АКАДЕМІЯ ВОЄННО-ПОЛІТИЧНИХ НАУК УКРАЇНИ

Семенюк Ю. В., Мокляк С. П., Лисецький Ю. М.

НОВА ГЕОМЕТРІЯ МІЖНАРОДНИХ ВІДНОСИН ТА РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

Монографія

Київ 2025

УДК 355. 40:007
М74

Рекомендовано до друку Вченою радою
Воєнно-політичної академії України
(протокол № 1 від 07.09.2025 р.)

Автори:
Семенюк Ю. В. – кандидат політичних наук;
Мокляк С. П. – доктор політичних наук, професор;
Лисецький Ю. М. – доктор технічних наук, доцент.

Рецензенти:
Петров В. В. – доктор політичних наук, доцент, професор кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка;
Коваль М. В. – доктор військових наук, начальник Національного університету оборони України.

За загальною редакцією С. П. Мокляка

М74 **Нова геометрія міжнародних відносин та розвідувальної діяльності:** монографія / Семенюк Ю. В., Мокляк С. П., Лисецький Ю. М.; за заг. ред. С. П. Мокляка. – Київ : Видавець Бихун В. Ю., 2025. 208 с.
ISBN 978-617-7699-96-4

Монографія присвячена проблемі трансформації міжнародних відносин та розвідувальної діяльності в сучасних умовах. У роботі досліджено геополітичну трансформацію сучасного світу в умовах повномасштабного вторгнення російської федерації в Україну. Проведено аналіз нового покоління російських війн: основні тенденції та концепції. Досліджено становлення й розвиток приватних військових компаній, їхні особливості та спроможності в умовах дестабілізації міжнародного середовища безпеки. Наведено концепт «розвідувальна діяльність» у сучасних умовах. Розглянуто місце і роль недержавних суб'єктів розвідувальної діяльності в контексті забезпечення національних інтересів.

Матеріали монографії будуть корисними для науковців, викладачів вищих навчальних закладів, аспірантів і фахівців, діяльність яких пов'язана з національною безпекою.

ISBN 978-617-7699-96-4

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

АНБ – Агентство національної безпеки
БПЛА – безпілотні літальні апарати
ВМС – Військово-морські сили
ВОД – військова організація держави
ВПС – Військово-повітряні сили
ВТЗ – високоточна зброя
ДНР – Донецька Народна Республіка
ЄС – Європейський Союз
ЗМІ – засоби масової інформації
ЗСУ – Збройні Сили України
ІДІЛ – Ісламська держава Іраку й Леванту
КВ – консцієнтальна війна
КНР – Китайська Народна Республіка
ЛНР – Луганська Народна Республіка
МВ – ментальна війна
МВС України – Міністерство внутрішніх справ України
ММУО – міжнародні міжурядові організації
МНУО – міжнародні неурядові організації
НАТО – North Atlantic Treaty Organization
НВАК – Народно-визвольна армія Китаю
НУО – неурядові організації
НФП – нові фізичні принципи
ОАЕ – Об'єднані Арабські Емірати
ОБСЄ – Організація з безпеки і співробітництва в Європі
ОВТ – озброєння та військова техніка
ООН – Організація Об'єднаних Націй
ПВК – приватна військова компанія
ПОК – приватна охоронна компанія
ППО – протиповітряна оборона

ПРК – приватна розвідувальна компанія
РБ – Рада Безпеки
РЕБ – радіоелектронна боротьба
РЄ – Рада Європи
РКВП – роботизовані комплекси військового призначення
РО – розвідувальні органи
РС – розвідувальне співтовариство США
рф – російська федерація
СНД – Співдружність Незалежних Держав
СРСР – Союз Радянських Соціалістичних Республік
США – Сполучені Штати Америки
ТВД – театр воєнних дій
ФБР – Федеральне бюро розслідувань
ЦПК – Центр протидії корупції
ШІ – штучний інтелект
ШОС – Шанхайська організація співробітництва
AM – Additive Manufacturing
ARPA-Ed – Advanced Research Project Agency for education
ASEAN – Association of SouthEast Asian Nations
BDI – Behavioral Dynamics Institute
BRI – Belt and Road Initiative
BRICS – Brazil, Russia, India, China, South Africa
CA – Cambridge Analytica
CSPG – China Security & Protection Group
DARPA – Defense Advanced Research Projects Agency
DREAD – Department of Research, Exploitation, Analysis and Development
DSEI – Defence and Security Equipment International
ECOWAS – The Economic Community of West African States
FTC – Federal Trade Commission
GARDA – Government Advant Research Development Agency
GEOMINT – Geospatial Intelligence
GMW – Global Modern War
GPF – Geopolitical Futures
IARPA – Intelligence Advanced Research Projects Activity
ITAR – International Traffic in Arms Regulations
K&R – Kidnap and ransom

MAD – Mutually Assured Destruction
MASINT – Measurement and Signature Intelligence
NDC – NATO Defense College
NESA – National Electronic Security Authority
NIE – National Intelligence Estimates
NLP – Natural Language Processing
NSA – National Security Agency
NWCC – NATO Warfighting Capstone Concept
OAS – Organization of American States
OSINT – Open Source Intelligence
OXFAM – Oxford Committee for Famine Relief
POA – Peace Operations Association»
QUAD – Quad group of nations
RAND – Research ANd Development
RIA – Radio Intelligence Agency
SAS – Special Air Service
SCL – Strategic Communication Laboratories
SIGINT – Signals Intelligence
SMM – Social Media Marketing
TAG – The Arkin Group
TTC – Trade and Technology Council
VUCA – Vision, Understanding, Creativity/Clarity, Agility
VUCA – Volatility, Uncertainty, Complexity, Ambiguity

ПЕРЕДМОВА

Сучасна геополітична арена переживає епоху змін, обумовлених відновленням старих і виникненням нових держав-акторів на міжнародній сцені.

Повномасштабна агресія російської федерації (рф) проти України виступає показовим маркером масштабних трансформацій у світовому порядку. Кривава війна в центрі Європи, що донедавна виглядала малоймовірною перспективою з огляду на гуманітарні досягнення сучасної людської цивілізації та політичний світогляд демократичних країн, стала реальністю.

Країна, яка є постійним членом Ради Безпеки (РБ) Організації Об'єднаних Націй (ООН), демонструє тотальне ігнорування норм міжнародного права та відверто робить ставку на військову силу та ядерний шантаж усього світу. Використовуючи продаж корисних копалин як головне джерело поповнення державного бюджету, рф висуває примітивні ультиматуми демократичним країнам.

Усе це окреслює контури нового світового порядку, де формується чітка лінія розмежування між демократичною західною цивілізацією та автократичним сходом. У цьому світі тепер немає союзів і союзників, немає взаємних зобов'язань, а старі договори можуть бути переглянуті в односторонньому порядку. Є лише великі сильні країни, які беруть те, що їм хочеться, і маленькі слабкі, які стають жертвами такої політики.

Тобто воєнно-силовий чинник поступово витісняє цивілізаційний та міжнародно-правовий фактори й стає домінантою в новому світовому порядку.

Намагаючись захистити себе, кожна нація озброюється й робить стратегічні, географічні та технологічні ставки, щоб вижити й перемогти в майбутньому протистоянні. Кожен із цих жестів, однак, посилює відчуття загрози з боку супротивників, які через це відчувають себе ще більш невпевнено й готуються до найгіршого, що, своєю чергою, виглядає ще більш загрозливим.

Особливу увагу привертають країни так званого Глобального Півдня. Геополітичний вплив Китайської Народної Республіки (КНР) є однією з основних глобальних амбіцій цієї держави. З моменту приходу на посаду Генерального секретаря Комуністичної партії Китаю Сі Цзіньпіна в 2012 році відбулася відмова від зовнішньої політики Ден Сяопіна, висловленої ним фразою «приховувати можливості та чекати свого часу; триматися в тіні й не показувати себе». Натомість у 2014 році голова КНР дав нове визначення зовнішньої політики Китаю – «прагнути до досягнень». У його новому багатополярному порядку глобальні інституції та норми будуть підкріплені китайськими уявленнями про спільну безпеку та економічний розвиток, китайськими цінностями політичних прав, що визначаються державою і китайськими технологіями.

