

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Факультет соціології і права

Кафедра соціології

«На правах рукопису»
УДК _____

До захисту допущено:

Завідувач кафедри

_____ Павло ФЕДОРЧЕНКО-КУТУЄВ

«15» грудня 2021р.

Магістерська дисертація

на здобуття ступеня магістра

**за освітньо-професійною програмою «Врегулювання конфліктів та
медіація»**

зі спеціальності 054 «Соціологія»

на тему: «Технології і методи гібридних конфліктів у світі»

Виконав:

студент VI курсу, групи СЛ-01мпв

Міщук Андрій Романович _____

Науковий керівник:

Доцент кафедри соціології, к. філос. н.

Пиголенко Ігор Вікторович _____

Рецензент:

Старший викладач кафедри теорії та практики управління, к. філос. н

Пашов Ростислав Іванович _____

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних посилань.

Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет соціології і права
Кафедра соціології

Рівень вищої освіти – другий (магістерський)

Спеціальність – 054 «Соціологія»

Освітньо-професійна програма «Врегулювання конфліктів та медіація»

ЗАТВЕРДЖУЮ

Завідувач кафедри

____ Павло ФЕДОРЧЕНКО-КУТУЄВ

«15» грудня 2021 р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Міщуку Андрію Романовичу

1. Тема дисертації «Технології і методи гібридних конфліктів у світі», науковий керівник дисертації Пиголенко Ігор Вікторович доцент кафедри соціології, к. філос. н., затверджені наказом по університету від «13» грудня 2021р. № 3962-с
2. Термін подання студентом дисертації: 15.12.2021
3. Об'єкт дослідження – гібридні конфлікти.
4. Предмет дослідження – гібридні конфлікти у світі, технології і методи їх ведення.
5. Перелік завдань, які потрібно розробити:
 - 1) узагальнити наявні матеріали щодо гібридних конфліктів;
 - 2) визначити причини початку, технології та методи ведення, та шляхи вирішення гібридних конфліктів;
 - 3) окреслити основні теоретичні підходи до тлумачення категорії «гібридна війна»;
 - 4) здійснити аналіз гібридного конфлікту в Україні.
6. Графічний (ілюстративний) матеріал відсутній в дисертації.

7. Орієнтовний перелік публікацій – публікації відсутні.

8. Дата видачі завдання: вересень 2021

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів роботи	Примітка
1	Визначення напрямку дослідження	Серпень 2020	
2	Формування джерельної бази дослідження	Вересень-листопад 2020	
3	Складання розгорнутого плану	Грудень 2020	
4	Написання вступу до роботи (визначення об'єкту, предмету, мети та завдань)	Січень-лютий 2021	
5	Підготовка і написання I розділу дипломної роботи («ДОСЛІДЖЕННЯ «ГІБРИДНОГО КОНФЛІКТУ» У СВІТОВІЙ ТЕОРІЇ ВІЙН)	Березень-квітень 2021	
6	Написання II розділу («ЗБРОЙНИЙ КОНФЛІКТ В УКРАЇНІ – МЕТОДИ І ФОРМИ ГІБРИДНОСТІ В ВІЙНІ НА СХОДІ»)	Травень-червень 2021	
7	Написання III розділу («СВІТОВИЙ ДОСВІД ВЕДЕННЯ І ШЛЯХІВ ВИРІШЕННЯ ГІБРИДНИХ КОНФЛІКТІВ»), висновків та коригування списку літератури.	Липень-листопад 2021	
8	Передача магістерської дисертації на кафедру	24 листопада 2021	

Студент

Науковий керівник дисертації

Андрій МІЩУК

Ігор ПИГОЛЕНКО

АНОТАЦІЯ

Міщук А. Р. Технології і методи гібридних конфліктів у світі. – На правах рукопису. Магістерська дисертація за спеціальністю 054 «Соціологія». – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», кафедра соціології. – Київ, 2021. – 93 с., список джерел з 71 найменування.

Дисертація присвячена проблемі гібридних конфліктів, які стали дуже розповсюдженими у наш час. В Дисертації розкривається тема технології та методів гібридних конфліктів у світі. Узагальнені наявні матеріали щодо гібридних конфліктів. Визначено причини початку, технології та методи ведення і шляхи вирішення гібридних конфліктів. Окреслено основні теоретичні підходи до тлумачення категорії «гібридна війна». Здійснено аналіз гібридного конфлікту в Україні.

Ключові слова: гібридний конфлікт, гібридна війна, інформаційна війна.

SUMMARY

Mishchuk AR Technologies and methods of hybrid conflicts in the world. - On the rights of the manuscript. Master's thesis on specialty 054 "Sociology". - National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky", Department of Sociology. - Kyiv, 2021. - 93 pp., List of sources with 71 names.

The dissertation is devoted to the problem of hybrid conflicts, which have become very common nowadays. The Dissertation reveals the topic of technology and methods of hybrid conflicts in the world. General available materials on hybrid conflicts. The reasons of the beginning, technologies and methods of conducting and and ways of the decision of hybrid conflicts are defined. The main theoretical approaches to the interpretation of the category "hybrid war" are outlined. The analysis of the hybrid conflict in Ukraine is carried out.

Key words: hybrid conflict, hybrid war, information war.

ЗМІСТ

ВСТУП	7
 РОЗДІЛ 1. ДОСЛІДЖЕННЯ «ГІБРИДНОГО КОНФЛІКТУ» У СВІТОВІЙ ТЕОРІЇ ВІЙН.	11
1.1 Гібридні конфлікти в теорії війн	11
1.2. Основні підходи до трактування гібридних конфліктів	16
1.3. Гібридні конфлікти як загроза для НАТО	22
 РОЗДІЛ II. ЗБРОЙНИЙ КОНФЛІКТ В УКРАЇНІ – МЕТОДИ І ФОРМИ ГІБРИДНОСТІ В ВІЙНІ НА СХОДІ.....	26
2.1. Конфлікт на сході України – історія та передумови	26
2.2 Методи ведення гібридного конфлікту на сході України.	35
 РОЗДІЛ III. СВІТОВИЙ ДОСВІД ВЕДЕННЯ І ШЛЯХІВ ВИРІШЕННЯ ГІБРИДНИХ КОНФЛІКТІВ.....	55
3.1. Світовий досвід ведення гібридних конфліктів.....	55
3.2 Шляхи вирішення гібридних конфліктів.....	69
3.3 Шляхи вирішення гібридного конфлікту в Україні	77
 ВИСНОВКИ.....	82
 СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	85

ВСТУП

Актуальність теми магістерської дисертації.

Розглядаючи класичні теорії війн в ХХІ столітті, можна зробити висновок, що вони стають неефективними в сучасних реаліях глобалізації. Тому науковці сучасності підходять до виділення нового типу конфлікту так званих «гібридних війн». Концепція таких війн являє собою комбінацію як звичайних так і нетрадиційних та нерегулярних військових дій, які охоплюють також економічне, дипломатичне, інформаційне (включаючи психологічне, кібер- та дезінформаційне) протистояння. Поєднання військових та невійськових методів із використанням протестного потенціалу населення стають основоположними засобами війн нового покоління. Концепція «гібридна війна» намагається досягти масштабних наслідків, використовуючи скромні засоби, такі як придушення військових дій супротивника або запобігання народній політичній підтримці.

В цілому, гібридні конфлікти це координація тонких продуманих дій, із використанням більш цілісної стратегії, інтенсивність якої змінюється на різних етапах конфлікту (початок, загострення, вирішення), яка прагне дестабілізувати внутрішні та зовнішні процеси держави. Передусім мета полягає в тому, щоб зруйнувати державу шляхом дестабілізації економіки, розчарування і невдоволення населення, порушенням прав національних меншин, створення умов, що стимулюють контрольовану та неконтрольовану міграцію, придушення громадянського опору та руйнування критично важливої інфраструктури. Цьому сприяє вибіркове застосування засобів розвідки, операцій сил спеціального призначення, звичайних збройних сил та нерегулярних комбатантів (терористів, злочинців, міліцейських груп, найманців, рухів опору, партизанів тощо). Сучасний приклад гібридних конфліктів може бути чітко продемонстрований сучасними та недавніми бойовими діями, що відбуваються в Україні, Грузії, та, у деяких регіонах країн-членів Євросоюзу.

Методи, що використовуються в гібридних конфліктах часто є традиційними для ведення війн, які посилюються завдяки використанню нових технологій, що дозволяють більше проникнути у критичні елементи та життєво важливі системи противника. Тиск на слабкі сторони може призвести до системних змін критичних компонентів та пов'язаних з ними систем.

Методи ведення гібридної війни це більше, ніж удари по життєво важливих системах, таким як комунікації, інфраструктура або транспорт. Держава, а також недержавні організації дедалі частіше знаходять уразливі точки в ідеологіях та інституціях, або використовуючи соціальне невдоволення розпочинають нові війни.

Таким чином, «гібридна війна» - це високотехнологічний конфлікт. Це продовження політики держави або коаліції, політичних груп, транснаціональних корпорацій та недержавних організацій. Метою конфлікту є нав'язування точки зору своїм опонентам шляхом інтегрованого адаптивного та асиметричного синхронізованого деструктивного впливу на них у багатовимірному просторі та в різних сферах життя. Гібридна війна раціонально поєднується із звичайними та нетрадиційними складовими, акцент робиться на кількох джерелах та способах нападу, сумарному ефекті результатів та високому рівні невизначеності для противників того, які кінцеві стратегічні цілі можуть бути. У гібридних конфліктах основними цілями є контроль над суспільством, вплив на загальнолюдські настрої людей та маніпулювання особами, відповідальними за прийняття важливих рішень в державі. Противник має на меті маніпулювати основними цінностями, мотиваційними факторами та культурною основою, а також стратегічно критичною інфраструктурою країни. Це досягається комплексною, збалансованою реалізацією ефектів з використанням м'якої та твердої сили. Ось чому об'єктами у гібридних конфліктах є важливі компоненти держави – це політична, дипломатична, соціальна, технологічна, енергетична, фінансова, кібер, соціальна, інформаційна та інші сфери. Вплив на них призводить до

бажаного результату – швидкі деструктивні системні зміни у структурах та процесах функціонування держави.

Наукова розробленість проблеми дослідження. Важливі публікації з цієї теми були зроблені такими, науковцями, як П.Мансур, Френк Г. Хоффман, Майкл Айшервуд, Шейн Рівс, Роберт Барнсбі, Тема дослідження є розробленою і українськими вченими, а саме актуальною і дискусійною, вона привертає увагу багатьох науковців.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація написана в рамках ініціативної науково-дослідної теми кафедри соціології «Соцістальний розвиток, модернізація та модерн в глобальному світі» (реєстраційний номер: 0116U008963), керівником якої є професор, доктор соціологічних наук Павло Володимирович Федорченко-Кутуєв.

Мета дослідження – здійснити компаративний аналіз гібридних конфліктів, які мали місце у світі.

Для досягнення поставленої мети необхідно вирішити **ряд завдань**:

- 1) узагальнити наявні матеріали щодо гібридних конфліктів;
- 2) визначити причини початку, технології та методи ведення, та шляхи вирішення гібридних конфліктів;
- 3) окреслити основні теоретичні підходи до тлумачення категорії «гібридна війна»;
- 4) здійснити аналіз гібридного конфлікту в Україні.

Об'єкт дослідження – гібридні конфлікти.

Предметом дослідження є гібридні конфлікти у світі, технології і методи їх ведення.

Методи дослідження. У роботі використовуються: загальнонауковий, історичних, метод аналізу і синтезу.

Наукова новизна отриманих результатів полягає у проведенні загального аналізу виникнення гібридних конфліктів, зокрема в Україні під час агресії РФ. Дослідження терміну «гібридна» агресія, конфлікт.

Теоретична цінність роботи. В даній роботі проведено аналіз термінології, щодо гібридних конфліктів. Розглянуто сучасні та історичні приклади використання способів гібридної діяльності під час збройного конфлікту.

Практична цінність роботи полягає приверненні уваги до проблеми гібридних конфліктів, розроблення способів та заходів припинення гібридних конфліктів.

Структура магістерської роботи зумовлена логікою дослідження і складається із вступу, трьох розділів, 8 підрозділів, висновків та списку використаних джерел.

Загальний обсяг роботи – 93 сторінки, з них – основного тексту – 79 сторінок. Список використаних джерел містить 71 найменування.

РОЗДІЛ І. ДОСЛІДЖЕННЯ «ГІБРИДНОГО КОНФЛІКТУ» У СВІТОВІЙ ТЕОРІЇ ВІЙН.

1.1 Гібридні конфлікти в теорії війн

Слід наголосити, що термін «гібридна війна» не є власне військовим. Традиційно у воєнній теорії застосовують низку специфічних критеріїв типізації воєнного конфлікту, які уможливлюють врахування всіх його основних аспектів. Зокрема, за критерії поділу конфліктів на типи беруть: ступінь охоплення дійсності; сферу дії; тип сторін – учасників конфлікту; соціально-політичний устрій цих сторін; характер соціально-політичних відносин; ступінь організації; рівень ескалації та ін. Класифікація воєнних конфліктів пов'язана з основними формами їх прояву та існування.

Залежно від форми прояву, яка визначається методами використання військової сили протиборчими сторонами, окремо виділено приховані (латентні) та явні конфлікти. Поєднання якісно різних елементів у воєнному конфлікті зумовлює велику розмаїтість форм його існування, які скрадатимуться з комбінації трьох моделей війни – формальної, неформальної та війни сірої зони.

Формальною війною вважається зіткнення збройних сил однієї держави зі збройними силами іншої. Таке зіткнення супроводжується формальним актом оголошення війни. Неформальні війни – це збройні конфлікти, в яких принаймні одна або обидві сторони є недержавними утвореннями. Нові загрози, що виникли після закінчення холодної війни, призвели до виникнення феномену сірої зони, тобто до комбінації війни і воєнних дій з організованою злочинністю (наприклад, конфлікту у Республіці Ічкерія). Формальні війни можуть набувати традиційної та нетрадиційної форм. Традиційні війни – це воєнні дії регулярних збройних сил однієї країни проти регулярних і нерегулярних збройних сил (партизанські війни) іншої країни із застосуванням звичайних засобів збройної боротьби. На сьогодні в доктрині міжнародного права розрізняють міжнародні збройні конфлікти та збройні конфлікти

неміжнародного характеру. Згідно з положеннями Женевських конвенцій 1949 р. міжнародними збройними конфліктами визнаються такі конфлікти, коли один суб'єкт міжнародного права застосовує збройну силу проти іншого суб'єкта.

Традиційні війни – контактні, їх подальший розвиток пов'язаний з розробленням нових способів і засобів збройної боротьби. У поєднанні з новітніми інформаційними технологіями вони породжують такі форми, як мережеві та мережоцентричні війни (Василенко, 2009, с.20-22). Зміст мережевої війни полягає в досягненні успіху в збройній боротьбі не через перевагу в чисельності й вогневій могутності військ, а завдяки їх перевазі в інформаційних можливостях та організаційній побудові за мережевою структурою. Суцільна інформатизація та інтелектуалізація систем управління військами і зброєю якісно змінили зміст воєнних операцій. Вони дістали назву мережоцентричних операцій (воєн), які проводяться складом різновидових тактичних угруповань, що керуються з єдиного стратегічного центру й одночасно діють як окремі ключові елементи системи державного й військового управління – частини й підрозділи «сил удару у відповідь» – на всій території противника.

Особливістю мережоцентричних конфліктів є застосування побудованих на нових принципах методів розвідки, управління й забезпечення, які дають можливість застосовувати сили й засоби збройної боротьби не в одній лінії, а відразу на всій глибині театру воєнних дій відповідно до своїх бойових і маневрених можливостей. Спільне застосування різновидових угруповань військ підвищує результативність воєнних операцій (Хамзатов, 2006, с.14).

Нетрадиційні війни – це зіткнення регулярних збройних сил країни з іррегулярними формуваннями, угрупованнями, загонами, які не визнають норм і правил ведення воєнних дій. Формальні та неформальні воєнні конфлікти можуть бути симетричними й асиметричними. Асиметричний конфлікт відбувається за участю суб'єктів, що якісно відрізняються стосовно силового потенціалу й принципів організації та управління.

Навіть без переходу до воєнної фази асиметричний конфлікт має ряд специфічних ознак, які є наслідком обмеженого арсеналу засобів для слабших учасників. В асиметричних відносинах сильний партнер зазвичай не потребує застосування додаткових силових заходів для нав'язування власної волі. Тому конфлікт часто відбувається в латентному вигляді, лише епізодично переходячи в збройну фазу у формі жорстоких і на перший погляд ірраціональних дій, зокрема терористичних актів. Такі дії є тим засобом з обмеженого арсеналу, за допомогою якого слабший партнер впливає (і потенційно перемагає) на сильнішого (Галака О. М., Ільяшов О. А., Павлюк Ю. М., 2007, с.24-26). Втім, традиційна термінологічна та методологічна база для визначення сутності та характеру війни не виключає винайдення та використання нових дефініцій, наприклад, «гібридної війни». Франк Хоффман (Frank G. Hoffman), консультант міністерства ВМФ США, один із авторів концепції «гібридної війни», наголошує, що кожній епосі властиві свої специфічні форми війни. Це вимагає щоразу нових термінологічних розробок. Загалом сучасна епоха, на думку Франка Хоффмана, характеризується процесами гібридизації, в тому числі і у військовій сфері.

Традиційні форми війни змішуються з діяльністю організованої злочинності, іррегулярними конфліктами та тероризмом. Організаційна структура «гібридної війни» має децентралізований вигляд, який приховує її реальну ієрархію (Котенко, 2017). Для характеристики цієї нової реальності він пропонує застосовувати поняття «гібридної війни», яке нехай і не є суто військовим, але дозволяє оперативно охопити та відобразити суть змін у характері сучасної війни.

Є різні варіанти визначення сутності гібридної війни:

1. військова стратегія, яка поєднує звичайну війну, малу війну та кібервійну;
2. атака з використанням ядерної, біологічної, хімічної зброї, саморобних знарядь для терористичних атак та інформаційного тиску;

3. складна та гнучка динаміка бойового простору (battlespace), яка передбачає швидку реакцію та адаптацію учасників протистояння;

4. сучасний вид партизанської війни, яка поєднує сучасні технології та методи мобілізації (Біл Неметт, підполковник Корпусу морської піхоти США);

5. основний метод у асиметричній війні, яка ведеться на трьох умовних фронтах – серед населення конфліктної зони, тилового населення та міжнародної спільноти (полковник Армії США Джек МакКуен);

6. Франк Хоффман визначає гібридну війну у вигляді будь-яких дій ворога, який швидко та гнучко використовує найрізноманітніші комбінації дозволеної зброї, партизанську війну, тероризм, злочини на полі бою, і все для досягнення політичних цілей (Арзуманян, 2011, с.22-39).

За останні сім із лишком тисяч років існування цивілізації людства майже жодної проблеми, що стосувалася політичного й регіонального устрою спільноти, не було розв'язано без застосування зброї (Чікін, 2006).

Власне, гібридну війну можна у найзагальніших рисах визначити як сукупність заздалегідь підготовлених і оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. До складових гібридної війни відносяться традиційні та нестандартні загрози, тероризм, підривні дії, коли використовуються новітні чи нешаблонні технології для протидії перевазі супротивника у військовій силі. Наголосимо, що ідея гібридної війни не є новою. Військова історія знає немало прикладів асиметричних воєн із використанням нелінійної тактики та нерегулярних збройних формувань, які є давнішими аналогами сучасної гібридної війни. Можна згадати війну Наполеона в Іспанії чи війну у В'єтнамі. Власне, війна загалом не є лише виключно протистоянням на полі бою, а включає в себе елементи економічного, психологічного протистояння, партизанщини. Співвідношення та міра впливу цих компонентів на загальний результат, їх роль та місце у конкретному протистоянні визначається рівнем розвитку суспільства та духом епохи. Війни та збройні конфлікти є просторово-часовими процесами, в основі

яких лежать найрізноманітніші суперечності, а також використання різномасштабних військових формувань на певних територіях для досягнення певних цілей. Не треба забувати, що крім «внутрішніх» учасників, на конфліктну ситуацію впливає безліч зовнішніх – державних і недержавних (Радецький, 2011).

Гібридні сили успішно використовують технологічно передові системи таким чином, що вони працюють на межі можливостей. Тому гібридні збройні сили мають перевагу над традиційною армією, яка діє суворо в рамках Статуту. «Гібридна війна», або «Війна керованого хаосу» - збройний конфлікт із поєднанням принципово різних типів та способів ведення бойових дій, що застосовуються скоординовано для досягнення спільних цілей (Клімчук Ю.В.).

