає як традиційні військові збройні заходи, так і новітні методи деструктивного впливу на державу та суспільство країни, яка зазнала агресії. Другий аспект – цивільно-військові операції є предметом соціально-гуманітарних дисциплін, зокрема соціології. Досвід України у протидії гібридним загрозам доцільно узагальнити з метою посилення національної безпеки та інформування союзників України щодо небезпеки і ризиків гібридної війни.

Аналіз останніх досліджень і публікацій показав, що проблематиці гібридної війни загалом і гібридній війні проти України зокрема присвячені роботи таких вітчизняних і зарубіжних авторів, як Е. Магда [1], І. Рущенко [2], В. Черниш [3], С. Корнієнко [4], Л. Шевцова [5], М. Сенченко [6], І. Яшин [7], Ф. Хоффман [8] М. Гелаотті [9], Дж. МакКуен [10], і багатьох інших фахівців у різних галузях знань. Варто зазначити, що для вітчизняних учених тематика гібридної війни стала актуальною тільки останніми роками, коли країна безпосередньо зіткнулася з цим явищем. Хоча кількість авторів, які працюють над проблемою, поки що від-

носно невелика, їх число поступово збільшується, охоплюючи різні сторони вивчення об'єкта. Подальший розвиток конфлікту зумовлює необхідність продовження вивчення інструментів нападу і протидії в рамках концепції гібридної війни.

З огляду на те, що за ситуації, яка постійно розвивається, наявні дослідження стають менш актуальними, а противник постійно вдосконалює свій арсенал інструментів впливу, новизна статті полягає в описі та узагальненні поточного досвіду протидії гібридним загрозам.

Метою роботи є опис сучасних методів гібридної агресії, що застосовуються проти України протягом останніх років, і узагальнення досвіду протидії їй як силами держави, так і силами громадянського суспільства. Для вирішення цього завдання в статті описані методи ведення гібридної війни, наведені конкретні випадки використання цих методів і актуальні в таких ситуаціях шляхи протидії.

Виклад основного матеріалу. За останні кілька тисячоліть, за різними підрахунками, відбулося від 5 до 15,5 тисячі воєнних конфліктів. Проте у науковому дискурсі відсутня усталена трактовка терміна «війна». Дослідники цього явища пропонують різноманітні дефініції терміна «війна», зосереджуючись на різних його аспектах. Один з найвідоміших теоретиків війни Карл Фон Клаузевіц дає таке визначення: «продовження політики іншими, насильницькими засобами». А основним її засобом, на думку прусського автора, є організована збройна боротьба як головний і вирішальний засіб досягнення цілей війни [11].

Здебільшого під цим поняттям мається на увазі усереднений варіант визначення: «війна – це конфлікт між державами або цивільними об'єднаннями, що відбувається у формі бойових дій з метою нав'язати противнику свою волю». Але у сучасних реаліях це визначення втрачає актуальність, адже більшість розвинених країн не можуть дозволити собі починати відкриті збройні зіткнення для досягнення своїх цілей. Поточну ситуацію добре описує концепція гібридної війни, висунута колишнім офіцером морської піхоти, а нині науковим співробітником Міністерства оборони США Френком Хоффманом. Відповідно до його визначення в гібридних війнах асиметрична компонента має вирішальне оперативне значення на полі бою, на відміну від звичайних воєн, де роль асиметричних гравців (наприклад, партизан) полягає у відволіканні сил противника на підтримку безпеки далеко від поля бою. Надалі, щоб уникнути плутанини, Хоффман запропонував використовувати для воєн, де метою асиметричної компоненти є відтягування сил противника від основного театру війни і створення труднощів в управлінні військами, термін «комбінована війна» [8].

До теперішнього моменту було висунуто безліч визначень «гібридної війни», але єдиної думки так і не сформувалося. У цій статті під цим поняттям мається на увазі сучасна форма ведення війни, що відрізняється переважанням невійськових методів впливу над традиційними бойовими діями або навіть повною відмовою від них.

Використання гібридних методів здебільшого передбачає заперечення агресором своєї причетності, тобто фактично це «неоголошена» війна. Важливими особливостями гібридних методів ведення війни, що зумовлюють ефективність, є їх низька ресурсомісткість порівняно з традиційними бойовими діями, а також висока вартість і складність захисту від них. Здебільшого реалізація того чи іншого методу зловмисного втручання виявляється на кілька порядків дешевшою і простішою, ніж організація захисних заходів і усунення наслідків втручання.

