УДК 341.32
DOI https://doi.org/10.32782/2524-0374/2022-5/160

РЕАЛІЗАЦІЯ ПРИВАТНИМИ ВІЙСЬКОВИМИ КОМПАНІЯМИ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ ОКРЕМОГО ТИПУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ. МІЖНАРОДНО-ПРАВОВИЙ ТА НАЦІОНАЛЬНО-ПРАВОВИЙ АСПЕКТИ

REALIZATION BY PRIVATE MILITARY COMPANIES OF SPECIAL OPERATIONS OF A PARTICULAR TYPE UNDER CONDITIONS OF HYBRID WARFARE. INTERNATIONAL LEGAL AND NATIONAL LEGAL ASPECTS

Тронько О.О., аспірант юридичного факультету
Дніпропетровський національний університет імені Олеся Гончара

Бережна К.В., д.ю.н., професор,
завідувач кафедри європейського та міжнародного права
Дніпропетровський національний університет імені Олеся Гончара

У статті розглянуто правовий аспект реалізації приватними військовими компаніями спеціальних операцій окремого типу в умовах гібридної війни. Приведено поняття національної та воєнної безпеки. Наведено поняття гібридної війни та війн четвертої генерації. Розглянуто теоретичні та практичні аспекти методів та способів ведення війн четвертого покоління і основні принципи, на яких базується стратегія таких війн: принципи асиметричності, маневреності, взаємодії, відсутності правил, хаосу, спецпідготовки і прихованості. Приведено визначення спеціальних операцій, інформаційних операцій, операцій в кіберпросторі, операцій, спрямованих на дестабілізацію протиборчої сторони, як їх окремий вид. Наведено поняття інформаційного протиборства, кібероперацій як окремого різновиду спеціальних операцій. Проведено аналіз окремих видів спеціальних операцій та їх застосування відповідно до норм міжнародного права та міжнародного права прав людини. Проаналізовано стан регламентованості інформаційного протиборства міжнародним гуманітарним правом. З урахуванням природи й особливостей проведено аналогію приватних військових компаній та окремих підрозділів сил спеціальних операцій в Україні та зарубіжних країн, до завдань яких відносяться заходи, спрямовані на інформаційну боротьбу. Досліджено можливості приватних військових компаній (далі – ПВК) діяти в інформаційному просторі, реалізовувати спеціальні інформаційні операції та кібероперації недержавними збройними формуваннями, а саме суб'єктами військово – консалтингової діяльності в умовах гібридної війни воєнних та збройних конфліктів, застосовуючи їх в обхід обмежень, які регулюються наявними механізмами контролю, не порушуючи норм міжнародного гуманітарного права та міжнародного права прав людини. Розглянуто можливість легітимного застосування ПВК в інформаційних обороні та нападі в умовах гібридної війни у відповідності до норм міжнародного гуманітарного права та національного законодавства. Наведено переважаючі аспекти застосування недержавних збройних формувань саме для проведення інформаційних спеціальних операцій в ході воєнного конфлікту. Проаналізовано та запропоновано внесення змін до законопроекту «Про військову консалтингову діяльність».

Ключові слова: гібридна війна, кібербезпека, Міжнародне Гуманітарне право, спецоперації, приватні військові компанії.