Загалом, гібридна загроза відзначається тим, що стирає традиційні уявлення та практики війни. Існує загалом два підходи до розуміння сутності війни. Перший, пов'язаний з традицією Карла фон Клаузевіца, визначає війну як організоване насильство, що має на меті досягнення соціальних та політичних цілей. Цей підхід дистанціюється від моральних, правових, етичних аспектів війни, або сприймає їх через призму військово-політичних інтересів. Другий підхід виходить із праць Цицерона, який твердив, що війна – це правова ситуація та умови, які легітимізують насильство та визначають його допустимі межі. Таким чином вводиться поняття «мирний стан» та «військовий стан», залежно від того чи є насильство легітимним. Розрізнення мирного та військового стану є критично необхідною річчю. Війна створює принципово іншу реальність, формує власне розуміння моральної, етичної, правової норми, яке потребує визначення засобами військового права. Поки правове поле залишається невизначеним, ми не можемо говорити про організоване ведення бойових дій, а насилля може стати неконтрольованим, що тим не менш, не означатиме війни (Арзуманян, 2011, с.39).

Так само стираються кордони війни та сценарії її початку та закінчення. Практично вся європейська політична та військова історія говорить про те, що еліти сприймають початок і закінчення війни як церемонію, певний набір дій.

Але у гібридній війні принаймні одна із сторін відчуває брак легітимності. Тоді на допомогу приходять пропаганда або створення маріонеткових урядів. Відтак, зміна стану з військового на мирний суттєво ускладнюється, а ворожість зростає та поширюється за межі конфлікту. І тут не треба забувати, що пропаганда дуже серйозно змінює політичні та суспільні погляди багатьох людей, тому навіть при супротиву влади гібридним атакам, все одно частина суспільства може не вірити своїй владі, а підтримувати ворога.

1.2. Основні підходи до трактування гібридних конфліктів

Аналіз геополітичних та геостратегічних середовищ натякнув на переформулювання як філософії, так і мистецтва ведення війни. Пояснення цьому – потужний розвиток нових технологій, що дозволяють змінювати інтенсивність та стратегії в конфліктах. Ці нові методи, коли вони поєднуються з традиційними розумінням війни, часто називають «гібридними» конфліктами (війнами).

Проаналізувавши літературу з теорії та практики військових конфліктів, варто зазначити, що традиційне поняття війни потребує корекції. Зокрема, сучасний український дослідник Євген Магда в своїх публікаціях вказує, дві основні точки зору на проблему. Згідно однієї – «традиційне бачення війни (way of war) застаріло і не може сприяти вирішенню проблем безпеки, які ставить перед нами XXI ст. Інша точка зору твердить, що трансформується характер та сутність війни, але незмінною залишається її природа» (Магда, 2014, с. 3). Для точного розуміння на скільки критичним є зміна традиційних уявлень про війну потрібно звернутись до класичної літератури.

Одним з основних теоретиків з цього питання є Карл фон Клаузевіц. Війна в концепції Клаузевіца розглядається як продовження політики держави насильницькими засобами, які використовуються для того щоб змусити противника виконати нашу волю. Основну роль у цій концепції відіграє застосування збройного насильства у всіх його формах. З погляду на таке трактування теорії класичної війни можна зробити припущення, що гібридні

конфлікти не мають схожості з традиційними війнами. Але не варто забувати тезу Клаузевіца, що війна має постійну природу та змінний характер, виходячи з цього класична війна може змінюватись і набувати різних форм ведення протистояння, тобто частково має схожість з новими – гібридними війнами. Отже, ми не можемо повністю відкинути концепцію війни Клаузевіца при вивченні гібридних конфліктів, адже сучасні війни мають ті ж елементи що й класичні, про те з залученням нових технологій, без яких не можливо виграти війну в сучасних умовах. Тому варто не забувати тезу Клаузевіца про те, що кожен вік має свою власну війну, власні обмежувальні умови а також свої власні сприйняття.

Визначення війни Клаузевіца ґрунтується на трьох незмінних характеристиках війни – війна пов'язана з насильством, війна використовується як інструмент і війна являється політичним явищем. Однак, підвищена увага, яку виявляють академічні кола, політики та світові організації (зокрема НАТО) до концепцій гібридних воєн, асиметричних воєн дає підставу думати, що характер війни змінився .

Використання термінів «неконвенційна» і «нерегулярна» тактика не обмежується тільки строгими рамками парадигми Клаузевіца про війну. Концепція намагається охопити ситуації, які знаходяться на межі війни завдяки своїй інтенсивності, законності або (що найцікавіше) невизначеності. Якщо треба використовувати цей термін в змістовному сенсі, то неконвенційна тактика може охоплювати інформаційні, дипломатичні або економічні операції, що не підпадають під визначення «війна».

Термін гібридна війна вперше з'явився в роботі американського військового експерта майора Вільяма Дж. Немета у праці, яку він написав у Монтерейській військово-морській академії у 2002 році під назвою «Future War and Chechnya: A Case for Hybrid Warfare». В. Намет на прикладі Чеченської республіки демонструє, яким чином збройні групи нерозвинених суспільств використовуючи передові технології та пристосовуючись до тактики свого опонента мають велику ефективність у конфлікті. Він стверджує, що гібридна

війна є сучасною формою партизанської війни, але більш ефективною з урахуванням застосування нових технологій та сучасних методів мобілізації до боротьби. Він зазначає, що завдяки своїм потребам чеченці легко змінилися від класичної до партизанської тактики і дуже часто могли об'єднати партизанські дії з терористичними атаками.

Потрібно розуміти, що є основні причини, які зумовили виникнення гібридних конфліктів. У ролі однієї з таких детермінант виступила передусім сучасна модель безпеки, яка сформувалася після Другої світової війни (Андрієвський, 2017, с.162).

З теоретиків, які працюють в різноманітних областях, які пов'язані з концепцією гібридної війни багато років, напевно найбільш цитованим є Френк Хоффман. Відповідно до його визначення, гібридна війна є відхилення від попередніх втілень війни: «Замість окремих викликів з фундаментально різними підходами (традиційний, нерегулярний, терористичний), ми можемо очікувати зустрічей з супротивниками, які будуть застосовувати всі форми війни і тактики, можливо, одночасно». Яскравим прикладом такої стратегії для Хоффмана була стратегія Хезболла у Другій ліванській війні в 2006 році, під час якої Хезболла завдала дуже потужного удару регулярним силам Ізраїлю (які мали величезну перевагу) шляхом використання конвенційних і нетрадиційних, нелінійних тактичних прийомів. Згідно міркувань Хоффмана, те, що робить конфлікт гібридним – це узгоджене використання різноманітних методів протистояння, як військових, так і невійськових, з метою досягнення результатів як у фізичному, так і в психологічному аспекті війни. Френк Хоффман у своїх працях підкреслює, що особливостями гібридних війн є поширеність актів терору та різноманітних форм злочинів проти суспільства. Він визначив гібридні загрози, як здатність одночасно і адаптивно застосовувати інтегрований зв'язок звичайної зброї та нерегулярної тактики, тероризму та кримінальних елементів у сфері боротьби за досягнення політичних цілей. Вищезгадане міркування вказує на дві групи дійових осіб в гібридних конфліктах: уряд та недержавні формування.

Ще один підхід до трактування гібридної війни демонструють А. Якобс і Г. Ласкоджаріас. Згідно їх тверджень в гібридних конфліктах задіяні окрім військових дій різноманітні методи, серед яких економічний тиск, розвідувальні служби, саботаж та дезінформація серед населення. Всі традиційні, нерегулярні та комбіновані форми ведення протистояння об'єднуються і становлять синтез руйнівних здібностей, що застосовуються в рамках гнучкої стратегії. Завдяки цьому гібридна війна стає невидимою на початку конфлікту і явною в момент, коли її вже неможливо попередити.

Концепція гібридної війни не є чимось абсолютно новим, представляючи поєднання конвенційних і неконвенціональних (нерегулярних) методів ведення війни, що виходять за межі поля битв і охоплюють економічні, дипломатичні, інформаційні (в тому числі психологічні, кібер і дезінформаційні) і політичні способи протистояння. Ця концепція ґрунтується по-перше на здатності цілеспрямовано впливати на віддалені об'єкти і процеси нетрадиційними військовими засобами, особливо на процеси і об'єкти, які є критично важливими для функцій держави і збройних сил. Як асиметричний підхід, гібридна війна спрямована на досягнення широкомасштабних наслідків з використанням скромних засобів, наприклад, перешкоджання військовим операціям супротивника або запобігання отримання політичної підтримки населення. В цілому, при гібридних конфліктах має місце координація так званих м'яких дій з використанням більш цілісної стратегії, яка варіює в плані інтенсивності на різних етапах (ініціювання, гостра фаза, рішення), і яка спрямована на дестабілізацію внутрішніх і зовнішніх процесів держави. Кінцевою метою є підриг цієї держави шляхом стимулювання дестабілізації економіки, розчарування і невдоволення населення, відчуження меншин або скривджених груп населення, створення умов для контрольованої і неконтрольованої міграції, придушення громадянського опору і підриву критичної інфраструктури. До цього додається використання певних розвідувальних здібностей, операцій сил особливого призначення, конвенційних збройних сил і нерегулярних комбатантів (терористів, злочинців,

міліцій, найманців, рухів опору, партизанів і т.д.). Сучасними прикладами гібридних конфліктів є недавні і триваючі бойові дії на Україні, в Грузії, і останнім часом, в деяких країнах Європейського союзу.

У гібридних конфліктах основними цілями є захоплення контролю над суспільством, здійснення впливу на настрої людей, маніпулювання людьми, які відповідають за прийняття важливих рішень у державі. Противник намагається маніпулювати основними цінностями, мотиваційними факторами, культурним базисом та стратегічною, комунікаційною та критичною інфраструктурою країни (Даник Ю., Малярчук Т., Бриггс Ч., 2017).

Застосування засобів гібридної війни направлено на найбільш критичні уразливості в матеріальних системах – комунікаціях, інфраструктурі або транспорті. Все частіше урядові, а також недержавні організації здійснюють напади на вразливі точки ідеологій та інституцій, а також використовують соціальне невдоволення або сприйняття корупції для посилення сил у конфлікті. Ці суттєві стратегічні слабкості дали можливість досягнення більшого успіху тим, хто використовує методи інформаційної або асиметричної війни. Домінування неоліберальних ідей привело до розширення прірви між багатими і бідними і збільшило тиск на середній клас. В результаті цього відбулися фундаментальні зміни в економічній, соціально-політичній і психологічній ситуації, відбувається переоцінка основних цінностей, має місце зростання популізму в багатьох країнах по всьому світу. Референдум про Брексіт в Об'єднаному Королівстві в 2016 році і обрання Дональда Трампа президентом США відображають стурбованість соціально-економічними умовами, ставлячи під сумнів такі інституції з багаторічною історією, як Європейський союз і НАТО.

Збереження конкурентоспроможності та провідної ролі на світовій арені вимагає відповідної економічної потужності і високого рівня розвитку освіти і науки, ресурсів, які знаходяться, головним чином, в розпорядженні центрів глобальної могутності. Країни, у яких немає доступу до цих ресурсів, відчувають відставання і втрату можливостей, а темпи інноваційного розвитку

в економічному секторі та секторі оборони неминуче призводить до втрати їх провідної позиції і перерозподілу сфер впливу між більш могутніми державами. Прагнення до захоплення контролю над конкуруючими «центрами світової могутності» і бажання отримати безперешкодний доступ до стратегічних ресурсів або, навпаки, запобігти такому розвитку ситуації, призводить до порушення кордонів або до поглинання зон безпеки і сфер впливу. В результаті цього має місце небезпечне взаємне зближення сфер впливу центрів світової могутності з неминучим конфліктом їх інтересів.

Ці конфлікти можна розглядати як зіткнення цивілізацій Гантінгтона, в яких культурні та релігійні відмінності народів є первинним джерелом конфліктів в світі після Холодної війни. Американський політолог Семюель Гантінгтон стверджує, що майбутні війни будуть вестися не між державами, а між культурами. Ці зіткнення можуть бути так само як і Макіавелівські спроби підризу стратегічних супротивників, оскільки лідери часто будуть відчувати потребу розвивати проекцію військової сили, яка не буде призводити до рішень, при яких збройний конфлікт може привести до знищення обох сторін. Є необхідність в нових інструментах досягнення цілей без прямої і видимої агресії. Одним з найгірших наслідків гібридної війни є своєрідний інформаційний вакуум, деморалізація населення, відчуття масового страху та незахищеності, зростання кількості біженців, загроза зубожіння, голоду, екологічних катастроф, застосування біологічної зброї, ядерна загроза тощо.

Намір був знайти технології, які можуть не тільки забезпечити новий рівень потужності озброєнь, а й здатність використовувати слабкі місця у всіх сферах функціонування держави. На відміну від інформаційних війн в минулому, нові технології дають можливість досягати стратегічних цілей неконвенційними методами (технології соціального впливу і маніпулювання, кібер сфера, інформаційна зброя, можливості нанесення завдання істотної шкоди системам управління держави).

1.3. Гібридні конфлікти як загроза для НАТО

Сіра зона між війною і миром є основною особливістю сучасних конфліктів. Карл фон Клаузевіц розглядає війну як продовження дуелі між двома сторонами, як акт насильства, який спрямований на примус опонента до виконання волі супротивника. Для більшої частини історії людства це визначення було самоочевидним. З часів Пелопоннеських війн стан війни означав наявність відомого противника з явними політичними цілями, які входили в суперечність із власними політичними цілями. Генерал Кертис ЛеМей казав про те, що вигравати війни було просто, потрібно було просто починати вбивати людей і коли вбивали достатню кількість, вони переставали чинити опір. Визначення війни Клаузевіца засноване на трьох незмінних характеристиках війни – війна пов'язана з насильством, війна використовується як інструмент і війна є політичним явищем. Однак, підвищена увага, яку виявляють академічні кола і політики (зокрема, в рамках НАТО) до концепцій гібридних воєн, невизначених воєн і обмежених воєн, дає підставу думати, що характер війни змінився – загрози з якими стикається Альянс стають все важче обумовленими.

Конфлікт в сірій зоні і гібридна війна не є взаємозамінними концепціями. Дійсно, використання терміну «конфлікт» для першої і «війна» для другої є навмисним. Використання термінів «неконвенційна» і «нерегулярна» тактика не обмежується тільки строгими рамками парадигми Клаузевіца про війну. Концепція сірої зони намагається охопити операції, які знаходяться на межі війни завдяки своїй інтенсивності, законності або (що найцікавіше) невизначеності. Якщо треба використовувати цей термін в змістовному сенсі, то неконвенційна тактика може охоплювати інформаційні, дипломатичні або економічні операції, що не підпадають під визначення «війна». Командування НАТО почали публічно висловлювати свою стурбованість такими неконвенційним загрозам. Якраз широке використання неконвенційної тактики сприяло розвитку кризи впевненості в НАТО. Командування спеціальними операціями США приступило до виконання дослідницького проекту

тривалістю в рік, під найменуванням «Сіра зона». Цей проект повинен дати керівництву США інструменти для розуміння загроз сірої зони і забезпечити ефективну відповідь на них. Сіра зона визначається як область між війною і миром, для якої все ще немає повного розуміння. Дії, що вживаються в сірій зоні, виходять за рамки нормального суперництва в мирний час, але трохи не доходять до повноцінної війни.

Російські дії на сході України і в Криму мали як гібридний, так і невизначений характер. У 2014 році Росія використовувала поєднання конвенційних військових сил (наприклад, збільшення чисельності граничних і морських патрулів на кордоні з Україною) та неконвенційних тактик (наприклад, «зелені чоловічки» і інформаційне протистояння, досягнуте використанням російської ідеології у східній Україні) для забезпечення анексії Криму. Ці дії викликали тривогу в Альянсі, незважаючи на те, що Україна не є членом НАТО. Навмисна двозначність російських дій і російської риторики паралізували здатність Альянсу ефективно реагувати і такий підхід має великий потенціал дати ті ж результати, якщо ця доктрина буде застосована проти членів НАТО в Східній Європі. Чи є така тактика новою або має історичні прецеденти залишається дуже спірним питанням. Однак, цілком очевидно те, що НАТО не готове до ведення конфліктів в сірій зоні.

Так як противники НАТО розробляють стратегії використання сірої зони, ймовірно, конвенційні сили будуть використовуватися новими способами і з'являться нові неконвенційні тактичні прийоми. Деякі неконвенційні тактичні прийоми, схоже, більш ефективні, ніж інші. Інформаційні операції являють собою неконвенційний підхід, який може бути дуже ефективним в конфліктах в сірій зоні. Отже, на межі тисячоліть людство увійшло в еру високотехнологічних локальних війн і воєнних конфліктів, яка характеризується тенденцією до нарощування переважно якісних показників засобів збройної боротьби (Сірий С., 2007, с.151).

Інформаційні операції (кібер-операції) спрямовуються на завдання ураження мережевим комунікаціям. У них використовується комп'ютерний код

для зміни, збору даних або деактивування комп'ютерних систем в яких є програмне забезпечення, апаратна частина і людський елемент. І вони в свою чергу є надто важливими для противника. Не можна вважати, що кібер-операції безпосередньо пов'язані з використанням насильства, оскільки комп'ютерний код не може безпосередньо завдати шкоди людині подібно кінетичній, енергетичній і хімічній зброї. Тим не менш, вони стали визначним елементом сучасних конфліктів для того, щоб шпигувати за чужими урядами. В опублікованій Національній стратегії безпеки та оборони і Великої Британії за 2015 рік, уряд вирішив виділити 1.9 мільярдів фунтів стерлінга на захист Сполученого Королівства від кібер-атак і на розвиток здібностей для захисту в кібер-просторі. Кібер-операції мають особливу цінність в конфліктах в сірій зоні завдяки двом своїм ключовим характеристикам: органічно властиві їм проблеми з відсутністю відповідальності за їх проведення та легкість з якої нападник може заперечувати свою участь.

У 2015 році Томас Рід і Бен Б'юкенен провели оцінку проблеми атрибуції в спробі зрозуміти її виклики і дати рекомендації людям, які провадять політику для вирішення проблеми кібер-загроз. Рід і Б'юкенен розробили систему, яку вони назвали «Q моделлю» атрибуції. Ця модель вимагає трирівневого вивчення ситуації, що включає тактичний (технічний), оперативний і стратегічний аналіз.

На тактичному рівні, спеціалісти встановлюють, що кібер-атака існує і використовують всі засоби, що знаходяться в їх розпорядженні, для того, щоб зрозуміти, як був здійснений напад. Як противник увійшов в систему і який бажаний результат отримав після доступу до неї? На цьому етапі аналіз може бути сфокусований на вистежуванні інтернет (IP) адрес, на спостереженні за рухами противника, на реверсивному інжинірингу шкідливого коду і на безлічі інших технічних аспектах. На оперативному рівні, результати технічного аналізу накопичуються і оцінюються на тлі інших джерел інформації, наприклад нетехнічного аналізу (агентурна розвідка), аналіз схожих атак у більш широкому геополітичному контексті, для створення гіпотез про кібер-

атаку. І нарешті, стратегічний аналіз допомагає зрозуміти хто і чому здійснив напад. На цьому етапі суб'єкти, які приймають рішення, розглядають оперативні гіпотези, обговорюють хто може нести відповідальність і формують відповідну реакцію на основі значущості атаки. Останнім моментом Q моделі є комунікація атрибуції до ширшого загалу.

Однак, ця модель не вирішує проблему атрибуції. Кваліфіковані опоненти все ще можуть певною мірою прикрити свою роль в кібер-атаках, найімовірніше вказавши на когось іншого. Рід і Б'юкенен звертають увагу на те, що «Досконала кібер-атака так само невловима, як і скоєний злочин». Однак, суперникам в гібридній війні не потрібно здійснювати вчинені кібер-атаки, які не підлягають атрибуції; їм потрібно просто викликати сумніви в головах аналітиків, достатні для обмеження або уповільнення реакції політиків.