У цьому «новому світі без порядку» Сполучені Штати Америки (США) не можуть залишитися осторонь. Розуміння, що стабільність і безпека в будь-якому регіоні впливають на стабільність у всьому світі, має стати ключовим фактором у розв'язанні геополітичних проблем. Співпраця, діалог і дотримання міжнародного права мають бути в основі будь-яких дій на міжнародній арені.

Таким чином, сучасні міжнародні відносини, динаміка геополітичних зрушень, посилення інформаційних атак та воєн потребують скоординованої стратегії щодо подолання загроз глобальній і національній безпеці держав.

ВСТУП

У сучасному глобальному контексті, коли геополітичні, геоекономічні, соціокультурні трансформації та технологічний прогрес різко прискорюються, міжнародна арена стає все більш складною і непередбачуваною. Ця динамічність породжує нові виклики, які, у свою чергу, вимагають глибокого розуміння, адаптації та невідкладних дій з боку всіх держав світу.

Сучасні світові процеси створюють умови для активного формування міжнародних партнерських відносин між державними та недержавними учасниками світової політики на різних рівнях співробітництва. За останні десятиліття значно зросли кількість, різноманітність і масштаби діяльності недержавних акторів міжнародних відносин, які справляють дедалі більший вплив на світові процеси, активно вибудовують сучасні політичні відносини та формують нові контури міжнародної системи світу, а також відіграють найважливішу роль у вирішенні проблем міжнародної безпеки.

Поширення гібридних загроз, зміна характеру низки традиційних загроз, ускладнення прогнозування майбутнього безпекового середовища в умовах невизначеності – усе це нові умови, у яких мають діяти розвідувальні органи (РО) України, що обумовлює необхідність їхнього адаптування, зокрема, шляхом упровадження нових методів та способів діяльності.

РОЗДІЛ І

ГЕОПОЛІТИЧНА ТРАНСФОРМАЦІЯ СУЧАСНОГО СВІТУ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ РФ В УКРАЇНУ

1.1. Воєнно-силовий чинник геополітичних трансформацій сучасності

Війна є невід'ємною частиною людської цивілізації. Від перших зафіксованих в історії цивілізацій існують свідчення щодо постійного ведення воєн між представниками різних суб'єктів, які намагалися підкорити навколишні народи і землі.

Нічого не змінилося і в наші часи, про що свідчить, зокрема, історія та трагедії Другої світової війни. Ліберальний світовий порядок, який виник на руїнах цієї війни, постав у результаті формування далеко не ідеальної, але все-таки досить ефективної системи компромісів між протиборчими ідеологіями.

Система багатосторонніх угод, конвенцій і договорів із питань безпеки, торгівлі та дипломатичних відносин, створена після Другої світової, виникла в безперервній боротьбі ідеологій, політичних та економічних інтересів так званого Заходу на чолі із США з так званим Сходом в особі СРСР і його нечисленних ідеологічних сателітів. Обидві сторони діяли в рамках післявоєнної світобудови, розуміючи згубність відкритої агресії. При цьому Захід ще й помилявся, вважаючи, що залучення комуністичних режимів до світових економічних процесів приведе до їх демократизації.

Помилкове оцінювання підсумків Холодної війни та нездатність чітко пояснити суть процесів, які відбувалися на пострадянському просторі на початку 1990-х років, спричинили низку неправильних політичних рішень із боку Заходу. Замість того, щоб створити збалансований простір безпеки, що виключало б нове ядерне протистояння, було ухвалено рішення про перезавантаження відносин із росією, її інтеграцію в міжнародні структури.

Початок XXI ст. ознаменувався складними трансформаційними процесами, які зумовлені викликами глобалізації, активізацією етнічних і релігійних чинників, кардинальними змінами міжнародного середовища та системи безпеки.

Сучасний світ продовжує розглядати воєнну силу як один із найважливіших інструментів вирішення зовнішньополітичних питань. Рішення про використання воєнної сили приймається світовими акторами виходячи з власного розуміння своїх національних інтересів та доречності її застосування навіть без резолюції ООН.

Форми безпосереднього прояву воєнної сили здатні коливатися в межах кількох імовірних моделей її об'єктивації. При цьому найпростішим сценарієм переходу держави до воєнно-силових акцій і на міжнародній арені, і в межах державних кордонів, на думку О. Панфілова, Л. Петрової, М. Требіна та інших дослідників [1], продовжує залишатися демонстрована нею загроза застосування силових засобів (явна – прихована, реальна – умовна); більш складним видом застосування воєнної сили залишається збройне насильство – прямий фізичний вплив на супротивну сторону за допомогою засобів збройної боротьби з метою її знищення або вигідного перетворення і, відповідно, досягнення власних політичних цілей.

У сучасних умовах, зазначають дослідники, трьома найбільш універсальними формами силових ресурсів є економічні, політичні та воєнні. Воєнна сила, порівняно з економічними або політичними перевагами, є найменш пристосованою до швидких конвертацій. Проте її цінність полягає в тому, що вона стає постійним фактором відносин, наявність якого забезпечує реалізацію всіх інших факторів. Дія силового фактора в мирний час подібна до дії гравітаційного поля в тому сенсі, що його вплив на всі процеси є непомітним із першого погляду, але водночас вирішальним. Воєнна сила виникає внаслідок синтезу відповідних ресурсів, чітко визначеної мети і створеної на базі цивілізаційного розвитку оптимальної моделі організації ресурсів для її досягнення. У зв'язку із цим доречними виглядають напрацювання О. Бодрука, у яких аналізуються особливості формування силового фактора в різних країнах світу [2, 3]. Виходячи з аналізу проблем, автор визначає декілька груп країн, що мають схожі підходи до формування воєнної сили.

Перша група – розвинені країни Європи. Тут завершився процес формування нації. У світовому геополітичному просторі вони давно існують як суверенні одиниці. Розвинена демократія та ринкова економіка дають змогу цим державам реально представляти інтереси нації, особи, соціального чи політичного угруповання. Як правило, такі країни виступають державами-націями. Проблеми воєнної могутності в них зосереджені на запобіганні зовнішнім загрозам та викликам на кшталт гібридних загроз, тероризму, неконтрольованої міграції, організованої злочинності, наркобізнесу тощо.

Друга група – країни, де формування націй ще не завершилося, але є реальні можливості досягти національної консолідації. Держава тут відіграє роль головного націєтворчого фактора. Національні цілі в цьому разі зорієнтовані на перспективу, а воєнна сила, по суті, спрямована на безпеку держави та її структурних компонентів. Тільки в тому чи іншому конкретному випадку вона поширюється на захист інших складових соціальної системи. Безпека цієї групи країн в основному зосереджена на внутрішніх проблемах: подолання політичної нестабільності та економічної кризи; запобігання сепаратизму та конфліктам на етнічному, політичному чи релігійному ґрунті; охорона території тощо. Зовнішні загрози для цих країн існують, що вимагає залучення значних ресурсів для утримання воєнної сили.

Третя група – багатоетнічні країни Азії, Африки та Латинської Америки. У них державні структури скопійовані з колишніх країн-метрополій, немає демократичних традицій, а складна етносоціальна структура створює величезні труднощі для прогресивно налаштованого уряду. Такі держави, особливо Африки та Азії, часто перетворюються на корумповані, неефективні, делегітимізовані внаслідок своєї неспроможності. У цьому разі є всі підстави говорити про «злам держави» і вбачати в ній головну загрозу для планети. У багатьох випадках дослідники констатують фактичну відсутність держави чи тривалу втрату державного контролю за частиною власної території. Численними є випадки перманентного співіснування слабкої центральної державної влади та опозиційного збройного формування, яке так міцно контролює частину території країни, що в змозі створити там органи адміністративного управління. Економіка таких країн, інститути державної влади, які мусять стояти на сторожі законності й порядку, – в явному занепаді.