This article examines the legal aspect of the implementation by private military companies of special operations of a particular type under conditions of hybrid warfare. The concept of national and military security is presented. The concept of hybrid warfare and fourth generation wars is presented. Theoretical and practical aspects of the methods of conducting fourth generation wars and the basic principles on which the strategy of such wars is based are described: the principles of asymmetricity, maneuverability, interoperability, absence of rules, chaos, special training and primitiveness. The definition of special operations, information operations, operations in the cyber space, operations aimed at destabilization of the opposing side, as their separate type is given. The notion of information warfare, and cyber operations as a separate type of special operations was introduced. An analysis of certain types of special operations and their application in accordance with international law and international human rights law was carried out. Analyzed the state of regulation of information warfare by international humanitarian law. Taking into account the nature and peculiarities, an analogy of private military companies and separate divisions of special operations forces in Ukraine and foreign countries, whose tasks include measures aimed at information warfare, was carried out. It examines the capabilities of private military companies (hereinafter – PMC) to operate in the information space, implementing special information operations and kiberooperations by non-persistent military formations, namely by the subjects of military-consulting activities in the conditions of hybrid warfare of military and military conflicts, using them in circumvention of restrictions, which are regulated by existing control mechanisms, without violating international humanitarian law and international human rights law. The article examines the possibility of legitimate use of PMC's in informational defense and attack under hybrid warfare in accordance with the norms of international humanitarian law and national legislation. The article describes the prevailing aspects of the use of non-military military formations for conducting special informational operations in the course of military conflict. The amendments to the draft law "On Military Consulting Activity" were analyzed and recommended.

Key words: hybrid war, cybersecurity, international humanitarian law, special operations, private military companies.

Постановка проблеми. Національна безпека набула статусу глобальної проблеми як для України так й для усієї світової спільноти. Значення воєнно-силових аспектів та вирішення ключових проблем в обхід норм міжнародного права продовжують залишатись суттєвими в міжнародних відносинах. В українському суспільстві особливо загострились проблеми кризових явищ, які залежать від динамічної трансформації міжнародних відносин. Наша держава переживає глибокі потрясіння, пов'язані із віроломним збройним втручанням російської федерації, корінними змінами в політиці, економіці, соціальній, духовній сферах та постає перед викликами реальних загроз національній безпеці практично в усіх сферах життєдіяльності.

Суверенітет держави не можна уявити без наявності потужних та підпорядкованих виключно національним інтересам Збройних сил, в тому числі, як підсистеми механізму захисту національної безпеки. В той час, коли бойовий потенціал держави все ж не відіграє вирішальну роль у досягненні стратегічних цілей, а поняття фронту та тилу або докорінно змінюються, або повністю розмиті, протидіяти доводиться таким чинникам сучасних асиметричних війн, як принципу створення хаосу, психологічним прийомам розкачування суспільства, відсутності шаблонів тактики, диверсійним та іншим інформаційним операціям. Кібервійна та інформаційна інтервенція є типовими компонентами гібридної війни поруч із використанням класичних способів збройної боротьби.

Попередження воєнної загрози та захист сфери державної та суспільної безпеки, для яких небезпеку складають розвідувальна та підривна діяльність спецслужб

«держави – агресора» являються першочерговими умовами забезпечення національної безпеки України. Перебуваючи в стані збройного конфлікту дев'ятий рік, на тлі повномасштабного вторгнення РФ, Україна повинна створювати новітні та дієві способи протидії не менш сучасним факторам загроз національній безпеці та тактикам гібридної війни. Вдосконалення засобів збройної боротьби та засобів інформаційно-психологічного ураження викликає цілком зрозуміле прагнення у необхідності переосмислення та способів пошуку нових, більш ефективних та універсальних існуючих форм конфлікту.

Окрім вступу в позиційну війну та «класичні» бойові дії, ключову роль серед засобів боротьби починають відігравати операції прихованого типу із залученням страйкового потенціалу населення, доповнених військовими заходами прихованого характеру, у тому числі, реалізацією заходів інформаційного протиборства. В тактиці ворога спостерігається чітка тенденція – «кинджальне» проникнення в глибину території «держави – жертви» малими групами за підтримки авіації та ракетно – бомбових ударів, захоплення адміністративних будівель та об'єктів критичної інфраструктури, а в разі неможливості здійснення прориву – ураження живої сили масованими ударами реактивних систем залпового вогню (РСЗВ), в подальшому – спроба нав'язати знеможеному подібною агресією населенню свої інтереси використовуючи агітацію, інформаційний вплив, «гуманітарну допомогу», обмеження та блокування в інформаційному просторі тощо.