Визначити винного за проведення кібер-атак важко і в деяких випадках причетність до їх проведення можна заперечувати, навіть якщо на винного можна вказати. Хоча комп'ютерна програма ніколи не вб'є безпосередньо людину, дуже можливо, що кібер-атака на промислову або соціальну інфраструктуру можуть призвести в подальшому до смерті людей. Наприклад, в 2006 році експеримент Аврора показав, що комп'ютерні програми можуть привести до кінетичних наслідків, і в 2010 вірус-черв'як Stuxnet виявився відповідальним за відмови центрифуг ядерного об'єкта Натанз в Ірані. Потенціал як для невизначеності, так і для ефективності, означає, що кібер-атаки досить імовірно будуть використовуватися противниками «сірої зони» в майбутньому, як це вони робили і в минулому.

РОЗДІЛ II. ЗБРОЙНИЙ КОНФЛІКТ В УКРАЇНІ – МЕТОДИ І ФОРМИ ГІБРИДНОСТІ В ВІЙНІ НА СХОДІ

2.1. Конфлікт на сході України – історія та передумови

Розглядати конфлікт на сході України неможливо без історичного екскурсу, хоча б починаючи з 1991 року. Треба розуміти, що від початку проголошення Незалежності України, РФ намагалася позбавити Україну незалежності та зробити частиною своєї федерації. Або як мінімум заважати Україні стати успішною, сучасною, європейською державою.

В 1996 році, коли відбувався поділ чорноморського флоту, який відбувався з постійним тиском російської сторони на українську, флот поділено було з перевагою РФ у 4 рази. Також не треба забувати про риторику депутатів держдуми РФ, які в період підписання договорів про дружбу і т.д., висловлювали неприпустимість затвердження непорушних кордонів України, а також хотіли, щоб Азовське море було внутрішнім морем РФ та України, тобто не регулювалось міжнародним законодавством та морськими конвенціями.

Найбільш гостро ця проблема постала у жовтні 2003 року. Росія в односторонньому порядку з боку Таманського півострова почала споруджувати дамбу в напрямку українського острова Тузла. Цей острів має площу 35 га, його довжина 6,5 км, ширина – 500 м, відстань від острова до українського берега – 4 км, до російського 5,5 км (Гай-Нижник, 2017, с.79).

Цей крок РФ, був звичайно не випадковим та добре спланованим актом гібридної агресії. РФ намагалась як перевірити слабкі сторони України у питанні захисту свого суверенітету так і побачити, чи країни НАТО, зокрема США – гарант незалежності України за Будапештським меморандумом, допоможуть Україні. Як виявилось Україні забракло політичної ваги щоб почати хоч якісь консультації на рівні країн – гарантів незалежності, а цим країнам, як виявилось було байдуже на цей конфлікт з РФ. Лише рішуча позиція та дії президента України Кучми Л. Д. не дали гібридному акту

російської агресії перерости у військовий конфлікт з захопленням українських територій.

Якщо взагалі поглянути на десятиріччя 1995-2005 щодо зовнішньої політики РФ, то конфлікт щодо о.Тузла не був таким несподіваним. Тузлу російська влада проголошувала російським островом ще з 1990-х років. Підписуючи договори про дружбу та кордони між державами, РФ робила висловлювання, які не співпадають з прописаними нормами у цих договорах.

Якщо поглянути на Будапештський меморандум, то порушення незалежності України вважається не тільки тоді, коли порушена територіальна цілісність, а й економічні інтереси, культурні, державні та інші інтереси України, та країна-підписант Меморандуму вдається до тиску на Україну у різних проявах та галузях.

Дивимось на риторику РФ щодо СНД та підписані там документи. СНД проголошується як сфера керування, інтересів і т.ін. РФ. Головною валютою СНД повинен бути російський рубль. Військова доктрина РФ, починаючи з 2003 року визначає що війська РФ можуть діяти як в межах СНД, так і за їх межами для забезпечення інтересів РФ. Також РФ прописує, що відтепер має право на превентивний удар.

Гібридні дії РФ проявлялись не тільки у військових маневрах, та погрозах. РФ вела проти України політичну війну, економічну війну, енергетичну, зокрема газову війну. На виборах 2004 року РФ відкрито підтримувала проросійського політика В. Януковича. Сепаратистський з'їзд «регіоналів» у Сєверодонецьку у 2004 році міг вже тоді призвести до військової агресії РФ, але мабуть РФ на той момент була не готова до таких дій.

Після перемоги на тих виборах В. Ющенко, який хоча і проголосив про дружбу з усіма, в тому числі з РФ, РФ почала вести гібридні дії для підризу української економіки, промисловості і т.д. У 2009 році РФ перекрила поставки газу в Україну, чим призвела до загибелі десятків людей в Донецькій області. Під час переговорів про поставки газу та підписання газового контракту РФ як завжди тиснула на Україну. Можна також згадати так звані «молочні, сирні» та

інші продовольчі війни того часу. РФ забороняла ввіз продукції з України чим призвела до великих збитків українських товаровиробників сільськогосподарської продукції.

Під час переговорів, і щодо газу, і щодо різної української продукції зі сторони РФ був шантаж, погрози, а також вимоги про зменшення або навіть припинення співпраці з ЄС та НАТО.

Щодо ситуації у Криму, то РФ в односторонньому порядку здійснювала модернізацію флоту, перевозила заборонені ракети в Крим, і не зважала на протести України. Складалося враження, що кремлівська верхівка та військове командування РФ цілеспрямовано виявляли зневагу до державного суверенітету України, демонструючи власну безкарність, й принизливими випадками своєї пропаганди та поведінкою російських збройних сил у Криму, ніби провокуючи українське політичне керівництво на відкритий воєнно-політичний конфлікт, прагнули таким чином розв'язати повноцінну війну між Україною і Російською Федерацією із далекоглядними геополітичними намірами та наслідками (Гай-Нижник, 2017, с.100).

Дивлячись на постійні негативні висловлювання владної верхівки РФ, Тернопільська обласна рада у 2009 році звернулась до Президента України та органів державної влади щодо перегляду Будапештського меморандуму, закріплення його на міжнародному рівні як юридичного договору, або підписання окремих двосторонніх договорів з країнами-гарантами: США, Великобританія, Франція, Китай, РФ. Тобто ми бачимо, що на той момент, українська влада на різних рівнях відчувала постійний тиск та загрози зі сторони РФ, та робила якісь кроки для захисту українського суверенітету.

РФ, в свою чергу, якщо прослідкувати її політичну активність, що в межах СНД, що інші вектори зовнішньополітичної діяльності підтримувала сепаратистські та проросійські партії, політиків, групи впливу, рухи. Не стало несподіванкою те, що РФ підтримала Януковича на виборах 2010 року. Та знову ж таки, неважливо чи відкрито вів би проросійську політику Янукович, чи намагався б балансувати між Європою та РФ, РФ вела свою гру. Хоча

Янукович і проголошував про зближення з РФ у різних сферах, РФ все одно тиснула і на Януковича і на Україну взагалі. В усіх галузях РФ хотіла мати набагато кращу позицію ніж Україна. При підписанні «Харківських угод» РФ досягла не просто своїх цілей, а й поставила у дуже погане та глузливе становище Януковича.

Ці події та взагалі політика Януковича та дії РФ викликали занепокоєння українського суспільства. Почалось публічне невдоволення політикою влади. Загалом на мітинги проти ратифікації угоди про подовження базування російського флоту в Україні і на підтримку цієї угоди вийшло від 10 до 15 тисяч осіб. Лідери опозиції, виступаючи перед мітингувальниками, звинуватили Президента В. Януковича й парламентську більшість у державній зраді й закликали народ до всеукраїнських акцій непокори (Гай-Нижник, 2017, ст.113).

При владі Януковича РФ так тисла на Україну як ніколи до того. Почалось втручання в усі сфери влади, економіки, армії та навіть освіти. РФ досягла того, що Україна проголосила про невходження до НАТО, позаблоковість, а також проросійські політики намагались зменшити роль української мови та збільшити роль російської. Все це є проявом гібридної агресії РФ.

Взагалі 2010 рік став роком, коли РФ почала систематичне знищення українського суверенітету, армії, економіки. З 2010 року у програму фінансування армії заклали зменшення фінансування кожного наступного року в середньому на 0,7 %. Загальний військовий призов відмінили у 2013 році, напередодні російської агресії, чим суттєво зменшили кількість української армії. На високі військові посади були призначені громадяни РФ, які отримали українське громадянство від Януковича. Були знищені військові структури, об'єднаний штаб та система ПВО. Боездатні комплекси ПВО були передані у АР Крим. Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою (Ільницька, 2016, с.29).

2011-2012 роки були роками економічного тиску на Україну. РФ одночасно шантажувала припинити поставки газу Україні, будувала Південний потік, вимагала від України погасити борги приватних енергетичних компаній, вимагала щоб Україна передала свою ГТС в управління РФ, об'єднала Нафтогаз і Газпром і т.д. Тиск був шалений. Україна перебуваючи у скрутному економічному, енергетичному, політичному становищі ставала все легшою мішенню для агресії РФ.

РФ у той час дуже нахабно шантажувала Україну та вимагала вступити в Митний союз та відмовитись від асоціації з ЄС. На цьому тлі 12 вересня 2013 р. Європейський парламент ухвалив резолюцію, яка засудила Росію за тиск на країни-учасниці «Східного партнерства», котрі бажають розвивати асоціаційні відносини з ЄС (Гай-Нижник, 2017, с.144). РФ в свою чергу усіма методами намагалась завадити зближенню України та ЄС. В РФ розробили документ «Про комплекс заходів із залучення України до євразійського інтеграційного процесу», який свідчить про те, що курс РФ на економічне та політичне поглинання України був ціллю номер 1.

Таким чином, найближчими цілями зусиль та заходів РФ визначалися:

1. Запобігання підписанню угод України з ЄС про Асоціацію.
2. Формування впливової мережі проросійських громадсько-політичних сил, здатних стримувати українську владу від несприятливих для Росії дій, а також примушувати її до входження України в МС і ЄЕП.
3. Нейтралізація політичного та ослаблення медійного впливу євроінтеграторів.
4. Створення умов для приєднання України до МС і ЄЕП до 2015 року. (Гай-Нижник, 2017, с.149).

РФ вела наступ на Україну усіма гібридними методами, працювали центри інформаційних маніпуляцій, вкладалися величезні кошти у пропаганду. РФ «поставила на карту» усе, щоб задушити Україну та примусити інтегруватись з РФ.

РФ вдало йшла до досягнення своєї кінцевої цілі у кінці 2013 року. У вересні-жовтні 2013 року Кабінет Міністрів України публічно оголосив про

недоречність Асоціації з ЄС та про розробку програми входження до Митного союзу з РФ.

Ми можемо проаналізувати та прослідити цілеспрямованість інформаційної агресії РФ проти України на різних прикладах, особливо після приходу до влади в РФ Путіна.

Загальмувавши дезінтеграційні процеси в РФ і надійно зацементувавши методами «батога і пряника» економічну та політичну еліту, нове російське керівництво на чолі з Путіним перейшло до безпосередньої реалізації реваншистської стратегії. Насамперед було поставлено завдання з'ясувати реакцію США та їх союзників, для чого Росія вдалася до застосування силових засобів проти України (жовтень 2003 року – криза навколо острова Коса Тузла, січень 2006 та січень 2009 року – «газові війни») та Грузії (війна 08.08.2008). Після цих подій у Кремлі сформувалося стійке уявлення про наявність у еліт західних країн, насамперед європейських, «мюнхенського синдрому» – готовності до поступок агресору за рахунок держав Балто-Чорноморсько-Каспійського регіону. Пасивна реакція західних держав на російські провокації суттєво сприяла формуванню у керівництва РФ переконання про безкарність та фактично заохочувала Кремль до агресивних дій проти держав колишнього СРСР та «соціалістичного табору». Поворотним моментом для Путіна стала Помаранчева революція 2004 року, яку російський національний лідер сприйняв як особисту поразку. Саме тоді було відпрацьовано сценарії, застосовані через 10 років. Зокрема, у 2004 році Росією було вперше розіграно мапу «східного українського сепаратизму». 26 листопада 2004 року Луганська обласна рада проголосувала за створення Південно-Східної республіки, 28 листопада на з'їзді депутатів усіх рівнів з 17 регіонів України, переважно східних та південних, у м. Сєвєродонецьк Луганської області, в якому брала участь представницька делегація з РФ на чолі з мером Москви Ю. Лужковим, обговорювалося створення Південно-Східної федеративної держави зі столицею у Харкові.

У квітні 2008 року під час Бухарестського саміту НАТО Путін заявив президенту США Дж.Бушу: Україна – це взагалі не держава. Частина її територій – це Східна Європа, а ще частина, і значна, подарована нами... якщо Україна піде до НАТО, то піде без Криму та Сходу – вона просто розвалиться». Такі уявлення стали основою стратегічного бачення цілей РФ на новому етапі експансії, що, ймовірно, було сформульовано на спільному засіданні Ради безпеки та Державної ради РФ 25 грудня 2008 року. Відповідні положення у прямій чи завуальованій формі були закріплені в російських стратегічних документах з питань зовнішньої та безпекової політики Стратегії національної безпеки РФ, Концепції зовнішньої політики РФ, Військової доктрини РФ, а також Концепції довгострокового соціально-економічного розвитку РФ. Задля реалізації стратегії Кремля російські державні органи створили комплексну систему примусу країн СНД до єдності. Така система включає інструменти політико-дипломатичного, економічного, насамперед енергетичного, інформаційно-пропагандистського і, у разі доцільності – військового тиску з широким використанням технологій підривної діяльності, теоретично розроблених і практично випробуваних ще за часів сталінського СРСР. Складовою цієї системи комплексного тиску мала стати теоретично опрацьована і практично випробувана парадигма «гібридної війни». Сучасне офіційне російське розуміння цієї парадигми викладено у доповіді начальника Генерального штабу ЗС РФ генерала армії В.Герасимова на загальних зборах Академії військових наук РФ у січні 2013 року. Важливим напрямом російської політики щодо України є підривна діяльність. У 2006 р. ФСБ РФ створила підрозділи для дій у соціальних мережах («18 центр»). Російські спецслужби активізували створення агентурних мереж в Україні. Почали діяти численні структури російського впливу всього політичного спектра – від праворадикальних та клерикальних до комуністичних. Після 2004 року російські спецслужби сформували в південно-східних регіонах та Криму розгалужену мережу антиукраїнських організацій, яку контролює або навіть очолює російська агентура – структури Партії регіонів, КПУ, ПСПУ, партій

«Батьківщина», «Російська єдність», різні православні групи, орієнти. «російського світу», сепаратистські політичні групи («Донецька республіка»), криміналізовані парамілітарні утворення (козацькі формування, бійцівські клуби, насамперед у Криму, організація «Оплот», охоронні структури, які активно використовувалися під час Революції гідності, так звані «титишки» »).

Переважа більшість цих груп не мала широкої громадської підтримки, водночас вони активно взаємодіяли з правоохоронними органами за часів режиму Януковича.

З 2008 року Кремль розпочав пропагандистську підготовку до агресії проти України. У пресі, на телебаченні, в Інтернеті реалізовувалися пропагандистські кампанії та спеціальні інформаційні операції. Масовими тиражами видавалися різні книги про майбутню російсько-українську війну. Ідеологічною основою російської пропаганди стала концепція «російського світу», яка сформувалася ще у 1970-х роках московською ліберальною інтелігенцією (з кола М.Гефтера) та була підхоплена у 2010-х патріархом РПЦ Кирилом (В.Гундяєвим). Російська пропаганда працювала на три основні цільові аудиторії: західну, українську та власне російську. Головним завданням на західному напрямку було довести «штучність» української нації та приреченість української держави, яка так і не відбулася. Серед українців поширювалися міфи про одвічну єдність з російським народом, про так званий «триєдиний, штучно розділений російський народ», переваги приєднання то до нової Російської імперії, то СРСР-2 «під геніальним керівництвом В.Путіна», і водночас , наголошувалося на неспроможності українських еліт, їх нездатність керувати незалежною державою, їх корумпованість, нездатність до знаходження компромісів тощо. Суспільство інфікувалося ідеями великодержавного шовінізму, імперства, неповноцінності інших народів у порівнянні з «найдуховнішим у світі» російським народом, ідеями православного фундаменталізму, російського фашизму тощо. При цьому російська пропаганда не зупинялася перед поширенням навіть брутальних вигадок, у яких пропагандистам гідну конкуренцію становили лише російські

політики та дипломати. Російську культурну політику на українському напрямі було повністю інтегровано у загальну стратегію ліквідації української державності. Для ведення російської пропаганди широко використовуються як засоби масової інформації, а й культурно-розважальна індустрія: кінематограф, шоу-бізнес, начебто не політичні, «культурні» програми телебачення і радіомовлення, Інтернет тощо. Російська культурна експансія проти України здійснювалася свідомо та наполегливо протягом усіх років незалежності, чому сприяла неефективність державної гуманітарної та культурної політики.

Російський капітал нерідко виступає як ефективний інструмент Кремля. В Україні до 2013 року російський капітал встановив повністю або частково контроль за галуззю зв'язку та телекомунікацій, паливно-енергетичним комплексом, частиною банківського сектора тощо. Ці процеси, що загрожують національній безпеці України, значно активізувалися після приходу Януковича до влади, чому сприяла ідентична кримінально-олігархічна сутність та відповідна бізнес-культура російських та українських кланів. Протягом усіх років незалежності України Росія із застосуванням усього наявного арсеналу підривних засобів мала антиукраїнські, антизахідні та проросійські настрої серед населення Автономної Республіки Крим та Севастополя.

Якщо повернутись до протистояння суспільства та уряду Януковича, то українське суспільство не сприйняло позицію Уряду, та вбачаючи зрадницькі дії влади вийшло на мітинг на підтримку Європейської асоціації. 24 листопада відбулася перша масова демонстрація за Україну в Європі та проти влади. За даними з різних джерел, у ній взяло участь від 50 тис. до 100 тис. осіб. Учасники акції вимагали відставки КМУ та розпуску ВРУ у разі непідписання документу про Європейську асоціацію. РФ не врахувало те, що народ України це не російський народ і українці не бояться ні своєї влади, коли вона діє злочинно, а також не бояться вийти на захист своєї Батьківщини від ворога.

Як бачимо, спроби розхитати Україну зсередини, за допомогою гібридних методів агресії, РФ робила задовго до 2014 року, коли вона вирішила діяти

напрямую – військовими методами, навіть не ховаючись від міжнародної спільноти, або маючи усіх за бовдурів.

В той час, і це важливо відмітити, Україна та світ перебував у стані розслабленості, та не вважаючи, що у XXI столітті в Європі може якась країна вирішити захопи іншу, тому навіть маючи безліч доказів гібридної агресії і суспільство міжнародне та українське і державні інституції не могли адекватно реагувати на таку нахабність.

2.2 Методи ведення гібридного конфлікту на сході України.

Методи ведення гібридного конфлікту на сході України не можна розглядати у відриві від методів захоплення АР Крим. Це є одним ланцюгом подій, який був розроблений російськими спецслужбами та підтриманий держдумою РФ.

Якщо звернутись до елементів гібридності у агресії РФ щодо України, то економічна агресія, політичний шантаж ні до чого успішного не призвів. Економіка України виявилась міцнішою ніж вважав Путін, а дії нової української влади, яка прийшла після Революції Гідності вельми успішними.

Маючи розграбовану казну владою Януковича, нова влада зуміла скоординованими діями налагодити економічну ситуацію в країні.

Другий метод агресії РФ – політичний, передбачав або збереження влади Януковича при повним контролем РФ та подальшу інтеграцію України в склад РФ, або посіяти такий політичний та суспільний хаос, щоб розвалити Україну без бойових дій. Це теж не вдалось. Янукович втік, народ України вибрав на демократичних виборах нову владу, яку підтримало міжнародне співтовариство.

Інформаційна атака, яка безупинно продовжувалась і вдень і вночі на російських каналах, в мережі Інтернет, через проросійських політиків завдавала великої шкоди Україні та її медіапростору. Найбільш ефективними прийомами інформаційних атак є: дезінформація, залякування, схематизм, глузування, вклинювання, фальшування (Курбан, 2016, с.132). Під прикриттям величезної

хмари пропаганди та нагнітанням суспільного невдоволення населення АР Крим (часто під дулами автоматів), РФ з одного боку показувала світу картинку небажання «кричан» жити в Україні, з іншого боку це давало можливість використовувати свої збройні сили, які б були без розпізнавальних знаків, немов би силами «самооборони Криму». Потім використовуючи місцеве населення, зокрема ним же і прикриваючись, військові РФ захоплювали військові частини, склади зі зброєю, органи місцевої влади.

