

Міністерство освіти і науки України
Ніжинський державний університет імені Миколи Гоголя
Факультет філології, історії та політико-юридичних наук
Кафедра всесвітньої історії та міжнародних відносин
291 Міжнародні відносини, суспільні комунікації
та регіональні студії

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітньо-кваліфікаційного рівня «бакалавр»

**ПРОБЛЕМИ МІЖНАРОДНОЇ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В
ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ-КОНФЛІКТІВ**

Студента:

Школьника Руслана Сергійовича

Науковий керівник:

Мицик Лариса Миколаївна

кандидат історичних наук, доцент

Рецензент: _____

Допущено до захисту:

(посада) (підпис) (дата) (ініціали та
прізвище)

Ніжин - 2023

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ	9
1.1. Міжнародна безпека: еволюція та структура поняття	9
1.2. Система та ієрархія національної безпеки	16
1.3. Поняття та характеристики гібридних війн та проксі- конфліктів.....	22
РОЗДІЛ 2. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ МІЖНАРОДНОЇ ТА КОЛЕКТИВНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ-КОНФЛІКТИ	29
2.1. Система підтримання миру в рамках ООН в часи гібридних загроз.....	29
2.2. Діяльність ОБСЄ в контексті гібридних війн та проксі-конфліктів.....	35
2.3. Регіональні безпекові організації в епоху гібридних війн та проксі- конфліктів.....	41
РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ- КОНФЛІКТІВ.....	49
3.1. Системи національної безпеки країн-членів НАТО при протидії гібридній агресії	49
3.2. Системи національної безпеки позаблокових країн при протидії гібридній агресії	55
3.3. Засоби та інструменти протидії гібридній агресії та запобігання проксі-конфлікту в структурі національної безпеки України	62
ВИСНОВКИ	74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ	78

ВСТУП

Актуальність обраної теми дослідження. В сучасному світі, міжнародні відносини стикаються зі значними викликами, які породжують нові форми загроз та конфліктів. Зростання гібридних війн та проксі-конфліктів стало актуальною проблемою для міжнародної та національної безпеки. Ці нові типи конфліктів поєднують у собі як військові, так і невійськові методи, включаючи кібератаки, дезінформацію, хакерські атаки, гібридну пропаганду та економічний тиск.

Дослідження проблем міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів є актуальним з кількох причин.

По-перше, ці конфлікти мають глибокий вплив на політичну стабільність, економічний розвиток та соціальну безпеку країн та регіонів. Вони породжують загрози для національної суверенітету, територіальної цілісності та глобальної безпеки.

По-друге, зростання ролі гібридних війн та проксі-конфліктів ставить під сумнів традиційні засади міжнародного права, включаючи принципи недоторканості територіальної цілісності та ненасильницького вирішення конфліктів. Це створює необхідність перегляду та адаптації існуючих норм міжнародного права до нових викликів та загроз.

По-третє, розуміння причин та наслідків гібридних війн та проксі-конфліктів є ключовим для розробки ефективних стратегій та політик з метою забезпечення національної та міжнародної безпеки. Дослідження цієї теми дозволить виявити уразливості та недоліки існуючих систем безпеки, а також розробити рекомендації для покращення превентивних та реагувальних заходів.

Крім того, зростання значення кіберпростору та цифрової сфери в сучасному світі ставить питання щодо кібербезпеки та захисту

національної інфраструктури. Гібридні війни та проксі-конфлікти використовують кібератаки як ефективний інструмент для досягнення своїх цілей. Вивчення цієї теми допоможе розробити стратегії кібербезпеки та захисту, а також забезпечити стійкість країн та організацій до кіберзагроз.

Особливо тема є актуальною для України. Починаючи з 2014 року Російська Федерація веде гібридну війну проти України, в цій роботі згадані аспекти системи національної безпеки України в сфері протидії гібридним загрозам та передбачення проксі-конфліктів. Тим самим, сьогодні це дослідження опрацьовує актуальні проблеми для України та безпеки в регіоні.

Таким чином, актуальність обраної теми дослідження полягає у необхідності розуміння та аналізу проблем міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів. Дослідження цієї теми внесе вагомий внесок у розвиток стратегій, політик та міжнародного співробітництва з метою забезпечення стійкості, безпеки та миру у сучасному світі.

Аналіз останніх досліджень та публікацій. У рамках написання дипломної роботи у нагоді стали праці наступних вітчизняних та зарубіжних фахівців : Брежнєвої Т. В. «Стійкість як ключовий елемент колективної оборони НАТО»[37], в цій роботі було досліджено проблему стійкості в середені НАТО, вагома частина роботи присвячена протистоянню гібридним загрозам в контексті колективної безпеки та європейського регіону загалом. Монографія Д. Паламарчук «Національна безпека» [41], в цій великій роботі висвітленні майже всі елементи національної безпеки, її структура, функції, а основне, що висвітлено вразливі місця системи національної безпеки перед новітніми формами агресії, такі як гібридні війни та проксі-конфлікти. Монографія за редакцією Власюка О. С. «Україна у системі міжнародної безпеки» [46], в

цій монографії більше висвітлюється саме проблема України як суб'єкта міжнародної безпеки який активно бореться з гібридними загрозами, наводиться приклади які характеризують проблему гібридних війн та проксі-конфліктів як загроз для системи міжнародної та регіональної безпеки, а також досліджуються методи та практики удосконалення національної безпеки України в цій сфері. Мамфорда Е. «Proxy Warfare» [56], основа цієї роботи полягає в дослідженні самого явища гібридних війн, методів ведення та застосування, але також наводяться приклади протидії таким загрозам. Прабхакаран П. «National Security: Imperatives And Challenges» [57], це дослідження присвячено сучасній системі національної безпеки, особливо цікавими є визначення, щодо викликів для цієї системи, вказується, що гібридні війни та проксі-конфлікти є одними з основних загроз сучасності і боротьба з ними є складним процесом який потребує стратегічного та оперативного концепту, і багатьох інших. Але окремі аспекти зазначеної проблеми залишаються дещо недостатньо висвітлені в науковій літературі.

Мета. Дослідити, основні проблеми міжнародної та національної безпеки в контексті сучасних загроз, теоретичну складову проблем, роботу міжнародних та регіональних безпекових організацій і проблеми національної безпеки окремих країн в цій сфері.

Завдання. Для досягнення даної мети потрібно виділити такі завдання:

1. Окреслити основні теоретичні засади дослідження: визначити еволюцію та структуру поняття «міжнародна безпека»; виокремити систему та ієрархію національної безпеки.
2. Проаналізувати діяльність міжнародних організацій на прикладі ООН та ОБСЄ, щодо протидії гібридній агресії, а також виокремити регіональні безпекові організації в цьому плані.

3. Спробувати систематизувати стратегії сектору національної безпеки в різних країнах світу: країнах-членах НАТО; позаблокових країнах.
4. Дослідити методи попередження і ліквідування гібридних війн і проксі-конфліктів в системі національної безпеки України.

Об'єкт дослідження – сьогодення система міжнародної безпеки та системи національної безпеки деяких країн.

Предмет дослідження – проблеми та прогалини в системі міжнародної безпеки та секторах національної безпеки в сфері боротьби з гібридними загрозами та проксі-конфліктами.

Практичне значення дослідження. Розробка стратегій протидії гібридним війнам та проксі-конфліктам: Дослідження також містить аналіз сучасних стратегій протидії гібридним війнам та проксі-конфліктам. Результати цього дослідження можуть бути використані для розробки більш ефективних стратегій протидії цим явищам. Практичні рекомендації, які будуть включені в дане дослідження, можуть стати основою для розробки політики та стратегій безпеки відповідних держав і міжнародних організацій.

Роль міжнародної співпраці: Дослідження зосереджується на важливості міжнародної співпраці у протидії гібридним війнам та проксі-конфліктам. Визначення конкретних областей співробітництва, обміну інформацією та координації дій може допомогти зміцнити колективний відповідь на ці загрози.

Освітнє значення: Це дослідження може мати значний освітній вплив, особливо для студентів, науковців та практиків у галузі міжнародних відносин і безпеки. Воно надасть їм можливість поглибити свої знання про сучасні виклики і ризики, пов'язані з гібридними війнами та проксі-конфліктами, і сприятиме розвитку нових дослідницьких

напрямоків у цій області.

Узагальнюючи, практичне значення даного дослідження полягає у сприянні розумінню проблем міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів. Воно може служити основою для розробки стратегій протидії, сприяти зміцненню міжнародної співпраці та мати освітній вплив на аудиторію, зацікавлену у галузі міжнародних відносин і безпеки.

Наукова новизна. Ця дипломна робота пропонує оригінальний підхід до вивчення та аналізу цієї актуальної теми:

Дана робота пропонує аналіз концепту гібридних війн та проксі-конфліктів, розкриваючи їхню сутність, особливості та вплив на міжнародну безпеку. Цей аналіз є новаторським, оскільки враховує сучасні тренди та розвиток цих явищ, а також звертає увагу на їхні наслідки для національних безпекових систем.

Дипломна робота поєднує різні дисципліни, такі як міжнародні відносини, безпекові студії, військова стратегія та політична наука, для більш повного розуміння проблеми. Цей інтегрований підхід дозволяє зрозуміти широкий спектр аспектів, що впливають на міжнародну та національну безпеку в епоху гібридних війн та проксі-конфліктів.

Дипломна робота пропонує використання та аплікацію різних теоретичних концепцій і моделей, що сприяють глибшому розумінню проблеми міжнародної та національної безпеки в контексті гібридних війн та проксі-конфліктів. Це дозволяє дослідникові пропонувати нові підходи та розробляти концептуальні рамки для аналізу цих явищ.

Основна увага роботи приділяється не лише аналізу проблем міжнародної та національної безпеки, але й їхньому впливу на регіональну та глобальну стабільність. Цей аспект дослідження є новаторським і сприяє більш глибокому розумінню міжзалежності цих процесів та необхідності спільних зусиль у їхньому врегулюванні.

Апробація. Дипломна робота пройшла апробацію у форматі виступів та доповідей на наукових конференціях. Виступ доповідь на V Міжнародній науковій онлайн конференції для студентів та молодих науковців «Європейська інтеграція: історичний досвід та політичні перспективи» яка проходила 8 – 9 жовтня 2021 року, також була написана наукова стаття до цієї конференції: Школьник Р. Гібридна війна як виклик європейській безпеці // Проблеми європейської інтеграції та демократії в рецепції української та польської молоді: збірник статей / за ред. Юлії Кузьменко, Матеуша Каміонки. - Ніжин: НДУ ім. М. Гоголя, 2021. – 191 с.. URL: <http://lib.ndu.edu.ua/dspace/handle/123456789/1993> . Доповідь та наукова стаття до Вісника студентського наукового товариства за 2022 рік: Школьник Р. Гібридна війна як доктрина зовнішньої експансії // Вісник студентського наукового товариства [електронне видання]: збірник наукових праць студентів, магістрантів і аспірантів / за заг. ред. О. В. Мельничука. Ніжин: НДУ ім. М. Гоголя, 2022. Вип. 27. – 90 с.. URL: http://www.ndu.edu.ua/storage/styd_visnuk/visnuk_stud_tov_27_2022.pdf .

Структура. Дипломна робота складається з вступу, трьох розділів, дев'яти підрозділів, висновків та списку використаних джерел та літератури.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Міжнародна безпека: еволюція та структура поняття

Говорячи про визначення поняття міжнародна безпека потрібно звернутися в першу чергу до класичних визначень які використовувалися протягом довгого часу в роботах багатьох науковців. Складність визначення цього поняття полягає в тому, що довгий час цей термін був надбанням військової термінології, але з розвитком політичних наук та вчень про міжнародні відносини зокрема, ми можемо визначити такі основні поняття: «Міжнародна безпека» – це:

I. система міжнародних відносин, що базується на дотриманні всіма державами загальновизнаних принципів та норм міжнародного права, що виключає вирішення спірних питань та суперечок між ними за допомогою сили або погрози силою [28].

II. система міжнародних відносин, базована на дотриманні всіма державами загальновизнаних принципів та норм міжнародного права, що виключає вирішення спорів між ними за допомогою сили чи її погрозою [27].

III. система міжнародних договорів та угод, що забезпечує збереження миру на основі визнання суверенітету, недоторканності кордонів та територіальної цілісності держав, відмови від застосування сили або її погрози у вирішенні міжнародних суперечок [29].

З практичної точки зору застосування терміну «міжнародна безпека» можна пов'язувати з формами багатосторонньої дипломатії. До прикладу можна привести Гаазьку конференцію 1899 року. Саме на ній було підняте питання міжнародної безпеки та її кодифікації вперше, проте ця спроба не була успішною як показує історія, але той прецедент який вона показала, щодо вирішення питань законів та правил ведення війни заклав підвалини для розвитку міжнародної безпеки як з практичної так і з наукової точки

зору.

Створення Ліги Націй тільки підіграло інтерес науковців до міжнародної безпеки. **Ліга Націй** — перша міжнародна міждержавна організація, створена з метою розвитку співробітництва, досягнення миру і безпеки між народами. На практиці основними завданнями були дотримання прав національних меншин і вирішення територіальних конфліктів у світі після Першої світової війни. Була заснована на Паризькій мирній конференції в 1919—1920 рр. Ініціатором її створення виступив 28-й президент США Вудро Вільсон [50].

З розвитком цієї організації розвивалося і розроблення нових концепцій міжнародної безпеки та державної політики війни та миру. У 1928 було підписано «Пакт Бріана – Келлога» відомого також як Паризька угода про відмову від війни. Хоч вона була підписана поза Лігою Націй вона була значним об'єктом в творенні міжнародної безпеки. **Загальний договір про відмову від війни як інструменту національної політики** — міжнародна угода про відмову від війни, як знаряддя національної політики. Підписана 27 серпня 1928 року в Парижі 15 державами. Угода отримала назву за іменами ініціаторів — міністра закордонних справ Французької республіки Арістида Бріана та держсекретаря США Френка Келлога [43].

Говорячи про кодифікацію в міжнародному праві, потрібно також згадати дві конвенції про визначення агресії, які були підписані в 1933 році. Обидві конвенції були зареєстровані як угоди в серії Ліги Націй. Довгий час саме ці конвенції були одними з найавторитетнішими джерелами міжнародного права в сфері забезпечення міжнародної безпеки.

Всі ці акти знайшли свій відбиток у Статуті ООН. Згідно Статуту, члени цієї міжнародної організації мають утримуватися від ведення агресивної війни, так як війна не відповідає цілям ООН. Завдяки цьому

цей принцип остаточно увійшов в норми міжнародних відносин та міжнародного права. В самому Статуті все це закріплено та кодифіковано, а саме в Розділі I; Стаття 1 та 2 – Цілі та принципи: *«Підтримувати міжнародний мир та безпеку і з цією метою вживати ефективних колективних заходів для запобігання та усунення загрози миру й придушення актів агресії, або інших порушень миру, і проводити мирними засобами, відповідно до принципів справедливості та міжнародного права, залагоджування або розв'язання міжнародних конфліктів або ситуацій, що можуть призвести до порушення миру.»* [4].

«Усі Члени Організації Об'єднаних Націй розв'язують свої міжнародні суперечки мирними засобами таким чином, щоб не наражати на загрозу міжнародний мир та безпеку і справедливість;» [4].

«Усі Члени Організації Об'єднаних Націй утримуються в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із Цілями Об'єднаних Націй;» [4].

«Організація забезпечує, щоб держави, які не є її Членами, діяли відповідно до цих Принципів, оскільки це може виявитися необхідним для підтримки міжнародного миру й безпеки;» [4].

Створення зброї масового ураження, а саме ядерної повністю змінив питання міжнародної безпеки та такого феномену як війна.

Вже в кінці ХХ століття ставало зрозуміло, що національна безпека тісно пов'язана з міжнародною безпекою і підтримання національної також залежить і від фактору міжнародної безпеки. Створення нових концепцій всеосяжної міжнародної безпеки в 1980-х роках показувало, що вчення про цю частину міжнародних відносин розвивається з величезною швидкістю. Саме сьогодні сучасна наука та методи аналізу дають зрозуміти, що підтримання національної безпеки неможлива лише

військовими засобами, навіть якщо ці засоби надзвичайно потужні.

Говорячи про забезпечення міжнародної безпеки, саме в це поняття науковці зводять, підтримання та відновлення миру, запобігання війнам та військовим конфліктам.

Єдиної концепції міжнародної безпеки ні в історії ні в теорії міжнародних відносинах немає. Можна сказати про класифікацію саме про види безпеки що являє структуру поняття, а саме: регіональна, екологічна, глобальна, національна та ін.. Ці об'єднує те, що кожен з них має витоки як історичні так і нормативно-правові.

Що мається на увазі «глобальна безпека» в контексті міжнародної безпеки. Це безпека всього світу, система та методика захисту загроз світового масштабу.

Такого виду загрози торкаються всіх цивілізацій та людства загалом. Саме загроза існування людства, націй та цивілізацій є основним фактором характеристики таких «глобальних загроз».

Глобальними називають проблеми, які стосуються всього світу, призводять до значних, нерідко незворотних соціально-економічних і біологічних втрат на планеті, створюють загрозу існуванню людства і потребують для свого розв'язання координованої співпраці всіх країн. Серед сучасних глобальних проблем розрізняють кілька груп: політичні, етнічні, демографічні, економічні, соціальні, продовольчі, екологічні. Серед них, своєю чергою, виокремлюють вузлі аспекти, що впливають на окремі сторони життя людства. Наприклад, проблема етнічних воєн, енергетична проблема, проблеми освіти та охорони здоров'я тощо [49].

Творення політики глобальної безпеки неможливе без задіяння більшості суб'єктів міжнародних відносин. Саме глобальна безпека як елемент міжнародної безпеки є відносно новим. Вперше про неї заговори в 1960-х роках, на сучасному етапі цей елемент має самостійну структуру та торкається загальних проблем, а ніж поняття міжнародної безпеки.