ПВК як недержавні актори в тій чи іншій мірі приймають участь у різних збройних конфліктах в усьому світі, їх роль та характеристики, як і потенційні загрози, які виходять від їх участі в конфліктах, безсумнівно відрізняються і зазнають певних змін. Вони так само можуть бути стороною військового протистояння, більше того, їх питома вага у військових конфліктах поступово імовірно зросте. На думку автора, такі суб'єкти могли б бути затребувані разом із регулярними збройними силами не лише для забезпечення їх дій, а саме для реалізації окремих видів спеціальних операцій. Визначення встановлення правового зв'язку між державою і ПВК в разі реалізації спеціальних інформаційних контроперацій в ході гібридної війни для визначення пов'язаності ПВК нормами міжнародного гуманітарного права та міжнародного права прав людини, є важливим питанням дослідження.

Аналіз останніх досліджень і публікацій. Проблематику збройних конфліктів сучасності, легалізації та застосування ПВК в Україні досліджують такі вітчизняні та зарубіжні науковці, як Я. Малик, О. Фролова, С. Люлько, М. Зінченко, Т. Макгонагл, Г. Майкл, Д. Скринька та інші. Предметом наукового аналізу виступили міжнародно-правові аспекти пропаганди війни та інформаційної війни, разом із цим досліджувані проблеми потребують подальшого з'ясування питання протидії інформаційній війні як інструменту пропаганди на національному рівні.

Мета дослідження. Актуальність розглянутого питання зумовила необхідність аналізу реалізації прихованих операцій інформаційного характеру, які можуть здійснюватися приватними військовими компаніями в умовах гібридної війни та збройного протистояння для забезпечення національних інтересів та безпеки держави у відповідності до норм міжнародного гуманітарного права та міжнародного права прав людини. Щоб на основі зазначених норм міжнародного права та національного законодавства та практики його реалізації проаналізувати значення та вплив реалізації інформаційного протиборства суб'єктами військово-консалтингової діяльності у випадку їх легалізації в Україні.

Виклад основного матеріалу. Стан захищенності життєво важливих інтересів держави, людини, громадянина та в цілому суспільства, який забезпечує його сталий розвиток, сприяє вчасному виявленню, запобіганню і нейтралізації реальних та потенційних загроз національним інтересам України визначає поняття національної безпеки.

Воєнна безпека це захист суверенітету держави, її територіальної цілісності, конституційного ладу та інших найважливіших державних та національних інтересів від воєнних загроз [1].

Сили і засоби забезпечення національної безпеки, всі складові воєнної організації держави створюються і діють в чітко визначеному правовому полі для безпосереднього виконання функцій підтримання національної безпеки в системі виконавчої влади. Конституцією України визначено їх функції у сфері національної безпеки і оборони в умовах воєнного і надзвичайного стану.

Міжнародна безпека та аналіз провідних подій у цій сфері підтверджують намагання провідних держав досягти своїх цілей шляхом політики з «позицій сили». Світ вступає в період «війн нового покоління», який характеризується іншими методами їх ведення та способами застосування сил та засобів. Високопрофесійні та високомобільні армії, забезпечені інноваційною електронною технікою управління і розвідки вестимуть війни в XXI ст., уникаючи використання зброї масового ураження.

Розвиток технологій підштовхує до змін та переходу до нових, невідповідних міжнародно – правовій кваліфікації видів та методів ведення війни, відходячи поступово від класичних бойових дій [2]. Породжуються так звані «The 4th Generation of Warfare»[1] – асиметричні війни четвертого покоління, подібні збройні конфлікти мають своєю стратегією зниження ролі державного впливу на суспільство, придушення волі особи до будь-якого супротиву та підкорення через самостійний інформаційно-психологічний вплив із застосуванням підривних операцій, реалізованих недержавними акторами, за всебічної політичної, юридичної та інформаційної підтримки «держави-нападника». Окрім того «держава – агресор» зухвало вдається до відкритого залякування суспільства, шляхом створення хаосу, поєднання інформаційних, електронних й десантно-штурмових операцій, які доповнюються використанням високоточної зброї. І лише останні осередки спротиву ліквідуються під час рекогносцирувальних, спеціальних операцій, артилерійських і ракетних ударів.