Валерій Герасимов, діючий голова Генштабу Російської Федерації, у 2013 році виступив з промовою про сучасні війни, роль пропаганди і підривної діяльності. Тоді він досить точно описав те, чим спецслужби РФ будуть займатися всі наступні роки: «Процвітаюча держава може протягом декількох місяців або днів перетворитися на арену запеклого збройного конфлікту, стати жертвою іноземної інтервенції і зануритися в цілковитий хаос, гуманітарну катастрофу і громадянську війну» [12].

Спектр методів та інструментів, які використовуються спецслужбами РФ проти України, – дуже широкий і весь час доповнюється. Поточні загрози можна розділити на кілька великих кластерів, що включають пропаганду і дезінформацію, збір персональних даних та стеження за громадянами, хакерські атаки, економічний тиск, впровадження в державний апарат замаско-

ваних представників, розпалювання громадянських конфліктів, створення та підтримку сепаратистських та терористичних угруповань. Робота по всіх цих напрямах здійснюється паралельно і централізовано, що вимагає прийняття відповідних централізованих заходів. Ці кластери слід розглянути окремо.

Пропаганда і дезінформація у цьому разі спрямовані на руйнування державності із самих її основ, історичної пам'яті, національної самосвідомості та конструювання альтернативної реальності, в якій Росію любить весь світ, а Україна незмінно виступає агресором. Для цього спецслужби РФ та спеціально створені для цього структури використовують підконтрольні їм засоби масової інформації і різного роду інформаційні ресурси, на зразок соціальних мереж, блогів, а також спеціально навченого штату тролів. В інформаційне середовище так само активно «вкидається» свідомо неправдива інформація, яка дає змогу маніпулювати громадською думкою. Машина пропаганди дає змогу маскувати злочини агресора, підносячи їх як добру справу і навіть викликати у своїх громадян почуття гордості за вчинене, придушувати невдоволення населення країни жертви, занижуючи значимість нанесеного удару і нав'язуючи ідею його правомірності і справедливості.

Пропаганда є найбільш масовою формою агресії, хоч і вимагає чималих витрат на проведення інформаційних кампаній, утримання телеканалів, мереж ботів, величезного штату тролів, що направляють громадську думку в мережі.

Основною складністю захисту від подібного роду агресії є мозаїчність інформаційного простору і наявність величезної кількості інформаційних каналів. Якщо від негативного впливу традиційних ЗМІ на кшталт телеканалів і Інтернет-видань можна відносно надійно захиститися, заблокувавши їх на своїй території, то запобігти впливу армії тролів неймовірно складно. Для цього необхідна серйозна модерація коментування на інформаційних ресурсах, що неминуче викликає захисну реакцію як агресора, так і простих користувачів у вигляді збурень з приводу свободи слова. Для ефективної боротьби за уми громадян необхідно поступове підвищення інформаційної грамотності населення і проведення регулярних інформаційних кампаній, які висвітлюють ті чи інші питання, що також потребує чималих ресурсів. Цілком можливо, що було б досить ефективним створення власної централізованої армії тролів, яка могла б скласти противагу агресору і так само впливати на його населення, але використання подібних методів залишається досить спірним. Все зводиться до того, що йде боротьба за уми населення, і оборонятися в цьому разі найчастіше істотно дорожче, ніж нападати.

Іншим напрямом діяльності агресора є збір персональних даних громадян країни-жертви та шпигунство за ними, що переважно здійснюється через підконтрольне програмне забезпечення та Інтернет-ресурси, на зразок поштового сервісу mail.ru, соціальної мережі ВКонтакте, пошукової системи Яндекс. Перераховані компанії охоче співпрацюють зі спецслужбами, надаючи всю необхідну їм інформацію про своїх користувачів, незалежно від громадянства останніх. Варто так само пригадати російські антивіруси «Касперський» і «DoctorWeb», які свідомо ігнорують розроблені спецслужбами РФ шкідливі програми і мають приховані функції для збору особистих даних [13]. Очевидно, що цими сервісами поле збору інформації не обмежується. Регулярно виявляються все нові спроби спецслужб РФ упровадити шпигунське програмне забезпечення [14]. Зібрана інформація обробляється, заноситься в бази і може бути використана для проведення таргетованих інформаційних кампаній і навіть вербування агентів серед місцевого населення.