Політика глобальної безпеки може бути спрямована на різні сфери життя і може виявлятися на різних часових та просторових рівнях:

- **Екологія:** деградація земель — екологічні проблеми сучасності — озонові діри — парниковий ефект — проблема регулювання промислових викидів — проблеми руйнування екосистем — екологічні лиха — проблеми геоактивності — проблеми геліоактивності — проблеми світового господарства [49].
- **Економіка:** Вичерпання факторів виробництва — глобальна конкурентноспроможність — економічна парадигма — Інтеграція та дезінтеграція господарських ринків (інтеграційні утворення в Європі, Азії, Америці) — затратні виробництва — нові моделі економічного розвитку — перерозподіл блага між традиційними та новими економіками — Ресурсний потенціал сучасної цивілізації — Сталий розвиток [49].
- **Енергетика:** Енергетична криза — проблема безпеки АЕС, нових енергоблоків та наслідки виведення АЕС з експлуатації — Аварії на атомних електростанціях (Японія, 1997, 2011; Україна, 1986) [49].
- **Медицина:** контроль народжуваності та демографічні програми у країнах, що розвиваються — СНІД — старіння людини — санітарно-ветеринарний контроль проти пандемій та їх загроз (грип пташиний, грип свинячий, COVID-19) [49].
- **Космос та космічні технології:** космічне сміття та забруднення космосу — Ноосферно-космічна цивілізація [49].
- **Озброєння:** контроль озброєнь — контроль атомних технологій («Атомний клуб») [49].
- **Природа:** межі розуміння природи — самозародження речовини [49].
- **Політика:** взаємоприспособлення господарських механізмів та інституціональних структур на міждержавному і міжнародному

рівнях — гармонізація національної й міжнародної економічної політики — уніфікація господарського законодавства [49].

- **Промисловість:** Постіндустріальна модель розвитку — Третя промислова революція [49].
- **Суспільство:** гіпотеза другого демографічного переходу — експорт демократії — зближення націй (асиміляційний характер глобалізації) — перенаселення — продовольча проблема — соціально-економічний розвиток — цивілізаційний розвиток — технологічна революція [49].
- **Технології:** інформатизація (у глобальному вимірі) — машинна ера — обмеженість сучасних технологій — технологізація [49].

Масштабні загрози безпосередньо пов'язані з регіональною безпекою. Але у різних регіонах вони проявляють себе по-різному. Політика міжнародних акторів впливає лише частково [25].

Регіональна безпека - міжнародна безпека у певному регіоні світу. Регіональна безпека схожа на міжнародну, проте має багато відмінностей, таких, як форми прояву, баланси сил, різні традиції. По-перше, забезпечити безпеку можуть як міжнародні організації (ОБСЄ), так і об'єднання держав (ОАЕ). Регіональна безпека займає центральне місце у діяльності міжнародних організацій і, також, переплітається з головними питаннями їхньої діяльності. По-друге, на підтримку безпеки в регіоні потрібна увага та інтерес багатьох держав [56].

Визначаючи подібну структуру потрібно сказати, що «**регіон**» в питанні безпеки є географічна група держав яких об'єднує спільна система безпеки яка діє саме в цьому регіоні та направлена на стримування та ліквідування загроз характерних для цього регіону.

Після «Холодної війни» звичайна конфігурація регіонів змінилася. Наприклад, регіони Близького Сходу і Середнього Сходу, що розглядалися окремо, в даний час об'єднуються в питанні безпеки в

єдиний регіон Великого Близького Сходу або Близького і Середнього Сходу. Подібні процеси можна побачити і в АТР. Але деякі держави дуже складно віднести до якогось певного регіону. Наприклад, Туреччина, у питанні безпеки, належить і до європейського, і до євразійського регіонів [26].

Одним з аспектів міжнародної-регіональної безпеки є так звана «напруженість» регіону з точки зору складності забезпечення безпеки. З однієї сторони є безпечні регіони, такі як Європа, а з іншої «напруженні», такі як Африка та Близький Схід.

Нових значень набуває пострадянський регіон, особливо з точки зору військово-політичної ситуації сучасності в цьому регіоні. Активна та пасивна конфліктність цього регіону зумовлює перерозподіл сфер впливу та появу авторитарних режимів прагнучих агресивної експансії, яка загрожує всім суб'єктам цього регіону.

Після розпаду СРСР в теорії міжнародних відносин та міжнародної безпеки в особливості почали створюватися все чіткіші міркування про регіональну безпеку, почалося ділення на субрегіональний вимір. Зазвичай такого роду значення охоплюються компактні та взаємопов'язані частини регіону. Наприклад цей процес характерний для Балтійського та Чорноморського субрегіонів.

Отже говорячи про міжнародну безпеку потрібно розуміти, що це дуже «динамічне» поняття. Постійні інтерпретації та використання термінології в міжнародних відносинах, політології, історії та військових науках зумовило розвиток поняття та вивчення цієї сфери загалом. Потрібно сказати, що це поняття постійно еволюціонує, а структура постійно змінюється.

1.2 Система та ієрархія національної безпеки

Національна безпека визначається як здатність держави своєчасно виявляти, запобігати та нейтралізувати реальні та потенційні загрози своїм національним інтересам. Національна безпека означає захист життєво важливих інтересів людини, громадянина, суспільства і держави, забезпечення сталого розвитку суспільства, своєчасне виявлення та запобігання реальним і потенційним загрозам національним інтересам [51].

Ефективне забезпечення національної безпеки передбачає визначення, класифікацію, деталізацію та систематизацію понять, що використовуються у дослідженнях в цій галузі. Сучасна теорія національної безпеки охоплює велику кількість понять, деякі з яких потребують більш детального розгляду. Серед найпоширеніших термінів, які можна виділити, входять "національні інтереси", "стратегія національної безпеки", "загрози національної безпеки", "системи національної безпеки", "забезпечення національної безпеки", "сектор безпеки" та інші.

Основними складовими національної безпеки є:

- *Національні інтереси* означають невід'ємні матеріальні, інтелектуальні та духовні цінності, які є життєво важливими для народу країни як суверенного суб'єкта та єдиного джерела влади. Вони визначають потреби суспільства та держави, і їх реалізація забезпечує державний суверенітет та прогресивний розвиток країни [20].
- *Загрози національній безпеці* включають актуальні та потенційно можливі явища і фактори, які створюють ризик для життєво важливих національних інтересів країни [20].

- *Воєнна організація держави* представляє собою збірну структуру державних органів, військових формувань, що утворені згідно з внутрішніми законами країни. Діяльність цих організацій підлягає демократичному цивільному контролю з боку суспільства і має безпосередню мету захисту національних інтересів країни від зовнішніх та внутрішніх загроз [20].
- *Правоохоронні органи* є державними органами, яким Конституцією та законами країни надано повноваження здійснювати функції забезпечення правопорядку [20].

Забезпечення національної безпеки базується на наступних основних принципах:

- Надання пріоритету правам і свободам людини та громадянина [20].
- Встановлення верховенства права [20].
- Дотримання пріоритету договірних (мирних) засобів при вирішенні конфліктів [20].
- Забезпечення своєчасних і належних заходів для захисту національних інтересів від реальних та потенційних загроз [20].
- Чітке розмежування повноважень і співробітництво між органами державної влади у забезпеченні національної безпеки [20].
- Здійснення демократичного цивільного контролю над Воєнною організацією держави та іншими структурами в системі національної безпеки [20].
- Використання міждержавних систем і механізмів міжнародної колективної безпеки в інтересах країни [20].

Аналізуючи типи національної безпеки, можна використовувати терміни "внутрішня" та "зовнішня безпека". Ці категорії є взаємопов'язаними і часто згадуються в публіцистичній літературі частіше, ніж інші терміни. В українській науковій літературі особливо використовуються ці поняття для опису внутрішніх та зовнішніх факторів,

що впливають на національну безпеку. Навіть якщо є відсутність чіткого законодавчого визначення цих термінів (наприклад, в Законі України "Про основи національної безпеки України"), ці поняття продовжують використовуватись з правової точки зору.

Внутрішня безпека - це міра (рівень, ступінь) захищеності національних інтересів від загроз, джерелами яких є процеси, явища, події тощо, а також дії (бездіяльність) юридичних та фізичних осіб, які розміщені в межах території держави і перебувають під її юрисдикцією. Інакше кажучи, масштаби, характер, спрямованість, інтенсивність, тривалість, тощо указаних загроз зумовлена внутрішніми чинниками, а їх нейтралізація (зниження рівня впливу на національну безпеку) визначаються переважно можливостями державної влади. Загрози внутрішній безпеці проявляються в різних сферах життєдіяльності суспільства і держави: політичній, економічній, соціальній та гуманітарній (духовній) [54].

Зовнішня безпека - це також міра (рівень, ступінь) захищеності національних інтересів від загроз, але джерелами їх є процеси, явища, події тощо, дії (бездіяльність) юридичних та фізичних осіб, які перебувають поза межами території держави і не підпадають під її юрисдикцією. Інакше кажучи, масштаби, характер, спрямованість, інтенсивність, тривалість, тощо указаних загроз зумовлені зовнішніми чинниками, а їх нейтралізація (зниження рівня впливу на нац. безпеку) визначаються не тільки можливостями державної влади, а й архітектурою та спроможностями міжнародних структур безпеки, станом системи міжнародних відносин, місцем та роллю, яку відіграє в них держава. Загрози зовнішній безпеці можуть проявлятися в політичній, економічній, гуманітарній (духовній) сферах [54].

Варто зазначити, що забезпечення зовнішньої безпеки передбачає не тільки наявність та підтримання на необхідному рівні оборонного

потенціалу, застосування комплексу різноманітних інструментів впливу на перебіг подій (дипломатичних, економічних та ін.), які є в розпорядженні суверенної держави. На зовнішню безпеку значною мірою впливає також стан справ щодо забезпечення її внутрішньої безпеки [54].

При аналізі системи та ієрархії нац.. безпеки, важливо враховувати розрізнення національної безпеки за сферами діяльності соціуму і держави. Для забезпечення безпеки та захисту національних інтересів, органи державної безпеки розробляють стратегію та приймають комплекс заходів, що відповідають цій стратегії.

Виявляється складністю аналізу є питання, пов'язані з визначенням структури та ієрархії національної безпеки та розподілом на конкретні сфери суспільства та держави. Поділ на різні сфери, типи або інші компоненти національної безпеки є великою мірою умовним. Часто це пояснюється недостатнім науковим обґрунтуванням, хоча такий поділ часто зустрічається в офіційних документах, таких як закони, накази виконавчих органів влади, концепції та стратегії, що згадувалися раніше.

Враховуючи загальний контекст, можна виділити такі сфери, що характеризують національну безпеку: державна, економічна, енергетична, політична, інформаційна, екологічна та воєнна безпека.

З іноземних публікацій найбільш детально про це виклав публіцист Прабхакаран Палері в своїй роботі «National Security: Imperatives and Challenges».

Прабхакаран Палері, індійський академік, перелічує більшу кількість елементів у своїй книзі «Національна безпека: імперативи та виклики» (2008): військова безпека, економічна безпека, Безпека ресурсів, Прикордонна безпека, Демографічна безпека, Безпека на випадок катастроф, енергетична безпека, геостратегічна безпека, інформаційна безпека, продовольча безпека, безпека здоров'я, етнічна безпека, екологічна безпека, кібербезпека, геномна безпека [46].

Палері обрав ці елементи, маючи на увазі, що кожен термін має бути принципово цілісною концепцією, універсально застосовною, яка має соціальний вплив на макрорівні та безпосередньо впливає на життя людини; постійно під загрозою; безперервна безперервність від свого походження до свого існування, навіть якщо це може бути періодичним; і, що зараз є модним у сучасній мові природної безпеки, на додаток до ряду інших атрибутів. Палері також досліджує та відкидає певні терміни, які зазвичай зустрічаються в дискусіях про національну безпеку, «тероризм», «соціальне забезпечення» тощо [46].

Одним з найголовніших аспектів структури національної безпеки та її ієрархії є **система національно безпеки**.

Складовими елементами системи національної безпеки є:

Об'єкти національної безпеки - Національні матеріальні й духовні цінності, інтереси особи, суспільства, держави.

Масив чинного національного законодавства - встановлює пріоритети державної політики національної безпеки і відображає офіційні переконання щодо підходів, принципів та механізмів захисту нац.. інтересів.

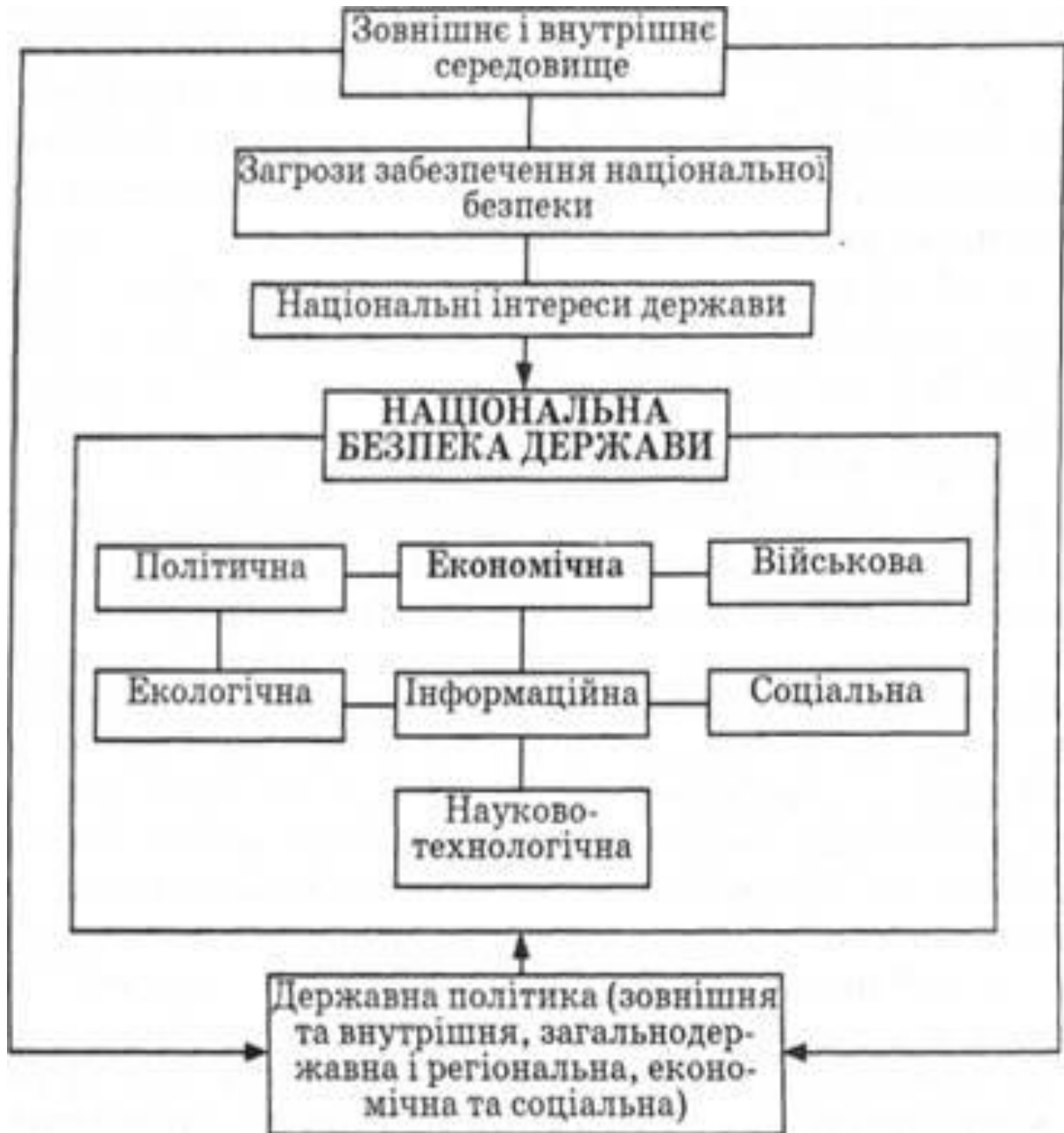
Сукупність зовнішніх та внутрішніх факторів, що впливають на нац.. безпеку, включає не лише змінні, такі як тенденції, показники та цілі, але й інші системи, наприклад, міжнародні структури безпеки, їх цілі та наслідки їх діяльності й інше.

Суб'єкти забезпечення національної безпеки - органи держ. влади та місцевого самоврядування, інститути громадянського суспільства, окремі громадяни, ЗМІ.

Загальна колекція владних інструментів, таких як політичні, економічні, воєнні та інформаційні, може бути використана для забезпечення адекватного рівня захисту національних інтересів. Ці інструменти включають збройні сили, спеціальні служби, підприємства

оборонно-промислового комплексу, дипломатичні засоби, державні та мобілізаційні резерви, а також інші ресурси, спрямовані на захист нац.. інтересів.

Національні джерела та суб'єкти - (фізичні та юридичні особи), які породжують загрози реалізації національних інтересів.



Отже структура та ієрархія національної безпеки на теперішній час є

дослідженою та вивченою, але на цьому етапі потрібно виділити деякі загальні аспекти розділу та підсумувати викладене у цьому розділі.

Можна виділити такі елементи структури та ієрархії національної безпеки:

Базові складові: Політичні, економічні та концептуально-світоглядні. На основі цих складових формується внутрішня стійка система безпеки суспільства, держави та громадян.

Інструментарій: Це визначений "арсенал" методів, стратегій, тактик, концепцій і основних напрямків використання, які використовуються для прямої підтримки національної безпеки та її забезпечення, а також для збереження належного рівня захищеності національних інтересів.

Апарат управління та прийняття рішень: Задля запобігання та ліквідації загроз національної безпеки на регіональному та загальнодержавному рівні.