Використовуючи відсутність в Україні достатньої військової могутності на той момент (лютий-березень 2014 р.), РФ дуже швидко захопила АР Крим, та провела «так званий референдум» про незалежність Криму та вступ до складу РФ. Ця «мирна» картинка показувалась на весь світ. Передумови виникнення конфлікту зумовлені помилками у процесі створення та розбудови європейської та північноатлантичної архітектури безпеки та співробітництва на початку 1990-х років, хибними параметрами залучення країн пострадянського простору до європейської та євроатлантичної інтеграції (Чупрій, Загребельний, 2017, с.68).

Тобто використовуючи ці перелічені три елементи гібридної агресії, за підтримки військових РФ здійснила захоплення частини території України – АР Крим.

Після цього, не зупиняючись, а навпаки збільшивши ступінь медійної пропаганди (про бажання вступити до складу РФ «півдня України»), та маючи вдалий досвід застосування такої тактики у Криму, РФ вважала, що подальше поглинання України гібридними методами буде легким. Вона дуже помилилась.

Так звані «експерти щодо України», які показували доповіді Путіну і малювали райдужну картинку про бажання жителів Сходу та Півдня України приєднатись до РФ, ввели в оману Путіна. Це можливо частково допомогло Україні, не всі методи та сили агресора були задіяні. Ну і Україна показала світу свою картинку: населення виступило проти окупантів, багато добровольців пішли у добровольчі батальйони. Спроби захоплення органів

місцевої влади не були успішними. В Одесі, Харкові були придушені такі спроби або спецназом, або місцевим населенням.

Розуміючи, що спроба провалилася, РФ кинула всі сили, уже не дуже прикриваючись на Донецьк та Луганськ. 24 серпня 2014 року взагалі без прикриття війська РФ просто через кордон їхали на територію України та вели артилерійські обстріли української території.

Тут було задіяно, ще один елемент гібридного конфлікту, так як і зі збитим Малазійським Боїнгом, підробка російською стороною матеріалів супутникових знімків, замальовування військ на знімках і т.д.

Знову ж таки, при успішному захопленні окремих районів Донецької та Луганської областей України, пішов в хід «референдум» про незалежність від України та подальше приєднання до РФ.

Тут потрібно занотувати такий момент, як введення міжнародних санкцій, блокада РФ у різних міжнародних організаціях та подібні політичні дії, які звичайно у сукупності з підняттям народно-бойового духу українського народу зупинив подальші дії РФ на той момент. Санкції показали себе непоганим засобом подолання гібридної агресії.

Щоб зрозуміти, чому саме поняття гібридності повернулося на порядок денний політичного дискурсу, слід звернутися до аналізу точки зору одного з головних ідеологів російської гібридної агресії проти України, та міжнародного злочинця, начальника Генерального штабу ЗС РФ Валерія Герасимова. Він використовує саме гібридний підхід при описанні методів ведення сучасної війни, вважаючи, що їх використання дозволить за лічені дні розхитати ситуацію у певній країні зсередини. Він пише, що у сучасних конфліктах все частіше акцент використовуваних методів боротьби зміщується у бік комплексного застосування політичних, економічних, інформаційних та інших неенних заходів, що реалізуються з опорою на військову силу. Розкриваючи зміст цих методів, Герасимов вказує, що вони полягають у досягненні політичних цілей шляхом мінімального збройного впливу на противника у вигляді підриву його військового та економічного потенціалу засобами

інформаційно-психологічного тиску, через активну підтримку внутрішньої опозиції, з використанням партизанських та диверсійних методів. Герасимов концентрує особливу увагу на інформаційної складової, коли свідомість громадян держав – об'єктів агресії піддається масованому цілеспрямованому впливу через Інтернет-мережі. Вищезазначені методи, вважає Герасимов, слід доповнювати військовими заходами прихованого характеру, в тому числі, з використанням екстремістських і терористичних організацій, що і робить РФ по всьому світу. Межі схованості закінчується тоді, коли сторони переходять до відкритого використання сили, як правило, під виглядом миротворчої діяльності та антикризового врегулювання ситуації, однак, до цього доходить лише у виняткових випадках. Його виклад гібридного підходу закінчується цинічним висновком про те, що непрямі та асиметричні дії та способи ведення гібридних війн дозволяють позбавити супротивника фактичного суверенітету без захоплення території держави.

Однією з характерних рис гібридної війни в Україні є те, наскільки вона займає всі аспекти суспільного життя, наскільки широкомасштабна, багатовимірна та використовує багатофакторну інформацію, орієнтовану як на психологічні, так і на кібернетичні джерела. Хорошим прикладом такої діяльності є інноваційні та високотехнологічні зразки зброї та військової техніки, що застосовуються під час анексії Криму в 2012 році, а також бойові дії на сході України 15 з 2014 року:

- Системи та комплекси електронної війни та інші типи електронних контрзаходів;
- Сучасні інформаційні та комунікаційні системи;
- Інноваційні системи управління зброєю;
- Комплексні розвідувально-ударні комплекси;
- Інноваційна, в тому числі автоматизована, програмне забезпечення;
- Комплекси для проведення інформаційно-психологічних заходів та дій в кібер-просторі;

- Екологічний контроль та космічні системи;
- Робототехнічні системи (особливо безпілотні комплекси літаків) та контрзаходи.

Ця технологія не існувала самостійно, але була частиною масштабної та стратегічно розробленої кампанії, яка підірвала довіру до центральних інституцій. Першою метою було встановлення загальної втрати громадянської довіри до уряду України шляхом започаткування інформаційної кампанії спрямована на дискредитацію органів державної влади, органів внутрішніх справ України та заохочення збільшення злочинності та сепаратизму. Ця інформаційна кампанія сприяла соціально-політичній дестабілізації в країні та продовжує негативно впливати на країну.

Ця стратегія успішно інтегрувала інноваційні кібер-технології в координацію з ретельно спланованими нетрадиційними і нерегулярними силами на місцях, що призвело до анексії Криму 2014 року та військового конфлікту в Південно-Східній Україні. У відповідь на нетрадиційні та звичайні загрози безпеці, як зазначалося вище, більшість країн з можливостями швидкої реактування зосереджують свою увагу на двох основних компонентах для своїх апаратів безпеки:

- Потенціал стримування, що складається з традиційних гілок збройних сил (сухопутних військ, повітряних сил, флоту);
- Потенціал інноваційної війни. Потенціал складається з військової техніки та персоналу Сил спеціальних операцій, інформаційно-психологічних операцій та електронної війни, а також кібер-сили (кібер-розвідка, безпека та операції), галузі розвідки (електронна війна, інтелект з відкритим вихідним кодом (OSINT), технічні види розвідки, спостереження та розвідки (ISR) та ін.), оперативне управління зв'язку, військові частини, оснащені робототворими (безпілотними) літальними комплексами та контрзаходами для атаків нападів, інших високотехнологічних ресурсів та заходів.

Покоління високотехнологічної війни

Технологічний прогрес завжди був рушійною силою військової стратегії. Технологічно інтенсивні війни пов'язані з проектуванням і широким використанням передових технічних засобів, а також систем та комплексів, створених найбільш розвиненими країнами. Ці події дають деяким країнам явну перевагу під час бойових дій без необхідності масового посилення переважних конвенційних сил. Проте, більш технологічно розвинені держави можуть бути більш вразливими до певних атак.

Нові можливості для націлювання на уразливість в поєднанні з новою зброєю та військовою технікою призвели до розробки, впровадження та практичного використання в провідних країнах нових стратегічних концепцій боротьби з війнами: Глобальна війна, Глобальна видимість, Глобальне охоплення, Чиста середня війна, Гібридні війни, Стратегічні Параліч, Паралельні війни, Воєн з контролем хаосу, Необмежені війни, Контрольовані війни і т. Д. Ці розширені поняття враховують бойові наслідки для потенційних ворогів з відстані через використання інформаційної підтримки інтелекту, інформації та точного зброї, робототехнічних технологій та інших засобів. Інноваційні технології управління, на відміну від бойових дій, дозволяють проводити атаки в першу чергу проти пріоритетних цілей з максимальною швидкістю та точністю дій, що впливають на критичні компоненти, на будь-якій території держави (регіону) без необхідності фізичної присутності. Реалізація такої сильної проекції дозволяє досягти стратегічних цілей без історичних перешкод для перемоги часу, дистанції та інтенсивної матеріально-технічної бази. Поки об'єктом стратегії безпеки є дестабілізація свого противника та експлуатація слабких місць у критичних вузлах (підсистемах, компонентах, об'єктах), то немає необхідності контролювати територію силою. Швидше за все, ці вразливі місця витоків безпеки, слабкі матеріально-технічні зв'язки, прогалини в безпеці, дозволяють зривати важливі системи, необхідні для продовження або навіть ініціації боротьби. Дисфункція системи або будь-яке інше руйнівне вплив на ціль перешкоджає стану, яка не змогла вжити запобіжних заходів для використання її здатності адекватно реагувати на

подальші війни та боротьбу з війнами. По суті, державна оборонна підтримка, в умовах гібридних загроз та гібридних бойових дій, вимагає існування збалансованого та повного спектру національної безпеки та оборонного сектора. Збройні сили залишаються ключовим компонентом національної безпеки, який має реагувати на сучасні та майбутні виклики та загрози. Збройні сили повинні бути оснащені постачанням сучасної зброї та військової техніки, відповідної організації та підрозділів, укомплектованих кваліфікованим персоналом. Кваліфікований персонал повинен мати можливість проводити потужні інформаційні та спеціальні операції з метою впливу на економіку, політику, енергетичні системи, інформацію та комунікації, управління та управління, місцеве та ворожнечу.

Військові компоненти гібридної війни

Особливості військової складової високотехнологічних і гібридних воєн включають:

- Перехід від стратегічного контролю до оперативного бойового контролю, основу якого є управління в реальному часі полем бою та інформаційне перевага над діями противника: розвідка, прийняття рішень та реалізація, наслідки.
- Перехід від основних обов'язків боротьби з вогнем до кібер-та повітряно-космічної середовища.
- Військова боротьба означає збільшення, ґрунтуючись на роботизація, приховані концепції та бойові дії на відстані.
- Формування та використання ситуаційних та автоматизованих систем спостереження та протистояння комплексів та систем.
- Широке застосування ефективного нелетального зброї.
- Зростаюче використання нерегулярних міліцейських груп (воєнізованих сил).
- Пов'язане збільшення асиметричних бойових дій.
- Зростаюча роль та розширення участі спецназу.

- Зростання залежності та використання радіоелектронної, психологічної та інформаційної війни через кібер-активи.
- Перехід до пристосованої до ворога війни у всіх сферах дії.

Інформаційні та кібер-дії

Поєднання досліджень та аналізів бойових дій показує, що дії, пов'язані з кіберзлочинністю, та інформаційна війна збільшуються як за масштабами, так і для вояків. У цьому контексті гібридна війна та використання кібер-активів в рамках цього є одним з найважливіших факторів для розуміння майбутньої дуги конфлікту. Бойові дії в Іловайську та Дебальцево в Україні передували значному вибуху активності в інформаційному просторі. Негативні відомості про основні повноваження Збройних Сил України та урядових представників широко поширювалися (звичайно, вибухи негативної інформації в Інтернеті передували початку нової бойової кампанії) .

Це загальна тактика, яку Дюгган назвав кібер-агресією разом із дезінформацією з проксі-серверів та фальшивих фронтів в Інтернеті.

Взаємодія стала організовуватись не шляхом об'єднання в вирішальних пунктах роздільних груп військ, а шляхом об'єднання їх вогневих та інформаційних можливостей (Хамзатов, 2006).

Інформаційно-психологічні операції (дії) противника в кібер-просторі вимагають використання різних інтернет-ресурсів. Прикладами інформації та психологічних операцій є підготовка та розповсюдження певної інформації в соціальних мережах та інших Інтернет-ресурсах для дискредитації української влади, командування та військового персоналу АТО в рамках кампаній «Якщо не генерали», генералів-переможців України, "Приходьте до української артилерії" та ін. Дезінформація чи безконтрольність, неправдива інформація, включаючи використання спеціальних технологій просування таких повідомлень через Інтернет, часто поширюються в національному кібер-просторі як військово-патріотичні ресурси. Варто зазначити, що деякі Інтернет-ресурси розміщуються Російською Федерацією в Москві.

Аналіз контенту та моделювання онлайн-потоків новин під час найбільш інтенсивної діяльності в Дебальцево у лютому 2015 року, використовуючи технологію новин моніторингу "InfoStream", ілюструють коливання амплітуди до ступеня важливого для розповсюдження повідомлень.

Медіа-аналіз продемонстрував значні наслідки масового віку широкомасштабних негативних соціально-політичних інформаційних кампаній. По-перше, кібер-агресія проти ключових діячів уряду, як очікується, сприятиме розширенню діапазону негативних інформаційних потоків з метою посилення існуючої громадянської недовіри та антиурядової поведінки. Коли це поширюється в соціальні мережі, розповсюдження фальшивої та зловмисної інформації заохочує вірування та поведінку, які, як правило, підлягають перевірці існуючими соціальними звичаями та громадянськими очікуваннями. Навіть якщо інформація не спричиняє свідомої зміни вірувань, це може вплинути на інтерпретацію майбутньої інформації, надаючи ефективні засоби для закріплення та зачистки.³⁰

Це може допомогти вітчизняному агресору, який бажає вплинути на хід конфлікту, щоб послабити підтримку цільового уряду. У деяких випадках така інформаційна війна може замінити кінетичні операції, підриваючи оборонні кампанії, перш ніж їх навіть потрібно починати. Кібер-агресія часто приховує своїх дійових осіб та мотивів, захищених технологічними методами, які можуть замаскувати свої маніпулятивні цілі. Методи приховування включають в себе анонімні претензії до влади, новини, що маніпулюють напівправами, повторення повідомлень, інформаційна перевантаженість, кібер-псевдопередачі (уряд ставить як повстанців), державні агенти, що грають роль онлайн-коментаторів, і створення фальшивих масових рухів.

В Україні наслідки таких дій з 2014 року призвели до дискредитації Збройних Сил, невдоволення та недовіри, спрямованої на головних військових та політичних владних структурах держави, висвітлення сумнівів щодо необхідності військових дій та шкоди громадянському моральному стану та заохочення дезертирства серед військовослужбовців. В умовах відсутності

спеціальних контрзаходів проти дискредитації Збройних Сил України, невдоволення та недовіри, можна сподіватися, що в результаті послаблюватимуться державні та військові можливості, необхідні для реагування на агресію. Більше того, дії національних ЗМІ, як навмисних, так і не організованих Російською Федерацією, ускладнили вже складну ситуацію за кликами заохотити прості наративи. ЗМІ залежать від ненадійних або хибних джерел, негативно сформованих новин та критики дій владних структур Збройних Сил сприяли інформаційній кампанії противника. Російські сили змогли використати існуючі вразливі місця в соціальних, політичних та економічних системах що призвело до відкритих конфліктів, з висотою таких операцій, що збігаються з настанням кінетичних операцій на Донбасі в 2014 році. Використання кібер-активів є формою прогнозування сили, яка допомагає започаткувати кризи далеко вперед і за межами фронтів, створюючи форми більш складних криз, які зачіпають енергетичну інфраструктуру, банківські системи та політичне керівництво, а не лише збройні сили, що борються на фронтах. Знову ж таки, продовження традиційного військового конфлікту не є новою стратегією, але нові технології змогли забезпечити як засоби, так і вразливі місця, щоб дозволити такі операції в масштабах, які часто не були свідками раніше, і з меншими інвестиціями в ресурси з боку агресор.

Ефективна попередження та виявлення інформації ворога та психологічні дії в кібер-просторі та наша швидка реакція вимагають створення національних центрів контрзаходів щодо інформації та кібератак. Національні центри повинні об'єднувати та полегшити координацію між міжнародними центрами, що здійснюють контрзаходи щодо кібер-загроз. Національні центри повинні забезпечувати моніторинг та виявлення руйнівних впливів та виявлення ознак, механізмів (стратегій, тактик, методів, форм і методів) їх реалізації. Вони повинні визначати джерела та варіанти поширення небезпечного вмісту, взаємозв'язку під час операції (дій) між різними ресурсами Інтернету для визначення мети дій та можливих результатів. Заходи щодо нейтралізації руйнівної інформації та кібер-ефектів та їх джерел:

Попередження власників (якщо вони відомі) інтернет-ресурсів про обмеження щодо поширення фальшивої, неправдивої інформації з рекомендацією його видалення, якщо інформація шкодить суб'єктам та об'єктам національної безпеки (людина, суспільство, держава)

Створення публічних реєстрів для ненадійних / підозрюваних ресурсів. У тих випадках, коли неможливо визначити власника або модератора, а вміст може перетворитися на реальну загрозу для суб'єктів та об'єктів національної безпеки, рекомендується блокувати електронні інформаційні ресурси, видаляти контингент і т. Д.

Нову тактику Кремля, яку він зробив на Донбасі в період з травня по серпень 2014 р., можна сформулювати як максимізацію насильства при маскуванні фактичної присутності. Основними агентами російської експансії на Донбасі стали загони «ополченців», які склалися переважно із чудово підготовлених до війни російських громадян, і тотальна, масована пропаганда.

Головна властивість цієї пропаганди – розмивання фокусу уваги людей та ліквідація альтернативних джерел інформації. Це включає як створення безлічі однотипних каналів комунікації, так і виробництво якомога більшої кількості інформаційних вкидів. Адже якщо сто джерел в інтернет-ЗМІ та соціальних мережах тиражують одну й ту саму неправдиву інформацію, спостерігачі схильні їй повірити. Особливо у ситуації відсутності альтернативних джерел. Після захоплення обласних ЗМІ (до якого ворог був однозначно готовий, оскільки переключення мовлення в області на ретрансляцію російських каналів було здійснено місцевими фахівцями протягом кількох годин після захоплення потужностей) в області створено ідеальні умови для поширення тоталітарної пропаганди.

У такій ситуації людям марно давати офіційні спростування. Не працюють традиційні канали комунікацій, на кшталт газет та телеканалів. Рациональна розмова стає не так неефективною, як безглуздою. Проте за місяці подальшої роботи у прифронтових умовах нам вдалося виробити кілька ефективних способів протидії тоталітарній ворожій пропаганді.

Більше того, влітку 2014 р. стала очевидною тактика ворога, спрямована на провокацію бойових зіткнень з метою створення та ретрансляції «правильної» картини для російських ЗМІ. У Донецьку від місцевих жителів було важко приховати той факт, що російські пропагандисти найчастіше опинялися на місці обстрілів житлових кварталів міста раніше, ніж відбувалися ці обстріли. Начебто вони знали, що станеться тут у найближчі хвилини. Звісно, пропаганда звинувачувала у всьому українську сторону. А насправді обстріл було здійснено силами окупантів. Завдання ворожих пропагандистів у цьому випадку полягало в тому, щоб першими дати обстрілам «правильну» інтерпретацію у ЗМІ та змусити українську сторону виправдовуватися. Часто брехня російської пропаганди і зовсім не потребувала підкріплення хоч якимись фактами, як це було у випадку з горезвісним «розіп'ятим хлопчиком» у Слов'янську.

Щоб протистояти цьому, право першої інтерпретації необхідно якомога раніше надавати собі. Показовою є історія зі збитком малайзійського «Боїнга». На момент скоєння цього теракту ми не мали всієї повноти інформації про те, що трапилося, і знаходилися в Маріуполі, більш ніж 120 км від місця трагедії. Про теракт ми дізналися в результаті дзвінка голови району губернатору і спочатку не могли оцінити те, що сталося. Глава району перебував у шоковому стані та його єдиною осмисленою фразою було те, що «на нас з неба падають мертві монголи». Після додаткового підтвердження інформації про збиття цивільного борту перед офісом губернатора постало завдання інформування громадян про катастрофу.

В умовах відсутності повної картини на той момент, потрібно було дати людям прості факти для розуміння ситуації. Отже, стався теракт, внаслідок якого загинули пасажери цивільного повітряного судна, це сталося на території, яка не підконтрольна українській владі, відповідальність за трагедію несе Російська Федерація та її ручні поплічники, які ведуть терористичну діяльність біля Донбасу, на місце трагедії мали б бути негайно допущені представники українського МНС та представники міжнародних організацій та

дипломатичних місій. Така заява від української влади була підхоплена всіма національними та міжнародними ЗМІ, що зробило подальші спроби терористів виправити інформаційну ситуацію безглуздими.