У контексті зазначеного цікавими є погляди керівництва США щодо застосування воєнної сили в міжнародних відносинах. *Адміністрація США 12 жовтня 2022 року представила нову Стратегію національної безпеки США (National Security Strategy of The United States of America)* [4].

У документі акцентується, що США не вагатимуться в застосуванні сили, коли йтиметься про захист національних інтересів. Проте застосування сили має бути зумовлене чіткими досяжними цілями, відповідати цінностям і законам та відбуватися за згодою американського народу.

У ситуації загострення конкуренції роль військових полягає у **збереженні та здобутті воєнних переваг при одночасному обмеженні можливостей конкурентів.**

Для реалізації максимального ефективного стримування агресії пропонується новий комплексний підхід – **інтегроване стримування** (*integrated deterrence*).

27 жовтня 2022 року Пентагон оприлюднив відкриту складову частину нової Національної оборонної стратегії (далі – Стратегія, National Defense Strategy) США [5].

Стратегія визначає такі пріоритети у сфері оборони: оборона США, стримування стратегічної атаки на США та їхніх союзників / партнерів, стримування агресії передусім з боку КНР, а потім рф, розбудова боєздатних збройних сил та екосистеми оборони.

Головними новаціями Стратегії можна вважати концепції інтегрованого стримування (integrated deterrence) і протиборства в умовах миру (campaigning). Саме в рамках цих концепцій США планують забезпечити реалізацію зазначених пріоритетів і цілей. Також важливе місце у втіленні пріоритетів Стратегії посідає взаємодія із союзниками і партнерами.

В основу концепції інтегрованого стримування покладено спроможність збройних сил США діяти в усіх сферах протиборства разом із потенціалом союзників та інших урядових відомств США. **Інтегроване стримування передбачає комбінування різних видів стримування з метою переконати іншу сторону відмовитися від агресивних намірів.** Ідеться про стримування за рахунок заборони (deterrence by denial), стримування за рахунок стійко-

сті (deterrence by resilience) та стримування за рахунок можливості завдання неприйнятного рівня втрат (deterrence by cost imposition).

Стримування за рахунок заборони ґрунтується на демонстрації противнику неможливості швидко захопити й утримати території чи швидко досягти поставлених агресивних цілей. Такий вид стримування доповнюється стримуванням за рахунок стійкості – здатності продовжувати виконувати завдання, незважаючи на нанесення противником певного рівня ураження (передусім системам командування і управління). Проте, як визначає Стратегія, інколи цих видів стримування може бути недостатньо, і тоді використовують стримування за рахунок можливості завдання неприйнятного рівня втрат – демонстрації здатності до ураження більш широкого спектру цілей. В основі такого стримування США – стратегічний ядерний арсенал і конвенційні системи дальнього вогневого ураження, наступальні спроможності в кіберсфері, нелінійне застосування наявних спроможностей (irregular warfare), підтримка оборони третіх країн, санкції та експортний контроль, дипломатичні заходи.

У випадку рф наголошується на стримуванні за рахунок заборони і стримуванні за рахунок стійкості. **Проте у випадку безпосередніх сусідів рф передбачено розробити опції для стримування за рахунок можливості завдавати росії неприйнятного рівня втрат.** У короткостроковій перспективі йдеться про модернізацію систем заборони й обмеження доступу, посилення взаємосумісності та стійкості, обмін розвідувальними даними в середовищі союзників по НАТО (North Atlantic Treaty Organization) та партнерів. У довгостроковій перспективі – це розвиток потенціалу союзників по НАТО вести війни високої інтенсивності, тоді як США зосередяться на таких видах бойового забезпечення, як розвідка та радіоелектронна боротьба (РЕБ), а також підтримка з повітря.

Концепція протиборства в умовах миру має стати відповіддю збройних сил США на різні практики тиску до порогу ескалації, які використовують противники. Протиборство в умовах миру передбачає демонстрацію військової діяльності в пріоритетних регіонах світу з метою посилити сумніви противника щодо його спроможності досягнути цілі, застосовуючи тиск. Така практика протиборства дасть змогу ліпше підготуватися до можливого переростання кризи в конфлікт завдяки кращій ситуаційній обізнаності, посиленню

взаємосумісності й доступу. Практика протиборства в умовах миру здійснюватиметься передусім щодо КНР і рф у спосіб відповідної прямої присутності сил США в пріоритетних регіонах Євразії. В інших випадках США спиратимуться на мережу союзів і партнерств.

Розвиток сил оборони США визначено основою підтримання й посилення ефекту стримування. Пріоритетними напрямами розвитку сил оборони є підтримання інформаційної переваги завдяки інтеграції, захисту і відтворення системи обробки інформації та ухвалення рішень; посилення швидкості й точності виявлення і нанесення ураження; логістичне забезпечення й утримання угруповання військ в умовах активних ворожих контрзаходів; розроблення концепцій і спроможностей для вибіркового ураження систем озброєння. Передбачається оптимальне поєднання технологічних рішень і способів застосування, які ускладнюють для противника проєктування сили. **В екстрених випадках міністерство оборони США може напряму надавати ефективні асиметричні спроможності для найбільш уразливих союзників / партнерів.**

Воєнно-силовий чинник, який дедалі більше потрапляє в центр уваги в геополітичних розкладах нового світового порядку, насправді виступає як компенсатор неспроможності створити власну м'яку силу. Наприклад, та сама росія не може нічого запропонувати світові з арсеналу інструментів XXI ст.: ані технологій, ані інновацій у сфері виробництва, ані космічних проривів, ані будь-яких інших сучасних досягнень. Натомість вона може запропонувати газ, нафту, військову агресію та ядерний шантаж.

25 квітня 2005 року в посланні президента рф Федеральним Зборам В. Путін назвав розпад СРСР «найбільшою геополітичною катастрофою XX століття» і цією публічною ностальгією за СРСР обґрунтував геополітичний реваншизм на майбутнє.

10 лютого 2007 року на Мюнхенській конференції з безпеки В. Путін розкритикував однополярність світу, політику США і НАТО щодо росії: «Для сучасного світу однополярна модель не лише неприйнятна, але й взагалі неможлива». На думку експертів, це був найрізкіший зовнішньополітичний виступ господаря кремля за пів століття – після спічів керівника СРСР Микити Хрущова на зустрічах із представниками США, а також із трибуни ООН. Мюнхенську промову Путіна назвали оголошенням другої Холодної війни.

На думку українського експерта М. Гончара, 2007–2008 рр. стали роками піку нафтових цін та першої у XXI ст. глобальної економічної кризи, яка розпочалася із США та призвела до світових негативних наслідків. Путінський режим на тлі занурення Заходу в економічні проблеми, перевантаженості США операціями в Афганістані та Іраку був окрилений як доходами від нафтоекспорту росії, так і своїм успіхом блокування рішень НАТО, використавши європейських лідерів – А. Меркель та Н. Саркозі. Президент росії натяknув, що «якщо НАТО надасть план дій щодо членства в НАТО Грузії, то росія визнає незалежність Абхазії та Південної Осетії, спираючись на косовський прецедент, і тим самим створить буферну зону між силами НАТО і своїми кордонами. Якщо Україну все ж таки приймуть у НАТО, ця держава просто припинить існування. Тобто фактично він погрожував, що росія може розпочати анексію Криму та окупацію Сходу України» [6].

20 лютого 2008 року Дж. Фрідман зі «Стратфор» досить чітко спрогнозував поведінку рф після проголошення незалежності Косова: «…захоплення дружніх до неї сепаратистських регіонів на її кордонах – особливо грузинських регіонів Абхазії і Південної Осетії, а можливо, навіть східної України і Криму… росія таким чином покаже, що незалежність Косово відкриває двері для неї, щоб змінити і свої кордони».