1.3 Поняття та характеристики гібридних війн та проксі-конфліктів

Гібридні війни та проксі-конфлікти не є новим явищем, але зростання їх кількості в наші часи та розвиток науки про міжнародні відносини дали змогу внести їх у спектр досліджень та вивести у нову тему для обговорень не тільки серед науковців, але і в колах політичних діячів та державних управлінців. На тлі еволюції та розвитку системи міжнародних відносин, з'явилися нові виклики для держав та інших суб'єктів міжнародних відносин та світової політики, тепер серйозною загрозою стали «тихі війни» та війни з використанням «проксі сегменту». Найнебезпечніше, що саме подібного виду явище стають популярними серед недемократичних держав з імперіалістичними ідеями.

На практиці ми бачимо, що такі явища як гібридні війни вже стали

звичним в інформаційному колі політиків, військових, громадських та інших діячів. Створюються експертні групи які спеціалізуються на цьому, цілі генеральні штаби збройних сил працюють і розвивають тему «систематичного гібридного конфлікту». Основні цілі можуть слугувати як досягнення своїх національних інтересів, послаблення або знищення конкурента на міжнародній арені, неможливо виключати і оборонні методи гібридного протистояння, коли проти держави ведеться гібридна війна вона розроблює свою тактику утримування агресора.

Хотілось би розпочати саме з такого явища як «гібридна війна». Є багато визначень цього поняття, все через те, що гібридні війни почали систематично вивчати не так давно, але все ж найбільш точне визначення є таким:

«Гібридна війна — війна з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною» [48].

Загалом гібридну війну можна визначити як сукупність заздалегідь підготовлених та оперативно реалізованих державою дій військового, дипломатичного й інформаційного характеру, спрямованих на досягнення стратегічних цілей. При цьому важливе значення має відсутність необхідності в розробці нових систем зброї та військової техніки. Гібридна війна включає реалізацію комплексу гібридних загроз різного виду, а саме: традиційних, нестандартних, масштабний тероризм, а також підривні дії, у ході яких застосовуються інноваційні технології для протидії військовій силі супротивника, такі як масовані кібератаки, підривні дії в енергетичній, економічній сферах тощо [35].

Авжеж, деякі приписи гібридних конфліктів уже доповнюються на

тлі нових подій в міжнародних відносинах, наприклад вторгнення Російської Федерації в Україну 2022 року, ще буде вивчатися науковцями та істориками, але головне розуміти, що до цього Росія вела 8 років гібридну війну проти України. До речі, саме гібридна війна Росії проти України стала причиною розгортання масштабної кампанії по вивченню цього явища та самої сутності гібридної війни.

Говорячи про характеристику гібридних війн, то вона є більш менш систематизованою, саме як елементи гібридних війн то можна окреслити такі:

- 1) Політико-дипломатичний – завдання шкоди супротивнику на міжнародній арені, іміджу країни-жертви закордоном, запобігання контактів з іншими акторами міжнародного співтовариства.
- 2) Економічний – завдання шкоди сектору економіки держави, фінансово-економічні операції поцілені на дестабілізацію соціально-економічного становища, операції з валютою та інші інструменти.
- 3) Інформаційно-психологічний – поширення дезінформації та фейків з метою розташування ситуації в країні та посіяння паніки, підбурювання до створення умов для соціальних катаклізмів.
- 4) Кібер-сектор – кібер-атаки на інформаційні ресурси держави та населення задля поширення пропаганди, вивід з ладу важливих джерел стратегічної комунікації, кібер-шпигунство та інше.
- 5) Енергетичний елемент – маніпулювання ринком енергетичних технологій з ціллю створення криз в країні-жертви, поставлення в залежність держави або держав від країни-агресора.
- 6) Військовий – підготовка та оснащення бойовиків для виконання завдань на території країни жертви, підтримка повстанців та

терористів, використання ПВК та парамілітарних формувань у збройному конфлікті.

- 7) Внутрішньополітичний – створення та підтримка маріонеткових політичних сил в органах державної влади країни-жертви, підкуп та шантаж чиновників, політичне шпигунство та інші інструменти.

Більш не визначене поняття «проксі-конфлікт» або «проксі-війна». Proxу war, також опосередкована війна, війна за дорученням, війна чужими руками – це все не так добре досліджено у вітчизняній науковій літературі, аніж наприклад гібридні війни. Саме постійний підбір в одну сферу з гібридними війнами зробило тему «проксі-війн» менш помітною, але говорячи про неї можна знайти багато аспектів як є набагато глобальнішими.

«Проксі-війна — міжнародний конфлікт між двома країнами, які намагаються досягти своїх власних цілей за допомогою військових дій, що відбуваються на території та з використанням ресурсів третьої країни, під прикриттям вирішення внутрішнього конфлікту в цій третій країні (класичне визначення, дане Карлом Дойчем у 1964 році)» [44].

Все ж таки точного визначення «проксі-війни» немає. Так, А. Мамфорд вважає, що сформоване Дойчем зі спостереження за конфліктами Холодної війни визначення не виправдано ігнорує недержавних гравців. За Мамфордом, суттєвим внеском у визначення є дев'ять питань, задані в 1980-х роках Яковом Бар-Сіман-Товом і наведені тут із відповідями самого Мамфорда:

«1. Чи можна вважати проксі-війною війну, в якій зовнішня сила безпосередньо бере участь? - Ні, непряме втручання - невід'ємний елемент проксі-війни [44].

2. Чи суттєво, що обидві сторони місцевого конфлікту виступають представниками зовнішніх сил? - Ні, ситуація з посередниками не повинна бути симетричною [44].
3. Чи можна вважати війну проксі-війною лише для одного боку? - Так. Як приклад, Мамфорд наводить війну в Афганістані, де війна була проксі-війною лише з американського боку [44].
4. Чи потрібне для визнання війни проксі-війною явне твердження про це хоча б від однієї зовнішньої сторони? — Ні, зовнішні сили швидше за все вдаватимуться до семантичних хитрощів типу «проекція сили», «іноземна допомога» тощо [44].
5. Чи достатньо для оголошення війни проксі-війною думки зовнішніх учасників, чи потрібна також заява про це з боку однієї з місцевих сил? — Ні, оскільки набагато ймовірніше, що конфлікт розглядатиметься як проксі-війна іншими державами, які не залучені до конфлікту [44].
6. Як відрізнити проксі-війни від військових спілок? — Іноді відмінність провести важко, але зазвичай союз характеризується готовністю всіх союзників проливати в загальних цілях свою кров, а проксі-війна вказує на небажання зовнішньої сили робити це [44].
7. Як відрізнити допомогу зовнішньої сили однієї зі сторін конфлікту від використання цієї сторони у проксі-війні? — Це суб'єктивна інтерпретація, яка ґрунтується на оцінці мотивів сторін [44].
8. Чи може невелика держава воювати великими руками? — Так, при цьому зазвичай велика держава не розуміє ефекту своїх дій (за Мамфордом, для класифікації конфлікту як війни чужими руками усвідомлення того, що відбувається всіма учасниками, не обов'язково; він вважає, що США в Іраку 2003 року ефективно воювали як посередник Ірану) [44].

9. Чи вимагає війна чужими руками неодмінної взаємодії між великими державами та маленькими країнами? — Ні, війна може залучати недержавні утворення.» [44].

Мамфорд проводить явний кордон між війною чужими руками та секретною операцією, в якій держава, хоч і таємно, але бере участь безпосередньо. Проте, проксі-війни найчастіше призводять до необхідності секретних операцій.

Технології проксі-війни має очевидні бенефіси для країни-спонсора, яка використовує проксі-сегмент. Зауважити потрібно також про жахливі наслідки які можуть виникнути в разі використання інструментарію проксі-конфлікту.

Залежність. Протягом періоду Холодної війни, проксі-війни, зокрема в Африці, призвели до небажаної залежності молодих держав від СРСР та США. Це створило нинішню ситуацію, в якій багато формально незалежних країн надмірно покладаються на зовнішні країни-спонсори у всіх сферах повсякденного життя, включаючи військову, політичну та економічну.

Більш тривалі та криваві конфлікти. Мамфорд вказує на те, що широко поширене уявлення про використання проксі-війн як найшвидшого способу завершення конфлікту є помилковим. Насправді, такі втручання зазвичай лише продовжують конфлікт, оскільки сторону, яка поступилася, можна легко посилити до рівня, достатнього для створення безвихідної ситуації. Мамфорд зазначає, що в проксі-війнах зазвичай не розширюються кордони початкового конфлікту, оскільки сторони намагаються мінімізувати прямі витрати. Тому, якщо розширення конфлікту все ж відбувається, воно зазвичай має несподіваний сценарій для учасників.

Розширення конфлікту. Війна чужими руками зазвичай передбачає ухвалення геостратегічного афоризму «ворог мого ворога — мій друг».

Однак, як показала практика, після закінчення війни існує цілком ймовірна можливість «зворотного удару» (англ. *blowback* у термінології ЦРУ), коли з'ясується, що позиції країни-спонсора та безпосередніх учасників бойових дій збігалися лише тимчасово. Як приклад несподіваного для країни-спонсора поширення конфлікту, Мамфорд наводить рішення США забезпечити антиурядові повстанці в Афганістані протиповітряними ракетами «Стінгер», які, незважаючи на спроби США згодом повернути їх, поширилися територіями та конфліктами від Боснії до Палестини. Мамфорд також відносить до «зворотного удару» результати завершення війни в Афганістані, коли надані моджахеди створили на території Афганістану тилову базу для ісламських фундаменталістів. Американці не замислювалися про наслідки перебування Талібану при владі досить довго; навіть у 1998 році Бжезінський ставив, як йому тоді здавалося, риторичне запитання: «Що було важливіше у світовій історії: Талібан чи падіння радянської імперії? Декілька Perezбуджених ісламістів чи визволення Центральної Європи...?». Усвідомлення того, що США проміняли одну війну на іншу, прийшло пізніше, 11 вересня 2001 року [44].

Отже, враховуючи вище викладене, слід констатувати, викладені теоретичні засади дослідження є досить вагомими з точки зору з'ясування основ як самих термінів «міжнародна безпека», «національна безпека», «гібридна війна» та «проксі-конфлікт» так і підґрунтя використання їх в наукових дослідженнях інших авторів. Ця інформація дає змогу нам використовувати її з практичної точки зору та поглибити вивчення даної теми та проблематики.

РОЗДІЛ 2. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ МІЖНАРОДНОЇ ТА КОЛЕКТИВНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСИ-КОНФЛІКТІВ

2.1 Система підтримання миру в рамках ООН в часи гібридних загроз

ООН - найважливіша міжнародна організація сучасності покликана підтримувати та зміцнювати міжнародний мир та безпеку, сприяти мирному співіснуванню держав та розвитку мирного співробітництва між ними. Їй належить значна роль системі сучасних міжнародних відносин [36].

Існували спроби створення міжнародних організацій з метою забезпечення миру та запобігання конфліктам задовго до ООН, але їх ефективність була сумнівною. Найвідомішою з цих спроб була Ліга Націй (1919-1946), але вона не змогла стати ефективним засобом запобігання кровопролиттю.

Повноцінним поштовхом до створення такої організації стала Друга світова війна, яка вразила світ своєю жорстокістю, але водночас об'єднала суспільство, незважаючи на ідеологічні протиріччя. Очевидно, на той момент ідея створення системи протидії гібридним загрозам не була закладена в основи такої організації через відсутність розуміння таких загроз.

Хоча у Хартії ООН нічого не сказано про суттєвість факту оголошення війни для міжнародного права. У статті 2- й Женевських конвенцій 1949 р. стверджується, що їхні положення застосовують в усіх випадках збройних конфліктів, а не тільки у випадках війн, які було формально оголошено [6].

Організація Об'єднаних Націй (ООН) з моменту свого заснування відіграє важливу роль у забезпеченні міжнародного миру та безпеки. Вона використовує різноманітні інструменти, причому система миротворців

ООН стала ключовим механізмом для запобігання та вирішення конфліктів у всьому світі. Однак, з часом змінився характер загроз міжнародному миру та безпеці, і традиційні підходи до миротворчої діяльності стали менш ефективними у зустрічі цим викликам. В такому контексті, система миротворців ООН стикається з новим набором викликів, оскільки гібридні загрози стають основною проблемою безпеки.

Використання терміну «агресія» також підпадає під цю тему. Визначення агресії дається в резолюції XXIX сесії Генеральної Асамблеї ООН від 14 грудня 1974 р. Під агресією слід розуміти застосування збройної сили державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави або будьяким іншим чином, що несумісний зі Статутом ООН. Свідченням агресії, як правило, є таке застосування збройних сил державою першою [1].

Проблематика гібридних загроз, саме в тому що ці загрози особливо важко ідентифікувати та протистояти їм, оскільки вони часто включають поєднання державних і недержавних акторів із неоднозначними та непрозорими стосунками. Останніми роками гібридні загрози стають все більш поширеними та становлять значний ризик для глобальної стабільності та безпеки.

Система миротворчості ООН традиційно зосереджена на боротьбі зі звичайними загрозами миру та безпеці, такими як міждержавні конфлікти та громадянські війни. Однак, оскільки гібридні загрози стають все більш поширеними, система повинна адаптуватися до мінливого середовища безпеки. Це вимагає нового підходу до миротворчої діяльності, який об'єднує широкий спектр військових, цивільних і дипломатичних інструментів, включаючи збір, аналіз і обмін розвідданими, а також кіберзахист і протидію дезінформації.

Ще однією проблемою є те, що гібридні війни починаються саме членами ООН і вони шляхом прихованого інструментарію реалізують

свою діяльність. Шляхом деяких історичних висновків, є кілька доступних стратегічних варіантів. Протидіяти деяким гібридним методам можна шляхом стримування, заспокоєння партнерів і шляхом вселення довіри до тих, на кого хочеться впливати. Треба було б встановити «червоні лінії», звичайно, і бути чіткими в дипломатії, щоб викрити ворога, пропагандистів, їхні протиріччя та лицемірство. Відповідно, не повинно бути протидії дискредитації ворожої діяльності в міжнародних інституціях, таких як ООН [30].

Щоб протистояти виклику гібридних загроз, ООН розробила низку ініціатив для посилення своїх миротворчих можливостей. Ці ініціативи включають створення Інтегрованої служби навчання, яка проводить спеціалізоване навчання миротворців щодо гібридних загроз, а також розробку нових технологій і обладнання для підвищення обізнаності про ситуацію та підтримки ефективності місії. Крім того, ООН підкреслила важливість партнерства з регіональними та субрегіональними організаціями, такими як Африканський Союз і Європейський Союз, для посилення колективної відповіді на гібридні загрози.

Наступна системна проблема є бюрократія. Міжнародно-правова кодифікація є дуже вагомою для ООН. Проблематично що, спеціалісти міжнародної організації затримують просування правової кодифікації гібридних загроз. Сучасна міжнародно-правова база боротьби з тероризмом складається з: Радбезу ООН Резолюції 1373 (2001) та 1624 (2005), Резолюції РБ ООН щодо Аль-Каїди та Талібану 1267 (1999), 1333 (2000), 1390 (2002), 1735 (2006) і 2178 (2014), Резолюції РБ ООН щодо зброї масового знищення 1540 (2004) і 1673 (2006) і конвенції ООН проти тероризму, серед яких Конвенція про боротьбу з тероризмом і Конвенцію про боротьбу з фінансуванням тероризму. Досить дивно, що разом із зростанням впливу екстремістів на Сході України в 2014-2015 році не було прийнято жодного документу з цього приводу ні РБ ООН, ні Генеральною

Асамблеєю. Робоча група розробляла проект нової конвенції щодо боротьби з міжнародним тероризмом згідно з принципом універсальної юрисдикції, але процес ухвалення нової конвенції затягнутий вже дуже довгий час, тоді як тодішні обставини вимагали негайних дій [47].

Може виникнути питання – до чого тут міжнародний тероризм, але основна конфігурація гібридних загроз в системі ООН припадає саме на цей термін, хоча ми вважаємо його не зовсім вірним з точки зору практичного підходу.

Відповідно до Резолюції РБ ООН 1373 (2001) фінансування терористичних актів криміналізовано. Кошти і економічні ресурси, які використовуються для спонсорювання тероризму, повинні бути заморожені. У зв'язку з цим держави-члени ООН повинні співпрацювати через двосторонні та багатосторонні угоди. Контртерористичний комітет, який складається з 15 членів РБ ООН, був створений для надання допомоги державам-членам у впровадження інструментів боротьби з тероризмом [47].

Миротворча система ООН стикається зі значними проблемами у боротьбі з гібридними загрозами. Однією з ключових проблем є відсутність консенсусу серед держав-членів щодо характеру цих загроз та відповідної відповіді. Крім того, ООН має керувати складними політичними та дипломатичними відносинами, особливо у випадках, коли державні та недержавні актори залучені до гібридних загроз. ООН також стикається зі значними проблемами в достатності ресурсів, які обмежують її здатність розробляти та розгортати необхідні інструменти та можливості для ефективного вирішення цих проблем.

Відмінною рисою гібридної війни є використання асиметрії. У юридичній сфері гібридні агресори використовують прогалини в міжнародному праві, щоб перешкоджати здатності жертви рішуче реагувати. У поєднанні із заходами примусу для спеціального

стримування протидії агресор може створити ситуацію асиметричної переваги. Є два ключові аргументи для вирівнювання умов сьогодення з точки зору міжнародного права. По-перше, держави можуть відповісти на агресію силою, наприклад, за допомогою Статті 51 Організації Об'єднаних Націй (ООН) і глави 7 Ради Безпеки ООН. І НАТО, і Європейський Союз мають договірні гарантії колективних дій згідно з міжнародним правом, яке змінюється відповідно до нових загроз. Наприклад, НАТО оголосило про намір відповідати на кібератаки та гібридну війну як збройний напад. Міжнародне право не стоїть на місці й буде залежати від подальших зусиль, щоб підвищити свою «стійкість» до експлуатації та підривної діяльності. По-друге, міжнародне право також передбачає низку заходів для протидії гібридній агресії без застосування сили. Приклади включають санкції, фінансовий захист, розбудову потенціалу, реформу сектору безпеки, боротьба з корупцією, диверсифікація ресурсів, освіта, захист інфраструктури, кіберзахист, м'яка сила або регулювання ЗМІ. Іншими словами, існує достатня правова база для творчої горизонтальної ескалації для протидії гібридній війні [57].