Одна з найстійкіших ліній критики української влади полягає у хронічному програші Росії в інформаційній війні. При цьому як у критиків, так і у симпатиків влади немає єдиної думки про те, як цей «програш» подолати. Ми повинні усвідомлювати, що терористи не можуть діяти самі по собі, їм потрібна певна підтримка місцевого населення, оскільки це закладено у природу будь-якого соціального конфлікту (Требін, 2014, с. 118).

Цілком очевидно, що Україна не може тягатись ресурсами з машиною кремлівської пропаганди. Більше того, одними лише комунікаційними інструментами неможливо досягти деокупації окупованих територій.

Очевидно і те, що інформаційна політика нашої країни не може базуватися на механічному спростуванні основних тез цієї пропаганди, тому що таким чином ми стаємо провідним суб'єктом і витрачаємо таку необхідну нам моральну перевагу.

Владі Росії здається сьогодні, що вони винайшли нову зброю масової поразки і можуть впливати через неї на результат виборів та формування політичних повісток в інших країнах світу. При цьому ігнорується один із базових законів фізики, згідно з яким будь-яка дія дорівнює протидії. Чим більше Росія задіює для дискредитації своїх супротивників інтернет, тим більший імунітет виробляється в аудиторії до різноманітних «фейкових новин», «альтернативних фактів» та «правди, яку від вас роками приховували». Цей імунітет виявлятиметься не тільки в технічних рішеннях, що дозволяє виявляти та локалізувати хвилі дезінформації, а й у втраті довіри до Росії з боку світової спільноти. І в цьому є колосальна перевага для України.

Завершення створення у Києві меморіалу Небесної сотні, створення національного Пантеону, ретельна документальна фіксація фактів окупації, впровадження в освітні стандарти інформації про російську агресію — це не військові, але не менш важливі способи протистояння гібридній тактиці

противника. Можна скільки завгодно наплодити сайтів, телеканалів, написати книг та зняти фільмів. Все це буде незначним у порівнянні з історичною пам'яттю та сімейним болем кількох десятків мільйонів людей. Тому що подолати цю пам'ять неможливо.

Ну і, зрозуміло, держава у своїх комунікаціях має перейти від слів до діла. «Дії, що говорять» повинні лягти в основу будь-якої державної політики. У цій моделі розмова про результати та досягнення передую розмові про наміри. Це надзвичайно складне завдання для політичного класу, що звикли до легких перемог на виборах виключно силою слів і примітивних маніпуляцій (характерним прикладом, до речі, є обіцянка одного з кандидатів у Президенти, дана їм у тому ж травні 2014-го, припинити війну з ядерною державою-агресором). Проте війна змусила нас подорослішати.

Кризові ситуації

Кризові ситуації з'являються як зовнішні сили (агресія та / або природні), які експлуатують вразливі місця та пригнічують критичні системи в цільовому регіоні чи силі. Ці кризи можуть виникнути внаслідок інформаційних та кібердіянь в умовах гібридного конфлікту, як реалізація інформаційних, психологічних та кібер-загроз (наприклад, тероризм, економічна, військова, дипломатична, політична тощо), спрямована проти критичних інфраструктур державні чи військові сили.

Ця втрата або інтенсивна деградація працездатності може бути реалізована як нелінійна функція, що означає, що впливи можуть не виявлятися до повного збою цільової системи. Ефективні контрзаходи до кризових ситуацій в кібер-просторі за даними АТО (операція на окупованих територіях України) досвід можна реалізувати в:

- Систематичне розроблення форм, методів та засобів оперативного виявлення, захисту та активних контрзаходів до інформаційних загроз у кібер-просторі
- Наукове дослідження та розробка спеціалізованого програмно-апаратного забезпечення інформаційної діяльності в кібер-просторі

- Професійна військова освіта та навчання, що базується на бойовому досвіді та уроках, отриманих у цій сфері
- Проведення прикладних національних та міжнародних тренувань, військових ігор та консультацій
- Підвищення рівня підготовки та навчання військових та цивільних фахівців у сфері інформаційної та кібербезпеки
- Оперативне впровадження уроків, накопичених у національних та міжнародних системах безпеки.

Досвід показує, що ефективне використання методів гібридної війни призводить до значного непередбачуваного характеру кризових явищ та їх реагування. Це незвично для практикуючих гібридних військових, щоб вони мали чітко визначені результати та шляхи подій, так що ті, хто реагує на такі стратегії, повинні мати можливість адаптуватися в динамічному та швидко зміненому середовищі.

Технологічний дизайн відомих систем контрзаходів у кризових ситуаціях, формах, методах та використанні систем повинен бути орієнтований на формування статичної надмірної структури цільової системи. Розподіл завдань між усіма компонентами кібератак в системі часто буває рівним, з вибором компонентів лише за їхньою метою. Збільшення кількості та щільності потоків кризових ситуацій призводить до структурної складності систем, розроблених для їх реагування. Цей дизайн розподілу забезпечує інформаційну надмірність даних та ускладнення при її передачі та обробці. Ті самі принципи є основою для розробки програмного забезпечення, призначеного для реалізації процесів оперативного виявлення, захисту та активних контрзаходів до інформаційних загроз у кібер-просторі. Зазначені підходи є неефективними в реальних умовах конфлікту, коли ворог застосовує рівні або переважаючі джерела інформаційної війни, а потім м'які сили та кінетичні сили для досягнення своїх цілей. Цей підхід є ключовою особливістю сучасних гібридних війн.

Ретельна реалізація принципів ситуаційного контролю забезпечує можливість для раціонального розподілу та перерозподілу власних ресурсів та

концентрації сильних сторін на критичних (для забезпечення безпеки) напрямках дій противника. Методи фрактального аналізу, самоорганізації та біфуркаційні моделі дають можливість виявляти загрози та критичні ситуації в часі, передбачати напрямки їх розвитку та реальні цілі.

Практично цей підхід підвищує ефективність контрзаходів щодо інформаційної війни в результаті систем попередження попередження, повноти та точності інформації та своєчасності реакцій.

Гібридні воєнні сфери

Важливим моментом є вплив дій агресора, який бажає посилити внутрішню нестабільність у багатьох сферах. Передбачувані наслідки можуть включати посилення недовіри в установах та спільних цінностях, ерозії економічної активності та довіри, а також плутанину об'єктивності, досвіду, ідеології та інших джерел соціальної єдності.

Гібридні війни суттєво відрізняються від традиційних воєн як при їх ініціюванні, так і при переслідуванні, використовуючи різні стратегії та засоби експлуатації. Гібридна війна ділиться з нерегулярними конфліктами (або IW - Irregular Warfare) з використанням нерегулярних чи невійськових сил або принаймні тих сил, які приховують свою національну відданість на користь анонімності або фальшивого камуфляжу як місцевої міліції. Спеціальні сили, саботаж-розвідувальні групи, підрозділи розвідки різних ароматів беруть участь у сприянні та проведенні операцій³⁵.

Для деяких збройних сил або сил державної безпеки спеціальні операції можуть включати в себе проведення специфічної інформації або діяльності, пов'язаної з кіберзлочинністю, електронних операцій або саботажних дій, спрямованих на знищення критичних вузлів, які інакше не можуть бути досягнуті за допомогою традиційних засобів. Тому розробка ефективних систем контрзаходів є високим пріоритетом державної оборони в сучасних умовах. Такі системи повинні включати в себе технологічно розширені види інтелекту, електронну розвідку, інформаційні та психологічні операції, а також кібер-операції, котрі можна узгоджувати для досягнення спільної стратегії, а

також можливість працювати як в залежності, так і в рамках інших операцій. Ключовим компонентом такої незалежної працездатності як в ISR, так і в бойових операціях є розробка та використання безпілотних літаків. Зростаюче використання безпілотників для різних функціональних областей (розвідка, електронна контрзаходи, прямі страйки тощо) та різні операційні середовища (земля, море, повітря, амфібія) є важливим приводом для гнучкості в динамічних конфліктних ситуаціях.

Розгортання передових розвідувальних та реагування сил має розвиватися паралельно з належним навчанням для військового та цивільного персоналу, які повинні працювати в рамках системи. Неможливо очікувати, що технології працюватимуть належним чином без висококваліфікованого персоналу, який зможе використовувати, підтримувати та розвивати складні системи, необхідні для вирішення змінних характеру поля бою. Повні, ефективні можливості можна очікувати лише тоді, коли стратегії та технології розробляються в координації з професійною підготовкою. Непрофесійне використання таких технологій нерідко є причиною їх низької продуктивності, оскільки стандартні операційні процедури в навчанні стосуються значно старших концепцій проблеми (наприклад, втручання в інформаційні мережі як технічна проблема, а не загроза національній безпеці).

Держава несе головну відповідальність за управління кар'єрою військових та підготовку персоналу оборони. Діяльність такої системи має бути забезпечена відповідною законодавчою, організаційною, фінансовою, методологічною та матеріально-технічною підтримкою з боку держави (Горбулін, 2009). Тому країни повинні зосередити увагу на створенні та розвитку систем технічного захисту, з комплексними дослідженнями та експериментами для забезпечення належного рівня оборонної підтримки. Розширюючи сферу охоплення за раннього попередження, доступного в центрах "гібридної загрози", як це встановлено в деяких країнах НАТО, ці кластери призначені для розробки відповідних технологій та стратегій для майбутніх загроз, які вони зможуть визначити.

Тому потрібно забезпечити надійну систему військових досліджень з належною науково-організаційної структурою, академічну орієнтацію на знання в області передових технологій, науково обґрунтований виробничий комплекс, що містить стаціонарні та мобільні зразки зброї та військової техніки, командні пункти та лабораторії, технологічно розвинені експериментальні бойові та бойові одиниці, розроблені відповідно до академічних та наукових досліджень.

Практичне навчання військовослужбовців, в тому числі вивчення інформаційних технологій, тестування та впровадження нових технологічних систем озброєння та військової техніки та формування нових підрозділів повинні базуватися на розробках оборонного технологічного кластеру та активних військових частин. Що стосується України, то необхідно створити Центр військово-технічного експертизи у передових технологічних сферах з метою:

- уникнути подвійного функціонування різних організацій
- концентрація в одному місці зусиль у галузі досліджень, проектування, створення, тестування та використання передових технологічних систем
- навчання персоналу в областях передових технологій для всіх галузей Збройних Сил та інших міністерств та відомств державного сектору національної безпеки та оборони
- використання військової складової, промислової та виробничої бази регіону
- уникаючи додаткових фінансових та тимчасових витрат.

Працездатність центру може бути обґрунтована та підтримана, спираючись на досвід провідних країн світу, зібраних у пошуках інноваційних ідей та їх реалізації у військовій сфері, наприклад DARPA (агентство передових дослідницьких проектів оборони США). Рациональна розробка всіх практичних питань в класі передових оборонних технологій повинна проводитися в тісній координації з центральними військовими командуваннями та контролюючими

організаціями. Він має працювати безпосередньо з силами, що співпрацюють з центральними контролюючими органами. Органи центрального контролю відповідають з військовими підрозділами та підрозділами з їх діапазоном бази та взаємодіючими організаціями / структурами.

Державна політика передових технологічних, інформаційних та кібербезпечних систем підтримки та захисту стали одними з найважливіших компонентів, які слід розглянути щодо політики національної безпеки у військовій сфері. Сучасні технології зміщують здатність впливати на сили противника, створюючи потребу в реорганізації, щоб керувати і захищати як від м'якого, гібридного так і від прямого збройного військового впливу, включаючи, зокрема, підготовку кадрів для підтримки готовності та безперервності сил. Досвід різних країн, які вже стали свідками нових форм гібридної війни, доводять, що рівень національної безпеки та оборони має зберігатися навіть у умовах світової економічної кризи та значно скоротити витрати на збройні сили. Розширення поля бою за межами кінетичних операцій та інфраструктурних атак вимагає комплексного використання як традиційних силових доктрин, так і нового технологічного та синергетичного планування. Практика військових конфліктів протягом останнього десятиліття демонструє, що стратегічна перевага надається акторові, який вперше розуміє та впроваджує нові технології, які можуть використовувати їх як мультиплікацію сил, а отже, подолати чудові звичайні сили і часто, навіть не провокуючи стійких відповідей. Генерали повинні використовувати нові методи, якщо тільки не забути нові методи та вчення, які ворог може розгорнути. Використання передових технологічних систем дає можливість підвищити ефективність вже існуючого державного військового потенціалу з меншими витратами, навіть на третину традиційних бюджетів. Беручи до уваги концепції національної безпеки та національних військових стратегій, уряди найбільш розвинених країн надають пріоритет освітній та науковій базі для технологічно інтенсивних засобів ведення бойових дій, впровадження інноваційних технологій управління, захисту від кібер та інформаційних атак, а також

забезпечення швидкої і переконливої перемоги в нинішніх і майбутніх військових конфліктах.

РОЗДІЛ III. СВІТОВИЙ ДОСВІД ВЕДЕННЯ І ШЛЯХІВ ВИРІШЕННЯ ГІБРИДНИХ КОНФЛІКТІВ

3.1. Світовий досвід ведення гібридних конфліктів

Один із підходів до гібридної війни ґрунтується на історичній перспективі. У цьому випадку термін гібридна війна визначається як просто паралельне використання конвенційних і нерегулярних сил в одній і тій же військовій кампанії. Військовий історик Петер Р. Мансоор, наприклад, визначає гібридну війну як «конфлікт, що передбачає поєднання конвенційних військових сил і нерегулярних сил (партизан, повстанців та терористів), які можуть бути державними чи недержавними акторами, які діють заради досягнення загальної політичної мети». З цієї точки зору, гібридна війна, очевидно, не є чимось новим. Є безліч прикладів гібридної техніки та гібридного підходу на тактичному, оперативному та стратегічному рівні, що йдуть далеко в минуле до часів Пелопонеської війни та робіт китайського філософа Сунь Цзи, який жив у п'ятому столітті до нашої ери.

Перший відомий прояв гібридної війни мав місце у V столітті до нашої ери, під час Пелопоннеської війни між Афінами та Спартою. Крім фронтального (традиційно військового) протистояння, Афіни тоді будь-якими шляхами підбурювали до повстання підлеглих спартанцям ілотів. У такий спосіб було застосовано один із найбільш суттєвих елементів гібридної війни – створення внутрішнього військового джерела напруження. Така тактика, врешті-решт, значною мірою сприяла перемозі афінян. Спарта змогла з честю витримати традиційні битви з військами Афін, але виявилася абсолютно безпорадною перед нищівною тактикою гібридної війни. Постав ризик втрати ілотів і розхитування ними ситуації всередині країни, – до цього не був готовий ані політикум спартанців, ані регулярна армія. Саме цей елемент тактики гібридної війни (чи боротьби) згодом можемо найбільш наявно простежити впродовж подальшого розвитку людства (2016, ст.75).

Щось подібне можна побачити у діях Ганібала, коли він організував військовий похід з Іспанії до Риму. Під час походу, перебуваючи на ворожій території, він не воював з місцевими племенами, а вів переговори. Під час перемовин часто племена як мінімум пропускали армію Ганібала без сутичок, а як максимум воїни цих племен вступали в армію Ганібала. Це, з одного боку посилювало військо Ганібала, без якихось затрат та втрат, з іншого це послаблювало позиції Риму. Сам похід, організований таким чином, що римляни готувались зустріти Ганібала з моря, а він перейшов через Альпи. Це теж є елементом гібридних дій під час військового конфлікту. Ну і не треба забувати, що Ганібал теж використовував найманців, нерегулярні бойові загони, що додавало гібридності, нелінійності у військові дії того часу.

Нерегулярні бійці довели, що можуть стати серйозним противником для численних регулярних збройних сил. Такі величезні армії, як Велика армія Наполеона і Вермахт Гітлера, важко боролися з нерегулярними бійцями, які розуміли та використовували місцевий людський потенціал та географічний ландшафт, і постійно нападали на вразливі бази постачання, склади та лінії комунікацій. Згодом партизанські операції починали істотно впливати на ширші конвенційні військові кампанії, частиною яких вони були. Антиповстанські кампанії в Іраку та Афганістані вкотре показали, наскільки важко перемогти переконаних нерегулярних бійців без порушення людських прав місцевого населення, тим самим підриваючи внутрішню та міжнародну громадську підтримку цієї кампанії.

Сама ідея у тому, що війна, це не прямі бойові дії, не нова. Вона висловлювалася ще у китайському трактаті Сунь-Цзи «Мистецтво війни», написаному ще у VI столітті до н. е. У ньому міститься таке: «Війна — це шлях обману. Найкраща війна — розбити задуми супротивника. На наступному місці — розбити його союзи. Потім розбити його війська. І найгірше — облягати міста». Тобто можна вважати, що етапи та компоненти «гібридних» дій були описані ще у VI столітті до нашої ери. Тим часом, аналіз існуючих визначень «гібридних воєн» та поглядів фахівців на їхню структуру показує, що основна

їх складова, це приховане залучення сторонніх збройних угруповань та організацій для вирішення завдань міждержавного протистояння при супроводі збройних дій всебічні маневри, що відволікають супротивника. Огляд історії військового мистецтва показує, що подібний принцип використовується досить давно: від грецьких найманих армій, описаних в «Анабасісі» Ксенофонта до ірландських найманців XVII століття. Широке поширення найманства в той історичний період пов'язане з економічними причинами: утримувати постійну готову до війни армію було дорого, дешевше було найняти професіоналів на вирішення конкретних військових завдань. Але це були ще навіть не зачатки «гібридних» форм дій, а лише економічніший спосіб ведення війни. Лише із встановленням перших, ще не надто формалізованих систем міждержавних відносин, дії найманих військових формувань довелося якимось чином приховувати. Принаймні у Європі. Хоча поза межами «цивілізованого світу», найм воїнів, як і раніше, вважався нормою. На тривалому історичному періоді можна простежити використання й інформаційної складової «гібридних» дій. Класичний приклад – формування англійцями негативного образу Росії часів Івана IV Грозного. Згодом подібні дії ставали дедалі ширшими і різноманітнішими: від видання книги «Записки про Московію» Сигізмунда Герберштейна, «методички» про Росію для наполеонівської армії, до агітаційних листівок часів Першої світової війни. Це все елементи гібридної війни через інформаційний вплив, пропагандистський. До речі, наполеонівські «методички» та агітаційні листівки послужили прототипом такої складової інформаційної компоненти сучасної «гібридної війни» як її медійний супровід. У формі, наближеній до сучасної, цей процес вперше запустила Великобританія, порушивши 1915 року негласну заборону публікацію фотографій убитих солдатів противника. У роки війни у В'єтнамі, з появою телебачення, війна буквально «зробила крок з екранів у кожен дім». Сьогодні, в епоху загальної інформатизації, війна ведеться майже в прямому ефірі. І для «гібридних» дій дуже важливо, хто формуватиме картинку цього ефіру.

З настанням постіндустріальної епохи інформаційне протистояння доповнилося діями в кіберпросторі та застосуванням деструктивних соціально-політичних технологій. Останні зараз використовуються настільки інтенсивно, що їх можна назвати ще однією складовою «гібридної війни». Більше того, їхня різноманітність навіть дозволяє проводити внутрішню класифікацію таких дій: від простої фінансової та інформаційної підтримки опозиційних течій та створення всередині держави-противника «п'ятої колони», до впровадження агентів впливу, які забезпечують так звану «м'яку окупацію» (soft occupation) країни та перехід країни під зовнішнє керування. Методи, що використовуються розрізняють за інтенсивністю та ступенем таємності, що застосовуються залежно від супротивника, проти якого вони використовуються. Історично це дуже помітно: від прихованого використання Німеччиною внутрішніх революційних сил Росії у роки Першої світової війни до майже відкритого застосування таких технологій проти Венесуели у 2019 році. Типовими прикладами сучасного використання таких технологій є організація «кольорових» революцій через діяльність різних некомерційних організацій. Практика показує, що такі дії не тільки ефективніші, а й суттєво дешевші за пряме військове втручання. Наприклад, на підтримку керованого військового режиму у Венесуелі в 60-70-х роках минулого століття США витрачали близько 200 мільйонів доларів щорічно. У XXI столітті спроба встановити у цій країні свій уряд коштувала США близько 10-15 мільйонів на рік, що витрачаються на фінансування політичної опозиції. Але річ навіть не в економії коштів: для протидії багатьом країнам пряме військове протистояння просто небезпечне, а «розхитування» їхньої державної системи через «насадження демократії» відносно безпечне. Зараз, в епоху глобалізації та інформаційної революції, активність інформаційного протистояння та застосування деструктивних соціально-політичних технологій стала настільки великою, що фахівці заговорили про настання так званої доби «постправди». Одним із аспектів практичного застосування інформаційного протистояння можна вважати використання як обґрунтування «гібридних» дій національного

питання. З давніх-давен чинник національного складу територій міг бути приводом їх анексії сусідніми державами, як це сталося в 1938 році з Судетською та Тешинською областями Чехословаччини, зайнятими під приводом захисту співвітчизників Німеччини і Польщею відповідно. Інший варіант «гібридних» дій – відокремлення етнічно відмінних регіонів та створення на їх основі окремих держав під зовнішнім протекторатом, як це сталося із Косово.