Під загрозу інформаційного «збройного» впливу потрапляє все суспільство з його матеріальними та духовними цінностями, поступово створюється атмосфера невизначеності та суцільного хаосу, відбуваються постійне розгойдування та координовані атаки на слабкі місця. Вже визнаним є той факт, що окрім зброї в її загальноприйнятому розумінні, для регулювання використання якої існує значна кількість міжнародних угод, з'являється небезпека завдати шкоди застосовуючи інформаційні технології.

Найбільш точно інформаційні війни визначаються як «різновид конфлікту, при якому протиборчі сторони мають завданням забезпечувати безпеку власних інформаційних систем та інформації, маніпулювання інформацією ворога або її спотворення, унеможливлення доступу і обробці інформації стороною противника» [3]. Такий підхід являється ідеальним засобом для забезпечення ментальної поразки противника ще до початку прямих бойових дій.

Основними інформаційними інструментами гібридної війни є такі заходи: військово-політична дезорієнтація ворога; дезінформація щодо власних дій; заходи ураження чи блокування інформаційних каналів спрямовані на дезорієнтацію та дезорганізацію, посилення стану напруженості серед суспільства та вплив на масову свідомість через поширення панічних настроїв від постійного очікування ударів і масованого наступу в глибині та по всій лінії фронту, з метою максимальної деморалізації [4].

[1] The 4th Generation of Warfare - Війна четвертого покоління (англ. Fourth generation warfare, 4GW) – конфлікт, який характеризується стиранням відмінностей між безпосередньо війною і політикою, між залученими в неї військовими і цивільним населенням.

Яніс Берзіньш найкраще описав цей спосіб ведення війни, наочно ілюструючи трансформацію від «традиційної» до гібридної війни як перехід:

– від прямого руйнування до прямого впливу;

– від прямого знищення опонента для його внутрішнього розпаду;

– від війни, веденої за допомогою зброї та технологій, до війни культур;

– від війни конвенційними засобами до війни спеціально підготовленими силами та нерегулярними комерційними угрупованнями;

– від традиційного поля битв до інформаційної/психологічної війни та війни сприйняття;

– від прямих зіткнень до безконтактної війни;

– від поверхневої та секторної війни до тотальної війни, включаючи внутрішню сторону та базу противника;

– від війни у фізичному середовищі до війни у людській свідомості та у кіберпросторі;

– від симетричної до асиметричної війни шляхом поєднання політичної, економічної, інформаційної, технологічної та екологічної кампаній;

– від війни у певному періоді часу до перманентної війни як природний стан національного життя [5].

Берзіньш стверджує: «стратегією є максимальне зменшення розгортання жорсткої військової сили, змушуючи громадянське населення та силовий блок ворога здійснювати підтримку нападника на шкоду власній державі» [5].

Сили Спеціальних операцій (далі – ССО) – окремий рід військ, здатний невеликими за чисельністю групами виводити з ладу об'єкти критичної інфраструктури, нейтралізувати управління та високоточну зброю противника, корегувати удари високоточної зброї у реальному часі. Оперативність, безперервність, раптовість, злагодженість за напрямами та цілями, взаємодія з приватними військовими компаніями, здатність до неконвенційних дій (створення партизанських рухів, прихована участь у державних переворотах, замаскованих формах агресії, тощо) являються головними принципами застосування спеціальних підрозділів. Це трансформує ССО в ключовий та результативний інструмент «гібридних війн».

Гібридний, невизнаний нормами міжнародного права характер протистояння, передбачає застосування підрозділів спеціальних операцій проведення інформаційно-психологічних операцій, метою яких є підрив морально-психологічного стану населення країни-жертви у тісній взаємодії з парамілітарними формуваннями [6];

Групою військової розвідки та безпеки Сполучених Штатів Америки Military Intelligence and Security Group (MISG) організовується та формується інформаційно-психологічний вплив.