Замість покарання росії санкціями за вторгнення в Грузію вона була фактично винагороджена – політикою перезавантаження з боку Адміністрації Барака Обами. Віцепрезидент США Джо Байден на Мюнхенській безпековій конференції 7 лютого 2009 року виголосив: «Настав час, перефразовуючи президента Обаму, настав час натиснути кнопку перезавантаження та переглянути багато сфер, де ми можемо й повинні працювати разом із росією». І вже 6 березня держсекретар США Хілларі Клінтон вручила міністру закордонних справ рф Сергію Лаврову символічну червону кнопку перезавантаження. А напередодні 5 березня 2009 року на зустрічі міністрів закордонних справ НАТО було вирішено відновити офіційний діалог із росією в рамках Ради НАТО – рф, незважаючи на те, що москва не виконала План перемир'я від 12 серпня 2008 року і не вивела свої війська з території Грузії.

Саміт НАТО в Страсбурзі-Кельні 3-4 квітня 2009 року зафіксував дворушницьку позицію Альянсу – вимагати виведення російських військ із Грузії – з одного боку, а з іншого – співпрацювати з

росією з питань протиракетної оборони, безпеки в Центрально-Східній Європі, Афганістану, протидії тероризму тощо.

У 2014-му – на початку 2022 року Україна опинилася в епіцентрі нової фази глобального протистояння між Заходом та росією, в осерді якого лежала спроба путінського режиму здійснити «геостратегічний реванш» за програш СРСР у Холодній війні та відновити статус росії як світової держави. Попри формальне визнання росією незалежності та суверенітету України, москва розглядала нашу державу як штучне утворення, що входить у сферу «особливих інтересів» кремля та є ключовою частиною геополітичного проєкту «руського міра». За 8 років конфлікту малої інтенсивності росія перетворила Донбас у «сіру зону», яка виступала як геостратегічний плацдарм воєнно-політичного тиску на Київ та потенційний «запобіжник» вступу України в НАТО та Європейський Союз (ЄС).

Унаслідок неможливості реалізації своїх цілей інструментами гібридної війни у 2021 році путін вирішив перейти до наступної фази своєї агресії проти України із застосуванням усієї повноти військової сили. Під прикриттям проведення військових навчань і маневрів рф зосередила на кордоні з Україною велике угруповання військ і техніки, що загрожувало ескалацією бойових дій і викликало широкий міжнародний резонанс. Повноцінна воєнно-політична та суто військова підготовка росії до вторгнення в Україну розпочалася щонайменше навесні 2021 році під прикриттям численних навчань, у т. ч. на території білорусі. Політико-дипломатичним прикриттям її здійснення стали переговори росії із Заходом, присвячені проєкту «договору» про європейську безпеку та «гарантіям безпеки» росії.

Широкомасштабна воєнна агресія проти України, яку росія розпочала 24 лютого 2022 року, змінила більш ніж піввіковий порядок мирного співіснування держав на європейському континенті, що ґрунтувався на взаємному визнанні суверенітету й територіальної цілісності згідно з нормами міжнародного права.

За оцінками експертів Центру Разумкова, війна висвітлила серйозні проблеми в системах глобальної і регіональної безпеки [7]. Розглянемо їх більш детально.

1. Практика використання права вето в РБ ООН гальмує, а в гіршому разі – унеможливлює ухвалення рішень щодо врегулювання

конфліктів, які прямо чи опосередковано зачіпають інтереси постійних членів ради. Неприпустимим є те, що в російсько-українській війні росія, постійний член РБ, є визнаним агресором, який блокує рішення, пов'язані з розв'язанням конфлікту. Це суперечить здоровому глузду й потребує негайного реформування ООН.

2. Система безпеки ООН не продемонструвала ні політичної волі, ні ефективності механізмів розв'язання конфліктів, дотримання міжнародних норм і взятих зобов'язань. З арсеналу РБ практично зникли передбачені Статутом ООН операції щодо примусу до миру через брак політичної волі, фінансових і військово-технічних ресурсів та ветування таких рішень. Натомість практикують більш м'які засоби: операції щодо побудови миру та підтримання миру (так звані операції згідно з главами VI+ або VII–). Намагання ООН та інших безпекових організацій уникати складних проблем призводить до їх поглиблення замість розв'язання. Надання пріоритету щодо припинення вогню в політичному врегулюванні збройних конфліктів призводить до їхнього заморожування з наступною ескалацією. Яскравим прикладом є заморожування конфлікту на Донбасі у 2014 році, який прогнозовано переріс у повномасштабну агресію рф проти України.

3. Захід у цілому, його безпекові інститути, системи забезпечення національної безпеки переважної більшості західних держав виявилися неготовими до повномасштабної агресії росії, яка поставила світ на межу Третьої світової війни. З іншого боку, для всього світу стало несподіваним, що такий потужний агресор, як росія, може зазнати не лише опору, але й поразки в протистоянні з країною, народ і влада якої є консолідованими в захисті свободи та територіальної цілісності. Ба більше, Захід міг би й не оговтатися або принаймні зазнав би суттєвих іміджевих втрат після такого нахабного й агресивного «підвищення ставок» кремлем, якби Україна не зірвала російський бліцкриг. Початкова фаза війни росії проти України, висунення рф ультиматумів НАТО, її черговий ядерний шантаж США та європейських країн засвідчили необхідність присутності в арсеналі систем колективної та національної безпеки засобів завчасного виявлення ризиків, запобігання загрозам, адекватного й ефективного реагування не лише безпосередньо на агресію, а й на погрози нею. Підвищилась актуальність як наявності й запасів сил, так і засобів

та ресурсів, а також й ефективних, опрацьованих механізмів їх залучення, готовності їх використовувати та надавати допомогу союзникам і партнерам.

4. Зростає ступінь гібридності міжнародних конфліктів і криз, що характеризується появою нетрадиційних видів зброї, таких як енергоресурси, політична корупція, агресивна пропаганда, кіберзброя. Останнім часом до них додалося продовольство. Застосування цієї зброї державою-агресором розкриває її як підступного та жорстокого актора. Головними напрямами та проявами використання цих видів зброї росією наразі є такі:

• тиск на Захід через намагання зганьбити його, закликаючи країни Азії й Африки згадати про їх колоніальне минуле, наголошуючи на нерівності між країнами Півночі та Півдня, поширюючи фейки про походження COVID-19 і несправедливий розподіл вакцин;

• підрив єдності Європи через поглиблення енергетичної кризи та посилення невдоволення населення європейських країн напередодні та під час зимового періоду;

• сподівання на зниження стійкості країн ЄС, відволікання їхньої уваги від війни в Україні через вимушене реагування на міграційні хвилі, спровоковані браком зерна, постачання якого з портів України було заблоковано самою росією;

• зміцнення своїх позицій на міжнародній арені через протиставлення росії «загниваючому» Заходу;

• пом'якшення наслідків санкцій способом неприєднання до них окремих країн через запровадження «сірих» і контрабандних схем постачання необхідних російській оборонній промисловості товарів і технологій;

• ослаблення економічного потенціалу України й блокування західної допомоги.