У новітній історії, зі зростанням мобільності населення, подібні «передгібридні» дії можуть реалізовуватися шляхом присвоєння громадянства чужої держави, легітимізації громадян шляхом купівлі землі чи нерухомості а також міграції. Все це посилює небезпеку і може вважатися одним із елементів, що передуює «гібридній війні» і наближає її. Найважливіший аспект «гібридних» воєн – їхня економічна складова. В історичній ретроспективі її використання почалося з переходом від натурального господарства та відокремлених національних економік до світової системи господарювання, пов'язаної з міждержавним поділом праці та міжнародною торгівлею. Історія показує велику кількість методів, що використовуються в рамках цієї складової протистояння. Франція під час наполеонівських воєн підробляла англійські, австрійські та російські гроші. В даний час, з настанням епохи глобалізації, фінансова складова «гібридних воєн» істотно посилилася. Як за масштабами застосування, так і різноманітністю використовуваних методів. Останні змінюються від прямого блокування фінансових рахунків окремих осіб і навіть урядів держав-противників до непрямих методів на основі заборон. Прикладом першого типу дій можуть бути блокування зарубіжних рахунків Іраку у 2012 році та Венесуели у 2019. Непрямі методи явно проглядаються у заборонах на проходження коштів через «треті країни» та компанії або блокування доступу іранських банків до системи SWIFT у 2018 році. Як один із перших прикладів економічної війни можна навести «континентальну блокаду»: комплекс заходів щодо блокування торгівлі Великобританії, які проводилися Францією в 1806-1814 роках. У період XIX-XX століть найбільш поширеним видом економічної

війни була саме морська блокада. До початку Першої світової війни блокаді піддавалися: Туреччина, Португалія, Нідерланди, Колумбія, Панама, Мексика, Аргентина та Сальвадор. Ініціаторами блокад були: Великобританія (12 разів), Франція (11 разів), Італія, Німеччина (3 рази), Австрія та Росія (2 рази) та Чилі. Після Другої світової війни економічні санкції залишалися активним інструментом міжнародної політики. У період із 1971 року можна назвати близько 120 випадків санкцій, насамперед у межах економічної війни Заходу проти СРСР. Зазначений інструмент використовується і в XXI столітті: від загороджувальних мит до американських законів «Про контроль над експортом», яким у 1949 році було створено Координаційний комітет з експортного контролю та «Про протидію противникам Америки за допомогою санкцій» (Countering America's Adversaries Through Sanctions Act, CAATSA) 2017 року. Цей тип санкцій фахівцями іноді виділяється на окрему форму дій – технологічне протиборство. Ще одна складова економічного протиборства, що лежить на межі гуманітарно-допустимого, це ресурсна складова. Її різновиди застосовувалися з давніх-давен, у формі блокування фортець при облозі, перекриття доступу провіанту і води. В даний час, зі зростанням технічних можливостей та різноманітності економічних зв'язків у сучасному світі, з'являються нові форми ресурсного протистояння у формі транспортної, енергетичної і навіть водної блокади, що своїми масштабами призводять до екоциду цілих територій. Типові приклади таких дій – спроба відвести води річки Йордан від Ізраїлю, що стала однією з причин «шестиденної війни» 1967 року або енергетична та водна блокада Криму, розпочата в 2014 році, кібердиверсії здійснені для руйнування електроенергетики Венесуели в 2019 році.

Дуже близьким до ресурсного протистояння за характеристиками вважатимуться потенційне застосування кліматичної зброї. Підтверджених відомостей про його наявність немає, є лише припущення про його розробку деякими країнами. Але, у разі появи такої зброї, вона стане ідеальним засобом ведення «гібридного» протистояння. Аналізуючи історію, можна дійти невтішного висновку, що сучасні «гібридні війни» не «ноу-хау», а лише

продовження раніше використовуваних різних форм міждержавного протистояння, які відрізняються комплексним використанням різних форм військового та невійськового протистояння, суттєво могутнішими технічними можливостями щодо реалізації тих чи інших форм агресивних дій та зовсім іншими масштабами, що визначаються глобалізацією сучасного світу.

У сучасній історії найбільш раннім з класичних прикладів «гібридних» дій, що реалізує всі компоненти їх складу, може служити громадянська війна в Іспанії 1936 - 1939 року. Аналіз цього конфлікту з погляду сучасної термінології показує, що в ньому велось типове «гібридне» протистояння між фашизмом, в особі Італії та Німеччини, за підтримки Португалії та комунізмом в особі СРСР. Боротьба не просто чужими руками, а й біля чужої країни, за дотримання угоди про «невтручання», підписаним іншими європейськими державами. При цьому аналіз структури «гібридних» дій, що проходили в період новітньої історії, показує, що, незважаючи на зміщення акцентів у бік несилових дій, військова компонента, як і раніше, залишається основною в їх структурі.

Втім, поступово відбуваються зміни у самій структурі конфліктів, а й у силовий компоненті. Щодо останньої, зміни визначаються тим, що хоч із вісімдесятих років минулого століття наймання офіційно заборонено документами ООН, але до теперішнього часу можна відзначити численні факти використання найманців, вже у формі приватних військових компаній (ПВК). Появі приватних структур багато в чому сприяла зміна законодавства окремих країн, згідно з яким з'явилася можливість використання приватних сил для забезпечення безпеки недержавних компаній, а згодом і для вирішення політичних завдань, а також відкрито агресивна та терористична політика таких країн як РФ, які на державному рівні створили приватні військові компанії (ПВК «Вагнер»). Одна з перших подібних компаній виникла у 1967 році у Великій Британії. На початку 1990-х років південноафриканська Executive Outcomes і британська Sandline практично повністю захопили ринок приватних охоронних і військових послуг. Обидві компанії відіграли істотну роль у

військових конфліктах на африканському континенті, зокрема, в Анголі та Сьєрра-Леоні. Пізніше, аж до теперішнього часу приватні військові компанії широко використовувалися США для встановлення лояльних режимів у Латинській Америці, під час воєн в Іраку та Афганістані. Сучасні приватні військові компанії – це дещо складніше явище, ніж просте найманство, хоча насправді й у структурі «гібридних війн» ПВК виконують саме силову лінію конфлікту. Втім використання ПВК є не єдиним прикладом силових дій «гібридного» характеру в наш час. Не менш типовим, хоч і досить екзотичним, прикладом є створення та озброєння бойових формувань усередині країни-противника з її громадян. Знову ж таки повертаємось до підтримки РФ бандитів на Сході України. Ще одна зміна у силовій компоненті «гібридних» воєн зумовлена появою концепції дистанційних бойових дій (Remote Warfare). Ця концепція, будучи логічним продовженням тенденції, що історично склалася на заході, вести конфлікти віддалено і чужими силами, що реалізується в нових технологічних умовах, визначає ведення операцій на віддалених територіях з використанням переважно безпілотних літальних апаратів. У деяких випадках - неофіційно, без розкриття приналежності розвідувально-ударних засобів, що ідеально вписується в принципи «гібридних» дій. Є всі підстави вважати, що в міру роботизації поля бою ця тенденція лише посилюватиметься. І, разом зі зростаючими можливостями кібер-нападу, що вирішує завдання пошкодження інфраструктурних об'єктів на будь-якій відстані та без явного фізичного впливу, концепція Remote Warfare істотно змінить силову складову «гібридних» дій, знизивши поріг рішення на застосування сили. Всі ці приклади підтверджують, що, незважаючи на існуючу тенденцію «гуманізації» міждержавних конфліктів, військова складова, як і раніше, залишається визначальною в їх структурі. У той самий час годі забувати, що у структурі «гібридних війн», крім силової, існують інформаційна, політична та економічна складові. І, як показує аналіз історичної ретроспективи, співвідношення між компонентами поступово змінюється на користь несилових, хоча від використання останніх поки що повністю відмовитися не вдасться.

У 2000-х роках використання терміну «гібридна війна» стало звичайним способом опису сучасної війни, зокрема, і через витонченість і смертоносність недержавних акторів, що використовують насильство, і зростаючий потенціал кібер-війни. Хоча не було спільної згоди, що це обов'язково є новою формою війни, у визначеннях гібридної війни підкреслювалося злиття конвенційних та нерегулярних підходів у всьому спектрі конфліктів. Наприклад, у 2007 році Френк Г. Хоффман, провідний коментатор цієї концепції, дефінував гібридну війну як загрози, які включають повний спектр різних способів ведення військових дій, у тому числі використання конвенційних здібностей, використання тактики нерегулярних сил, терористичні дії із застосуванням недискримінуючого насильства, а також заворушення, ініційовані злочинними елементами, що застосовуються обома сторонами та різними недержавними гравцями. Під час війни з Грузією у 2008 році Росія, наприклад, використала поєднання регулярних збройних сил, південноосетинських та абхазьких міліцій та російських сил особливого призначення, які діють під прикриттям способу «місцевої оборони». Вважається, що такі гібридні війни відрізняє від їх форм у минулому комбінування конвенційних та нерегулярних методів війни. У минулому конвенційні та нерегулярні операції проводилися паралельно, але окремо один від одного, а не інтегрованим чином, як зараз. З іншого боку, операції, проведені нерегулярними бійцями, зазвичай були допоміжними для кампаній конвенційних збройних сил.

До 2014 року найбільш часто наведеним прикладом військових дій, що відповідають сучасним дефініціям гібридної війни, був конфлікт між Ізраїлем та рухом «Хезболла». «Хезболла», яка отримує підготовку та обладнання від Ірану, стала несподіванкою для Ізраїлю витонченим поєднанням партизанської та конвенційної військової тактики та використанням озброєння та комунікаційних систем, що асоціюються із збройними силами розвинутих країн. На стратегічному рівні «Хезболла» ефективно використовує Інтернет та інші медіа для інформації та пропаганди. Її інформаційний менеджмент із самого початку конфлікту виявився набагато успішнішим у впливі на світову

думку, ніж менеджмент Ізраїлю. Як показує наведена вище дискусія, гібридне поєднання конвенційних та нерегулярних методів війни застосовувалося протягом усієї людської історії. Але приклад «Хезболла» та інші приклади, у тому числі партизани в Чечні та останнім часом Ісламська держава (ІД), демонструє, що сучасні системи зброї суттєво підвищили смертоносність недержавних акторів. Розвиток інформаційних технологій також дав цим групам безпрецедентну можливість брати участь в інформаційній війні та ефективно конкурувати з державою при формуванні громадської думки.

Багато з методів, які Росія застосувала в Україні, сягають радянської доби та використання маскування, або військової дезінформації. Вони були ефективно використані радянськими силами під час Другої світової війни та у проксі конфліктах під час Холодної війни. Наприклад, маскування використовувалася у широкому масштабі під час операції «Багратіон» 1944 року, коли було знищено цілу групу армій Німеччини. На іншому кінці спектру конфліктів техніка маскування була застосована у Східній Європі, коли радянські війська міністерства внутрішніх справ (НКВС) використовували потайливі засоби для захоплення державних інституцій, підризу громадянського суспільства та придушення всієї опозиції для нав'язування комуністичної влади. У двадцять першому столітті прогрес інформаційних технологій суттєво розширив охоплення маскування, дозволяючи російському керівництву використовувати мультимедійну пропаганду та дезінформацію у широкому масштабі. Ці методи застосовувалися для забезпечення підтримки зовнішньої політики держави всередині самої Росії та ведення широкої «інформаційної війни» проти України та Заходу. Зараз НАТО Френч визначає маскування як війну, яка перебуває на межі війни, цілеспрямовану стратегію помилки, в якій поєднуються використання сили з дезінформацією та дестабілізацією для створення невизначеності в умах керівників Альянсу щодо того, як слід реагувати.

Ключовим елементом маскування є концепція «рефлексивного контролю» (менеджменту сприйняття). Ця концепція перегукується з роботою

колишнього радянського психолога Володимира Лефевра, який розробив цю теорію, коли вивчав способи надання впливу управління процесом прийняття рішень противником. Цю теорію можна описати як використання спеціально підготовленої інформації, яка схиляє опонента до добровільного ухвалення рішення, яке попередньо було визначено як бажане ініціатором цієї інформації. До методів входять шантаж, камуфляж, помилка і дезінформація, створені задля втручання у процес прийняття рішень опонента, що призвело б до сприятливої для Росії політики.

На практиці здійснення війни нового покоління піднімає суттєві проблеми. Для досягнення кінцевих військових та політичних цілей доводиться координувати, інтегрувати та контролювати широкий спектр учасників – цивільних та військових, регулярних та нерегулярних, а також їх дії. Особливо важким є єдине політичне управління, оскільки нерегулярні та державні актори часто мають різні політичні інтереси. Навіть для такої авторитарної країни як Росія, управління та координація виявилися важкими під час операцій в Україні, які, схоже, скоординовані набагато меншою мірою, ніж думали західні коментатори в той час. Наприклад, в одному аналізі Центру імені Вільсона робиться висновок, що російські дії в Україні не були частиною добре скоординованої головної стратегії, а швидше відбивали «неплановану послідовність спроб підбирати різні інструменти для різних – часто несподіваних – оперативних реалій».

Росія давно проводить політику ослаблення, поділу і, зрештою, нейтралізації НАТО. Балтійські держави дають Путіну потенційний важіль для досягнення цієї мети. Цілком також, як російське втручання у справи України почалося задовго до анексії Криму, постійно збільшується політичний та соціальний тиск на Балтійські держави. Деякі європейські розвідувальні агентства як і висловили побоювання щодо Болгарії, на яку вважається, що політична система компрометована кримінальними організаціями, пов'язані з російським державою через російські розвідувальні агентства. Стратегія НАТО для боротьби з російською гібридною загрозою вимагає поєднання

дипломатичних, військових, інформаційних, економічних та правоохоронних заходів. Причому такий комплексний підхід має бути відповідно інтегрованим, а не просто залучати до участі цивільні відомства для підтримки збройних сил або для заміни збройних сил цивільними структурами через небажання застосовувати силу.

У разі кризи за участю балтійських держав Росія, ймовірно, спробує розділити членів НАТО, залишаючись нижче за очевидний поріг Статті 5, принаймні на початку. Як і в агресії проти України 2014 року, дезінформація, залякування та пропаганда будуть використовуватися для схилення менш стійких членів НАТО до російської точки зору на події, що відповідно зміцнить їхній настрій, щоб уникнути воєнної реакції. Дезінформація буде використовуватися проти керівництв НАТО і широкої громадської думки для виведення Альянсу з політичної та військової рівноваги. Залякування, ймовірно, полягатиме у наголошенні на очевидній готовності Росії використовувати ядерну зброю для деескалації «агресії» НАТО. Ефективна стратегічна комунікація могла б протистояти російським дискурсам, але вона має бути більш чуйною та послідовною. Хоча ЄС приймав план дій зі стратегічної комунікації на 2015 рік, однак немає жодних ознак, що процес планування в ЄС включає координацію з НАТО у вимірі дієвих дій а не просто декларацій. Така координація була б життєво важливою для ефективної реакції на російську дезінформаційну та пропагандистську кампанію. На жаль, у цьому плані авторитарні суспільства мають перевагу, оскільки їм легше мобілізувати всі ресурси держави для досягнення політичних цілей, не зважаючи на обмеження, що накладаються децентралізованим розподілом влади та демократичним процесом формування консенсусу. Ліберальні демократії, навпаки, спостерігають неприязнь до пропаганди та психологічної війни, тому НАТО буде важко узгодити зміст і способи ведення стратегічної комунікаційної кампанії. Як стверджують дослідники гібридних конфліктів, РФ має потенційну асиметричну перевагу над Заходом, оскільки вільні ЗМІ Заходу

неспроможні змагатися з централізованими і синхронізованими російськими інформаційними пропагандистськими операціями.

Проте НАТО може виявитися не настільки вразливим щодо інформаційної війни, як багато хто зараз вважає. Пропаганда може мати особливо сильний вплив, коли у населення, як в РФ, немає альтернативних джерел інформації, але скрізь в інших місцях пропаганда має бути достатньо правдоподібною, щоб формувати переконання та почуття та щоб використовувати невпевненість, недовіру та параною. Заяви російського керівництва та російські медіа джерела стають дедалі дискредитованішими на Заході, особливо після їхньої реакції на те, як було збито літак, який виконував політ МН 17 над Україною в липні 2014 року. Посилений контроль над національними ЗМІ та Інтернетом, а також переслідування інакодумців дають можливість формувати російську громадську думку. Однак, незважаючи на спроби Russia Today і справжньої армії інтернет тролів, портали новин і соціальні медіа, які займають антиросійські позиції, російські інформаційні операції в цілому не встигли вплинути на не-російськомовну публіку. Українські урядові джерела заявляють, що спостерігається дуже низький рівень суспільної довіри до будь-якого офіційного російського ЗМІ, і незважаючи на інтенсивну російську інформаційну кампанію, підтримка проросійських сепаратистів навіть серед російськомовних громадян України нижча, ніж можна було очікувати. Це певною мірою пояснює напад РФ на Україну.

Під час кризи російська тактика, ймовірно, включатиме приховану підтримку місцевих проросійських активістів. Як і в Україні, невпевненість і неможливість довести участь ускладнюватимуть підтвердження факту нападу. Марка Галеоті, щодо елементів пропаганди особливо яскраво показав та описав такі методи діяльності. Він написав, що першим маленьким «зеленим чоловічком» може бути 15-річна російська естонська дівчинка. Якщо криза почне розростатися, Росія може піддатися спокусі захопити територію вразливих фронтових держав відкрито військовими силами доти, доки Альянс організує ефективну колективну відповідь. Жахливим для НАТО сценарієм

була б окупація частини держави-члена, навіть якщо це тимчасово. Така дія змусить Альянс застосувати статтю 5 Вашингтонського договору і наразитися на ризик прямої збройної конфронтації з ядерною Росією або не зреагувати на агресію і наразитися на ризик краху НАТО як життєздатний військовий союз. Незважаючи на побоювання таких держав, як Німеччина, ефективне стримування вимагатиме постійної дислокації значних багатонаціональних сил на території держав, які перебувають у ризиковій ситуації, для того, щоб не дати можливості Росії зробити військове рішення dokonаним фактом. Хоча Об'єднана оперативна група військ високого ступеня готовності (ООГВ) чисельністю в 5000 чоловік має бути в змозі розвернутися дуже швидко, але вона все ж таки може запізнитися для запобігання російському авантюризму. Російський підхід до гібридної війни не виключає пряме використання військової сили, коли це необхідно. Влітку 2014 року, коли Росія вичерпала свій запас невійськових гібридних методів, військові операції в Україні набули характеру обмеженої конвенційної війни. Російські батальйонні тактичні групи втручалися безпосередньо у бої проти української армії. Військові дії включали зіткнення між бронетанковими силами, інтенсивні міські бої піхоти, вогонь важкої артилерії та, принаймні з російської сторони, використання БЛА для спостереження та цілевказівки, електронну війну та використання засобів ППО. Війська НАТО вже почали засвоювати уроки українських військових, що стосуються російської тактики та технології, зокрема використання БЛА для наведення вогню артилерії та використання російських електронних засобів придушення. Однак лише тактичні вдосконалення навряд чи будуть достатні для забезпечення надійного конвенційного стримування проти збройного нападу. Наближення геополітичної точки біфуркації - важливий момент не тільки для великих держав, а й для України. Від того, як Європа, США і Росія її пройдуть, залежатиме нова конструкція світового порядку (Горбулін В.П., 2016).

Потрібно здійснити такі заходи, щоб медійна та інформаційна пропаганда зі сторони супротивника була неможливою. Це перше. Без можливості вести

інформаційний наступ, ворог лишиться частини можливих прибічників, та не зможе зменшити рівень довіри населення об'єкта агресії до своєї влади та армії. Друге, що потрібно зробити це, вибудувати таку систему захисту, як кіберсистем країни, тобто енергетики, комунального господарства, так і військовий захист. При високому рівні захисту дії агресора можуть не мати тієї дії яка йому потрібна. Отримавши або в теорії при організації нападу, якщо агресор отримає серйозну відсіч, а об'єкт нападу буде перебувати в повній, своєчасній готовності, в тому числі і моральній, то це може як ліквідувати можливість здійснення ворожої гібридної агресії так і зробити її малошкідливою.