На даний момент глобальна система переживає значні коливання. Концепція національної держави, яка є основним елементом цієї системи, сама по собі зазнає змін. Етнічна нестабільність, повстанські рухи та заворушення загрожують майже третині усіх країн-членів ООН. Національні кордони стають вразливими, курси валют підлягають контролю центральних банків, імпорт та імміграція легко перетинають межі, а тероризм, наркотики та зброя загрожують суверенітету. В такому хаосі виникає нова політична теорія, відома як постнаціональна держава. Для розуміння складних аспектів глобальних змін та їх наслідків для національної безпеки, політичних, соціально-економічних, культурних, ідеологічних та політичних складових суспільства, надзвичайно важливо мати вірне уявлення. Це допоможе сформулювати міцну стратегію

майбутнього прогресу, благополуччя, виживання людства та розвитку.

Потрібно звернути увагу і на участь миротворців ООН в війнах які мають характер гібридних. Після ізраїльського вторгнення в 1982 році Ліван змушений був боротися з довгою громадянською війною. Зі змішаним населенням приблизно 59,7 відсотка мусульман і 39 відсотків християн і присутність іноземних військових сил питання врегулювання та стабілізації було вкрай важким. Щоб заповнити порожнечу влади, Хезболла, недержавний актор, набув популярності з близькими по ідеології організаціями та військовою і фінансовою підтримкою Ірану. Насамперед шіїтське бачення, яке мало політичну роль соціального забезпечення та все ж використовувало і досі використовує насильство як інструмент, особливо проти Ізраїлю. Соціальний склад і роздробленість державного апарату дозволив Хезболлі розвивати свої інтереси в південному Лівані. Внутрішнє становище країни змінилося з виведення сил Ізраїлю з півдня в 2000 році та сирійських військ 2005 р. Але держава залишалася слабкою. У 2006 році Хезболла вбила трьох і викрала двох ізраїльських солдатів. Ізраїль відповів жорстко, це все призвело до 34-денної Другої Ліванської війни, спрямованої на знищення Хезболли. Це класичний випадок бойових дій між державою та зовнішнім недержавним гравцем, фактично, це підпадає під термін "гібридна війна". Тепер ООН, з однією з найбільших місій — Тимчасовими силами ООН у Ліван (UNIFIL) — розгорнула понад 12 400 миротворців для спостереження та припинення бойових дій і підтримки ліванської армії на півдні Лівану [24].

Підсумовуючи, гібридні загрози є серйозним викликом міжнародному миру та безпеці, і миротворча система ООН повинна адаптуватися, щоб ефективно протистояти цим викликам. Це вимагає нового підходу до миротворчої діяльності, який об'єднує широкий спектр військових, цивільних і дипломатичних засобів. Незважаючи на те, що ООН розробила ряд ініціатив для посилення свого миротворчого

потенціалу, існує потреба в більшій міжнародній співпраці та розподілі ресурсів для ефективної боротьби з гібридними загрозами.

2.2 Діяльність ОБСЄ в контексті гібридних війн та проксі-конфліктів

Організація з безпеки та співробітництва в Європі (ОБСЄ) є регіональною організацією безпеки, яка була створена в епоху холодної війни для сприяння миру, безпеці та співпраці в Європі. Протягом багатьох років ОБСЄ відіграла важливу роль у запобіганні конфліктам, моніторингу виборів, просуванні прав людини та наданні допомоги державам з перехідною економікою. Проте останній час ОБСЄ зіткнулася зі значними труднощами у вирішенні нових форм конфліктів, зокрема гібридних війн і проксі-конфліктів.

Протягом останніх років світові міжнародні інституції, а також регіональні, зокрема ОБСЄ, напружують механізми оперативного надання адекватних відповідей на новітні загрози типу - гібридних війн та проксі-конфліктів. На засіданні Ради безпеки ООН 12 грудня 2016 року, де обговорювався транснаціональний характер сучасного тероризму і потреба тісної співпраці між державами в цьому питанні, було прийнято резолюцію щодо зміцнення механізмів взаємної правової допомоги в збиранні та опрацюванні доказів тероризму. Раніше, у листопаді 2016 року, схожий документ прийняла й ОБСЄ [24].

Участь цієї організації в вирішенні подібних конфліктів є підтвердженою, саме гібридна війна Росії проти України (2014-2022 рр.) є прикладом для аналізу діяльності ОБСЄ у вирішенні таких конфліктів в Європі.

“Гібридна” війна проти України засвідчила також відсутність рішучості міжнародних глобальних і регіональних безпекових інститутів

(таких як ОБСЄ) у врегулюванні міжнародних конфліктів і локальних воєн та як наслідок – втрату ними міжнародного авторитету [34].

У контексті гібридних воєн і проксі-конфліктів ОБСЄ взяла на себе кілька ролей для сприяння миру та стабільності в Європі. Одним із основних напрямків діяльності ОБСЄ є моніторинг і звітування про безпекову ситуацію в зонах конфлікту. Спостерігачі ОБСЄ направляються в зони напруженості для збору інформації та звітування про порушення угод щодо припинення вогню, порушення прав людини та іншу діяльність яка пов'язана з безпекою. Наприклад, в Україні ОБСЄ відігравала ключову роль у моніторингу припинення вогню та відведення важкого озброєння в зоні конфлікту.

Іншим важливим напрямком діяльності ОБСЄ є сприяння діалогу та посередництву між конфліктуючими сторонами. ОБСЄ організувала проведення кількох раундів переговорів між Україною та Російською Федерацією для пошуку мирного вирішення конфлікту на сході України. ОБСЄ також була залучена до посередництва в конфліктах в інших регіонах, таких як Балкани та Кавказ.

Причому російська “гібридна” експансія відбувається одночасно з тотальною девальвацією глобальної і регіональної структур безпеки (ОБСЄ перебуває у кризовому становищі, а її діяльність зокрема з врегулювання російсько-українського конфлікту блокується російською стороною) [34].

ОБСЄ намагається активно протидіяти дезінформації та пропаганді. Офіс представника ОБСЄ з питань свободи ЗМІ здійснює моніторинг та сприяє розвитку відповідальної журналістики в регіоні. ОБСЄ також брала участь у розробці програм медіа-грамотності, щоб допомогти громадянам виявляти та протидіяти неправдивій інформації. Це один з аспектів в яких, можна сказати, що організація показує хороші результати.

У протистоянні російській експансії ЄС та ОБСЄ здійснили ряд

різних контрзаходів. Зокрема, у 2014 р. запроваджено спільну санкційну політику щодо Росії, ухвалені документи (в рамках ЄС, ОБСЄ, ПАРЄ) щодо засудження російської агресії проти України. У березні 2015р. на саміті ЄС ухвалене рішення про необхідність боротьби з російськими кампаніями дезінформації, а влітку створено в рамках Служби зовнішніх дій оперативну групу зі стратегічних комунікації на Сході (East StratCom Task Force), для інформаційної підтримки політики ОБСЄ і протистояння “зовнішній дезінформації” [34].

Найцікавішим згадуванням ролі ОБСЄ в конфлікті України та Росії відбулося ще в 2014 році. Так, коли 2 листопада 2014р. “республіки”, підтримані Кремлем, організовують у Донецьку та Луганську щось на зразок виборів без найменшої легітимності, ОБСЄ – міжнародна визнана організація з офіційними повноваженнями зокрема спостерігати за демократичністю перебігу виборів у всьому світі – не відряджає жодного спостерігача. Проте представники європейських праворадикалів знову прибувають, щоб надати видимість серйозності того, що відбувається. В той же час, EODE Л.Мішеля та польська маріонеткова організація яка фінансувалася з РФ напередодні створюють АБСЄ (Асоціацію безпеки та співробітництва в Європі). Схожість звучання має на меті виставити ОБСЄ на посміховисько та створити плутанину. А.Шеховцов у своєму блозі опублікував 44 імені цих “спостерігачів”: у цьому списку єдиним французом є Жан-Люк Шафхаузер [34].

Щодо гібридної війни Росії проти України потрібно також згадати саме створення спеціальної моніторингової місії ОБСЄ в Україні.

Спеціальна моніторингова місія ОБСЄ в Україні — місія неозброєних цивільних спостерігачів ОБСЄ, яка тимчасово проводить моніторинг та звітує про ситуацію з дотримання прав людини та гуманітарну ситуацію як у зоні конфлікту на Донбасі, так і по всій території України.

СММУ утворена 21 березня 2014 року на запит уряду України до ОБСЄ та на підставі консенсусного рішення 57 країн-учасниць ОБСЄ, у складі 100 осіб строком на 6 місяців. Влітку 2014 року, після загострення конфліктів, чисельність СММ в Україні було збільшено до 500 осіб, а мандат продовжений до 31 березня 2016 року. Мандат місії продовжувався кожного року, останній річний період — з 1 квітня 2021 року по 31 березня 2022 року. Після російського вторгнення в Україну, мандат СММ ОБСЄ не продовжили через позицію Російської Федерації. На той час СММ була найбільшою місією в ОБСЄ, персонал налічував 1 291 особу (814 міжнародних та 447 місцевих співробітників) [14].

Незважаючи на всі зусилля, ОБСЄ стикається з кількома проблемами у боротьбі з гібридними війнами та проксі-конфліктами. Однією з головних проблем є відсутність консенсусу серед держав-членів ОБСЄ щодо того, як вирішувати ці нові форми конфліктів. Деякі держави розглядають гібридні війни та конфлікти як новий тип війни, який потребує іншого підходу, тоді як інші стверджують, що існуючого міжнародного права та норм достатньо. Ця відмінність в підходах важко узгодити, і це може створювати перешкоди для розробки спільних стратегій та дій. Недостатня узгодженість також може призвести до того, що деякі держави не дотримуватимуться рекомендацій та рішень ОБСЄ, які вони не будуть вважати як необхідні.

Іншою проблемою є обмежені ресурси та фінансування, доступні ОБСЄ. Організація покладається на внески держав-членів, і деякі держави останнім часом скорочують свої внески. Це ускладнило ефективну діяльність ОБСЄ, особливо в зонах конфлікту. Ця проблема може призвести до того, що ОБСЄ не зможе виконувати свої функції та зобов'язання в повному обсязі. Також може бути складно залучити та зберегти належних фахівців та персонал, і забезпечити їх необхідними матеріально-технічними засоби, які допомагатимуть їм для успішного

виконання місії ОБСЄ.

На думку окремих українських посадовців, зокрема тодішнього очільника луганської ВЦА (де відбувалися бойові дії) у 2014-15 роках Геннадія Москаля, це (ОБСЄ) значною мірою паразитарне утворення від якого немає жодної користі:

«Я бачив роботу ОБСЄ, і чесно говорю, що від них, як від мінеральної води— ні користі, ні шкоди нема. Серед них дуже багато прихильників Росії. Це такий змішаний орган який імітує, що він дуже потрібний. Їм платять гарні гроші, їх страхують на випадок смерті або нещасного випадку. Я, окрім як у ресторанах, пивбарах за чаркою горілки або віскі, майже на передовій їх не бачив.» [53].

Якщо говорити про загальну характеристику місій та операцій ОБСЄ, а також іншу практичну діяльність в сфері безпеки, то організація присутня в багатьох не стабільних районах регіону.

Польові операції ОБСЄ надають приймаючим країнам допомогу у практичному виконанні взятих ними зобов'язань ОБСЄ та нарощуванні місцевого потенціалу, здійснюючи контроль конкретних проектів. До них належать ініціативи щодо підтримки діяльності правоохоронних органів, прав національних меншин, перегляду законодавства, верховенства закону та свободи ЗМІ, а також щодо просування тем терпимості та недискримінації та багатьох інших напрямків. Ряд польових структур роблять внесок у роботу у напрямі раннього попередження та запобігання конфліктам. Керуючись своїми відповідними мандатами, деякі польові операції ведуть також моніторинг розвитку подій на місцях та подають звіти. Це дозволяє їм регулювати кризи та виконувати ключову роль у пост-конфліктному відновленні. Польові операції налагоджують та підтримують численні партнерські зв'язки з адміністративними органами, відомствами та установами на місцевому та загальнонаціональному рівні, об'єднаннями громадянського суспільства, а також з міжнародними

організаціями. Наявність таких партнерських зв'язків дозволяє координувати зусилля, забезпечувати взаємодоповнюваність та підвищувати з обох сторін віддачу у тих напрямках, де ведеться спільна робота. Центр ОБСЄ із запобігання конфліктам (ЦПК) відповідає за планування процесу заснування, реструктуризацію та закриття польових операцій. ЦПК відіграє ключову роль у підтримці та координації діяльності ОБСЄ на місцях: він веде аналітичну роботу, представляє політичні рекомендації, а також є сполучною ланкою між польовими операціями, Секретаріатом та Головуванням ОБСЄ [55].

На прикладі цих місій ми бачимо одну з ключових проблем, а саме відсутність відповідальності та механізмів реагування на порушення міжнародного права та норм у контексті гібридних конфліктів. ОБСЄ має обмежені можливості для примусового втручання у події, що відбуваються у державах-членах, а також відсутність механізмів ефективного контролю та реагування на дії третіх країн у гібридних конфліктах.

Для успішного вирішення цих проблем необхідна більша співпраця та координація між державами-членами ОБСЄ. Крім того, ОБСЄ має зосередитися на збільшенні своїх ресурсів та фінансування, щоб забезпечити ефективність своєї діяльності. Важливо також розробити механізми реагування на порушення міжнародного права та норми, які б забезпечували відповідальність за дії в гібридних конфліктах.

Нарешті, для забезпечення успішної боротьби з гібридними війнами та проксі-конфліктами необхідна більш глибока інтеграція міжнародних організацій, таких як ОБСЄ, Європейський Союз та НАТО. Вони повинні спільно працювати над розробкою стратегій та механізмів реагування на нові форми конфліктів, щоб забезпечити мир та стабільність у регіонах.

На завершення зазначимо, що діяльність ОБСЄ в контексті гібридних війн і проксі-конфліктів мала б мати вирішальне значення для

сприяння миру та стабільності в Європі. Програми ОБСЄ з моніторингу, діалогу та посередництва допомогли запобігти конфліктам і пом'якшити їх наслідки. Проте ОБСЄ стикається з кількома проблемами, вирішуючи ці нові форми конфліктів, і потрібно зробити більше зусиль, щоб організація мала ресурси та політичну підтримку, все це необхідно для ефективного виконання своїх завдань.

2.3 Регіональні безпекові організації в епоху гібридних війн та проксі конфліктів

В міжнародній системі спостерігається зростання кількості гібридних війн і проксі-конфліктів, які створюють значні виклики безпеці для країн і регіонів. Регіональні організації безпеки стали вирішальними суб'єктами для пом'якшення цих загроз і забезпечення стабільності. У цьому розділі досліджується роль організацій регіональної безпеки в епоху гібридних війн і проксі-конфліктів, їхні сильні сторони й обмеження, а також виклики, з якими вони стикаються.

Колективна безпека є системою спільних дій держав світу або **певного регіону** для запобігання загроз загальному миру, придушення агресії чи інших порушень миру у світі чи регіоні. Сприймаючи систему колективної безпеки через призму ефективності, слід визнати, що:

1. Колективна безпека підвищує можливість того, що агресор зіштовхнеться з коаліцією держав, що мають переважаючу міць. Порівняно з цим без колективної безпеки агресори могли б очікувати у найгіршому випадку, приблизно рівне протистояння [22].

2. Колективна безпека створює організації, що самі по собі будуть сприяти створенню умов, сприятливих для збереження миру: шляхом надання інформації, корисної для скорочення занепокоєності стосовно

експансіоністських намірів інших держав, а також шляхом створення міжнародних форумів з обміну ідеями та зміцнення спільних цінностей [22].

3. Колективна безпека сприяє регламентуванню дилем безпеки. Держави потребують меншого наступального потенціалу в зв'язку з тим, що всі учасники колективної безпеки роблять свій наступальний внесок у перемогу над агресором. Транспарентність, що надається організаціями колективної безпеки допомагає скорочувати непевність стосовно потенціалу окремих держав, тим самим зменшується невірне тлумачення намірів та відпадає необхідність у попереджувальних заходах з превентивного нарощування сили [22].

Регіональні організації безпеки є формою багатостороннього співробітництва, яка спрямована на сприяння миру та безпеці в певній географічній зоні. Вони відрізняються за сферою діяльності, складом і функціями. Приклади включають Організацію Північноатлантичного договору (НАТО), Африканський Союз (АС) і Асоціацію держав Південно-Східної Азії (АСЕАН).

Специфічним регіоном в сфері безпеки є Європа, оскільки на її території діє декілька регіональних організацій (договорів) у сфері колективної безпеки. Це, насамперед ОБСЄ, Організація Північноатлантичного Договору (НАТО), а також Організація Договору про колективну безпеку, які носять міжрегіональний характер [42].

НАТО, як вже зазначалося, на відміну від інших організацій має досить дієвий механізм реалізації рішень, маючи у своєму розпорядженні військові можливості і інфраструктуру. Окрім того члени організації зобов'язані дотримуватися встановлених спільних технічних стандартів в їхніх військових силах. Зумовлюючи високий рівень взаємодії, Організація має у своєму розпорядженні військові ресурси, включаючи командний склад, засоби транспортування і збору інформації. Ці інституційні риси

надають НАТО можливість координувати застосування сили країнами-членами більшою мірою, ніж деякі регіональні організації з колективною безпеки позбавлені які таких механізмів. Даючи порівняльну оцінку в застосуванні механізмів підтримання миру в контексті діяльності глобальних та універсальних організацій, очевидним є розгляд з точки зору ефективності та функціональності [42].