Статутом Сухопутних Сил США FM 100-6 «Інформаційні війни» передбачаються як комплекс заходів у виді впливу на інформацію, процеси та системи та комп'ютерні мережі ворога з метою досягнення інформаційного панування. Водночас передбачено інформаційний захист.

Активне вивчення та розвиток стратегій інформаційного нападу і оборони спостерігається на даний час у Франції, Німеччині, Великій Британії та деяких інших державах. Французькими експертами в даному контексті визначаються два головні елементи концепції інформаційної війни – військовий та економічний (цивільний). Перший елемент розглядається в сфері збройних конфліктів та миротворчих операцій, а цивільний включає більш широкий діапазон потенційного застосування інформаційних операцій.

В Україні наразі інформаційне протиборство здійснюють такі підрозділи інформаційно-психологічних операцій (далі ІПсО) як 83-й центр ІПсО ССО ЗСУ, 74-й центр ІПсО ССО ЗСУ, 72-й центр ІПсО ССО ЗСУ, 16-й центр ІПсО ССО ЗСУ. До завдань зазначених підрозділів відносяться збір та аналіз інформації, розповсюдження пропаганди й відпрацювання реакції на конкретні політичні події, виявлення та попередження інформаційних і психологічних загроз, сприяння формуванню позитивного іміджу України в світі, моніторинг суспільно-політичної обстановки в зазначених районах. В своєму штаті вони мають інформаційно – аналітичні підрозділи, групи збору і обробки інформації, підготовки та проведення інформаційних заходів, розробки друкованої продукції, групи розробки в соціальних мережах та ін.

«Гарячі» інформаційні війни, з найвищим ступенем впливу на інформаційні системи супротивника, породжують питання щодо застосування міжнародного гуманітарного права та визнанні статусу учасників конфлікту військовослужбовців – операторів спеціальних підрозділів, залучених до виконання інформаційних операцій.

Інформаційна війна існує в комплексі з воєнними діями, та в ході проведення визначених операцій з втручання в державну інформаційну систему, являється одним з засобів досягнення стратегічно важливої цілі.

Нажаль, Міжнародним Комітетом Червоного Хреста не відпрацьовано єдиної доктрини, котра б однозначно відповідала на всі питання, пов'язані з міжнародно-правовим регулюванням інформаційних війн.

Держави повинні виконувати покладені на них міжнародні зобов'язання у відношенні діянь, у відповідності до міжнародного права, що стосуються інформаційної безпеки, та приписуються їм, не дивлячись на заклики щодо недопускання використання представників держав для здійснення міжнародно-протиправних діянь із застосуванням кібертехнологій.

Незастосування сили або погрози силою, непорушність кордонів, територіальна цілісність держав, мирне врегулювання спорів, як керівні принципи взаємовідносин між державами задекларовані та юридично закріплені Заключним актом наради з безпеки та співробітництва в Європі від 1 серпня 1975 року [7].

Відповідно до п. 4 ст. 2 Уставу ООН заборона стосується застосування виключно збройної сили в міжнародних відносинах, при цьому в сферу дії цієї норми не входять усі інші складові зовнішньополітичного потенціалу [8].

Отже, до теперішнього часу обмеження права використовувати силу, передбачає та визначає такою лише збройну силу.

Міжнародне співтовариство підкреслює важливість вирішення цих проблем в рамках угод про права людини. Так, пунктом D доповіді Генерального секретаря ООН, здійсненної у 2012 році, наголошується головне завдання – необхідність розроблення шляхів вирішення проблеми інформаційної безпеки [9].

К.У. Уоткин вважає, що подібні конфлікти викличуть «питання визначення статусу, озброєних комп'ютерами цивільних осіб, які знаходяться на іншому континенті, та контролю за їх діями». Подібно класичній війні у даному способі породжуються проблеми розмежування по об'єктах і особах; визначення учасників та необхідних ознак комбатантів; можливість їх ураження традиційними видами зброї; набуття ними статусу військовополонених, тощо. Окреме питання – інформаційна війна поза рамками «класичної війни» є лише її різновидом, або являється збройним конфліктом [10].