3.2 Шляхи вирішення гібридних конфліктів

Аналіз «гібридних» процесів, зокрема, у новітній історії, дозволяє зробити ряд висновків. Усі складові гібридної війни: військова, економічна, інформаційна, застосовуються і під час «класичних» військових процесів. Відмінність «гібридних» форм протиборства – у прихованні факту участі тієї чи іншої держави у них, котрий іноді спроба надання їм легітимного характеру. А щодо сучасного «гібридного» протиборства: ще й у співвідношенні частки складових у конфлікті, у зв'язку з чим поняття «гібридної війни» перестає бути однорідним і потребує вже внутрішньої класифікації. Теорія і практика ведення «гібридних війн» не військове «ноу-хау», а давно використовується і перевірений тип міждержавного протиборства, який дещо по-іншому використовується в сучасних умовах і, ймовірно, буде активно і з зростаючою ефективністю використовуватися і надалі. Щодо стратегії ведення «гібридних» війн, то вона є типовим випадком війни «на виснаження», що повною мірою потребує безлічі ресурсів, що служить слабким місцем цього виду протиборства і потенційно може бути використане для протидії йому. З часу війни в Іспанії «гібридні війни» в основному ведуться кількома сторонами, кожна з яких має власну мету та різні відносини між собою. Типовий приклад – бойові дії в сучасній Сирії, де численні сторони, що беруть участь, володіють не тільки

різними цілями і різним ступенем легітимності участі в конфлікті, але й досить складними відносинами між собою. У подібних умовах аналізувати конфлікт, прогнозувати його перебіг і результат, управляти протиборством вкрай складно, необхідно уточнення положень теорії збройної боротьби, методів прогнозування їх перебігу і результату. Економічні санкції або блокади, що здійснюються в рамках «гібридного» протиборства, як показує історичний досвід, часто призводять до переростання конфлікту в «гарячу фазу», що вимагає оперативної реакції на них усієї міжнародної спільноти, не меншу небезпеку переростання в гарячу фазу несе така складова, як використання деструктивних соціально-політичних технологій, що потребує вироблення заходів правового регулювання їх застосування. Останній чинник, як свідчить аналіз історичної ретроспективи, зростали в міру глобалізації та інформатизації суспільства. І, ймовірно, їхній вплив продовжить посилюватися в найближчому майбутньому. Проведений аналіз дозволяє зробити певні висновки та рекомендації. По-перше, жодним чином не можна визнати «гібридну війну» принципово новим способом протиборства. Це навіть дозволяє деяким фахівцям предметної області робити висновок у тому, що виділяти таку форму протистояння окремий вид небажано. Визнаючи певну логічність такого підходу, слід зазначити, що хоча всі складові «гібридного» протистояння використовуються і в рамках «класичних» конфліктів, зворотного проектування немає. "Гібридний" конфлікт може вестися і без переходу у фазу прямого військового протиборства, не переходячи рівня проксі-війни. По-друге, різноманітність «гібридних» дій показує, що вважати «гібридну» війну якимось єдиним, однорідним явищем не можна. Подібні дії розрізняються за цілями, що застосовуються методами та ступенем «гібридності», що потребує уточнення їх класифікації. При цьому необхідно врахувати тенденцію усунення акцентів «гібридних» дій від ведення «проксі-війн» у сферу невійськового протистояння. Як не парадоксально, це тільки збільшує рівень їхньої небезпеки. Інтенсивне застосування «гібридних» методів протистояння в економіці, соціально-політичній сфері та кіберпросторі, в сучасному глобалізованому світі виявляє

руйнівний вплив не менший, а може й більший, ніж ті ж локальні збройні конфлікти. У зв'язку з цим останнім часом спостерігається сплеск досліджень, спрямованих на формування основ кібернетичної безпеки держави (Даник Ю, Труш О.О. 2010, с.15). А ефективних заходів протидії їм досі не вироблено. Ця небезпека потребує уточнення системи документів, що регулюють міжнародні відносини, запровадження у них положень про неприпустимість застосування санкцій та проведення інформаційних операцій без схвалення міжнародних організацій. Можливо, буде потрібно уточнення понятійного апарату, наприклад, введення в правове поле понять, що вже використовуються фахівцями: «інформаційне вторгнення», «ресурсна блокада» та інших. Відповідно, існуючі документи щодо регулювання силової складової «гібридних воєн» також вимагають уточнення, наприклад, щодо зміщення акценту покарання за наймання від приватних осіб до держав, у яких зареєстровані ПВК. За економічними та інформаційними компонентами потрібне прийняття міжнародних законодавчих актів, аналогічних тим, що регулюють їхню силову складову. У тому числі, за діями, що передують «гібридному» протиборству, що забезпечує його підготовку («передгібридним»). Після ухвалення відповідних актів, всі економічні та інформаційні заходи, що виходять за межі встановлених міжнародним законодавством рамок, на основі уточнених документів, повинні визнаватися оголошенням війни з боку держави, яка їх використала. По-третє, особливості «гібридних воєн», частота їх виникнення вимагають від збройних сил усіх держав, які розраховують вести самостійну політику, уточнення структури збройних сил, способів їх застосування, коригування керівних документів тощо. Насамперед, враховуючи особливості переходу «гібридного» протистояння в силову фазу: уточнення щодо підвищення готовності збройних сил до дій у мирний час, без оголошення війни, щодо розширення автономності військових частин та підвищення самостійності їх командирів у прийнятті рішень. Цілком це стосується і нашої країни. Як одна з основних умов, для реалізації цих пропозицій потрібно законодавчо встановити точні межі, що

визначають, де закінчується конкуренція, не важливо, економічна чи ідеологічна, і починаються військові дії. І, в рамках цього, уточнити класифікацію «гібридних війн». У сучасних умовах це вже не однорідне поняття, а набір варіантів дій, у яких, залежно від мети та завдань, превалює та чи інша складова. Часто, набір динамічний, що цілеспрямовано розвивається від «передгібридних» дій у напрямі збройного протистояння. Це завдання нетривіальне, але його рішення в перспективі послужить підвищенню безпеки сучасного світу. А затягування рішення – навпаки, призведе до зростання ризиків і загроз.

Розмірковуючи про природу гібридних конфліктів, необхідно розглянути їх базові елементи, що призвели до появи нового типу конфліктів та які можна вважати основними аргументами на захист концепції сучасного конфлікту гібридного типу. У ролі однієї з таких детермінант виступила, перш за все, модель безпеки, яка сформувалася після Другої світової війни. В умовах нинішньої парадигми міжнародних відносин держави, що планують здійснити агресивні дії проти іншого суб'єкта, почали активно шукати нові способи обійти міжнародне право, міжнародне гуманітарне право, Женевські конвенції та визначення «агресії» як таке, залишаючись при цьому «чистими» в очах міжнародного співтовариства та приховуючи свої справжні задуми.

Таким чином, ми виокремлюємо одну з ключових ознак гібридного конфлікту – прихованість, бажання агресора непрямыми діями досягти власної цілі, використовуючи різних посередників для того, щоб уникнути відповідальності. Другим фактором, що вплинув на появу нового типу конфлікту, став науково-технічний прогрес та глобалізація. Поява сучасних комп'ютерів, смартфонів, Інтернету та соціальних мереж кардинально змінило підходи до ведення бойових дій. По-перше, коли майже кожна людина має смартфон з камерою і доступом до всесвітньої мережі, агресору важко непомітно ввести свої війська – потрібно будь-яким шляхом прибрати можливість визначення їх приналежності до військ противника. По-друге, сучасні інформаційно-комунікаційні технології відкривають широкий спектр

можливостей для ведення інформаційної, психологічної війни на території противника. До того ж, концепція сучасного інформаційного суспільства підказує, що й війна 21-го століття є іншою, більш інформатизованою, складнішою, коли суспільство повністю інтегрується у війну та навпаки. Поєднання всіх перерахованих вище умов і є причиною виникнення гібридних конфліктів.

Узагальнивши досвід воєнних конфліктів минулого століття та тенденцій розвитку звичайних конфліктів нового покоління можна зробити висновки, що як гібридна, так і звичайна війна мають такі загальні риси, як збройне протистояння, з можливістю використовувати повний спектр незабороненої зброї, використання забороненої зброї залежить від доброї волі сторін. Також широко застосовується пропаганда, ведення інформаційної війни та психологічного тиску як щодо збройних сил противника, так і населення держави в цілому, оскільки «через свою специфічність інформаційне протистояння є невід'ємною складовою сучасних війн. Відбувається використання повного спектру сил спеціальних операцій, здійснення диверсій, підривної діяльності в тилу противника, використання партизанських, а іноді терористичних рухів. Дії ведуться на тактичному, оперативно-тактичному та оперативному рівнях. І, мабуть головний момент: сучасні війни можуть вестися без офіційного оголошення війни.

Серед основних відмінностей між гібридним та звичайним видами війни можна виділити такі відмінності. Звичайні війни майже завжди носять відкритий характер: існує чітке розуміння щодо сторін конфлікту, хто з ким воює, тоді як за гібридного конфлікту, у свою чергу, подібне розуміння відсутнє принаймні на початковому етапі конфлікту (замість комбатанта об'єкт агресії зустрічає невідомих «зелених чоловічків»). Тому з першої тези випливає розуміння того, що при гібридному конфлікті майже неможливо приховано вести бойові дії на стратегічному рівні - тобто задіяти одночасно кілька фронтів. Ну і гібридні війни вимагають більш тривалої підготовки, а

завершення конфлікту залежить лише від рівня розвитку військово-промислового потенціалу країни.

Таким чином, для досягнення бажаних результатів необхідні роки ідеологічної «обробки» населення противника і сприятливе середовище для виявлення сепаратизму, внутрішніх протиріч, сплеску активності криміналітету і тому подібне.

Як зазначалося вище, гібридній війні передуює досить тривала і комплексна підготовка, а тому їй передують гібридні загрози, які, по суті є викликами для держави. До таких загроз можна віднести: створення політичних та громадських рухів, які симпатизують майбутньому агресору, налагодження сприятливого інформаційного поля, пропагування, нав'язування агресором власних історичних, культурних, ідеологічних цінностей тощо. Саме тому пропонується виділити термін «гібридні загрози» і відрізнити його від поняття гібридної війни. Звичайно, критерієм концептуального розмежування двох термінів повинен бути факт порушення суверенітету держави: перетин озброєними або диверсійними формуваннями кордону, захоплення ними стратегічно важливих об'єктів, вбивство військовослужбовців тощо.

Сьогодні існує велика потреба у врегулюванні міжнародних конфліктів. В ситуації конфлікту можуть бути два типи поведінки сторін: спроба вирішити конфлікт шляхом односторонніх кроків або ж завдяки спільним діям з іншою стороною (Шібель, 2018, с.151). Цьому сприяють об'єктивні тенденції світового розвитку. По-перше, у світі виникає розуміння беззмістовності та небезпечності воєнних методів вирішення спірних питань – сторони зазвичай переходять до політичного діалогу та стратегічних комунікацій на переговорах. По-друге, посилюються інтеграційні процеси шляхом руйнування міждержавних та міжрегіональних бар'єрів, що створює умови для формування союзів, асоціацій, об'єднань держав, що ставлять за мету об'єднання сил та можливостей для забезпечення максимальної співпраці, яка буде зменшувати можливість конфліктних ситуацій.

Тому зараз існує два основні способи врегулювання конфлікту: замороження конфлікту на одній з трьох стадій, залагодження конфлікту – використовується, тоді, коли сторони не мають ресурсів продовжувати конфлікт, або мета конфлікту вже не має сенсу.

Врегулювання конфлікту не анулює існуючі протиріччя, які лежать в основі конфлікту, а всього лише може максимально їх згладити і виробити правильну формулу компромісного рішення, яка перешкоджає подальшій ескалації конфлікту. Розв'язання політичних конфліктів не має носити тимчасовий характер, а свою мету має вбачати в остаточному вирішенні існуючої проблеми та усуненні протиріч, які лежать в основі конфлікту. Політичний конфлікт може бути перерваним на будь-якій зі стадій його розгортання, якщо його основні причини будуть викоренені. Саме цю мету й має переслідувати процес політичних та інших можливих комунікацій у розв'язанні конфліктів.

При виборі способу мирного вирішення конфлікту необхідно чітко визначати виявлені розбіжності, адже такими значно легше керувати, ніж прихованими. Крім того, важливим завданням для обох сторін стає те, що вони мають розглядати опонента в якості партнера, а не супротивника (чи ворога). За таких умов учасники конфлікту приходять до висновку, що абсолютної безпеки можна досягнути тільки тоді, якщо забезпечується безпека обох сторін.

Дослідники конфліктів, зокрема і гібридних, серед можливих методів, які ведуть до завершення конфлікту називають: переговори, щодо законодавчого врегулювання на існуючій законодавчій базі; створення нової законодавчої бази і врегулювання за допомогою неї; примирення сторін.

До важливих інструментів урегулювання сучасних міжнародних конфліктів відносять дипломатію та її основну форму – стратегічні комунікації. Так, у міжнародних відносинах з дипломатією пов'язують коректне ведення переговорів, пошуки згоди і взаємоприйнятних для обох сторін рішень, розширення міжнародного співробітництва, поширення національних цінностей та захисту інтересів.

Врахування уроків «гібридної війни» Росії в Україні, які повинні винести з російсько-українського конфлікту на Донбасі армії України та провідних країн Заходу, однозначно сприятиме розбудові та посиленню секторів безпеки і оборони як окремих країн, так і коаліцій країн в умовах проведення «війн нового покоління» («війн нової генерації») (Радковець, 2016).

Головним завданням дипломатії є досягнення державами їхніх зовнішньополітичних цілей шляхом використання дипломатичних засобів.

Інструменти дипломатичного впливу на конфлікти дають в перспективі більш зважені та довготривалі результати. Саме тому на дипломатичні методи та стратегічні комунікації у XXI ст. доводиться щонайменше половина всього навантаження по врегулюванню міжнародних конфліктів. Адже дипломатичне врегулювання потребує менше витрат, зокрема може зменшити людські жертви. До компетенції дипломатів входять наступні напрями управління конфліктами, які реалізуються ними як у межах зовнішньої політики окремих держав, так і в межах діяльності міжнародних організацій, що здійснюють миротворчу діяльність: переговорний процес та посередництво між сторонами конфлікту.

У тих випадках, коли традиційна дипломатія стає недостатньо ефективною (як правило, це ті випадки, коли швидкість вироблення зовнішньополітичних рішень поступається швидкості і динаміці розвитку конфлікту, сторони не можуть домовитись про проведення переговорів і т.д.), на передній план висуваються нові формати дипломатичної діяльності.

До такої діяльності належать: місії індивідуальних політичних та громадських діячів, які схвалені світовою спільнотою; формування необхідної громадської думки за кордоном, в основному, здійснювана недержавними діячами, що беруть участь у врегулюванні конфліктів та миротворчій діяльності завдяки делегуванню їм прав та повноважень державами і міжнародними організаціями. Можемо зробити також ще один висновок – міжнародне право має реагувати на зміни безпекової реальності у світі, появу новітніх загроз (Яворська, 2016, с.18).

Попередження конфлікту є надзвичайно важливим аспектом у розв'язанні міжнародних кризових ситуацій, адже слід враховувати, що конфлікт легше зупинити на самому початку, до переходу з гібридної форми у відкриту, коли він ще не набув широкомасштабного та руйнівного характеру. Помітне місце в розробці засобів подолання міжнародних конфліктів належить прогнозуванню. Передбачення виникнення міжнародних криз має можливість своєчасно вжити належних заходів щодо їх попередження. Так, якщо превентивних заходів вчасно вчинено не було, а конфліктна ситуація вже перейшла у тривалу стадію (прийняла затяжний характер), то на цьому етапі її вирішення стає проблемним.

Тому, все ж таки, політичний шлях врегулювання конфлікту повинен бути ключовим. Для цього уряди країн та міжнародні організації, такі як ООН повинні прикладати зусилля, щоб виявляти можливі конфлікти, які можуть статися у окремих регіонах чи між декількома країнами. Для цього вони повинні проводити моніторинг у різних галузях міжнародних відносин, соціальній сфері у конкретній країні, заздалегідь проводити законодавчу роботу для забезпечення прав національних меншин і т.д.

3.3 Шляхи вирішення гібридного конфлікту в Україні

Як ми побачили, методологія боротьби з гібридними конфліктами розширюється, з'являються різні способи захисту держав від гібридних загроз. Є напрацювання в різних країнах як щодо захисту різних сфер своєї країни так і світового співтовариства від агресивних дій злочинних організацій чи авторитарних режимів зокрема.

Україна веде боротьбу з гібридною агресією РФ вже не один рік, але ситуація знаходиться у такому собі замороженому стані. З одного боку покращується армія, з'являються нові зразки озброєння, військові постійно проходять курси покращення кваліфікації та керування різною технікою, в тому числі безпілотними апаратами. Постійно в Україні проходять навчання з

іноземними військовими чи інструкторами. Ведеться робота на дипломатичному рівні.

Але оцінюючи ситуацію в цілому ми бачимо що рецепту вирішення гібридного конфлікту не лише на сході України, а й повернення АР Крим не видно навіть на горизонті.

Хоча західні країни й намагалися вплинути на РФ вводячи санкції, та роблячи політичні заяви про підтримку територіальної цілісності України, але ми бачимо, що санкції в тому обсязі, на який спромігся Захід не працюють в тій мірі, на яку вони розраховували. А політичними заявами налякати владу РФ Заходу не вдалось.

Для початку треба подивитись на ті загрози, які може отримати та отримує влада РФ від Заходу, зокрема санкціями. По-перше: санкції введені дуже вибірково, і як здається лише для «галочки». Особи з провладних ешелонів РФ, проти яких ввели персональні санкції, це ті фігури, якими може пожертвувати режим Путіна. Якихось непоправних збитків, зокрема для армії РФ не отримала від санкцій. Ті запчастини чи технології, доступ до яких РФ втратила, не вирішували так сильно ситуацію в армії. По-друге: ті збитки, які вплинули на рівень забезпеченості населення РФ, для влади РФ взагалі не мають значення. РФ продовжує нарощувати військовий потенціал навколо України, постачає техніку в ОРДЛО, та використовує і надалі гібридні методи боротьби проти України.

Нам треба створити такий механізм протистояння гібридним загрозам РФ, щоб для початку у короткостроковій перспективі повністю виключити вплив РФ як на населення України (у різних ракурсах), на міжнародну спільноту через інформаційну пропаганду. Встановити такий режим захисту території України на кордоні, щоб у РФ не було можливості насичувати технікою окуповані території. І у подальшому, в довгостроковій перспективі повністю звільнити усю територію України від московських окупантів.

Світ вже пройшов через подібні ситуації щодо звільнення територій або відмову від окупованих територій різними політичними та військовими

методами. За останні 30 років сталося декілька конфліктів, які мали гібридні складові. Зокрема відбулось хорватське вирішення конфлікту військовим шляхом. Пакистан відмовився від території Бангладеш після розуміння, що військовим шляхом повернути територію не вдасться. Ще був конфлікт щодо Косово, який був злагоджений політично, та залишив багато питань.

В українській політичній верхівці, а також в міжнародній спільноті є різні теорії як завершити конфлікт на Донбасі. Про Крим поки не думають.

У даній роботі можна запропонувати декілька механізмів вирішення гібридного конфлікту з РФ на користь України.

По-перше треба через впровадження кримінальної відповідальності заборонити всіляке пособництво агресору. Дипломатичні установи РФ повинні бути зачинені, персонал видворений з території України, до повного звільнення території України. Повністю повинні бути заборонені різні російські спілки і товариства, через які відбувається інформаційна гібридна війна проти України.

Усі колишні і діючі депутати всіх рівнів, якщо у них була співпраця з РФ, і це доведено у законному порядку, повинні бути заарештовані. Це буде прикладом усім, хто захоче співробітничати з окупантом. Після вирішення питань внутрішньо слабких, на які давить РФ, ми забезпечимо внутрішній захист від можливих сепаратистських дій чиновників, колишніх депутатів, які мають зв'язки з РФ.

В Україні повинні бути повністю заборонені та відключені усі російські ЗМІ, інтернет видання, сайти, та інша пропагандистська інформація.