5. Війна висвітлила проблемні питання стосовно ефективності чинних економічних і безпекових союзів. Головними проблемами тут є помилки в оцінюванні ризиків, неспроможність запобігти кризовим явищам, запізнення в реагуванні на них, безвідповідальне ставлення окремих союзників до потреб у ресурсах. На цьому тлі лунають апокаліптичні висновки про кінець глобалізації, завершення епохи крупних союзів та перехід ініціативи до мережевих структур у вигляді автономних регіональних і субрегіональних союзів, альянсів, коаліцій. Ознаки

таких процесів справді трапляються, проте їх спрямовано на пошук способів домогтися внутрішньої солідарності та стійкості наявних міждержавних альянсів і коаліцій. Прикладами можуть бути такі:

• уже наявний в Європі Північно-європейський оборонний союз, Вишеградська четвірка, Люблінський трикутник, проєкт Тримор'я;

• ініціатива Б. Джонсона щодо створення поза межами ЄС під егідою Великої Британії нового воєнно-політичного та економічного союзу за участю України, Польщі, Естонії, Латвії, Литви й Туреччини;

• ідея Е. Макрона, що вже почала втілюватися, щодо створення Європейської політичної спільноти із залученням, окрім членів ЄС, усіх країн Західних Балкан, України та Молдови;

• коаліції держав, що склалися навколо допомоги Україні в боротьбі з російською агресією (процеси «Рамштайн» і «Копенгаген»).

Тобто ця війна стала індикатором неоімперської політики кремля. Російське керівництво розглядає війну в Україні лише як частину великої гри, націленої на досягнення світового лідерства. Підтвердженням цьому стали подальші дії рф на Близькому Сході та Африканському континенті.

У жовтні 2023 року відбулося загострення конфлікту між Ізраїлем та ХАМАСом – ісламістською організацією, яка контролює сектор Гази з 2006 року. У наслідок атаки ХАМАСу на підконтрольні Ізраїлю території загинуло понад 1 400 ізраїльтян та громадян інших держав, понад 5 000 були поранені і ще приблизно 250 знаходяться в заручниках. Дана широкомасштабна атака призвела до того, що Ізраїль був вимушений оголосити війну та проведення «смертоносної операції у відповідь». Терористичні дії угруповань ХАМАСу отримали підтримку від ряду арабських країн, таких як Катар, Ірак, Іран, Туреччина, Кувейт, Сирія, Йорданія, Туніс, Алжир та Ємен, а також від Афганістану та Північної Кореї. З іншого боку, у цьому конфлікті Ізраїль отримав підтримку більшості європейських країн, включаючи Україну. США також оголосили про повну дипломатичну та військову підтримку ізраїльським збройним силам. ЄС випустив заяву, у якій засуджує численні та невибіркові атаки ХАМАСу й закликає до негайного припинення насильства. Якщо проаналізувати перелік країн, які підтримують ту чи іншу сторони в даному збройному

протистоянні, можна дійти висновку, що майже весь арабський світ рішуче налаштований на збройне відстоювання своїх інтересів та застосування будь-яких сил задля досягнення поставлених цілей.

Серед доказів того, що даний конфлікт виходить за межі Ізраїлю та Палестини, свідчить той факт, що 26 жовтня 2023 року керівництво ХАМАСу прибуло до москви задля зустрічі з високопоставленими чиновниками. Міністерство закордонних справ Ізраїлю осудило рішення запросити членів ХАМАС до москви та назвало це «актом, що підтримує тероризм», а також закликало росію вислати делегацію з москви. Однак офіційний кремль не поспішає заявляти своїх намірів щодо підтримки Ізраїлю у даному протистоянні. Більш того, кремль офіційно засудив удари Ізраїлю по сектору Гази, а само керівництво ХАМАСу не раз наголошувало на тісній співпраці з російським керівництвом. У даному випадку причин щодо такого союзу може бути декілька, але головна та найважливіша – це сподівання кремля на зменшення військової допомоги Україні у війні з росією за незалежність.

Про російський вплив в Африці заговорили після 2014 року, коли проти країни почали запроваджувати перші санкції. Континент виявився особливо важливими для оборонного сектора росії, якого позбавили багатьох контрактів у світі. Ще до 2013 року частка російської зброї в Африці коливалася в межах 11-25 %, а вже після 2017 року зросла до понад 40 %. Станом на 2020 рік половина імпортованої зброї Африкою була російською.

Іншим важелем впливу рф на Африканському континенті є енергетика. Майже 600 млн африканців не мають постійного доступу до електроенергії. Посухи й інші катаклізми лише погіршують їхнє становище. З 2019 року Алжир, Гана, Замбія, Нігерія, Руанда зробили ставку на російську ядерну енергію. Зокрема, країна-терорист пообіцяла їм згодом збудувати декілька атомних електростанцій.

Російсько-африканський саміт 2023 року підкреслив прагнення москви розширити свою економічну присутність, орієнтуючись на сільське господарство, гірничодобувну промисловість та енергетику з метою подвоїти показники торгівлі до 2030 року.

Рф та її підприємства – «Росатом» в енергетичному секторі та «Русал» у гірничодобувній галузі – беруть участь у проєктах, які хоч і не масштабні за обсягом інвестицій, але мають значну політичну та стратегічну вагу.

Ці проєкти нерідко стосуються критично важливих ресурсів. Передусім ідеться про уран, який є ключовим для ядерної енергетики й може дозволити рф отримати значний контроль над цими ресурсами. Наприклад, «Росатом» активно збільшує свої запаси урану, у тому числі через придбання проєкту в Танзанії за 1,15 млрд дол. [8].

Російський контроль над ураном стосується не лише сировини, а й усього ядерного паливного циклу. Хоча росія є відносно невеликим виробником «сирого» урану, їй належить значна частка світової інфраструктури його переробки та збагачення – близько 40 % та 46 % відповідно. Ці можливості критично важливі, оскільки дозволяють переробляти «сирий» уран на паливо для ядерних реакторів.

Крім того, росія домінує в експорті атомних електростанцій. У 2012-2021 роках вона ініціювала будівництво 19 ядерних реакторів, причому 15 із них – за кордоном. Це набагато більше за будь-яку іншу країну за той самий період.

Хоча економічна присутність росії в Африці не настільки широка, як китайська, її роль у постачанні стратегічних товарів та військової техніки в африканські країни – це багатогранний виклик. Якби росія отримала контроль над критично важливими ресурсами на кшталт літію чи урану, вона могла б створювати залежності, впливати на ринкові ціни та використовувати їх для політичного впливу – те, що відбувається в інших регіонах.

Потенційні ризики такої діяльності величезні. Контроль над критично важливими ресурсами з боку іноземної держави, особливо агресивної, впливає на суверенітет країн та створює стратегічний виклик глобального масштабу, оскільки ці ресурси критично важливі для «зеленого» енергетичного переходу і технологічного розвитку в усьому світі.

Зрештою, скромна економічна участь росії в Африці може не мати великого значення для москви. Справжні мотиви росії для залучення Африки полягають у просуванні її геостратегічних інтересів – забезпеченні плацдарму в Середземному морі на південному кордоні НАТО, витісненні впливу Заходу та нормалізації світогляду росії. Іншими словами, Африка є засобом для досягнення більших стратегічних цілей росії [9].

Хоча рф вітає розширення можливостей торгівлі з Африкою, найбільш переконливими є політичні вигоди. Маючи 54 голоси в Генеральній Асамблеї ООН, Африка є привабливою «мішенню» для підтвердження військової агресії росії та порушення норм міжнародного права.

Крім того, росія отримує найбільший вплив в Африці за допомогою нетрадиційних, асиметричних інструментів, які вона використовує – кооптації еліти, дезінформації, втручання у вибори, розгортання воєнізованої групи Вагнера та угод зі зброєю в обмін на ресурси.

Починаючи з 2018 року, коли найманці з «Вагнера» розмістилися в ЦАР, москва крок за кроком нарощує присутність і вплив в Африці. Зокрема, у зоні Сахелю, який простягнувся від Атлантичного океану до Червоного моря: **після того, як у Буркіна-Фасо, Малі, Нігері відбулися військові перевороти, хунти, що захопили владу, згортають військове й політичне співробітництво із США та Францією і зміцнюють відносини з росією.**

Водночас, як вважають експерти [10–12], **для Китаю**, який скупив і контролює Африку набагато більше, ніж Сполучені Штати та Франція, **проникнення росії на африканський континент є вигідним, оскільки послаблює вплив США. Конкуренція ж, яка іноді виникає між китайськими й російськими компаніями, не є критичною**, оскільки китайці націлені на участь у розробленні природних ресурсів континенту й наданні кредитів африканським державам, а пріоритет росіян – військова й військово-технічна сфери.