Очевидним способом захисту є блокування небезпечних ресурсів і продуктів на своїй території і підвищення інформаційної грамотності населення. Але сучасні реалії такі, що ці ресурси є досить популярними, а реалізація повного блокування практично неможлива і вимагає величезних ресурсів. Будь-який бажаючий з легкістю знайде спосіб обходу блокування, і саме ці бажаючі є найбільш вразливою до кремлівської пропаганди категорією населення.

Одним з ключових кластерів загроз є забезпечення присутності замаскованих представників агресора у внутрішньому політичному середовищі держави, що відкриває великі перспективи зовнішнього впливу і контролю ситуації. Маніпуляції громадською думкою і розкол суспіль-

ства від імені «вибраних народом», саботування роботи уряду, шпигунство на вищих рівнях і багато інших можливостей доступні агресору у разі успішного закріплення ставлеників.

У разі загальної аполітичності суспільства метод має неймовірну ефективність, аж до створення повністю підконтрольного уряду, що можна було спостерігати всього декілька років тому. Навіть зараз у політичному просторі нашої держави є відверто проросійські сили, які всіма засобами намагаються дестабілізувати ситуацію.

Боротися з цим явищем вкрай складно, адже ці люди володіють серйозними адміністративними і матеріальними ресурсами, більш того, підтримкою деякої частини населення (або ж переконливою видимістю підтримки). Позбавити їх таких можливостей іноді практично неможливо. Для прийняття ефективних заходів необхідні серйозні докази і така інформаційна кампанія, яка переконає громадськість у необхідності таких заходів. Водночас в історії нашої держави вже є кілька епізодів успішної протидії цьому явищу. Але повністю вирішити проблему зможе лише розвиток повноцінного громадянського суспільства, що цікавиться політикою і здійснює контроль за своїми обранцями в уряді.

Ще одним важливим напрямом діяльності агресора є хакерські атаки, які можуть бути використані для широкого спектра задач, основні з яких:

– отримання стратегічних даних, що стосуються обороноздатності держави або операцій спецслужб;

– крадіжки персональних даних держслужбовців для подальшого їх використання у своїх цілях;

– втручання у внутрішні справи країни, на кшталт проведення виборів або референдумів, шляхом саботування їх проведення або спроб вплинути на результат. Основним завданням тут є зміцнення позицій «своїх» політичних сил і дискредитація неугодних агресору;

– виведення з ладу критично важливих об'єктів інфраструктури. Насамперед системи електропостачання, пошкодження якої може привести до соціальної та економічної катастрофи і навіть до загибелі людей. Не кажучи вже про атомні електростанції, збій на яких може бути вкрай небезпечним для всього регіону. Об'єктом атак часто стають засоби зв'язку, на зразок телекомунікаційних мереж і вузлів Інтернету. Так само однією з пріоритетних цілей є транспортна система, зокрема управління залізничним сполученням, порушення роботи якого може паралізувати значну частину транспортних операцій в країні, в тому числі і військового призначення. Банківський сектор так само постійно перебуває під загрозою хакерських атак.

Важливою перевагою методу є вкрай низькі витрати фінансових і людських ресурсів на реалізацію, адже для однієї атаки може бути досить усього декількох фахівців. А силами кількох десятків команд атаки можна проводити на постійній основі і практично безперервно.

Протидія таким атакам вимагає колосальних ресурсів на рівні держави і активного міжнародного співробітництва. Забезпечення комп'ютерної безпеки об'єкта – це цілий комплекс заходів, що часто вимагає багато часу, зусиль і кадрів.

Економічний тиск так само є важливим напрямом діяльності агресора, виснаження фінансових і матеріальних ресурсів держави шляхом посягань на енергетичну незалежність, транзитний потенціал і дискредитації держави на міжнародній арені. Економіка України, довгі роки залежна від РФ і пов'язана з нею, особливо сильно відчула удар, оговтатися від якого виявилося не просто. Найбільш болючий етап відриву вже позаду і подальший розвиток подій залежить від грамотності менеджменту держави та успішності переорієнтації економіки та експорту на інші країни.