Регіональні організації безпеки відіграють ключову роль у вирішенні цих викликів, надаючи платформу для діалогу та співпраці між своїми державами-членами, координуючи реагування на загрози безпеці та сприяючи зусиллям у запобіганні та вирішенні конфліктів. Наприклад, Організація Договору про колективну безпеку (ОДКБ) активно займається проблемами безпеки в Центральній Азії, включаючи боротьбу з тероризмом і незаконним обігом наркотиків. Однак, ефективність ОДКБ щодо цих завдань залишається під сумнівом.

У зв'язку з активізацією гібридних та проксі-конфліктів та збільшенням загроз для людини в сучасному суспільстві, ЄС також активно почав видозмінювати свою систему безпеки, хоч основою його формування були економічні фактори. Події в Югославії висвітили необхідність для ЄС докладати зусиль, спрямованих на встановлення миру поза його зоною стабільності. Завдяки інтеграційним договорам створились умови, коли війна між державами-членами ЄС не лише малоймовірна, а й неможлива [39].

Регіональні організації безпеки також мають сильні сторони, які роблять їх добре придатними для вирішення гібридних війн і конфліктів за дорученням. По-перше, вони краще розуміють місцевий контекст і динаміку, що має вирішальне значення для виявлення основних причин конфліктів і розробки відповідних заходів. По-друге, вони мають легітимність і авторитет, щоб діяти як посередники та фасилітатори мирних процесів. По-третє, вони забезпечують форум для зміцнення

довіри та впевненості між державами-членами, що має вирішальне значення для вирішення проблем безпеки, які вимагають колективних дій.

Регіональні організації безпеки також зазнають кількох проблем при вирішенні гібридних війн і конфліктів. По-перше, вони можуть стикатися з обмеженими ресурсами та можливостями, необхідними для ефективного реагування на складні загрози безпеці. Наприклад, у деяких регіональних організаціях можуть бути обмежені військові або розвідувальні можливості, що унеможлиблює їх здатність відстежувати гібридні загрози та ефективно реагувати на них. По-друге, внутрішні розбіжності або відсутність консенсусу серед держав-членів можуть стати проблемою для деяких регіональних організацій, підірвавши їх ефективність. Наприклад, Рада співробітництва Перської затоки (GCC) зіткнулася з внутрішніми розбіжностями, особливо стосовно кризи в Катарі. По-третє, регіональні організації можуть стикатися зі зовнішнім втручанням великих держав, які мають конкуруючі інтереси в регіоні, що ускладнює зусилля щодо врегулювання конфлікту.

У цілому оцінка характеру можливих загроз, передусім гібридних, повинна спиратися на такі висновки: по-перше, зростає небезпека внутрішньодержавних конфліктів; по-друге, не варто забувати про можливі вибухи у майбутньому міждержавних воєн на Європейському континенті; по-третє, зберігається загроза для всіх держав за межами Європейського континенту, головним чином, з боку тоталітарних режимів Близького Сходу й Азії та дій Російської Федерації. З'явилися й нові виклики та загрози стабільності та сталому соціально-економічному розвитку в суспільстві [39].

Політична наука застосувала системний аналіз для дослідження механізмів регіональної безпеки і розробки її окремих компонентів, включаючи військово-політичні, соціально-економічні, соціальнокультурні, політико-інституційні та інші, зосереджуючи

пріоритетні дослідження на державно-політичних інститутах та системі забезпечення національної безпеки. Протягом «холодної війни» більшість принципово важливих, фундаментальних теоретичних аспектів зазначеної проблеми не мали вичерпного пояснення, адекватного реаліям ядерного протистояння, внаслідок чого значна увага надавалася пошуку доказів, що прихильність ідеалам миру визначає саме природа окремих громадянських суспільств [41].

Традиційна парадигма регіональної безпеки була зосереджена на військовому вимірі безпеки з упором на територіальну оборону та запобігання міждержавним конфліктам. Однак для гібридних війн і проксі-конфліктів характерне поєднання звичайних і нетрадиційних засобів, включаючи кібератаки, пропаганду, дезінформацію та використання нерегулярних сил. Ці складні виклики безпеці вимагають нової парадигми регіональної безпеки, яка є більш комплексною та гнучкою.

Однією з нових парадигм регіональної безпеки є концепція безпеки людини. Людська безпека наголошує на захисті окремих людей і спільнот від широкого кола загроз, включаючи економічну незахищеність, погіршення стану навколишнього середовища та порушення прав людини. Цей підхід визнає, що традиційні загрози безпеці часто взаємопов'язані з іншими нетрадиційними викликами безпеці, і що вирішення цих взаємопов'язаних загроз вимагає цілісного підходу. Наприклад, Асоціація держав Південно-Східної Азії (АСЕАН) прийняла підхід до безпеки людини, який зосереджується на сприянні економічному зростанню, соціальному розвитку та екологічній стійкості.

До країн з колективними моделями регіональної безпеки можна віднести більшість країн-учасниць Північноатлантичного альянсу, АНЗЮС, АСЕАН, з певними обмеженнями держави Африканського Союзу тощо. [41].

Ще однією новою парадигмою регіональної безпеки є концепція кооперативної безпеки. Кооперативна безпека наголошує на необхідності регіональної співпраці та діалогу для вирішення викликів безпеці. Цей підхід визнає, що загрози регіональній безпеці часто є транснаціональними і вимагають колективних дій. Наприклад, Шанхайська організація співробітництва (ШОС) працює над усуненням загроз безпеці в Центральній Азії через співпрацю в боротьбі з тероризмом, торгівлею наркотиками та кібербезпекою.

Третьою новою парадигмою регіональної безпеки є концепція стійкості. Стійкість підкреслює здатність суспільства та інституцій протистояти загрозам безпеці та відновлюватися від них. Цей підхід визнає, що загрози безпеці часто непередбачувані та можуть мати каскадний вплив на кілька доменів. Наприклад, Європейський Союз (ЄС) прийняв підхід, заснований на стійкості до гібридних загроз, включаючи кіберзагрози, дезінформацію та енергетичну безпеку.

Ці нові парадигми регіональної безпеки мають кілька сильних сторін. По-перше, вони визнають взаємозв'язки між традиційними та нетрадиційними загрозами безпеці та забезпечують більш комплексний підхід до вирішення проблем безпеки. По-друге, вони наголошують на важливості регіонального співробітництва та діалогу у боротьбі із загрозами безпеці, що є критично важливим в епоху складних викликів безпеці, які часто вимагають колективних дій. По-третє, вони наголошують на важливості стійкості до загроз безпеці, яка є важливою у світі, де загрози безпеці часто непередбачувані та можуть мати каскадні наслідки.

Негативним фактором є те, що регіональні безпекові організації можуть вступити у протистояння між собою.

Тривала напруга між групами породжує постійну гонку озброєнь, яка обтяжує членів групи і збільшити ризик розповсюдження на інших.

Така напруга створює умови коли важко впоратися з більш універсальними компонентами загрози у кооперативний спосіб. Будь-яке тривале протистояння також має тенденцію залучати інших гравців до гри з такими ж ролями з нульовою сумою. Під час холодної війни ціною уникнення прямого конфлікту між блоками в Європі були оплачені, не в останню чергу, серією «проксі-війн» в інших місцях між країнами чи територіями, нестабільний стан розвитку яких спричинив те що ми маємо сьогодні. [23].

Однак ці нові парадигми регіональної безпеки також є проблемними і дискусійними. По-перше, їм може бракувати необхідних ресурсів і можливостей для протидії складним загрозам безпеці. По-друге, вони можуть зіткнутися з протидією з боку акторів, які мають особистий інтерес у збереженні незахищеності та нестабільності в регіонах. Нарешті, вони можуть зіткнутися з внутрішніми розбіжностями між державами-членами, що може підірвати їх ефективність.

Підсумовуючи, регіональні організації безпеки відіграють важливу роль у вирішенні гібридних війн і проксі-конфліктів. Вони забезпечують платформу для діалогу та співпраці, краще розуміють місцевий контекст і можуть діяти як посередники та фасилітатори мирних процесів. Однак вони також стикаються з кількома проблемами, включаючи обмеження ресурсів, внутрішні розбіжності та зовнішнє втручання. Вирішення цих проблем вимагатиме більшої співпраці та координації між регіональними організаціями, а також підтримки з боку великих держав. Зрештою, ефективність регіональних організацій безпеки у вирішенні гібридних війн і проксі-конфліктів залежатиме від їх здатності адаптуватися до викликів безпеки, що розвиваються, і працювати разом, щоб просувати мир і стабільність у відповідних регіонах.

На завершення зазначимо, що в епоху гібридних війн і проксі-конфліктів потрібні нові парадигми регіональної безпеки. Ці парадигми,

які включають безпеку людини, безпеку на основі співпраці та стійкість, забезпечують більш комплексний підхід до вирішення проблем безпеки та підкреслюють важливість регіональної співпраці та діалогу. Однак вирішення цих викликів вимагатиме більших ресурсів, можливостей і політичної волі від регіональних гравців і міжнародної спільноти. Зрештою, ефективність цих нових парадигм регіональної безпеки залежатиме від їх здатності адаптуватися до нових викликів безпеці та сприяти стабільності та миру в регіонах.

РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ-КОНФЛІКТІВ

3.1 Системи національної безпеки країн-членів НАТО при протидії гібридній агресії

Організація Північноатлантичного договору завжди мала вагомую роль у забезпеченні безпеки, переважно в Європі. Явно очевидним є той факт, що з моменту свого заснування до кінця холодної війни головним завданням, що стояло перед Північноатлантичним альянсом, було стримування Радянського Союзу. Однак після закінчення холодної війни, НАТО почало проходити трансформацію відповідно до нових викликів, що постали.

Безсумнівно, більшість держав-учасниць Північноатлантичного договору мали власні інтереси в продовженні існування цього військово-політичного блоку. Наприклад, для Сполучених Штатів Америки НАТО виявився ефективним засобом участі у забезпеченні безпеки європейських країн. Розпад такої потужної країни, як Радянський Союз, кардинально змінив баланс сил у Європі. В таких умовах американський естеблішмент не міг дозволити собі відмовитися від платформи впливу на процес забезпечення безпеки на європейському континенті. З свого боку, країни Західної Європи очевидно розглядали НАТО як гаранта безпеки в період політичних перетворень.

Динамічний характер загроз безпеці та еволюція стратегій ведення війни примусили європейські країни переглянути свої системи національної безпеки. Гібридна агресія, що включає різноманітні військові тактики, кібервійну, кампанії дезінформації та підривну діяльність, представляє собою складний виклик, на який потрібно реагувати комплексно. Усвідомлюючи потребу в спільних діях, європейські країни використовують рамки співпраці в межах НАТО для посилення своїх

систем національної безпеки та зміцнення своєї здатності ефективно протистояти гібридній агресії.

З метою вдосконалення колективної і національної стійкості, НАТО застосовує широке коло інструментів, одним з яких є проведення регулярних оцінювань. Оцінювання є необхідними для визначення галузей, в яких було досягнуто поступу, поряд із викликами, що належить розв'язати. Із ухваленням у 2022 році Аналізу стійкості за поточний рік, у рамках НАТО розпочато новий цикл планування і огляду у галузі стійкості. В Аналізі наведено оцінку стану колективної стійкості загалом в Альянсі, а також викладено здобутки щодо виконання вимог у семи базових галузях. Виходячи з висновків Аналізу, розроблятимуться заходи, спрямовані на усунення виявлених недоліків і вдосконалення стійкості на рівні Альянсу [2].

Доктрина колективної оборони НАТО, що ґрунтується на засадах спільної оборони, є важливою платформою для європейських країн у вирішенні спільних проблем безпеки. Стаття 5 Альянсу, яка закріплює принцип нападу на одного члена як напад на всіх, є невід'ємною частиною доктрини колективної оборони НАТО. У боротьбі з гібридною агресією НАТО створює основу для координації, обміну розвідувальною інформацією та спільного оперативного планування між державами-членами, забезпечуючи єдину відповідь на гібридні загрози.

В офіційних документах щодо діяльності НАТО згадуються «кризи», а саме таке визначення може підпадати під гібридні загрози, тому в деяких джерелах літератури під «кризами» потрібно розуміти саме гібридний конфлікт на ранніх етапах.

Запобігання і врегулювання криз є одним із трьох основоположних завдань НАТО. У Стратегічній концепції від 2022 року наголошується, що держави – члени Альянсу поділяють зацікавленість у тому, щоб сприяти стабільності і разом розв'язувати конфлікти за допомогою НАТО. Альянс

готовий запобігати і реагувати на кризи у разі, якщо ті можуть потенційно позначатися на безпеці його членів. Запобігання кризам – це реалістичний спосіб сприяння стабільності і безпеці Альянсу. НАТО віддана виконанню завдання із запобігання кризам, зокрема, шляхом запровадження програм підготовки і розбудови потенціалу, завдяки яким держави-партнери стають більш вправними, безпечнішими і краще підготовленими реагувати на кризи, як у своїх країнах, так і за кордоном. На рахунку НАТО десятиріччя здобутків у галузі розбудови оборонних установ і розвитку потенціалу спільно з партнерами, як по сусідству з НАТО, так і більш віддаленими. Спроможності і досвід НАТО у галузі врегулювання криз є унікальними й охоплюють координацію, проведення, підтримку і забезпечення багатонаціональних операцій із врегулювання криз [2].

У сучасних безпекових умовах актуальність забезпечення стійкості НАТО настільки зросла, що дедалі частіше пропонується розглядати її як окремий напрям діяльності Альянсу на додаток до колективної оборони, кризового менеджменту та співробітництва у сфері безпеки [33].

Визнаючи мінливий ландшафт безпеки, НАТО адаптувала свої стратегії для ефективною відповіді на гібридну агресію. Альянс посилив свої можливості, інтегрувавши кіберзахист, інформаційні операції та підвищення стійкості до свого оборонного планування. Ініціатива НАТО «Посилена передова присутність» (eFP), наприклад, розгортає багатонаціональні бойові групи в країнах-членах Східної Європи для забезпечення стримування та реагування на гібридні загрози.

Європейські країни розробили комплексні рамки політики, які відповідають цілям НАТО та вирішують складні питання гібридною агресії. Ці рамки підкреслюють інтеграцію військових, дипломатичних, економічних та інформаційних інструментів для забезпечення національної безпеки. Вони також підкреслюють важливість міжвідомчої координації, співпраці з НАТО та співпраці з іншими європейськими

партнерами для підвищення стійкості та можливостей реагування.

Враховуючи значну роль кібероперацій у гібридній агресії, європейські країни надають пріоритет розробці надійних заходів кібербезпеки. Системи національної безпеки створили спеціалізовані підрозділи кіберзахисту, покращили механізми обміну інформацією та збільшили інвестиції в дослідження та розробки для ефективної боротьби з кіберзагрозами. Співпраця в рамках НАТО сприяє обміну найкращими практиками та гармонізації стандартів кібербезпеки в європейських країнах.

Одним із найбільш уразливих місць НАТО вважається кіберпростір. Стрімкий розвиток інформаційних технологій значно ускладнює роботу спецслужб та інших державних органів щодо захисту від кібератак, а також вимагає постійного пошуку нових засобів захисту елементів військової та цивільної інфраструктури. З метою вирішення цієї проблеми у рамках НАТО вжито наступних заходів:

- створені команди кіберреагування;
- підписано Меморандум про порозуміння між Альянсом і окремими його країнами-членами щодо забезпечення захищених підключень для обміну інформацією і врегулювання криз;
- Центр передового досвіду з кіберзахисту НАТО активізував діяльність у напрямку розвитку спеціальних можливостей щодо протидії шкідливим програмам та підготовки фахівців відповідного рівня;
- налагоджується співпраця між Альянсом і малими та середніми компаніями-розробниками кібертехнологій, які часто найбільш інноваційні в цій сфері;
- у ході саміту НАТО у Варшаві був підписаний документ під назвою «Зобов'язання щодо кіберзахисту», згідно з яким країни-члени

Альянсу підтвердили курс на розвиток сил і засобів з метою зміцнення загальної стійкості організації [7].

Побудова стійкості суспільства та протидія кампаніям з дезінформації є ключовими компонентами систем національної безпеки європейських країн. Інвестуючи в освіту, кампанії з підвищення обізнаності громадськості та програми медіаграмотності, ці країни прагнуть пом'якшити вплив гібридних загроз на громадську думку. В рамках НАТО стратегічні комунікаційні зусилля спрямовані на протидію дезінформації, сприяння прозорості та зміцнення довіри громадськості до демократичних інститутів.

Враховуючи те, що Вашингтон протягом багатьох років активно підтримує ідею про те, що НАТО має залишатися головним консультативним форумом у питаннях безпеки серед союзників (тобто і в питаннях європейської безпеки), і протидіє будь-яким політичним рішенням, які можуть завдати шкоди альянсу, Європейсько-американське співробітництво у сфері протидії гібридним загрозам та підвищення рівня національної безпеки в цьому секторі неминуче зводиться насамперед до союзницьких відносин у рамках Північноатлантичного договору.

У контексті реалізації «Плану дій НАТО щодо забезпечення готовності» ще у грудні 2015 р. міністри закордонних справ країн Альянсу ухвалили нову Стратегію реагування на прояви гібридної війни, основні положення якої передбачають:

- удосконалення обміну розвідувальними даними і механізмів раннього попередження для прогнозування і фіксування гібридної воєнної діяльності (передусім, з боку РФ);

- використання державними та недержавними суб'єктами у протистоянні гібридним загрозам широкомасштабних і тісно поєднаних між собою традиційних та нетрадиційних засобів, відкритої та прихованої військової сили, воєнізованих формувань та заходів цивільного характеру;

- розроблення набору показників раннього попередження для опрацювання різних варіантів реагування на кризові ситуації;

- можливість прийняття Північноатлантичною радою НАТО рішення про приведення у дію статті 5 Вашингтонського договору для протидії гібридній війні у рамках колективної оборони;

- продовження ефективної співпраці та координації зі своїми партнерами та відповідними міжнародними організаціями (зокрема, ЄС), відповідно до домовленостей, спрямованих на протидію гібридній війні [8].