У свою чергу, США на офіційному рівні обговорюють готовність до можливих одночасних воєн із росією та Китаєм. Зокрема, у Звіті Комісії зі стратегічної позиції США [13] зазначається, що США та їхні союзники мають бути готовими стримати та перемогти обох противників одночасно. Також зазначено, що міжнародний порядок «перебуває під загрозою з боку авторитарних режимів Китаю та росії».

Автори звіту вважають, що китайська та російська загрози загостряться у 2027–2035 роках. Через це «рішення необхідно ухвалювати зараз, щоб нація була готова».

Також вони рекомендують до 2046 року повністю профінансувати 30-річну програму модернізації ядерної зброї США, яка в 2017 році оцінювалася в 400 млрд дол.

Серед рекомендацій є і розміщення більшої кількості тактичної ядерної зброї в Азії та Європі та розроблення планів розміщення деяких або всіх резервних ядерних боєголовок США. Крім того, рекомендовано збільшити виробництво стратегічних бомбардувальників B-21 та нових атомних підводних човнів класу «Колумбія».

У березні 2025 року Міністр оборони США Піт Гегсет підписав документ під назвою «Тимчасове стратегічне керівництво з національної оборони». У ньому йдеться про реалізацію концепції президента Дональда Трампа щодо підготовки США до можливої війни з Китаєм та захисту національної безпеки, включно з такими стратегічними точками, як Гренландія та Панамський канал.

Окрім переорієнтації військових ресурсів на Індо-Тихоокеанський регіон, меморандум також визначає нові завдання для Міноборони США.

У документі Гегсета зазначено, що потенційне вторгнення Китаю на Тайвань є пріоритетною загрозою, що перевищує інші можливі виклики. Відповідно, структура та ресурси американських збройних сил будуть спрямовані насамперед на протидію Пекіну.

Водночас Вашингтон планує чинити тиск на своїх союзників у Європі, на Близькому Сході та у Східній Азії, вимагаючи від них збільшення витрат на оборону та активнішої участі у стримуванні загроз із боку росії, Північної Кореї та Ірану.

Документ також передбачає, що Пентагон змінить підхід до контртерористичних операцій. Пріоритет буде надано боротьбі з угрупованнями, які можуть безпосередньо загрожувати США, тоді як увага до терористичних мереж, що діють локально без міжнародних амбіцій, зменшиться.

«Китай – єдина загроза, на яку орієнтується міністерство, а запобігання захопленню Тайваню – ключовий сценарій, навколо якого будується оборонна стратегія США», – заявив Гегсет у меморандумі.

1 травня 2025 року Піт Гегсет підписав Меморандум щодо розроблення нової Стратегії національної безпеки США. Відповідно до прес-релізу міністерства оборони США, структурним підрозділам відомства поставлено завдання розробити нову стратегія з урахуванням передвиборчих обіцянок президента Трампа – «Америка понад усе» та «Мир через силу» [14].

1.2. Глобальний Південь як мегасуб'єкт сучасної геополітичної гри

Повномасштабне вторгнення рф в Україну докорінно змінило сприйняття безпекової ситуації у світі як на глобальному, так і на регіональному й субрегіональному рівнях. Картина сучасного світу явно контрастує з тією, що була в другій половині XX ст., коли холодне протистояння між геостратегічним Сходом та Заходом базувалося швидше на міжнародній статиці, аніж динаміці.

Як слушно зауважив Надзвичайний і Повноважний Посол України в Японії Сергій Корсунський: «Стан геополітики на сучасному історичному етапі можна описати не надто простою, але зрозумілою для втаємничених формулою: кількість країн, які бажають закласти свою цеглу у фундамент нового світового порядку, більша або дорівнює кількості потенційних посередників у можливих переговорах із росією щодо припинення війни й набагато менша за кількість вітчизняних експертів із Південно-Східної Азії, які ніколи там не були, але все добре розуміють. На виправдання останніх слід визнати, що розібратися в суперечливих діях деяких найважливіших країн регіону справді важко» [15].

Таким чином, важливість Східної та Південно-Східної Азії для світової політики й економіки є аксіомою сучасної геополітики. Глобалізація й Інтернет практично унеможливили ізоляціонізм, усунули віддаленість від зон конфліктів, і нині те, що відбувається в Європі, безпосередньо відгукується в Азії. Росія десятиліттями просувала свої інтереси в Індії та Китаї, постачала до Індо-Тихоокеанського регіону зброю, відкривала в багатьох країнах освітні центри й формувала експертне середовище. Міфи про «велику російську культуру», «боротьбу СРСР, а потім і росії проти імперіалізму-колоніалізму», агресивне нав'язування вигідних і вигаданих історичних наративів і пряма політична корупція – далеко не повний перелік інструментів, які москва використовувала для формування системи впливу на громадську думку та політичні кола.

Звісно, що кремль вважав, що його вторгнення не викличе сильної та рішучої відповіді Заходу, проте російське вторгнення привело до надзвичайної єдності та дій ліберально-демократичного

світу. Країни Заходу скоординували безпрецедентний перелік економічних санкцій проти росії.

2 березня 2022 року була прийнята перша резолюція одинадцятої надзвичайної спеціальної сесії Генеральної Асамблеї ООН (Резолюція Генеральної Асамблеї ООН ES-11/1) [16]. У документі висловлено жаль з приводу російського вторгнення в Україну та вимогу повного виведення російських військ і скасування рішення про визнання самопроголошених Донецької та Луганської Народних Республік. Резолюцію було ухвалено: 141 голос – «за», 5 – «проти», 35 – «утрималися», 12 – «відсутні».

У свою чергу, більшість «неєвропейських» країн, які проголосували за засудження агресії росії в березні 2022 року, не ввели санкції проти цієї держави.

Загалом у серії голосувань в ООН з початку війни близько 40 країн, що становлять майже 50 відсотків населення світу, регулярно утримувалися або голосували проти пропозицій із засудженням російського вторгнення.

На думку експертів впливового видання *Foreign Affairs,* суперечки викликані не розбіжностями щодо війни в Україні, а, натомість, є симптомом ширшого синдрому: гніву з приводу подвійних стандартів Заходу та розчарування з приводу зусиль щодо реформування міжнародної системи. Зокрема, деякі з них зазначають, що заснований на правилах міжнародний порядок не служить інтересам Африки. Навпаки, він зберіг статус-кво, за якого великі світові держави – західні чи східні – зберегли свої позиції домінування. Через РБ ООН , зокрема, Китай, Франція, росія, Великобританія та США здійснили величезний вплив на африканські країни та понизили африканські уряди лише до сторонніх спостерігачів у їхніх власних справах [17, 18].

Авторитетний індійський дипломат Шівшанкар Менон підкреслив цю думку на початку 2024 року, написавши: «Відчужені та ображені, багато країн, що розвиваються, бачать війну в Україні та суперництво Заходу з Китаєм як відволікання від нагальних питань, таких як борги, зміна клімату та наслідки пандемії» [18].

Тобто можемо констатувати, що Realpolitik зіграла свою роль у визначенні позицій окремих країн щодо повномасштабного вторгнення рф в Україну. Індія традиційно була залежною від росії щодо

військово-технічного співробітництва. Приватна військова компанія (ПВК) «Вагнер» співпрацює з урядами Західної та Центральної Африки, щоб підтримати їхні режими та виживання. А Китай, який є одним із головних джерел підтримки росії, – найбільший торговельний партнер понад 120 країн світу.

Таким чином, так званий Глобальний Південь останніми роками став актуальним чинником сучасних геополітичних процесів. Хоча ніхто на світовій арені нині не уявляє Глобального Півдня загалом. Дуже хоче його організувати й очолити об'єднання БРІКС (англ. BRICS від Brazil, Russia, India, China, South Africa), другий кандидат – ШОС (Шанхайська організація співробітництва).