Вкрай дієвим методом, активне використання якого ми можемо спостерігати ще з радянських часів, є розпалювання громадянських конфліктів на території противника з метою розколу і руйнування суспільства зсередини шляхом зовнішнього втручання і маніпулювання ситуацією за допомогою провокацій і активного впливу на інформаційний простір. Навіть мирний і відносно невеликий конфлікт можна перетворити на запекле протистояння, яке може розколоти суспільство. Подібні втручання можна спостерігати по всьому світу, практично в будь-яких місцях, де є хоч якесь протиріччя. Останніми найбільш яскравими прикладами

є паразитування сторонніх деструктивних сил під час Брекзіту, протестів у Каталонії, на русі «Жовтих жилетів» у Франції та “Black Lives Metter” по всьому світу. Під прикриттям масових протестів надзвичайно легко радикалізувати конфлікт, змішавшись з натовпом. Агресор використовує кожну зручну нагоду, щоб дестабілізувати ситуацію у навколишньому світі, ще нещодавно, з початком поширення епідемії коронавірусу, Україна підверглася серії атак, спочатку у Санжарах, куди привезли декілька автобусів провокаторів і знімали сюжети про те, що українці готові забити камінням своїх співвітчизників, які повернулися. Потім, використовуючи підконтрольну Кремлю УПЦ МП, агресор дав інструкції виводити людей на вулиці та збиратися в храмах, водночас пояснюючи прихожанам, що ніякого вірусу не існує.

Метод загалом вимагає невеликих, відносно традиційних бойових дій, витрат. Для керування на місцях потрібно зовсім небагато спеціалістів, які навіть можуть працювати віддалено. Надання інформаційної та фінансової підтримки вже сформованим групам незрівнянно дешевше самостійного ведення бойових дій. Основним засобом захисту від цього методу втручання є робота спецслужб держави, які безперервно стежать за ситуацією і контролюють інформаційний простір.

В окрему категорію слід винести створення на території держави-жертви терористичних і сепаратистських організацій, які здатні дестабілізувати ситуацію в цілому регіоні і навіть привести до порушення територіальної цілісності держави. Яскравим прикладом цього методу є застосована РФ технологія створення республік на території України [2]. У результаті масштабної підготовки і вдало вибраного моменту агресору фактично вдалося позбавити Україну близько 7 відсотків території. Наявність на тілі держави рани, яка не загоюється, у вигляді зони АТО/ООС дозволяє регулярно проводити різного роду провокації і витягувати ресурси з економічно більш слабкої держави.

Цей метод втручання є досить нестандартним з двох причин. По-перше, втручання є занадто очевидним, на межі з повноцінним військовим вторгненням, хоча з точки зору міжнародного права все залишається в деяких рамках. З цього так само виходить друга причина, а саме висока вартість застосування на пізніх етапах розвитку методу, тому фактично ресурсів для підтримання сепаратизму потрібно не набагато менше, ніж для повноцінного вторгнення. При цьому реалізація цього методу можлива лише за умови бездіяльності державних органів безпеки, що майже унеможливлює нові спроби використання проти України.

Постійна загроза застосування проти України перерахованих методів зумовлює необхідність постійної роботи над усуненням шкоди, завданої агресором, і модернізації засобів захисту від неї. Основним державним органом, що відповідає за цю діяльність, є Служба безпеки України.

Лише за перше півріччя 2019 року СБУ було нейтралізовано більш ніж 300 хакерських атак і заборонено в’їзд 254 іноземцям, причетним до тероризму. Активно ведеться робота з блокування Інтернет-ресурсів, які використовуються спецслужбами РФ для маніпуляції громадською думкою і дестабілізації ситуації в країні. Ці ресурси заносяться у список Ради національної безпеки і оборони України і блокуються. Це значною мірою обмежує спецслужбам РФ можливості ведення підривної діяльності, хоча насправді, далеко не всі ресурси блокуються, а замість багатьох старих з’являються нові [15].

Так само під постійним наглядом перебувають різні святкування та заходи, особливо ті, що мають гостросоціальне значення. Наприклад, регулярно попереджаються провокації, які плануються до 9 Травня і річниці трагедії в Одесі. У співпраці з іншими державними органами знешкоджуються агентурні мережі, котрі готують акції у різних містах України.

Важливим напрямом роботи СБУ так само є спостереження за соціальними мережами і адміністрацією груп, тому як вони є однією з пріоритетних цілей вербування спецслужбами противника. Через соціальні мережі поширюється значна доля пропаганди, при цьому значно більш радикальної, ніж це допускається в традиційних ЗМІ.