Щодо співпраці між НАТО та ЄС можна сказати, що вона перебуває на етапі розвитку, але відомі приклади спільних дій. Наприклад, Європейський Союз та НАТО одночасно впроваджували концепцію сил швидкого реагування. У межах ЄС були створені так звані бойові групи, які склалися з до 1500 осіб, а в рамках Північноатлантичного альянсу – сили реагування НАТО. Ще одним наочним прикладом є досвід обох організацій у Дарфурі (Судані). Однак, замість об'єднання зусиль, діяльність ЄС та НАТО супроводжувалась дублюванням функцій та політичною конкуренцією. Іншими словами, різне бачення ролі цих організацій виконанні певних завдань заважає розкриттю потенціалу тісної взаємодії між ЄС та НАТО.

Але, процес співпраці між цими двома організаціями ускладнюються іншими факторами. По-перше, не всі члени Європейського Союзу мають членство в Північноатлантичному альянсі. Звичайно, більшість з таких країн можуть брати активну участь в обговоренні питань забезпечення європейської безпеки в рамках офіційних зустрічей на різних рівнях та постійно діючих структур, створених для здійснення активної співпраці між ЄС та НАТО. Проте деякі з цих країн, зокрема Мальта та Кіпр, просто позбавлені можливості брати активну участь у процесі забезпечення безпеки на Європейському континенті. Справа в тому, що ці країни

приєдналися до ЄС у 2004 році і не мають угод про обмін секретною документацією з НАТО. Так, представники цих країн беруть участь в обговореннях з питань безпеки на неофіційних зустрічах, але варто визнати, що такий стан справ не є ідеальним [5].

Підсумовуючи, системи національної безпеки європейських країн, засновані на їхньому співробітництві в рамках НАТО, є вирішальними у протидії гібридній агресії. Завдяки механізмам колективного захисту, комплексній політиці, надійним заходам кібербезпеки та стратегічним комунікаційним зусиллям європейські країни розробили стійкі та адаптивні системи для протидії викликам, пов'язаним з гібридними загрозами. Інтеграція ресурсів, досвіду та розвідки в рамках НАТО зміцнює їхню готовність і покращує їхню колективну відповідь на гібридну агресію, захищаючи їхню національну безпеку та сприяючи регіональній стабільності.

3.2 Системи національної безпеки позаблокових країн при протидії гібридній агресії

Міжнародні організації і союзи держав, які згадувалися вище, погоджуються з тим, що розбудова національної безпеки в секторі протидії гібридній агресії є сферою відповідальності держав, які мають самостійно визначати цілі й пріоритети на цьому напрямі. Нині держави використовують різні практики у сфері забезпечення національної безпеки, що зумовлено відмінностями їхніх національних інтересів, умов та особливостей розвитку [21].

У світі, що стає все більш сприятливий до глобалізації, системи національної безпеки країн, що не приєдналися до блоків та альянсів, стикаються з унікальними викликами під час протидії гібридній агресії. Гібридна агресія означає поєднання звичайних і нетрадиційних методів,

які використовуються державними та недержавними суб'єктами для підриву суверенітету та стабільності нації-мішені. Позаблокові країни, які зберігають нейтральну позицію в глобальній динаміці сил і альянсах, часто виявляються вразливими до гібридної агресії через обмежений військовий потенціал і залежність від міжнародного співробітництва.

Дослідження специфіки формування державної політики щодо забезпечення національної безпеки та стійкості в умовах гібридних війн та проксі-конфліктів, а також аналіз особливостей створення відповідних систем у різних країнах, таких як Індія, Фінляндія (до вступу в НАТО), Сінгапур, Австрія, Швейцарія, Швеція, Нова Зеландія, Ірландія, Австралія, Нова Зеландія, Велика Британія, Нідерланди, Японія та інші, дозволило виявити низку спільних рис і відмінностей у цих процесах.

Індія, як видатна позаблокова країна, розробила надійну систему національної безпеки для протидії гібридній агресії. Країна стикається зі складним середовищем безпеки, яке характеризується загрозами, починаючи від транскордонного тероризму до кібервійни. Індійська доктрина національної безпеки надає пріоритет багатовимірному підходу, який об'єднує військові, дипломатичні, економічні та технологічні аспекти. Наприклад, Індія створила комплексну розвідувальну мережу для виявлення та реагування на гібридні загрози в режимі реального часу, використовуючи як людський інтелект, так і передові технології спостереження.

Щоб протистояти гібридній агресії, Індія зосередилася на посиленні своїх кіберспроможностей. Країна інвестувала в розробку надійної інфраструктури кібербезпеки для захисту критично важливих інформаційних мереж від кібератак. Індія також бере активну участь у двосторонніх і багатосторонніх партнерствах для покращення обміну інформацією та співпраці у протидії гібридним загрозам. Крім того, зусилля Індії з оборонної модернізації зосереджені на розробці передових

технологій і систем спостереження для виявлення та нейтралізації нетрадиційних загроз.

Приклад протистояння гібридній агресії Індія має в результаті довготривалого конфлікту з Пакистаном.

Витоки конфлікту сягають ще 1947 року, коли князівство Дхамму і Кашмір ділили між Індією і Пакистаном. Більшість колишня британської території відійшла до Індії. Проблема полягала в тому, що її населяли здебільшого мусульмани, які тяжіли до Ісламабаду, але тодішній очільник Кашміру був індуїстом і приєднав князівство до Індії. З того часу етнічні та релігійні конфлікти тут не вщухають [12].

Щодо гібридної складової конфлікту то тут вона проявляється найбільш точно. Повномасштабно воюють поки що кібер-війська. Хакери з Пакистану атакували майже сотню урядових сайтів та критично важливі системи інфраструктури Індії. Індія не забарилась з відповіддю – її кібер-солдати завдали аналогічної атаки по сусідній країні. Поки що особливих втрат, принаймні, так твердять чиновники обох країн, всі ці атаки не завдали. Але факт залишається фактом. До того ж вони заявляють про елементи гібридної війни – поряд з атаками хакерів відбувся сплеск активності тролів в інтернет-просторі: у соцмережах та на сайтах новин з'явилися різноманітні і суперечливі повідомлення про атаки, бої, колосальні втрати, відставки політичних та військових керівників. Обидві країни явно вивчали досвід російсько-української війни, коли дії військових на фронті завжди координуються з діями бото-ферм в інтернет-просторі та супроводжуються потужною медіа-кампанією. Поки що конфлікт зайшов у стадію загострення, обидві сторони “грають м'язами”, але разом з цим демонструють готовність сісти за стіл переговорів. Коли і чим закінчиться чергове загострення у штаті Дхамму і Кашмір, поки прогнозувати важко [12].

Фінляндія, країна яка до 2023 року була позаблоковою, сформулювала комплексну систему національної безпеки, яка ефективно протидіяла гібридній агресії. Як сусід Росії, Фінляндія стикається з унікальними проблемами через складну геополітичну динаміку в регіоні. Стратегія безпеки Фінляндії поєднує стримування, стійкість і співпрацю як ключові елементи протидії гібридним загрозам.

Авжеж, у зв'язку з вступом країни в НАТО система національної безпеки буде змінюватися, буде йти інтеграція елементів протидії гібридній агресії в сторону координації з Альянсом, але до вступу Фінляндія приділила значну увагу заходам із підвищення стійкості, щоб пом'якшити вплив гібридної агресії. Це включає в себе розробку надійної системи стійкості суспільства, яка передбачає співпрацю між урядовими установами, організаціями приватного сектору та громадянським суспільством. Фінляндія також інвестувала у вдосконалення своїх можливостей кібербезпеки для захисту критичної інфраструктури від кібервторгнень. Активна участь країни в міжнародних організаціях, таких як Європейський Союз і НАТО, наприклад програма «Партнерство заради миру», дозволяє їй користуватися перевагами механізмів колективної безпеки та платформ обміну інформацією.

Ще у 2016 році Комітет національної безпеки в уряді Фінляндії оновив список дій, які він вважає загрозливими та ймовірними методами гібридної війни. Раніше фінські військові традиційно вважали найбільшими загрозами національній безпеці тероризм і війну з іншими країнами [18].

Сінгапур, позаблокова країна, розташована в геополітично нестабільному регіоні, розробила комплексну систему національної безпеки для протидії гібридній агресії. Визнаючи взаємопов'язаний характер гібридних загроз, підхід Сінгапуру до безпеки поєднує військове стримування, ефективне управління та стратегічне партнерство.

Сінгапур інвестував значні кошти в можливість збору та аналізу розвідувальних даних, щоб швидко виявляти гібридні загрози та реагувати на них. Країна також розробила передові заходи кібербезпеки для захисту критичної інфраструктури, боротьби з кампаніями дезінформації та забезпечення цілісності інформаційних мереж. Сінгапур бере активну участь у регіональних форумах з питань безпеки та військових навчаннях, щоб покращити оперативну сумісність зі своїми партнерами та обмінятися передовим досвідом у протидії гібридній агресії.

Наприклад, Сінгапур та Україна співпрацюють в сфері кібербезпеки, ще у 2018 році Міністр внутрішніх справ України Арсен Аваков та віцепрем'єр-міністр з питань нацбезпеки Сінгапуру Тео Чі Хін домовилися про співпрацю між кіберполіцейськими двох країн. Також Аваков повідомив, що провів зустріч із міністром внутрішніх справ Сінгапуру Касівісванатаном Шанмугамом, в ході якої були обговорені спільні гібридні загрози у сучасному світі та досягнуто домовленості про спеціальну співпрацю підрозділів кіберполіції [17].

Географічне розташування та політичний ландшафт **Австрії** роблять її сприйнятливою до тактики гібридної війни. Розташована в серці Європи, Австрія є важливим транзитним вузлом і мостом між Західною та Східною Європою. Її історичні та культурні зв'язки з різними сусідніми країнами роблять країну вразливою до кампаній впливу та дезінформації, спрямованих на використання розбіжностей у суспільстві. Крім того, залежність Австрії від критичної інфраструктури та її статус фінансового центру роблять її потенційною мішенню для кібератак та економічного примусу.

Безпекова політика Австрії базується на Стратегії національної безпеки, яка була прийнята в 2013 році. Її основною метою є забезпечення суверенітету та територіальної цілісності держави, надання допомоги з боку військових інституцій цивільній владі та участь в кризовому

врегулюванні закордоном в рамках миротворчих операцій. Міграційна криза та близькість до Балкан (одного з основних коридорів руху мігрантів-біженців до Європи) вимагає від Австрії підвищеної уваги до контролю за національними кордонами, а в умовах протистояння нетрадиційним методам війни, країна має більше уваги приділяти цьому питанню [38].

Оборонна стратегія **Швейцарії** окреслюється низкою документів 2016 року. У травні 2017 року в контексті визначення актуальних загроз була оприлюднена доповідь швейцарської розвідки. В серпні парламент країни схвалив нову доповідь, в якій визначались пріоритети національної безпекової та оборонної політики. У порівнянні з попереднім документом, датованим 2010 роком, підвищена увага приділяється погіршенню відносин Росії та Заходу внаслідок гібридної війни, зростанню російського військового потенціалу, посиленню терористичної та кіберзагроз, міграційній кризі в Європі, розвитку технологій гібридних війн. В доповіді підкреслюється, що сучасні загрози стали різноманітнішими та менш передбачуваними. Найактуальнішою проблемою для Швейцарії залишається міграційна криза. У цьому контексті деякі політики наголошують на необхідності зміни пріоритетів при формуванні безпекової політики на користь підтримки поліцейських та прикордонних сил, а не армії. Ще одним важливим завданням в сфері національної безпеки є виявлення серед населення країни прибічників терористичних угруповань та боротьба з вербувальниками терористів. Пряма терористична загроза Швейцарії знаходиться на низькому рівні, оскільки країна не є пріоритетною ціллю джихадистів. Російська агресивна політика теж напряму не загрожує Швейцарії, втім її вплив на міжнародне середовище представляє довготривалий вимір стратегічного оточення держави. Швейцарські експерти вважають, що наслідки конфронтації РФ та Заходу залишатимуться актуальними протягом десятиліть. Основним

завданням швейцарських збройних сил визначається оборона території держави та обмежена участь в миротворчих операціях [38].

Швеція, країна, відома своєю відданістю нейтралітету, стикається з серйозними проблемами у підтримці національної безпеки в епоху, позначену поширеністю гібридної війни. Прецедент той самий, що і з Фінляндією, а саме вступ в НАТО, тому тут будуть розглядатися, саме аспекти національної безпеки Швеції в позаблоковому стані.

Гібридні загрози також займають важливе місце в порядку денному безпеки в Швеції. Країна наражається на загрози сірої зони породжені недержавними та державними суб'єктами, пов'язані, наприклад, із діяльністю впливу салафітів/джихадистів, кампанії з дезінформації, кібератаки та операції економічного впливу. У результаті країна поступово почала покращувати свої можливості соціальної стійкості. У 2018 році Швеція призначила свого першого спеціального уповноваженого з питань протидії гібридним загрозам у Міністерстві закордонних справ. Завдання уповноваженого полягають у координації діяльності МЗС щодо гібридної агресії, аналізуючи наслідки середовища гібридних загроз для зовнішньої політики та політики безпеки, представлення Швеції в міжнародному співробітництві та обговоренні питань протидії гібридним загрозам, а також є частиною внутрішньодержавної координації з метою розуміння та протидії гібридним загрозам (Löjdquist, 2019). Інші країни, як-от Фінляндія, зробили подібні кроки. Ці дії є важливими, оскільки вони допомагають координувати дії у відповідь і подолати розбіжності, особливо коли технології гібридних загроз за визначенням створені для того, щоб ускладнити скоординовані контрзаходи. Наприклад, шведське дослідницьке співтовариство також отримало підтримку у проведенні політичних досліджень, аналізу і спостережень щодо гібридних загроз. Тут ключовим є створення Центру досліджень асиметричних загроз

(CATS) у складі Центру соціальної безпеки Національного університету оборони (CATS, 2021). Як ключовий елемент у протидії гібридним загрозам дослідницька спільнота відіграє важливу роль у підвищенні обізнаності та підтримці заснованих на знаннях прийняття рішення в цій сфері [45].

Позаблокові країни стикаються з особливими проблемами під час протидії гібридній агресії через свою нейтральну позицію та обмежений військовий потенціал. Однак за допомогою комплексних систем національної безпеки ці країни можуть ефективно боротися з багатовимірною природою гібридних загроз. Використовуючи розвідувальні мережі, покращуючи можливості кібербезпеки, зміцнюючи стійкість і залучаючись до стратегічних партнерств, країни, що не входять у блоки, можуть розробити надійний захист для оборони своїх інтересів національної безпеки у все більш складному та взаємопов'язаному світі.

3.3 Засоби та інструменти протидії гібридній агресії та запобігання проксі-конфлікту в структурі національної безпеки України

Очевидним є той факт, що сьогодні, в епоху глобальних викликів і загроз, світ переживає новий етап геополітичного протиборства між провідними країнами світу за ресурси, комунікації, ринки збуту, розширення сфер впливу та інше. Можна з упевненістю сказати, що Україна зразка 2013-2014 років не була готова до викликів гібридної війни, оскільки отримані внаслідок розпаду СРСР у 1991 році можливості рік за роком Україна втрачала, не маючи рішучості покінути із радянським минулим, передусім у сфері державного управління. Все це призвело до зависання в певному «пострадянському вакуумі». Така нерішучість призвела до того, що в Україні за допомогою агентів впливу,

тобто певних манипуляторів, у науковій та блогосфері стали поширюватися різноманітні інтерпретації концепції «failed state», в якій усіляко із застосуванням маніпулятивних технологій обґрунтовується неможливість реалізації Україною свого суверенітету, і фактично готувалась наукова та теоретична база для доведення факту неспроможності України та української політичної нації мати власну незалежну та суверенну соборну державу. Тому будь-які анексії та паради суверенітетів або сепаратизмів трактуються як природна відповідь на неспроможність державної влади України управляти всією країною, задовольняти національні інтереси, а не потреб окремих осіб з числа олігархату [32].

Все це призвело до того, що у 2014 році проти України був застосований метод гібридної війни з боку Російської Федерації. Ця боротьба триває і на сьогоднішній день [32].

Гібридна агресія та проксі-конфлікти створюють значні виклики національній безпеці, вимагаючи ефективних засобів та інструментів протидії таким загрозам. Україна, розташована на геополітичному роздоріжжі, стикалася з численними випадками гібридної за останні роки. Після аналізу російської гібридної агресії (з 2014 року до сьогодні) можна дійти висновку, що вона є гібридною за своїм характером і змішаною за діями, технікою та методами, зміною ролі цивільного населення, місцевих громадських рухів і політичних організацій та перетворення їх на активних учасників вимушеного протистояння.

Перш ніж загострювати увагу на конкретних викликах, які стоять перед Україною, треба дати визначення даних понять, та описати їх структурні елементи. Законодавче визначення поняття національної безпеки наводиться у однойменному Законі України «Про Національну безпеку України», за яким під даним терміном розуміють захищеність державного суверенітету, територіальної цілісності, демократичного

конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Тобто ми можемо побачити, що національна безпека України є багатокомпонентним та багатоаспектним поняттям, і для її активної практичної реалізації повинні тісно співпрацювати майже всі внутрішні та зовнішні державні системи [52].

Однак, важливою складовою російсько-української гібридної війни є не лише використання Російською Федерацією військової стратегії зі знищення української державності, але й систематичне руйнування політичних інститутів України. Це створює загрозу для національної безпеки країни. Більше того, Росія активно проникала в українські владні структури та активно здійснювала політику рекрутингу в армії та спецслужбах.

Говорячи про самі методи, інструменти та рекомендації, щодо покращення системи національної безпеки, зараз будуть наведені конкретні приклади секторів національної безпеки які можуть бути зв'язані з відбиванням гібридної агресії.