Аналіз показує, що кожен, хто згадує про Глобальний Південь, розуміє під ним щось своє. Одні мають на увазі групу держав із колоніальним минулим; інші – широкий спектр країн, що розвиваються, або в крайньому разі – членів Руху неприєднання або «групи 77». Ніхто й ніколи не складав переліку країн Глобального Півдня, і кожне зі згаданих визначень не є ні вичерпним, ні однозначним.

Поділ на умовні Південь і Північ виник в умовах Холодної війни, коли світ поділився на два табори: східний, керований СРСР, та західний – на чолі із США та країнами Західної Європи. В умовах цього протистояння виникла третя сила: країни, які не приєдналися ані до першого, ані до другого табору.

Термін «Глобальний Південь» уперше до широкого загалу ввів у 1969 році американський політичний експерт Карл Оглсбі. В одній зі своїх статей він висловив думку, що війна у В'єтнамі завершує еру домінування цивілізаційної Півночі над Півднем. Під «Північчю» він мав на увазі світові імперії, метрополії, тоді як терміном «Глобальний Південь» узагальнив колоніальний світ. У 60-х щодо колишніх колоній європейських (переважно) країн частіше вживали термін «третій світ». Малося на увазі, що «перший світ» – це найрозвинутіші демократичні країни з ринковою економікою, «другий світ» – соціалістичні країни, а «третій світ» – відповідно всі інші. Тобто країни, які за своїми якостями неможливо віднести до жодного з перелічених світів.

У такій класифікації явно відчувався дискримінаційний підтекст та симпатія до країн «першого світу». Здебільшого такими країнами були колишні колонії, які, отримавши незалежність, не завж-

ди швидко орієнтувалися в перипетіях міжнародних відносин та не приєдналися до жодного з таборів. Оскільки за цим формулюванням читалося словосполучення «третій сорт», то його вважали не зовсім коректним. Відтак з 1991 року (коли припинив своє існування «другий світ») частіше став вживатися саме термін «Глобальний Південь».

У 1980-му очолювана колишнім канцлером Федеративної Республіки Німеччини Віллі Брандтом комісія опублікувала доповідь. Комісія констатувала величезну прірву в економічному розвитку різних країн світу. Цей поділ демонструвала так звана лінія Брандта. Ця лінія охоплює планету на рівні 30° північної широти, проходить між Північною та Центральною Америкою, північною частиною Африки, Близьким Сходом і більшою частиною Східної Азії. Далі лінія опускається на південь так, щоби показати належність Японії, Австралії та Нової Зеландії до Глобальної Півночі [19].

Географічно термін «Глобальний Південь» застосовується до 32 країн, розташованих нижче екватора (у Південній півкулі), що відрізняє їх від 54 країн, які цілком розташовані на північ від нього. Однак цей термін нерідко помилково використовують як коротку назву для глобальної більшості, хоча більшість світового населення живе вище екватора (і там же розташована основна частина світової суші). Наприклад, ми часто чуємо, що Індія, найбільш густонаселена країна світу, і Китай, який посідає друге місце за чисельністю населення, змагаються за місце лідера Глобального Півдня. Із цією метою обидві країни нещодавно провели дипломатичні конференції. Однак обидві розташовані в Північній півкулі.

Крім цього, якщо брати до уваги географічну складову, то можна взяти за основу визначення Світового Банку, яке об’єднує в собі країни середнього доходу, розташовані в Африці, Азії, Океанії, Латинській Америці та Карибському басейні. Не всі країни, які знаходяться на півдні, належать до Глобального Півдня – так, до нього не входять Австралія та Нова Зеландія, натомість межі півдня є досить умовними, і деякі експерти вважають, що до нього належить, наприклад, Туреччина.

А отже, цей термін є переважно політичним гаслом, ніж точним описом світу. І в цьому сенсі він, судячи з усього, набув популярності, виконуючи функцію евфемізму для заміни менш прийнятних термінів.

У сучасній геополітиці термін «Глобальний Південь» особливо активно експлуатують ревізіоністські держави, які прагнуть нового переділу світу. Наприклад, представляти інтереси неіснуючого об'єднання країн хочуть Китай і росія. Щоправда, розуміючи своє політичне банкрутство, рф придумала ще один варіант назви – **«глобальна більшість»,** який, як і всі попередні варіанти, не має ні визначення, ні класифікації. Якщо судити з результатів голосування за резолюції Генеральної Асамблеї ООН, то росія якраз у меншості, а якщо пробувати поміркувати над спробами зарахувати до «глобальної більшості» найбільш густонаселені країни світу – Китай та Індію, які з різних причин входять і до БРІКС, і до ШОС і водночас претендують на власне лідерство в представленні інтересів «Глобального Півдня», то треба спершу запитати в них, чи згодні вони з претензіями рф зрівнятися з ними.

Країни Глобального Півдня дуже різноманітні. До них належать держави з майже ідеальними показниками демократії й відверті диктатури. Частина країн, що належать до Глобального Півдня, засудила вторгнення росії в Україну, але є й чимало держав, які зайняли нейтральну позицію, точніше, **позицію «не висловлювати жодної позиції».**

Борцем за права Глобального Півдня та членом БРІКС є **Південна Африка.** За даними «The Africa Wealth Report 2024» компанії «Henley&Partners» у цій країні за підсумками 2023 року налічувалося 37 400 доларових мільйонерів, 102 мультимільйонери й п'ять мільярдерів [20]. Ця країна посідає перше місце в «індексі нерівності» швейцарського банку UBS із показником 82 зі 100 можливих, зростання – 17,7 % проти 2008 року. Тільки в Йоганнесбурзі – 12 300 мільйонерів і два мільярдери.

Бразилія – на другому місці в «індексі нерівності», **Індія** – на четвертому. **США**, яким БРІКС кидає виклик, – на почесному третьому місці. Країни Глобального Півдня, як-от **Єгипет, Нігерія, Кенія, Марокко, Маврикій, Алжир, Гана, Ефіопія й Намібія,** належать до лідерів континенту за кількістю доларових мільйонерів, і прогнози кажуть про зростання їхньої кількості на 80 % упродовж наступних десяти років.

За даними звіту OXFAM **(Oxford Committee for Famine Relief),** традиційно представленого в Давосі, 1 % багатих людей Аф-

рики володіє майже половиною багатства континенту. Майно сімох найбагатших людей становить 52 млрд дол., що перевищує доходи 700 млн африканців. Єдиний мільярдер Зімбабве збільшив своє майно на 40 % з 2020 року, а найбагатша людина Африки – нігерієць, у нього монополія на цемент, і він платить податок в 1 % із прибутку вже 15 років.

Цікаво, що, за даними OXFAM, **країни Африки щороку недоотримують по 200 млрд дол. через різні схеми ухиляння від податків найбільших корпорацій – національних і міжнародних**. Тим часом саме корпоративні податки для африканських держав **є основним джерелом фінансування соціальних програм і формування бюджетів**. Узагалі всі ці проблеми – не африканські й не «південні», а загальносвітові. П'ятеро найбагатших людей планети подвоїли свої статки за останні три роки, тоді як доходи 5 млрд людей за цей час зменшилися [21]. **13,5 % населення Індії живе на 15 дол. на місяць, ВВП (**валовий внутрішній продукт) **на душу населення трохи перевищує 2 тис. дол.** Водночас у липні 2024 року засоби масової інформації (ЗМІ) повідомили про триденні святкування з нагоди весілля сина найбагатшої людини в Індії й Азії **Ананта Амбані**. За різними оцінками, витрати на грандіозний захід становитимуть до 350 млн дол. На весілля запросили не лише прем'єр-міністра найбільшої демократії Азії Нарендру Моді, членів уряду й парламенту, а й Марка Цукерберга, Білла Гейтса, Гілларі Клінтон, Тоні Блера, Бориса Джонсона, сестер Кардаш'ян, Бекхемів, доньку Трампа Іванку й багатьох інших [22].