Одночасно з цим повинен бути розпочатий судовий процес проти РФ з приводу порушення Будапештського меморандуму. Як мінімум, потрібно наполягати на порушення статей 1,3 та 2. Меморандум забороняє не тільки ядерний чи збройний напад на Україну, він також забороняє невизнання територіальної цілісності України. Забороняє економічний тиск проти України. Ми побачили що за останні років 20 економічний тиск здійснюється постійно за сторони РФ, а територіально цілісність і суверенітет також постійно ставляться під сумнів зі сторони російської влади, і це все було ще до агресії.

Україна, на жаль не є членом НАТО, тому розраховувати на захист з боку Альянсу не варто, але ми можемо спробувати стати партнером США поза НАТО. Нам потрібно прикласти усі зусилля для двосторонньої співпраці з США через укладення різних військових договорів. Ми повинні запропонувати такі умови, такі можливості використання для військових потреб своїх об'єктів військовими США, щоб вони бачили у цьому перспективу і для себе і як елемент стримування РФ.

Щодо санкційного режиму, то тут потрібно виділити 2 моделі санкцій. Перша модель повинна стримувати РФ від агресивних дій щодо України, а друга модель економічно задавити агресора, щоб він не тільки вивів війська з Донбасу а й з Криму.

Дії проти РФ потрібно вести жорстко, наступально та виважено.

Для початку треба поставити такі умови, що якщо РФ піде на ескалацію конфлікту, то усі газову домовленості, купівля енергоресурсів з РФ до ЕС буде припинена. В цей же час за допомогою військових точних методів, потрібно зробити неможливим насичення військовою технікою РФ територій ОРДЛО.

Якщо вони будуть нести важкі втрати, та витрачати великі гроші на це, то це зупинить агресора. БПЛА, як ми побачили вже можуть виконувати такі завдання на відмінно.

Санкціями в той же час можна економічно душити агресора, щоб втрати коштів були дуже відчутними і окуповані території обходились дуже дорого.

На політичній міжнародній арені РФ повинна бути виключена з усіх міжнародних організацій, влада РФ повинна бути визнана злочинною

Щодо населення окупованих територій, то Україна повинна за допомогою сучасних інформаційних технологій повинна вести транслявання радіо та ТБ на окуповані території для впливу на населення, яке при повній невдоволеності владою окупантів може повстати проти РФ.

Як ми бачимо інструментарій методів боротьби проти гібридної агресії РФ великий, головне те, як цим скористається українська влада. Роботу потрібно вести не тільки всередині України а й на міжнародній арені.

Якщо використати увесь наявний інструментарій проти РФ, то Україна зможе вирішити гібридний конфлікт на свою користь та повернути захоплені агресором території.

ВИСНОВКИ

Гібридні методи ведення війни не змінюють сутність війни. Насильство залишається основою гібридної війни, як і за будь-якої іншої форми війни, і їхня мета та сама, як і за будь-якого іншого акта війни, а саме, використовувати загрозу застосування, тобто шантаж або застосування організованого насильства для отримання фізичних чи психологічних переваг перед противником. Однак, саме існування термінології – гібридна, асиметрична, неконвенційна, нелінійна, нового покоління, четвертого та п'ятого покоління, сіра війна – показує труднощі, із якими продовжують зіштовхуватися стратеги і теоретики при класифікації складних збройних конфліктів XX та XXI століття. Хоча термін «гібридна» на даний момент є найпопулярнішим, він аж ніяк не є єдиним для опису такого типу війн. Факт, що при багатьох збройних конфліктах розмивається межа між війною та миром і використовуються інструменти, які традиційно не є частиною воєнних дій, ще більше ускладнює цю проблему. Це, безперечно, є викликом для традиційного істеблішменту із сектору безпеки, який має розглядати широке коло загроз, ідентифікованих аналітиками та теоретиками гібридної війни. Якщо розкинути мережу визначення надто широко, термін гібридна війна стає надто всеосяжним для практичного використання політиками. Якщо дати надто вузьке визначення, люди, які визначають політику, не зможуть усвідомити значення багатьох нетрадиційних технологій, які використовуються противником, як прелюдія чи доповнення до застосування військової сили.

Незалежно від того, яким ярликом позначена загроза, стратеги повинні вирішувати, як найкраще впоратися з методами, які застосовують противник, хоч би ким він був – державним чи недержавним гравцем. Іноді найбільш відповідна реакція може включати застосування специфічних політичних, інформаційних, економічних, дипломатичних, або у разі фізичної загрози, військових засобів державності. Більш складні загрози потребують цілісного державного чи комплексного підходу. Зазвичай найкраща стратегія включає

координацію та спрямування всіх ефективних інструментів державної могутності та зусиль, незалежно від того, яким чином визначено загрозу.

Міжнародні відносини і міжнародні конфлікти XXI ст. насправді є окремою главою історії людства, де активний вплив мають глобалізаційні процеси та стратегічні комунікації, які носять як антагоністичний так і регулюючий характер. Характерними ознаками міжнародних конфліктів XXI як ми побачили, є: руйнація міждержавних та міжрегіональних кордонів, використання гібридних засобів ведення міжнародної боротьби (гібридні війни, міжнародний тероризм, приватні військові компанії, інформаційні й кібернетичні атаки. Часто основою для виникнення конфліктів стають такі чинники, як сепаратизм, націоналізм, повстанські рухи.

Також можна вказати на такий факт, який можемо зараз спостерігати. За допомогою гібридних дій менш розвинені країни, використовуючи прогалини або в законодавстві демократичних, та більш розвинених країн, або прогалини у сфері безпеки (відсутність військового захисту кордонів між країнами ЄС), наносять великої шкоди та несуть велику загрозу для цих країн.

Стратегічні комунікації стосовно врегулювання міжнародних конфліктів спрямовані як на глобальне безпекове середовище, яке постійно змінюється, так і на виклики в інформаційному середовищі завдяки ретельній координації, синхронізації та взаємодії різних комунікаційних функцій у сфері міжнародних відносин.

Також потрібно міжнародним структурам та організаціям провести аналіз існуючого законодавства з міжнародного гуманітарного права, права захисту національних меншин, прав людини. Потрібно змінити законодавство відповідно до нинішніх загроз гібридних конфліктів. Треба розуміти, що такі країни, як РФ, почали дуже вдало використовувати гібридні методи боротьби, адже реальної військової могутності їм не вистачить для боротьби з цивілізованим світом.

Методи та способи гібридної боротьби наразі стали настільки різноманітними, що при бажанні, а в авторитарних та терористичних країн це

бажання зараз проявляється дуже явно, вони використовують навіть найменшу можливість нанести Заходу шкоду. Ми побачили, що навіть не застосовуючи зброю, можна принести країні, на яку спрямована агресія, економічні збитки, екологічні, соціальні, політичні.

Тому потрібна загальна координація цивілізованих країн для вирішення питань можливості агресивних країн проводити гібриду агресію. Санкції, ембарго, відключення агресора від економік, фінансових джерел, науки, технології Західного світу повинні використовуватись рішуче, відразу після перших проявів гібридної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Андрієвський Т.Г. Гібридна війна як специфічний тип гібридного конфлікту. (2017).

Андрієвський Т. Гібридна війна: сутність та базові стратегії. (2017).
Доступно з https://desecuritate.uph.edu.pl/images/De_Securitate_12_Andrewskij.pdf

Арзуманян Р.В. Определение войны в 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегических исследований Армейского военного колледжа, 6-8 апреля 2010 / Р.В. Арзумян. – Ереван, (2011). – 60 с.

Батрименко О.В. Особливості сучасних збройно-політичних конфліктів: дис. канд. політ. наук: 23.00.02. Нац. ун-т ім. Т. Шевченка. Київ, (2006). 238 с.

Березовська-Чміль О., Юлія Кобець. Політичний конфлікт гібридного типу: глобальний та регіональний виміри. *Sociology*.23.08.(2020).с.93-101.

Бжежинский З. Великая шахматная доска: господство Америки. Его геостратегические императивы)/ книга – (1997) / перевод О. Ю. Уральский//перезидат - М.: Междунар. отношения, 1998. ISBN 5-7133-0967-3
Доступно http://hists.narod.ru/doc/new/knigi/Brzezinski_Velikaja_shachmatnaja_doska.pdf.

Бондаренко О.Г., Я. О. Бондаренко. Динаміка міжнародних конфліктів та роль стратегічних комунікацій у їх врегулюванні. (2020).

Бондаренко О.Г.. Динаміка міжнародних конфліктів та роль стратегічних комунікацій у їх врегулюванні. (2020).

Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, (2015).— 288 с.

Василенко О.В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому / О.В. Василенко//Наука і оборона. (2009). – № 4. – С. 18–22.

Василь М. Телелим, Д. П. Музыченко и Ю. Ж. Пунда, «Планирование сил для сценариев ‘Гибридной войны’», Наука и оборона 20, № 3 (2014): 30-35. Доступно з <https://connections-qj.org/ru/article/planirovanie-sil-dlya-scenariev-gibridnoy-voyny>.

Воєнні аспекти протидії “гібридній” агресії: досвід України : монографія / колектив авторів ; за заг. ред. А. М. Сиротенка. – К. : НУОУ ім. Івана Черняхівського, (2020). 176с. Доступно https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf.

Воротнюк М.О. Особливості міжнародних конфліктів пост-біполярного періоду / М. О. Воротнюк // Стратегічна панорама. – (2009). – № 4. – С. 41–44.

Гай-Нижник П. П. Росія проти України (1990–2016 рр.): від політики шантажу і примусу до війни на поглинання та спроби знищення / Павло Гай-Нижник. – К.: «МП Леся». (2017). – 332 с.

Галака О. М., Ільяшов О. А., Павлюк Ю. М. Основні тенденції розвитку та ймовірні форми воєн і збройних конфліктів майбутнього/ О. М. Галака, О. А. Ільяшов, Ю. М. Павлюк // Наука і оборона. (2007).– № 4.– С. 10–15.

Гантингтон С. Столкновение цивилизаций. М.: ООО «Издательство АСТ», (2003). 603 с.

Гібридна війна: in verbo et in praxi: монографія. Під. заг. ред. проф. Р.О. Додонова. Вінниця: ТОВ «Нілан-ЛТД», (2017). 412 с. Доступно з <https://jmonographs.donnu.edu.ua/issue/view/94>.

Голобуцкий А. П., Шевчук О. Б. Судный век: Информатизация, глобализация, терроризм и ближайшее будущее человечества. – К.: Вид. дім „КМ Академія”, (2004). – 96 с.

Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок; Ін–т пробл. нац. безпеки. – К.: Інтертехнологія, (2009). – 136 с.

Горбулін В.П. Точка біфуркації. (2016). Доступно з <https://zn.ua/ukr/internal/tochka-bifurkaciyi-.html>

Даник Ю., Малярчук Т., Бриггс Ч. Гибридная война: хай-тек, информационные и кибер конфликты. (2017). Доступно з <http://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiber-konflikty>.

Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, (2019). – 320 с.

Даник Ю., Ищенко Д., Манько О., «Военные аспекты классификации передовых технологических систем», Научный журнал Житомирского военного института им. С. Королева 8 (2013): 5-13.

Даник Ю., Труш О.О., «Особенности обеспечения национальной безопасности в среде передовых технологий», *Государственная организация 1* (2010), Доступно з http://nbuv.gov.ua/UJRN/DeBu_2010_1_42.

Динис Г. Агресія Російської Федерації проти України та міжнародно-правові зобов'язання ERGA OMNES Росії перед іншими державами та міжнародним співтовариством . № 4/2014.Український часопис міжнародного права. Науково- практични журнал.ISSN 1814- 3385. Спецвипуск: Міжнародна науково-практична конференція. «Інтереси країни: міжнародно-правовий захист». Київ,06 лютого (2015). – С. 61-77. – [Електронний ресурс].- Доступно з http://jusintergentes.com.ua/index.php?option=com_k2&view=item&id=216

Динис Г.Г. Проблематика ефективності механізму міжнародно-правового регулювання збройних конфліктів (на прикладі міждержавного збройного конфлікту Росії та Грузії)// Геополітика України: історія і сучасність: збірник наукових праць. Вип. 1. – Ужгород: Ліра, (2009). – С. 61-77. – [Електронний ресурс].- Доступно з <http://www.uzhnu.edu.ua>uk/infocentre/get/>.

Динис Г. Сучасні гібридні збройні конфлікти: правові аспекти. (2013).

Женевська конвенція про поводження з військовополоненими від 12 серпня 1949 року [Електронний ресурс] // Верховна Рада України. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_153.

Загребельний О.В. Особливості врегулювання воєнно-політичних конфліктів: дис. канд. політ. наук: 23.00.02. Нац. ун-т ім. Т. Шевченка. Київ, (2017). С. 242

Інформаційні виклики гібридної війни: контент, канали, механізми протидії. Монографія НІСД, Київ, (2016). – Доступно з <http://uk.x-pdf.ru/5mehanika/2292151-1-informaciyni-vikliki-gibridnoi-viyni-kontent-kanali-mehanizmi-protidii-analitichna-dopovid-kiiv-2016-pri-p.php>.

Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник. За ред. В. Б. Толубка. – К.: НАОУ. (2004). – 176 с

Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. (2016). с. 27-32. Доступно з <http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf>

Клаузевиц К. О войне. Сочинение: в 2-х т. М.: ООО «Изд-во АСТ»; СПб.: Terra Fantastica, (2002). Т.1. 558 с.; Т.2. 574 с. 21.

Клаузевиц К. Принципы ведения войны; М.: ЗАО “Центрполиграф”, (2007). 130 с.

Климчук Ю.В. Гибридная война как вид вооруженного конфликта. Доступно з http://www.rusnauka.com/34_NNM_2014/Pravo/13_179711.doc.htm

Конвенція про захист цивільного населення під час війни, Женева, від 12 серпня 1949 року [Електронний ресурс] // Верховна Рада України. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_154/paran6#n6.

Конвенція про поліпшення долі поранених і хворих у діючих арміях від 12 серпня 1949 року [Електронний ресурс] // Верховна Рада України. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_151.

Конвенція про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі від 12 серпня 1949 року [Електронний ресурс] // Верховна Рада України. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_152.

Котенко А. О. Гібридна війна як форма сучасного міжнародного конфлікту. Міжнародні відносини. Серія «Політичні науки». (2017). № 13. Доступно з http://journals.iir.kiev.ua/index.php/pol_n/article/view/3070/2758

Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, (2016). - 286 с. Доступно з https://mil.univ.kiev.ua/files/222_1044284240.pdf

Лещенко О.Я. Трансформація системи цивільного захисту України в умовах сучасних воєнно-політичних конфліктів гібридного типу. (2020). Доступно з <https://niss.gov.ua/sites/default/files/2020-01/proekt-rukopisu-leschenka-ost.-utoch.-09.01.2020.pdf>.

Луцишин Г. Особливості сучасних збройних конфліктів в умовах глобалізації.(2014).Доступно з <http://ena.lp.edu.ua/bitstream/ntb/24522/1/22-128-133.pdf>.

Магда Є.М. Гібридна війна: сутність та структура феномену (2014). Доступно з http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489.

Малышева Е.М. Мировые войны и локальные военные конфликты в истории: последствия, уроки. (2005). № 1. С. 69. Доступно з <https://cyberleninka.ru/article/n/mirovye-voyny-i-lokalnye-voennye-konflikty-v-istorii-posledstviya-uroki>.

Панова В.В. Современные западные исследования международного конфликта / В.В. Панова // Международные процессы. (2005). – Т. 3. – № 2 (8). – С. 128–135.

Панова В.В. // Международные процессы. (2005). – Т. 3. – № 2 (8). – С. 128–135.

Перепелиця Г.М. Генезис конфліктів на посткомуністичному просторі Європи / Г. М. Перепелиця. – К.: Стилос - ПЦ «Фоліант» (2003). – 256 с.

Попович К. В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри. Науковий вісник Ужгородського університету, серія «Історія», вип. 2 (35), (2016).

Радецький В. Г. Класифікація сучасних воєнних конфліктів і види миротворчої діяльності. (2009). Доступно <http://vmv.kymu.edu.ua/series/vmv/vipusk9/04.pdf>

Радковець Ю. Гібридна війна Росії проти України: уроки та висновки. (2016). Доступно з <https://www.ukrinform.ua/rubric-politics/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html>.

Сірий С. Особливості локальних війн і воєнних конфліктів в умовах глобалізації. (2007). Доступно <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/8857/14-Sirui.pdf>

Ситник Г. П. Вплив глобалізації на воєнну сферу та принципові особливості сучасних воєнних конфліктів/стаття (2016). Доступно з http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=nivanb_2016_1-2_10.

Ситник Г. П.: Шляхи удосконалення системи державного управління забезпеченням національної безпеки України : навч. посіб. : Ч. 2 / В. І. Абрамов, В. А. Мандрагелята ін. - К. : НАДУ, (2012). - 44 с

Стасюк С. В. Особливості регулювання сучасних збройних конфліктів: проблеми та перспективи / С. В. Стасюк. // Юридична наука. – (2011). – № 1 (1). – С. 206–210.

Стасюк С. Регулювання сучасних збройних конфліктів міжнародними гуманітарними засобами / С. Стасюк // Віче. – (2010). – № 24. – С. 20–24. 11. Досупно http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=viche_2010_24

Сунь-Цзы. Трактаты о военном искусстве. М.: ООО «Изд-во АСТ»; СПб.: Terra Fantastica, (2002). 558 с.

Смола Л.Є. Аспекти нелінійної війни в контексті українсько-російського конфлікту на Донбасі. Науковий часопис НПУ ім. М.П. Драгоманова. Серія 22. К.: (2015). Вип. 16. С. 74-78.

Тоффлер Э. Война и антивоина : что такое война и как с ней бороться. Как выжить на рассвете XXI века / Элвин Тоффлер, Хейди Тоффлер. – М : АСТ: Транзиткнига, (2005). – 412 с. Доступно з <http://library.khpg.org/files/docs/1449832479.pdf>

Требін М.П. «Гібридна» війна як нова українська реальність. Український соціум. (2014). № 3. С. 113-127. Доступно з http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Usoc_2014_3_13

Требін М. Інформаційне суспільство. Війни нової епохи / М. Требін // Віче. – (2002). – № 4. – С. 64–68.

Требін М. П. Війна в історії людства та її особливості у XXI столітті / М. П. Требін // Наук. вісн. Східноєвроп. нац. ун-ту ім. Лесі Українки. Серія: Міжнар. відносини. – (2016). – № 2 (327). – С. 43–48. Доступно з http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnyua_2015_4_17

Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций / М.М. Хамзатов // Военная мысль. (2006). – № 7. – С. 1317. Доступно http://pentagonus.ru/publ/vlijanie_koncepcii_setecentricheskoj_vojny_na_kharakter_sovremennykh_operacija/19-1-0-1757

Храпач Г. С. Національна могутність як чинник стійкості держави в умовах загострення міжнародної конфліктності. (2017). С. 126-130. Доступно з <http://znp-cvds.nuou.org.ua/article/view/124423/118950>.

Чікін О. А. Ескалація розвитку збройних конфліктів / О. А. Чікін, О. О. Чікін // Персонал. – (2006). – № 9. – С. 48–51. Доступно з <http://personal.in.ua/article.php?ida=364>

Чупрій Л. В., Загребельний О. В. Особливості та шляхи вирішення в оєнно-політичного конфлікту на сході України. (2017). Доступно з http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=vdonnupn_2017_2_17

Цыганков П. А. Теория международных отношений: Учебное пособие. – М.: Гардарики. (2003). – 590 с.

Шібель В. Миротворчий процес: методологічні аспекти дослідження. Політичний менеджмент. Вип. 6. (2009). Доступно з http://ipiend.gov.ua/wp-content/uploads/2018/08/shibel_myrotvorchy.pdf.

Шляхтун П.П. Політологія (теорія та історія політичної науки). К.: Либідь, (2005). 576 с.

Яворська Г.М. Концепт «війна»: семантика і прагматика. Стратегічні пріоритети. Сер.: Філософія. (2016). № 1. С. 14–23. Доступно з http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=spa_2016_1_4.

Яворська Г.М. Гібридна війна як дискурсивний конструкт. (2016). Доступно з <http://ippi.org.ua/sites/default/files/yavorskaya.pdf>.

Яворська Г. Мова як складник конфлікту. Media Studies. Междисциплинарные исследования медиа. Материалы конференции. Харьков, (2016). С. 103–108. Доступно з https://www.academia.edu/29059852/%D0%BC%D0%BE%D0%B2%D0%B0_%D1%8F%D0%BA_%D1%81%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%

[B8%D0%BA_%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D1%96%D0%BA%D1%82%D1%83_pdf?auto=download.](#)