У сфері захисту від кібератак у співпраці з трастовим фондом Україна-НАТО був розвинений Ситуаційний центр забезпечення кібербезпеки. Устаткування та комплектуючі, ПЗ для його роботи було надано Україні в рамках першого етапу Угоди про реалізацію трастового фонду

Україна-НАТО з питань кібербезпеки. Його характерними рисами є автоматизована система виявлення, аналізу та реагування на відповідні інциденти і професійна комп'ютерна криміналістика. Ситуаційний Центр уже довів свою високу ефективність. Силами центру були відбиті численні атаки на органи державної влади, великі державні та приватні компанії, об'єкти оборонно-промислового комплексу. У 2019 року, під час виборів Президента України, була попереджена масштабна кібератака на виборчу комісію. Тільки протягом 2019 року СБУ нейтралізувала діяльність 20 хакерських груп, виявила та локалізувала близько 1 тис. кібератак. 200 з них були здійснені саме на органи державної влади та об'єкти критичної інфраструктури. Також кіберфахівці СБУ за рік заблокували 400 вебресурсів, які використовувались у злочинних цілях [16]. У рамках реалізації другого етапу Трастового фонду Україна-НАТО з питань кібербезпеки має відбутися збільшення кількості ситуаційних центрів і розширення мережі об'єктів критичної інфраструктури, що захищаються. Центр також надає безкоштовні послуги консультування і допомогу у сфері кібербезпеки для бізнесу будь-якого розміру. Для цієї мети так само запущена платформа для обміну інформацією про кібератаки MISP-UA.

Також слід зазначити значний внесок у протидію гібридній агресії створеної волонтерською групою в 2014 році недержавної організації «Миротворець». За 6 років свого існування її членам удалося легальними, напівлегальними і нелегальними способами зібрати майже повну базу даних бойовиків ЛНР і ДНР. А в результаті більш ніж 14 проведених операцій проникнути в ряд агентурних мереж, зруйнувати їх, перевербувати або захопити працюючих у них агентів [17].

Методи роботи і публікація особистих даних журналістів викликали серйозний громадський резонанс і засудження значної частини світу, але сайт продовжує працювати, а сама організація активно співпрацювати із СБУ, ЗСУ, МВС, прикордонною службою, Державною пенітенціарною службою і багатьма іншими державними і комерційними організаціями, серед яких, наприклад, є великі банки.

Говорячи про захист від інформаційної агресії, варто згадати засновану в 2014 році українськими професорами і студентами організацію StopFake, яка протягом усього конфлікту стежить за інформаційним простором і займається викриттям російської пропаганди. Крім цього, організація бере активну участь у міжнародних проєктах, присвячених проблемам пропаганди [18].