Покращення служб зовнішньої розвідки і ситуаційна обізнаність.

Україна визнає критичну роль розвідки та ситуаційної обізнаності у протидії гібридній агресії. Посилення розвідувальних можливостей, у тому числі розвідувальних мереж, сигнальної розвідки та розвідки на основі відкритих джерел (OSINT), дозволяє своєчасно виявляти та оцінювати гібридні загрози. Відстежуючи дії супротивників, аналізуючи їхні наміри та виявляючи вразливі місця, Україна може активно реагувати на потенційні гібридні атаки чи «тригери» проксі-конфлікту.

При своєчасному розкритті планів підготовки гібридної війни з метою протидії формується відповідна довгострокова військово-політична стратегія, створюється **спеціальний національний (коаліційний) орган для координації зусиль розвідки** на всіх рівнях, від стратегічного до тактичного, виробляються принципові підходи щодо ефективного та

прихованого використання сил спеціальних операцій і нанесення ударів високоточною зброєю. Ретельно визначаються райони, які можуть бути охоплені гібридною війною, попередньо вивчаються всі їх характеристики. При плануванні та організації розвідки важливо розуміти, що в сучасних умовах перемога у війні не обов'язково полягає в повному розгромі збройних сил протилежної сторони, в їх фактичному знищенні або взятті в полон, окупації або встановленні тотального контролю над територією противника. Сенс гібридної війни полягає в дезінтеграції військового організму держави-жертви агресії, в руйнуванні основних елементів державної влади, в досягненні тотального контролю над свідомістю населення, що вимагає наявності централізованої системи протидії цьому виду конфлікту. Синергетичний ефект застосування гібридних загроз обумовлює їх особливу небезпеку для всієї системи забезпечення національної безпеки країни, що вимагає своєчасного розкриття загроз розвідкою на основі науково обґрунтованого прогнозування сенсу і цілей дій противника, визначення сил та засобів гібридної агресії, об'єктів впливу загроз. Головне завдання полягає у своєчасному розкритті підготовчих заходів супротивника по розв'язуванню гібридної агресії, комплексу гібридних загроз, які планується використати для підривання безпеки країни. Успішне рішення головної задачі опирається на комплекс розвідувальних завдань, що стоять перед усіма видами розвідки і контррозвідки. Завдання охоплюють сфери діяльності супротивника, в яких формуються стратегії підривних дій, створюються необхідні ресурси, встановлюються канали зв'язку і взаємодії. Загальна цільова установка по руйнуванню держави-жертви агресії розробляється і узгоджується країною-агресором на рівні урядових органів, керівництва транснаціональних корпорацій, фінансово-банківських структур, окремих впливових осіб. Тому, важливим завданням розвідки є добування планів дій країни-агресора з дестабілізації

адміністративно-політичної, соціально-економічної і культурно-світоглядної сфер, які передбачають створення на території країни-жертви розподілених мережевих структур з високою мірою самостійності і здатністю до самосинхронізації, каналів їх забезпечення : фінансових, матеріально-технічних, інформаційних, кадрових, створення складів зброї, боєприпасів, засобів зв'язку, підбирання місць для підготовки бойовиків тощо. Також важливим завданням розвідки є виявлення умов підготовки спецоперацій противника, спрямованих на прискорення процесів розвалу держави і замаскованих під дипломатичні демарші, економічні санкції, інформаційні «вкидання», диверсійні акти проти важливих об'єктів [16].

Створення Україною Спільного розвідувального центру у 2019 році покращило координацію розвідки та співпрацю між різними силовими відомствами. Цей централізований розвідувальний центр покращує обізнаність про ситуацію в країні, забезпечуючи більш ефективну відповідь на гібридні загрози.

Окреме питання це діяльність російських розвідувальних служб на території України, яка має на меті діяти відразу по декількох напрямках, це і збір інформації з обмеженим доступом, вербування місцевого населення, підривна діяльність. Дієво протидіяти цьому можна буде коли Служба безпеки України трансформується у виключно контртерористичний та контррозвідувальний орган, по прикладу хоча би британської MI5, яка займається виключно 3 функціями: боротьба з тероризмом, шпіонажем та розповсюдженням зброї масового ураження. Таким чином цілком слушною є ідея виведення зі складу СБУ підрозділу «К» (Головне управління боротьби з корупцією та організованою злочинністю), з передачею повноважень даного відділу ДБР, Національній поліції чи новоствореному Бюро економічної безпеки. Це зменшить кількість кадрів, фінансування, та сфокусує СБУ дійсно на нагальних проблемах, а не на питаннях господарських злочинів [52].

Кібербезпека та інформаційні операції.

Гібридна агресія часто включає кіберпростір та інформаційні операції для маніпулювання громадською думкою, поширення дезінформації та порушення критичної інфраструктури. Україна визнає важливість надійних заходів кібербезпеки та активних інформаційних операцій для протидії гібридним загрозам.

Використання кіберпростору як виміру асиметричної агресії є явищем порівняно новим і менш опрацьованим з точки зору розуміння рівня загроз та можливої протидії. Як відзначає Д.Дубов, начальник відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, дискусія щодо сприйняття природи кібератак та відповідей на них почалася в 2010-2011 роках. У 2011 році був прийнятий документ «Галліннське керівництво із застосування міжнародного законодавства у кіберсфері», а в 2012 році НАТО визнало кіберпростір новим театром воєнних дій. Однак у практичній площині реагування є досить проблематичним, оскільки важко довести причетність конкретних країни чи груп до здійснення атак [9].

Передовсім, як відзначають експерти, активність російських спецслужб у кіберпросторі України до 2013 року не була відчутною. Водночас уже був відомий досвід здійснення Росією кібератак проти Естонії та Грузії. А в 2013 році українські спеціалісти почали фіксувати низку АРТ-атак, спрямованих на збір таємної інформації чи інформації з обмеженим доступом. У більшості атак аргументовано підозрюються російські спецслужби та контрольовані ними хакерські спільноти [31].

Створення в Україні Національного координаційного центру кібербезпеки (NC4) у 2017 році посилило здатність країни захищатися від кібератак. NC4 співпрацює з міжнародними партнерами та розробляє комплексні стратегії кібербезпеки для захисту критичної інфраструктури, державних систем і даних громадян.

На даний момент потрібно більше зосереджувати увагу на: підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування, розвиток механізмів виявлення та попередження кіберзагроз та ліквідації наслідків їх прояву, підвищення захищеності громадян та територій від наслідків надзвичайних ситуацій, спричинених інформаційно-технічним чи військовим впливом на об'єкти критичної інформаційної інфраструктури. Певна річ, захист критичних галузей, які функціонують на базі широко розповсюджених інформаційних систем, наприклад телекомунікацій або охорони здоров'я, також має приділятися значна увага, але, на нашу думку, сучасні засоби забезпечення кібербезпеки при грамотному їх використанні здатні значно знизити ризики, що виходять від самих різних загроз: починаючи від звичайних шкідливих програм і до складних таргетованих атак. У промислових інформаційних системах ці методи просто непридатні через безліч причин [40].

Зміцнення стійкості та соціальної згуртованості.

Розвиток стійкості в суспільстві має вирішальне значення для протидії гібридній агресії та запобігання конфліктам, пов'язаним з іншими. Україна зосереджується на посиленні суспільної згуртованості, просуванні демократичних цінностей і протидії кампаніям дезінформації, які спрямовані на використання розбіжностей.

Після окупації Криму та агресії РФ на Сході України виникли нові виклики в сфері захисту прав і свобод людини. Експерти вказують, що сьогодні ключовими проблемними факторами у цій сфері є окупація, воєнні дії і гальмування реформ. Вони пов'язані зі «зневагою до верховенства права та прав людини, популізмом, який породжує політичну корупцію та безвідповідальність влади, запевнення великих груп політиків та громадських активістів, що складні проблеми можна вирішити простими шляхами, зокрема, за рахунок застосування сили і

примусу» [3].

В Україні відзначаються прояви таких гібридних впливів, як використання квазі-громадських організацій, медіа та соціальних мереж для дестабілізації міжнародних відносин, експлуатація теми політики пам'яті та соціокультурних питань. Наприклад, у травні 2017 року в деяких регіонах було розгорнута зовнішня рекламна кампанія «Опозиційного блоку» з провокативними гаслами, які стимулювали ескалацію конфліктів: «Требуем остановить репрессии и наступление нацизма», «Требуем прекратить войну» тощо. В червні 2016 року повідомлялося про намагання створення Бессарабської народної республіки [10].

У російських ЗМІ активно висвітлюється ситуація в сфері міжрелігійних відносин, зокрема, переходи громад з УПЦ МП до УПЦ КП подаються як факти порушення прав вірних УПЦ МП. Експерти фіксували випадки таких гібридних впливів, як поширення чуток про загрозу закриття і спалення храмів УПЦ МП (зокрема, в Білгороді-Дністровському Одеської області), що несло конфліктні ризики. В травні 2017 року заявляли, що УПЦ МП готує свої статuti за зразками Російської православної церкви, згідно з якими єпархіальні управління отримали б право контролю за всім життям і діяльністю релігійних організацій. Негативний резонанс в УПЦ МП викликали законопроекти №4128 та №4511 [11].

Український уряд, організації громадянського суспільства та навчальні заклади співпрацюють, щоб підвищити обізнаність про гібридні загрози, дезінформацію та важливість критичного мислення. Освітні програми та громадські кампанії сприяють медіаграмотності та громадянській активності, зміцнюючи стійкість суспільства проти тактики гібридної війни.

Боротьба за молодь в контексті згуртованості, вона є дуже

важливою. Тому що старше покоління, воно вже є зі своїми сформованими якимись думками, сформованими позиціями. Є великий спектр, який ми вже не згуртуємо ніколи. Згуртовувати треба тих, кого ще можливо згуртувати [13].

Покращення сектору правоохоронної системи в контексті гібридної агресії.

Гібридна агресія ставить перед націями складні виклики, долаючи традиційні кордони війни та безпеки. Щоб подолати цю багатогранну загрозу, уряди повинні зосередитися на зміцненні своїх правоохоронних систем. У цьому розділі підкреслюється важливість посилення правоохоронного сектору в ширшому контексті гібридної війни.

Тривалий час правоохоронна система поступово деградувала, перетворюючись на каральний орган у руках авторитарного й низькоморального керівництва. До служби в правоохоронних органах потягнулися люди, які планували власне збагачення саме за рахунок використання свого службового становища. Загальна ситуація в державі не сприяла тому, щоб у рядах правоохоронної системи затримувалися професійні, компетентні, моральні і відповідальні кадри. Низький рівень фінансового та матеріально-технічного забезпечення спонукав правоохоронців до пошуку додаткових заробітків, що призводило до процвітання корупції, «кришування», сприяння незаконній діяльності. Корумпованість силових відомств більшість (56,8%) українських експертів назвали першим за важливістю фактором для початку агресії Росії проти України [15].

Важливе значення у втраті правоохоронними органами здатності протистояти гібридним загрозам мало проникнення агентури держави-агресора до системи правопорядку та безпеки держави. Зокрема, за свідченням голови СБУ у 2006- 2010 роках Валентина Наливайченка, «Альфа» й інші підрозділи СБУ станом на лютий 2014 року були

інфільтровані російською ідеологією та агентурою настільки, що до кінця квітня 2014 року були переконані – Росія не агресор, а росіяни є братами. Тому в Криму вірними присязі залишилися близько 30% співробітників СБУ [19].

У світлі унікальних характеристик гібридної агресії правоохоронні органи повинні надати пріоритет розробці спеціалізованих навчальних програм. Ці програми мають бути зосереджені на покращенні розуміння концепцій, тактики та методів гібридної війни серед персоналу правоохоронних органів. Ці знання дозволять їм виявляти гібридні загрози в межах своєї юрисдикції та ефективно реагувати на них.

Проблема вдосконалення державного управління правоохоронними органами в умовах гібридної війни ще недостатньо досліджена і потребує більш детального вивчення та обговорення. Протистояти гібридним загрозам Україна зможе лише кардинально реформувавши власну систему правоохоронних органів у напрямку посилення можливості як вертикальної координації дій усіх правоохоронних структур так і горизонтальних зв'язків між ними. Модернізація механізмів державного управління правоохоронними органами на сучасному етапі розвитку держави має проводитись поетапно, з урахуванням вимог сьогоденності та міжнародного досвіду. На першому етапі необхідно затвердження концепції реформи правоохоронних органів, із визначенням періодів та термінів, потрібних ресурсів, індикаторів та критеріїв оцінювання результатів. На другому етапі необхідно прийняття загального закону про правоохоронні органи, розроблення законодавчої бази у відповідності вимогам цього закону, зокрема відповідних положень про роботу правоохоронних органів. На третьому етапі має відбутися реалізація реформи. Вдосконалення системи державного управління правоохоронними органами в цих умовах має бути спрямоване на забезпечення керівництва ним як цілісною системою, що побудована на

наступних принципах: чіткої регламентації діяльності кожного правоохоронного органу з метою уникнення дублюючих та неприбуткових функцій; налагодження співробітництва та ефективних стратегічних комунікацій між правоохоронними органами; застосуванні адаптивних стратегій управління, які передбачають залучення незалежних експертних організацій; залучення громадянського суспільства до прийняття найбільш важливих стратегічних рішень з питань забезпечення внутрішньої безпеки, співпраця з населенням та місцевими громадами; суттєвого підвищення рівня професійності та відповідальності працівників, що підвищуватиме довіру суспільства до правоохоронної системи; забезпечення необхідного рівня фінансового, матеріально-технічного та соціального забезпечення працівників, що гарантує їм гідне місце і роль у суспільстві. У результаті реформування правоохоронна система має перетворитися на суспільно-орієнтовану структуру, побудовану на сервісній моделі діяльності органів правопорядку, позбавитися репресивних функцій та бути орієнтованою на вирішення проблем населення в рамках загальноновизнаного у світі підходу партнерських відносин. Загальний успіх у протидії гібридній війні буде залежати від здатності правоохоронних органів продемонструвати населенню держави та у першу чергу – окупованих районів, переваги української моделі розвитку з ефективною системою верховенства права, високими соціальними та демократичними стандартами, ефективним державним управлінням. Таким чином, новими функціями правоохоронних органів у сучасних умовах мають стати оновлена діяльність задля забезпечення цілісності та стабільності держави, а також захист від новітніх загроз та здатність до реагування на новітні виклики [37].

Еволюція характеру гібридної агресії вимагає постійного вдосконалення правоохоронного сектору. Зосереджуючись на навчанні,

зборі та аналізі розвідданих, технологічному прогресі та міжнародній співпраці, уряд України може посилити свою здатність ефективно протистояти гібридним загрозам. Зміцнення правоохоронної системи є життєво важливим для захисту національної безпеки, збереження стійкості суспільства та збереження верховенства права перед обличчям гібридної агресії.

Протидія гібридній агресії та запобігання проксі-конфліктам є першочерговими для національної безпеки України. Покращуючи можливості розвідки, зміцнюючи кібербезпеку, сприяючи стійкості суспільства та покращення сектору правоохоронної системи, Україна прагне пом'якшити вплив тактики гібридної війни. Ці засоби та інструменти разом із постійною адаптацією та інноваціями сприятимуть збереженню суверенітету, стабільності та національної безпеки України перед обличчям гібридних загроз, що розвиваються.

Підсумовуючи матеріал викладений в розділі, ера гібридних воєн і проксі-конфліктів створює значні виклики для систем національної безпеки в усьому світі. Ці виклики включають швидкий розвиток технологій, складність гібридних загроз і потребу в покращенні координації та співпраці між державами. Розширення можливостей розвідки, інвестиції в передові технології, сприяння міжнародній співпраці та розробка комплексних стратегій є важливими для систем національної безпеки задля ефективною протидії гібридній агресії та запобігання проксі-конфліктам. Вирішуючи ці основні проблеми, країни можуть підвищити свою стійкість, захистити свій суверенітет і захистити свою національну безпеку перед обличчям загроз, що розвиваються, розвивалися і будуть розвиватися.

ВИСНОВКИ

В даній дипломній роботі автор розглянув проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів. Дослідження зосереджувалися на теоретичних та практичних аспектах цих проблем, а також на оцінці та аналізі використаних досліджень.

Щодо теоретичних аспектів, було розглянуто концепцію гібридних війн та їх вплив на міжнародну та національну безпеку. Зазначено, що гібридні війни характеризуються поєднанням військових та невійськових методів ведення конфлікту, таких як інформаційна війна, кібератаки, фінансовий тиск та інші. Висвітлено важливість адаптації національних систем безпеки, на прикладі позаблокових держав та України, до нових загроз та необхідність розвитку міжнародного співробітництва для протидії гібридним загрозам.

У практичній частині були проаналізовані дослідження, які звертаються до проблеми гібридних війн та проксі-конфліктів. Виявлено, що багато досліджень фокусуються на ролі кібербезпеки та інформаційної війни в контексті гібридних загроз. Висвітлено значення обміну розвідувальною інформацією та співпраці між державами в контексті протидії гібридним загрозам.

Оцінюючи використані дослідження, слід зазначити їх значний внесок у розуміння проблеми гібридних війн та проксі-конфліктів. Вони надали необхідні теоретичні засади та підходи до практичних досліджень, які можуть бути використані для розвитку стратегій та політик безпеки на національному та міжнародному рівнях.

Однак, варто відзначити, що деякі аспекти проблеми міжнародної та

національної безпеки в епоху гібридних війн та проксі-конфліктів залишаються недостатньо дослідженими. Наприклад, важливо дослідити більш детально вплив економічних факторів та економічної залежності на безпеку держав, а також роль громадської думки та медіа в контексті гібридних загроз.