Указом Президента України від 15.03.2016 No 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року», затверджено Стратегію кібербезпеки України, яка дозволяє проводити моніторинг інформаційного кіберпростору на предмет пошуку проявів пропаганди війни [11].

Доктрина інформаційної безпеки України затверджена Указом Президента України від 25.02.2017 No 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року», містить конкретні засади визначення загроз, що можуть виникати в інформаційному просторі [12].

Інформаційна зброя обмежується в застосуванні саме у випадку його застосування проти об'єктів, руйнування яких може викликати невиправдані втрати серед цивільних осіб та/або значні та масштабні наслідки, які негативно позначаться на здоров'ї людей, на стані навколишнього середовища тощо [13].

На думку Михаэля Н. Шмидта, зброя «інформаційної ери» забезпечує дотримання принципу розрізнення цивільних та військових об'єктів оскільки здатна до розпізнавання об'єктів ураження.

На практиці ж гібридні інструменти і розроблені для того, щоб уникати звинувачень у порушенні Статуту ООН. Це досягається різними шляхами, і один з них – здійснення інформаційних спеціальних операцій.

Інформаційні спеціальні операції характеризуються безперервністю, планомірністю і комплексністю. Під час їх реалізації повністю виключаються розриви та «логічні стрибки». Одночасно розвиток системи масової комунікації призводить до «стирання кордонів» та розширення можливостей маніпулятивного впливу на свідомість суспільства «країни-суперника» з нав'язуванням власних ідей [14].

В сенсі війн четвертої генерації породжується досконало невизначена підсистема гібридної війни, являючись сукупністю заздалегідь підготовлених та оперативно реалізованих дій військово-дипломатичного, економічного, інформаційного характеру, спрямованого на досягнення головних цілей [15].

Найбільший вплив спецоперації можуть оказати на противника на етапі створення нестабільної обстановки в протиборчій державі. Серед них:

– підривні акції спрямовані на дестабілізацію обстановки;

– підготовка і координація дій агентури, партизанських рухів та незаконних збройних формувань;

– проведення інформаційних (психологічних) операцій (акцій) по залякуванню населення;

Приватні військові компанії являються комерційними підприємствами, які пропонують спеціалізовані послуги, пов'язані з участю у війнах та воєнних конфліктах, включаючи безпосередньо бойові операції, стратегічне планування, збір розвідувальних відомостей, аналітику, оперативну підтримку і логістику.

Таким чином, ПВК, подібно підрозділам Сил спеціальних операцій, маючи більш гнучке оперативне управління, мають розглядатися як цивільні особи і підпадати під захист міжнародного гуманітарного права (далі – МГП). У разі їх участі у збройних конфліктах вони самі мають дотримуватися вимог правил ведення війни, а за їх порушення повинні притягуватися до відповідальності встановленої чинним законодавством і МГП [16].

Неоднозначність та невизначеність статусу ПВК дає унікальну змогу «обійти» міжнародне право, швидкими темпами розширювати масштаби своїх операцій (у тому числі і спеціальних), стрімко нарощуючи вплив у нестабільних регіонах [17]. Складна та гнучка динаміка бойового простору ПВК відповідають їх швидкій реакції та адаптації, а уміння діяти, організовувати свою діяльність і мислити у відмінний від опонента спосіб у поєднанні із захопленням ініціативи або забезпечення простору для маневру відповідатиме асиметрії у військовій справі і у сфері національної безпеки.

Законопроектом № 3005 від 04.02.2020 про Військово-консалтингову діяльність, запропонованим депутатом від партії «Слуга народу» Ольгою Василенко-Смаглюк, [18] пропонується законодавчо врегулювати правові засади організації, порядок створення та діяльності суб'єктів військово-консалтингової діяльності. Положеннями законопроекту, зокрема, передбачається таке обмеження, як заборона використовувати та застосовувати вогнепальну зброю, спеціальні засоби та фізичну силу на території України.