Протистояння триває вже 6 років і видимих причин його припинення поки не передбачається. І саме тому необхідно докласти всіх зусиль до дослідження методів зловмисного впливу, що застосовуються проти нашої держави і способів захисту від них, а також зосередитися на вивченні іноземного досвіду, зміцненні міжнародного співробітництва в галузі протистояння гібридним загрозам. Уже залишилося не так багато країн, які б не зіткнулися з гібридними загрозами, досвід кожної є корисним для України, кожна країна розробляє свої унікальні методи протидії, створюються міжнародні центри та об'єднання, участь у яких є серйозним підґрунтям для укріплення обороноздатності нашої держави. Як показує практика, необхідністю для подолання настільки різноманітної гібридної загрози є всеосяжне та систематичне залучення зусиль державного апарату та всього суспільства. Можна сказати, що формування відносної стійкості до гібридних загроз, окрім реформування наявних інституцій та створення нових, потребує значних змін у свідомості громадян. Аполітичність та низька інформаційна грамотність населення є серйозною загрозою не тільки для обороноздатності держави, а й для процвітання загалом. Останніми роками ситуація потрохи виправляється, але здебільшого завдяки активній меншості. Широкі верстви населення все ще дуже схильні вірити популізму політиків та приймати рішення під впливом яскравих рекламних образів, незважаючи на зміст. Актуальною також залишається проблема присутності проросійських агентів впливу як серед політиків, медійних персон, так і серед духовенства. З 2014 року задля забезпечення захисту України від гібридних загроз багато що було зроблено, але ще багато що належить зробити, світові держави вже усвідомили загрозу і тепер об'єднаними зусиллями всього цивілізованого світу треба розробляти дієві стратегії протидії гібридній агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Магда Є.В. Гібридна війна: вижити і перемогти. Харків : Віват, 2015. 304 с.
2. Рущенко І.П. Російсько-українська гібридна війна: погляд соціолога : монографія. Харків : ФОП Павленко О.Г., 2015. 268 с.
3. Черниш В. Інформаційний вимір гібридної війни / В. Черниш, Прем Махадеван. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право* : збірник наукових праць. 2017. № 1/2 (33/34). С. 9–21.
4. Корнієнко С. Путін веде в Україні гібридну війну – генерал Каппен. *Радіо Свобода*, 27.04.2014. URL: http://www.radiosvoboda.org/content/article/25363591.html (дата звернення: 22.09.2020).
5. Шевцова Л. Путин ищет новые способы удушения Украины. URL: http://news.liga.net/interview/politics/3329055-liliya_shevtsova_putin_ishchet_novye_sposoby_udusheniya_ukrainy_.html (дата звернення: 22.09.2020).
6. Сенченко О. Новий виклик людству – гібридна війна. *Вісник Книжкової палати.* 2017. № 5. С. 41–45. URL: http://nbuv.gov.ua/UJRN/vkp_2017_5_14 (дата звернення: 22.09.2020).
7. Яшин И. Гибридная агрессия Кремля. Аналитический обзор. URL: www.4freerussia.org (дата звернення: 22.09.2020).
8. Hoffman Frank G. Hybrid vs. compound war. *Armed Forces Journal.* 2009: 1–2.
9. Hybrid War as a War on Governance / M. Galeotti. *Small Wars Journal*. 2015. August 19. URL: http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance_(дата звернення: 22.09.2020).
10. McCuen J.J. "Hybrid Wars". *Military Review.* 2008. URL: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080430_art017.pdf (дата звернення: 22.09.2020).
11. Фон Клаузевиц К. О войне. Москва : Логос; Наука, 1998. С. 106.
12. Герасимов В. Ценность науки в предвидении. *Военно-промышленный курьер*. № 8 (476), 27 февраля – 5 марта 2013, с. 1–3. URL: www.vpk-news.ru (дата звернення: 22.09.2020).
13. Bloomberg: Kaspersky Lab Has Been Working With Russian Intelligence. URL: https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence (дата звернення: 22.09.2020).
14. СБУ викрила групу компаній на реалізації програмного забезпечення зі шпигунськими продуктами спецслужб РФ. URL: https://ssu.gov.ua/novyny/sbu-vykryla-hrupu-kompanii-na-realizatsii-prohramnoho-zabezpechennia-z-shpyhunskymy-produktamy-spetssluzhb-rf (дата звернення: 22.09.2020).
15. Сайт Служби Безпеки України. URL: https://ssu.gov.ua/ (дата звернення: 22.09.2020).
16. Ситуаційний центр забезпечення кібербезпеки. URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky (дата звернення: 22.09.2020).
17. Сайт організації «Миротворець». URL: https://myrotvorets.center/_(дата звернення: 22.09.2020).
18. Сайт організації "StopFake". URL: https://www.stopfake.org/ru/glavnaya-2/ (дата звернення: 22.09.2020).

REFERENCES

1. Mahda, Ye.V. (2015). Hibrydna viina: vyzhyty i peremohty. [Hybrid war: survive and win]. Kharkiv: Vivat, 2015. 304 s.
2. Rushchenko, I.P. (2015). Rosiisko-ukrainska hibrydna viina: pohliad sotsioloha: monohrafiia [Russian-Ukrainian hybrid war: the view of a sociologist: a monograph]. Kharkiv: FOP Pavlenko O.H., 2015. 268 s.
3. Chernysh, V. (2017). Informatsiinyi vymir hibrydnoi viiny / Vadym Chernysh, Prem Makhadevan [Information dimension of hybrid warfare]. Visnyk NTUU "KPI". Politolohiia. Sotsiolohiia. Pravo: zbirnyk naukovykh prats. 2017. No. 1/2 (33/34). S. 9–21.
4. Korniienko S. (2014). Putin vede v Ukraini hibrydnu viinu – heneral Kappen [Putin is waging a hybrid war in Ukraine – General Kappen]. Radio Svoboda, 27.04.2014. Retrieved from: http://www.radiosvoboda.org/content/article/25363591.html.
5. Shevtsova, L. Putyn yshchet novie sposoby udushenyia Ukrainy [Putin is looking for new ways to stifle Ukraine]. Retrieved from: http://news.liga.net/interview/politics/3329055-liliya_shevtsova_putin_ishchet_novye_sposoby_udusheniya_ukrainy_.html.