З метою вирішення розглянутих у роботі проблем, висновки та пропозиції включають наступні пункти:

1. Посилення міжнародного співробітництва: З метою ефективної протидії гібридним загрозам, важливо розвивати міжнародне співробітництво та обмін інформацією між державами. Вироблення спільних стратегій та механізмів координації може покращити здатність держав протидіяти гібридним загрозам.
2. Розвиток кібербезпеки та захисту інформації: У зв'язку з ростом кіберзагроз та інформаційної війни, необхідно залучати більше ресурсів до розвитку кібербезпеки та захисту інформації. Це включає покращення технічних засобів захисту, підвищення кваліфікації фахівців та розробку політик та норм, спрямованих на протидію кіберзагрозам.
3. Розширення області досліджень: Необхідно залучати більше ресурсів та зусиль для дослідження та розуміння проблеми гібридних війн та проксі-конфліктів. Це може включати проведення більш детального аналізу економічних аспектів безпеки, розробку стратегій ефективної комунікації та управління громадською думкою, а також вивчення впливу новітніх технологій, таких як штучний інтелект та кіберфізичні системи, на безпеку.
4. Збалансований підхід до безпеки: Важливо підходити до питання безпеки в комплексному та збалансованому способі. Це означає поєднання військових та невійськових засобів протидії загрозам,

залучення дипломатичних та політичних інструментів, зміцнення резервів та розвиток регіональних та міжнародних механізмів колективної безпеки.

5. Виховання свідомих громадян: Покращення безпеки також потребує виховання свідомих громадян, які здатні розпізнавати гібридні загрози та вчасно реагувати на них. Це може включати освіту населення про безпекові ризики, розвиток медійної грамотності та посилення критичного мислення.

У цілому, проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів є складними та багатограними. Вирішення цих проблем вимагає збільшення співробітництва, розвитку кібербезпеки, розширення області досліджень та застосування збалансованого підходу до безпеки. Ініціативи на національному та міжнародному рівнях, спрямовані на цільову боротьбу з гібридними загрозами, можуть сприяти поліпшенню ситуації

Одним із ключових висновків роботи є те, що загрози, пов'язані з гібридними війнами та проксі-конфліктами, не обмежуються територією окремих країн чи регіонів. Вони мають глобальний характер і вимагають спільних зусиль та міжнародної координації для ефективного протидії. Створення міжнародних механізмів співробітництва, обмін досвідом та розвідувальною інформацією стануть ключовими елементами у формуванні колективної безпеки.

У контексті розглянутих проблем, необхідно звернути увагу на необхідність більш широкого дослідження економічних аспектів безпеки. Гібридні війни та проксі-конфлікти мають значний вплив на економічну стійкість держав, зокрема через залежність від енергетичних ресурсів, міжнародну торгівлю та фінансову систему. Детальне дослідження цих аспектів може допомогти в розробці стратегій зменшення ризиків та підвищення економічної стійкості в умовах гібридних загроз.

Крім того, важливо звернути увагу на роль громадської думки та медіа в контексті гібридних війн та проксі-конфліктів. Зловживання медійним простором та маніпуляція громадською думкою можуть стати ефективними інструментами в руках акторів, що здійснюють гібридні атаки. Посилення медійної грамотності та розвиток стратегій ефективної комунікації можуть зменшити вразливість суспільства перед гібридними загрозами.

Загалом, у цій дипломній роботі автор проаналізував проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів. Результати досліджень свідчать про серйозні загрози, з якими зіткнулися сучасні держави та міжнародна система в цілому. Висновки вказують на необхідність змін у підходах до безпеки, як на теоретичному, так і на практичному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

ДЖЕРАЛА

Офіційні документи

1. Визначення агресії: резолюція від 14.12.1974. № 995_001-74. [Електронний ресурс]. - Режим доступу: https://zakononline.com.ua/documents/show/169633_169633
2. Щорічний звіт Генерального секретаря за 2022 рік. Офіційна інтернет-сторінка НАТО. 21 березня 2023. [Електронний ресурс]. - Режим доступу: https://www.nato.int/cps/en/natohq/opinions_212795.htm?selectedLocale=uk#sg4
3. Права людини в Україні 2016. [Електронний ресурс]/ Українська Гельсінська спілка з прав людини. – Режим доступу: https://helsinki.org.ua/wp-content/uploads/2016/12/HumanRight2016-sokr_web.pdf
4. Статут ООН. Департамент громадської інформації ООН. Київ. [Електронний ресурс]. - Режим доступу: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf
5. Щорічна доповідь за 2002 рік щодо діяльності ОБСЄ. Відень. 2003. ОБСЄ.
6. Final Report on the Meaning of Armed Conflict in International Law. The Hague Conference (2010). Use of Force. [Електронний ресурс]. - Режим доступу: <http://www.ila-%20hq.org/download.cfm/docid/2176DC63->

[%20D268%E2%80%934133%E2%80%9389A664754F9F87%20\(Last%20accessed:%2030.09.2016\).](#)

7. NorthAtlantic Treaty Organization. Cyber Defence Pledge. [Електронний ресурс]. –Режим доступу: https://www.nato.int/cps/su/natohq/official_texts_133177.htm
8. North Atlantic Treaty Organization. Warsaw Summit Communiqué, 9.7.2016. [Електронний ресурс]. – Режим доступу: https://www.nato.int/%20cps/en/natohq/official_texts_133169.htm

Матеріали ЗМІ

9. Військова відповідь на кібератаки Кремля? І так, і ні. [Електронний ресурс]. Укрінформ. – Режим доступу : <https://www.ukrinform.ua/rubric-technology/2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni.html>
10. Голова СБУ пояснив, навіщо ФСБ знадобилось обмінювати сепаратистів з Одеси. [Електронний ресурс]/«5 канал». – Режим доступу: <https://www.5.ua/suspilstvo/holova-sbu-poyasnyvnavishcho-fsb-znadoylos-obminiuvaty-separatystiv-z-odesy-117784.html>
11. Десятки тисяч віруючих підписали звернення до Верховної Ради. [Електронний ресурс]/ УПЦ МП. – Режим доступу: <http://news.church.ua/2017/05/15/desyatki-tisyach-viruyuchix-pidpisalizvernennya-do-verhovnoji-radi/>
12. Індія-Пакистан: ядерної війни поки немає, в розпалі гібридна. Інформаційне агентство «Український інтерес». 04.03.2019. [Електронний ресурс]. - Режим доступу: <https://uain.press/news/world/indiya-pakystan-yadernoyi-vijny-pokuy-nemaye-v-rozpali-gibrydna-1004885>

13. Інтерв'ю з Віктором Міщишиним «Війна та згуртованість суспільства». Інститут Громадського Суспільства. 22.01.2022. – Режим доступу: <https://www.csi.org.ua/news/vijna-ta-zgurtovanist-suspilstva-viktor-mishhyshyn/>
14. Прес-реліз: Чинний голова та Генеральна секретарка висловили жаль щодо недосягнення консенсусу для продовження дії мандата СММ в Україні. Офіційна інтернет-сторінка ОБСЄ. 31 березня 2022. [Електронний ресурс]. - Режим доступу: <https://www.osce.org/uk/chairmanship/515018>
15. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. Результати експертного опитування. [Електронний ресурс]. – Режим доступу: https://geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%20%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%20%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf
16. Ткач В. Про роль розвідки в гібридній війні і «дзеркальну проекцію». Інформаційне агентство «ОПК». 01.04.2019. [Електронний ресурс]. - Режим доступу: <http://opk.com.ua/%D0%BF%D1%80%D0%BE-%D1%80%D0%BE%D0%BB%D1%8C-%D1%80%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B8-%D0%B2-%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D1%96%D0%B9-%D0%B2%D1%96%D0%B9%D0%BD%D1%96-%D1%96/>
17. Україна і Сінгапур домовилися про співпрацю між кіберкопами. Інформаційне агентство «Укрінформ». 29.10.2018. [Електронний ресурс]. - Режим доступу: <https://www.ukrinform.ua/rubric-society/2568057-ukraina-i-singapur-domovilisa-pro-spiypracu-miz-kiberkopami.html>

18. Фінляндія через побоювання гібридної війни внесла продаж землі росіянам до списку загроз безпеці. Інформаційне агентство «УНІАН». 03.03.2016. [Електронний ресурс]. - Режим доступу: <https://www.unian.ua/economics/realestate/1282030-finlyandiya-cherez-poboyuvannya-gibridnoji-viyni-vnesla-prodaj-zemli-rosiyanam-do-spisku-zagroz-bezpetsi.html>
19. Як ми втрачали Крим. Свідчення перших осіб України. [Електронний ресурс]/«Українська правда». - Режим доступу: https://www.pravda.com.ua/cdn/graphics/2017/04/jak_my_vtrachaly_krym_svidchennja_pershyh_osib_ukrainy/

ЛІТЕРАТУРА

Монографії

20. Національна безпека. Монографія. Д. Паламарчук. Борисфен Інтел. 24 травня 2020.
21. Національна стійкість в умовах мінливого безпекового середовища. Монографія. О. О. Резнікова. – Київ 2022. [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf
22. Україна у системі міжнародної безпеки. Монографія. За ред. О.С. Власюка. – Київ. Фоліант; Стилос, 2009. – С. 94.
23. ALYSON J. K. BAILES and ANDREW COTTEY. Regional security cooperation in the early 21st century. SIPRI Yearbook 2006: Armaments, Disarmament and International Security. 2006. [Електронний ресурс]. - Режим доступу: <https://www.sipri.org/sites/default/files/YB06ch04.pdf>

Довідкові матеріали

24. Гібридна війна і журналістика - проблеми інформаційної безпеки: навчальний посібник. Вид-во НПУ ім. М. П. Драгоманова. Київ. 2018. – 12 с.. [Електронний ресурс]. - Режим доступу: <https://enpuir.npu.edu.ua/bitstream/handle/123456789/25597/Kulias%2012-27.pdf;jsessionid=0D21A2B67B6130AAA69627C2AAE64D3B?sequence=1>
25. Міжнародне право. Особлива частина: навчальний посібник для студентів юр. факультетів та ВНЗ // І. І. Лукашук. Академія правових вчень. Вид. №3. 2005.
26. Міжнародне публічне право: підручник // за ред. Д. К. Бекашева. 2002.
27. Політична наука: словник-довідник. Санжаревський І. І. Вид №6.. Тамбов. 2016. - 1290 с.
28. Прохоров А. М. Великий енциклопедичний словник. Вид № 3. 2004 . – 1456 с.
29. Соціологія: енциклопедія. Грицанов О. О., Абушенко В. Л.. Мінськ. 2003. – 1312 с.
30. Shifting Paradigm of War: Hybrid warfare. Turkish National Defense University. Istanbul (2017). [Електронний ресурс]. - Режим доступу: <https://www.msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf>

Наукові статті

31. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». – К.: НІСД, 2016. – 258с.
32. Бахметьев А. Є. Забезпечення національної безпеки України в умовах ведення гібридної війни. НУ «Одеська юридична академія». [Електронний ресурс]. - Режим доступу: <http://dspace.onua.edu.ua/bitstream/handle/11300/21740/%d0%91%d0%b0%d1%85%d0%bc%d0%b5%d1%82%d1%8c%d1%94%d0%b2%20%d0%90.%20%d0%84.%20%d0%97%d0%b0%d0%b1%d0%b5%d1%81%d0%bf%d0%b5%d1%87%d0%b5%d0%bd%d0%bd%d1%8f%20%d0%bd%d0%b0%d1%86%d1%96%d0%be%d0%bd%d0%b0%d0%bb%d1%8c%d0%bd%d0%be%d1%97%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b8%20%d0%a3%d0%ba%d1%80%d0%b0%d1%97%d0%bd%d0%b8%20%d0%b2%20%d1%83%d0%bc%d0%be%d0%b2%d0%b0%d1%85%20%d0%b2%d0%b5%d0%b4%d0%b5%d0%bd%d0%bd%d1%8f%20%d0%b3%d1%96%d0%b1%d1%80%d0%b8%d0%b4%d0%bd%d0%be%d1%97%20%d0%b2%d1%96%d0%b9%d0%bd%d0%b8.pdf?sequence=1&isAllowed=y>
33. Брежнєва Т.В. Стійкість як ключовий елемент колективної оборони НАТО // Стратегічні пріоритети. –2017. –№ 3 (44). –С. 13
34. Гібридна війна Росії – виклик і загрози для Європи. Центр Разумкова. Київ, грудень 2016. [Електронний ресурс]. - Режим доступу:

https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRID-WAR-FINAL-1-1.pdf

35. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/public/File/2015_book/012315_Gorbulyyn.pdf
36. Донеллі Дж. Права людини у міжнародній політиці // переклад з англ.. Т. Завалій. – Львів. 2004. – 280 с.
37. Загорулько А. П. Удосконалення державного управління правоохоронними органами як фактор підвищення їх ефективності в умовах гібридної війни. УДК 355/359.07. Київ. - Режим доступу: http://repositsc.nuczu.edu.ua/bitstream/123456789/7741/1/ilovepdf_com-14-23.pdf
38. Замікула М. О. Безпекова та оборонна політика нейтральних країн Європи в умовах дестабілізації системи міжнародних відносин. Національний інститут стратегічних досліджень. Відділ проблем зовнішньої політики та міжнародної безпеки. 2017. [Електронний ресурс]. - Режим доступу: <https://niss.gov.ua/sites/default/files/2017-07/bezpeka-93fb8.pdf>
39. Іванчик М. Роль міжнародних організацій у системі безпеки країн регіону. ДВНЗ «Ужгородський національний університет». [Електронний ресурс]. - Режим доступу: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/22764/1/%D0%A0%D0%9E%D0%9B%D0%AC%20%D0%9C%D0%86%D0%96%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%98%D0%A5%20%D0%9E%D0%A0%D0%93%D0%90%D0%9D%D0%86%D0%97%D0%90%D0%A6%D0%86%D0%99.pdf>
40. Козьмініх А. В. Кібербезпека та кібератаки в умовах гібридної війни. НУ «Одеська юридична академія». [Електронний ресурс]. - Режим доступу:

<http://dspace.onua.edu.ua/bitstream/handle/11300/19153/%D0%9A%D0%BE%D0%B7%D1%8C%D0%BC%D1%96%D0%BD%D0%B8%D1%85%20%D0%90%D0%BB%D1%8C%D0%BE%D0%BD%D0%B0%20%D0%92%D1%96%D1%82%D0%B0%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y>

41. Коломієць О. В. Особливості системи міжнародної безпеки в умовах глобалізації. Автореферат. НУ «Одеська юридична академія». Одеса, - 2015. [Електронний ресурс]. - Режим доступу: <http://dspace.onua.edu.ua/bitstream/handle/11300/2187/%d0%9a%d0%be%d0%bb%d0%be%d0%bc%d1%96%d1%94%d1%86%d1%8c%20%d0%9e.%d0%92..pdf?sequence=1&isAllowed=y>
42. Кучик О. С. Механізми та форми реалізації колективної безпеки у діяльності міжнародних організацій. Наукова стаття. Журнал «Актуальні проблеми міжнародних відносин». Випуск 99 (Частина II). 2011. [Електронний ресурс]. - Режим доступу: https://intrel.lnu.edu.ua/wp-content/uploads/2015/10/apmv_2011_992_7.pdf
43. Стівен Пінк. Просвітництво сьогодні. Аргументи на користь розуму, науки та прогресу. «Наш формат». – 560 с.
44. Andrew Mumford. Proxy Warfare. John Wiley & Sons, 2013. №. 13.
45. Mikael WIGELL, Harri MIKKOLA, Tapio JUNTUNEN «Best practices in the whole-of-society approach in countering hybrid threats». Policy Department for External Relations Directorate General for External Policies of the Union PE 653.632 - May 2021. [Електронний ресурс]. - Режим доступу: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU\(2021\)653632_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf)

- 46.Paleri, Prabhakaran (2008). National Security: Imperatives And Challenges. New Delhi: Tata McGraw-Hill. p. 521. ISBN 978-0-07-065686-4. Retrieved 23 September 2010.
- 47.V. Vlasiuk. HYBRID WAR, INTERNATIONAL LAW AND EASTERN UKRAINE. European political and law discourse. 2015. ISSN 2336-5439. [Електронний ресурс]. - Режим доступу: <https://eppd13.cz/wp-content/uploads/2015/2015-2-4/04.pdf>

ІНТЕРНЕТ-РЕСУРСИ

- 48.Гібридна війна // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0
- 49.Глобальні проблеми людства // Вікіпедія. [Електронний ресурс]. - Режим доступу:
https://uk.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8_%D0%BB%D1%8E%D0%B4%D1%81%D1%82%D0%B2%D0%B0
- 50.Ліга Націй // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9B%D1%96%D0%B3%D0%B0_%D0%9D%D0%B0%D1%86%D1%96%D0%B9
- 51.Національна безпека // Вікіпедія. [Електронний ресурс]. - Режим доступу:
https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0

52. Національна безпека України: Складові елементи та виклики сьогодення. Інтернет-блог «Military». 23 березня 2021. [Електронний ресурс]. - Режим доступу: <https://mil.in.ua/uk/blogs/natsionalna-bezpeka-ukrayiny-skladovi-elementy-ta-vyklyky-sogodennya/>
53. Організація безпеки та співробітництва в Європі. Україна і ОБСЄ // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D0%B7%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D1%96_%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%B0_%D0%B2_%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D1%96#%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0_%D1%96_%D0%9E%D0%91%D0%A1%D0%84
54. Офіційна інтернет-сторінка Міністерства розвитку громад та територій України. Навчальний посібник «Національна безпека». [Електронний ресурс]. - Режим доступу: <https://www.minregion.gov.ua/wp-content/uploads/2017/11/Navchalniy-posibnik-GPNB.pdf>
55. Офіційна інтернет-сторінка ОБСЄ. Розділ: Де ми знаходимося. [Електронний ресурс]. - Режим доступу: <https://www.osce.org/ru/where-we-are>
56. Проблеми безпеки Південно-Східної Європи. [Електронний ресурс]. - Режим доступу: <http://kimo.univ.kiev.ua/CCE/39.htm>
57. MCDC Countering Hybrid Warfare Project. A Multinational Capability Development Campaign project. March 2019. [Електронний ресурс]. - Режим доступу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