Зазначимо, що даним законопроектом, серед спектру послуг ПВК не передбачено не лише наступальних, а й оборонних дій (окрім послуг охоронного характеру), особливо розвідувальна діяльність та проведення спецоперацій прихованого типу, однак зазначається надання суб'єктами військово-консалтингової діяльності інформаційно-аналітичної підтримки, яка в свою чергу із необхідними доопрацюваннями зможе виступити серйозною зброєю та вирішальними кроками боротьби в інформаційному просторі.

Крім того, проект закону передбачає надання можливості здійснення суб'єктами військово – консалтингової діяльності послуг військового або охоронного характеру лише за межами України, що в умовах сьогодення зовсім не сприяє зміцненню обороноздатності нашої держави.

Висновки. Інформаційні операції з боку російської федерації завдають Національній та воєнній безпеці Україні значної шкоди. Щодня окрім загрози обстрілів, наступальних операцій ворога, під інформаційним впливом супротивника перебувають ще все більше людей, завдяки чому ворог силоміць примушує вдаватись панічним настроям та відчаю, схиляючи на антиукраїнський бік.

Ворог продовжує нарощувати бойову міць у кордонів нашої держави, розмиваючи фронт, окрім того, для масованих ударів та наступу можуть бути також застосовані раніше окуповані рф території Молдавської республіки, в подальшому, не зважаючи на зменшення або закінчення активної фази бойових дій, повномасштабного наступу, застосування авіа- та бомбових ударів – збройний конфлікт на території України може набути рис замороженого, що включатиме приховану підривну діяльність, точкові теракти та звичайно активної фази інформаційної боротьби. З метою попередження інформаційної небезпеки, необхідною є консолідація усіх сил, спроможних її зупинити, потрібно застосувати заходи з проведення контрнаступальних операцій на тимчасово захоплених територіях.

До теперішнього часу не визначено таку правову категорію як «інформаційна зброя». Не розроблено механізми, здатні обмежити розповсюдження інформаційних систем та інформації, яка потенційно може рахуватися інформаційною зброєю.

Так, сьогодення демонструє інформаційну пріоритетність Телеграм-каналів навіть над інтернет-ресурсами та над іншими ЗМІ, в сенсі формування суспільної думки та навіть настрою широкого загалу. Чи не кожен із співвітчизників підписувався на різні канали цього месенджеру з початку повномасштабної війни 24 лютого 2022 року та слідкує за розвитком подій до теперішнього часу. Проте зовсім не кожен здійснює аналіз належності цих каналів та їх «власників», відповідність наданої інформації об'єктивній реальності. Серед останніх можна виокремити здачу в полон військовослужбовців 503-го полку морської піхоти в м. Маріуполь, висловлення міжнародної підтримки «державі-агресору» з боку Ізраїлю, прогнозів «військових аналітиків» стосовно термінів активних бойових дій на території України та ряду інших прикладів дезінформації.

27 лютого 2022 року президент України Володимир Зеленський закликав іноземних громадян долучатися до опору російським військам в Україні. З іноземців, які виявили бажання долучитися, створено окремий Інтернаціональний легіон територіальної оборони при Головному управлінні розвідки Міністерства оборони України. Крім того запроваджено тимчасовий безвізовий режим для іноземців-добровольців.

Легітимізація дозволу участі добровольців з інших країн в збройному конфлікті на території України, в свою чергу надає можливість іноземним приватним військовим компаніям виконувати завдання за призначенням на території нашої держави, звісно на добровільних засадах.

Вважаємо, що легалізація в Україні суб'єктів військово-консалтингової діяльності, надання їм можливості здійснювати діяльність на території нашої держави та дозволу

на проведення спеціальних інформаційних операцій сприятиме проведенню деокупації та призведе до переваги усіх сил, спрямованих надати відсіч ворогу у будь-яких сферах та, найважливіше, перевести вектор з оборони до впевненого наступу.

Окрім того, застосування кібероперацій повинно унеможливити напади невибіркового характеру, знизити ущерб цивільним об'єктам завдяки винятковій точності.