6. Senchenko, O. (2017). Novyi vyklyk liudstvu – hibrydna viina [A new challenge to humanity is a hybrid war]. Visnyk Knyzhkovoi palaty. No. 5. S. 41–45. Retrieved from: http://nbuv.gov.ua/UJRN/vkp_2017_5_14.

7. Iashyn, Y. Hybrydnaia ahressyia Kremlia. Analytycheskyi obzor [The Kremlin's hybrid aggression. Analytical review]. Retrieved from: www.4freerussia.org.

8. Hoffman, Frank G. Hybrid vs. compound war. Armed Forces Journal. (2009): 1–2.

9. Hybrid War as a War on Governance / M. Galeotti. Small Wars Journal. 2015. August 19. Retrieved from: http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance.

10. McCuen, J.J. (2008). "Hybrid Wars". Military Review. Retrieved from: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080430_art017.pdf.

11. Fon Klauzevyts K. O voine [About the war]. Moskva: Lohos; Nauka, 1998. S. 106.

12. Herasymov, V. 2013. Tsennost nauky v predvydenyy [The value of science in foresight]. Voenno-promushlennyi kurer. No. 8 (476), 27 fevralia – 5 marta 2013, pp. 1–3. Retrieved from: www.vpk-news.ru.

13. Bloomberg: Kaspersky Lab Has Been Working With Russian Intelligence. Retrieved from: https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

14. SBU vykryla hrupu kompanii na realizatsii prohramnoho zabezpechennia z shpyhunskymy produktamy spetssluzhb RF [The Security Service of Ukraine has exposed a group of companies selling software with spy products of the Russian special services]. Retrieved from: https://ssu.gov.ua/novyny/sbu-vykryla-hrupu-kompanii-na-realizatsii-prohramnoho-zabezpechennia-z-shpyhunskymy-produktamy-spetssluzhb-rf.

15. Website of the Security Service of Ukraine. Retrieved from: https://ssu.gov.ua/.

16. Sytuatsiinyi tsentr zabezpechennia kiberbezpeky. Retrieved from: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky.

17. Website of Myrotvorets organization. Retrieved from: https://myrotvorets.center/.

18. Website of StopFake organization. Retrieved from: https://www.stopfake.org/ru/glavnaya-2/.

Kryvoruchko Maksym Hennadiiovych
Postgraduate Student at the Department of Sociology and Politology
National Technical University "Kharkiv Polytechnic Institute"
2 Kirpychova str., Kharkiv, Ukraine

COUNTERACTING HYBRID THREATS: DIFFICULTIES AND EXPERIENCE OF UKRAINE

The article is devoted to the problem of the Russian-Ukrainian war, which combines both traditional military measures and the latest methods of destructive influence on the state and society of the country that is the object of aggression. This creates an interdisciplinary situation. In particular, civil-military operations are studied in socio-humanitarian disciplines, including sociology. The traditional definition of war "conflict between states or civilian associations, which takes the form of hostilities to impose their will on the enemy", in modern realities loses relevance because most developed countries cannot afford to start open armed conflicts to achieve their goals. The current situation is well described by the concept of hybrid warfare, put forward by a former Marine officer and now a researcher at the US Department of Defense Frank Hoffman. In this article, this concept refers to the modern form of warfare, characterized by the predominance of non-military methods of influence over traditional hostilities or even complete abandonment of them. Ukraine's experience in combating hybrid threats should be generalized in order to strengthen national security and inform Ukraine's allies about the dangers and risks of hybrid warfare. The aim of the article is to describe the modern methods of hybrid aggression used against Ukraine in recent years and to summarize the experience of countering hybrid threats by both the state and civil society. To address this, current threats are divided into 8 clusters, including propaganda and disinformation, personal data collection and surveillance, hacking, economic pressure, the introduction of disguised members of the state apparatus, incitement to civil conflict, and the creation and support

of separatist and terrorist groups. The degree of danger of these threats is considered, the corresponding examples are given, the examples of counteraction to hybrid threats from the state and civil society are described.

Key words: *war, hybrid war, civil conflict, negative management of civil conflict, ways of counteracting hybrid threats, methods of conducting hybrid war.*