Незважаючи на колосальні витрати бюджетних коштів на армію, підготовка офіцерів з технічних засобів розвідки та кібербезпеки не лише обійдеться державі у багатомільйонні збитки, а й не надасть можливості підготувати фахівців, які б відповідально ставились до виконання завдань за призначенням, що б дало змогу залучати професіоналів ІТ сфери до ПВК та проведення операцій.

ЛІТЕРАТУРА

1. Про національну безпеку України : Закон України від 16.07.2021 № 1702-IX. URL: https://zakon.rada.gov.ua/laws/main/2469-19#Text (дата звернення: 22.05.2022).
2. Черч, У. Информационная война. *Международный журнал Красного Креста*. 2000. С. 49–61.
3. Colonel K.W. Watkin. Combatants, Unprivileged Belligerents and Conflicts in the 21st Century. ackground Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge. 2003. № 1, January. P. 27–29.
4. Феськов І. В., Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики*. 2016. № 58. С. 66–76.
5. Bērziņš J., Russia's New Generation Warfare in Ukraine. *Policy Paper*. 2014, № 2. URL: https://sldinfo.com/wp-content/uploads/2014/05/New-GenerationWarfare.pdf (дата звернення: 22.05.2022)
6. Слюсаренко А. Сили спеціальних операцій як функціональний компонент збройних сил: перспективи наукового дослідження. *Військово-історичний меридіан*. 2017, № 2. С. 27–36
7. Заключний акт Наради з безпеки та співробітництва в Європі (Гельсинський заключний акт) від 01.08.1975. URL: https://zakon.rada.gov.ua/laws/show/994_055#Text (дата звернення 22.05.2022)
8. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду від 16.09.2005. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text (дата звернення 22.05.2022)
9. Доклад Генерального Секретаря ООН, 67 сесія «Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки від 23.07.2012. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/67/167&referer=/english/&Lang=R (дата звернення 22.05.2022)
10. Colonel K.W. Watkin. Combatants, Unprivileged Belligerents and Conflicts in the 21st Century. ackground Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge. 2003. № 1. January. P. 27–29.
11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 27 січня 2016 року № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 22.05.2022).
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України № 685/2021 від 28.12.2021 URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 22.05.2022).
13. Коваль Д.А., Короткий Т. Р. Понятие информационной войны в международном праве. *Альманах международного права*. 2010. № 2. С. 331–343.
14. Феськов І. В., Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики*. 2016. № 58. С. 66–76.
15. Магда Є.М. гібридна війна: сутність та структура феномену, INTERNATIONAL RELATIONS, PART «POLITICAL SCIENCES» URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489/2220 (дата звернення 22.05.2022)
16. Кириченко С. О. Роль приватних військових компаній у воєнних конфліктах *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2021. № 1(71). С. 12–17.
17. Калетнік В.В., Костюк І.А., Возний О.О. Приватні військові компанії як асиметричний потенціал стримування противника. *Системи озброєння і військова техніка.* 2021. № 2(66). С. 144–153. URL: https://doi.org/10.30748/soivt.2021.66.19 (дата звернення 22.05.2022)
18. Про військово-консалтингову діяльність : проект Закону України від 04.02.2020 № 3005. URL: https://ips.ligazakon.net/document/JI01319A?an=3 (дата звернення: 22.05.2022)
19. Дідур О. Спеціальні інформаційні операції – початок гібридної війни. URL:https://armyinform.com.ua/2019/11/11/spezialni-informaczijni-operacziyi-pochatok-gibrydnoyi-vijny-2/ (дата звернення: 22.05.2022)
20. Хаджитодоров С., Соколов М., Сочетание методов ведения войны нового поколения и 5 мягкой силы: гибридные измерения российско-болгарских отношений. *Connections QJ 17*. 2018. № 1. P. 5–22. URL: https://doi.org/10.11610/Connections.rus.17.1.01 (дата звернення: 22.05.2022)