У свою чергу, науковці Берлінського університету імені Гумбольдтів порахували, що 2004 року поняття «Глобальний Південь» зустрічалося в публікаціях близько 20 разів. Тоді як 2014-го таких публікацій було вже сотні.

Боротьба за Глобальний Південь була завжди й активізувалася в 50–60-ті роки через розпад колоніальної системи, коли в Африці, Азії і на Близькому Сході постали нові держави.

Але останнім часом ця увага справді зростає. У країнах Глобального Півдня живе більшість населення планети. А демографія показує, що через 25 років кожен п'ятий на Землі буде африканець. Географічні та кліматичні фактори, забезпечення міграційної безпеки – усі ці питання не дозволяють Глобальній Півночі не враховувати те, що відбувається тут.

Крім того, зауважує Ігор Семиволос, зростання уваги до Півдня збігається з певною кризою Заходу, який тривалий час активно контролював цю територію, а тепер відмовляється від цієї ролі. І в цих місцях виникає порожнеча, яку намагаються заповнити інші держави, зокрема Китай чи Індія [23].

Відомий індійський аналітик Сі Раджа Мохан зазначив: «Три саміти – один у Давосі, Швейцарія, а інші два (*NAM* і *G77*) у Кампалі, Уганда – вказують на те, що глобальна політика зміниться у 2024 році. Багаті та могутні люди світу в Давосі та знедолені в Кампалі мають спільну думку. Проблема – вирішення структурних змін у міжнародній системі. Старі гасла – про глобалізм у Давосі та колективізм Глобального Півдня в Кампалі – більше не заслуговують на довіру та не є стійкими». Саміти, на його думку, також підкреслюють контраст між планами на майбутнє провідних держав Азії – Індії та Китаю, які змагаються, з-поміж іншого, і за вплив на Глобальному Півдні. Щорічна зустріч у Давосі є визнанням того, що відновлений конфлікт великих держав та економічний націоналізм загальмували «візок глобалізації», тоді як саміти в Кампалі виявили, що відновлена протягом останнього року політична ейфорія щодо Глобального Півдня недостатня для вирішення викликів і можливостей мінливого світового порядку [24].

Тобто публічно доступні дані свідчать про **деяку невідповідність ідейного образу жертв колоніального минулого й практичних інтересів бізнес-еліти «жителів півдня».**

Але ж, виходячи з тих подій, які переживає Україна та й увесь світ у зв'язку з повномасштабною військовою агресією рф, слід говорити про наочну політичну кризу в сучасних міжнародних відносинах та важливість залучення держав Глобального Півдня до обговорення міжнародного порядку денного.

І, щоб досягти успіху на цьому шляху, ми маємо підходити індивідуально до кожної із цих країн, бо немає загального Глобального Півдня. Є партнери, які вже з нами або яких уже треба переводити на наш бік.

Більшість країн Глобального Півдня намагаються представити свою **позицію щодо російсько-української війни як нейтральну**. Серед основних причин такої позиції можна виділити:

- загальні антиамериканські настрої в окремих країнах, які при цьому необов'язково автоматично стають проросійськими у своїй позиції;

• асоціація рф із так званою антиімперіалістичною потугою, ідеологічною спадкоємицею СРСР, а відповідно більшості західних країн, які підтримали Україну, як представників імперіалістичних держав, що асоціюються з диктатом і колоніальним минулим;

• несприйняття української боротьби як антиколоніальної. Тут відбувається нашарування як стереотипного мислення, що «білі не можуть бути колонією», так і асоціація України з Європою, яка завжди сприймається як колонізатор;

• одночасна залежність від західної економічної допомоги та обіцянок економічної допомоги або існуючих контрактів із рф;

• історична приналежність до руху неприєднання.

У частини країн є нерозуміння, **яким чином може відбуватися формування умов для закінчення конфлікту, якщо до переговорів не залучена інша сторона – росія**. Тобто для країн залишаються незрозумілими формат і мета ініціативи. Ті, хто представляє себе як нейтральних, мають застереження, оскільки вважають, що поточні зустрічі мають на меті формування позиції однієї «сторони» (України та Заходу) проти іншої (росії). А відповідно їхня участь у зустрічах, присвячених українській «Формулі миру», буде розцінена як займання української сторони в конфлікті.

Інше важливе нерозуміння в середовищі країн так званого Глобального Півдня – **чому вони взагалі повинні цікавитися українськими питаннями** та долучатися до вирішення конфлікту, який знаходиться так далеко від них. Цьому, зокрема, сприяє і значна дипломатична та пропагандистська робота рф щодо просування фейкової інформації щодо причин війни, ситуації з українськими біженцями, причин відсутності експорту зерна тощо. Але часто у внутрішніх дискусіях лунають і аргументи, що Україна ніколи не цікавилась їхніми проблемами, відповідно, немає підґрунтя для солідарності.

Через низький рівень грамотності населення країн Глобального Півдня можна сміливо стверджувати, що про Україну там у кращому разі знають як про колишню радянську республіку. І новітню історію чули у викладеному російською пропагандою варіанті. Проте в цих державах більшу роль відіграють настрої еліт, а еліти, як відомо, мислять більш прагматично, ніж ціннісно. Російська пропаганда намагається показати Глобальний Південь у світлі якщо не союзника, то співчуваючих держав.

1.3. Стратегічні виклики в умовах війни: пріоритети і завдання

Війна в Україні прискорила глобальні процеси, зумовила зростання невизначеності, непередбачуваності та, відповідно, нервозності в поведінці окремих гравців. Це суттєво ускладнює прогнозування майбутнього, визначення стратегічних і тактичних пріоритетів, координацію поточної співпраці країн у межах спільних дій, спрямованих на подолання кризових явищ.

Глобальні трансформації, що відбуваються у світі, стосуються не лише безпеки та протистояння ідеологій, а й формування нової економічної моделі, яка без перебільшення визначить майбутнє людства.

Світова спільнота має віднайти нову модель свого функціонування й розібратися з нинішніми політичними й економічними проблемами. Захід – як провідна цивілізація – перебуває сьогодні у кризі. Хоча ліберальним демократіям удалося розширити «велику Європу» за рахунок включення в неї постсоціалістичних держав, але цим справа й обмежилася.

Зокрема, колишній радник Президента США з питань національної безпеки Герберт Макмастер так охарактеризував ключові уроки із вторгнення росії в Україну [25]:

По-перше, чергове жорстоке вторгнення в Україну в лютому 2022 року показало, що немало представників вільного світу «прикипіли» до своїх надміру оптимістичних припущень про світ після Холодної війни. Наприклад, припущення, що логіка історичного процесу нібито гарантує перевагу вільних і відкритих демократичних суспільств над закритими авторитарними системами. Західні політики вирішили, що протистояння великих світових потуг залишилося на смітнику історії. Проте голова КНР Сі Цзіньпін і президент рф В. Путін мали іншу думку. Виголошена двома диктаторами напередодні Олімпійських ігор у Пекіні спільна заява хоч і сповнена дезінформації, безкінечної підміни понять та орвеллівського перекручування правди, однак у ній було донесено чітку позицію. Вони націлилися перехопити глобальне лідерство у демократій, які вважають розділеними, ослабленими та занепалими. Висновок із цього можна зробити такий: партнери-однодумці у всьому вільному світі мають визначити нові способи ефективного протистояння росії та Китаю.

По-друге, Захід зрозумів, що тристороння дипломатія, яку практикували Президент США Річард Ніксон і державний секретар США Генрі Кісінджер у 1970-х роках, прагнучи зробити відносини США окремо із СРСР та з Китаєм більш тісними, ніж ці дві держави мали між собою, просто неможлива у світі, де дві реваншистські потуги заприсяглися, що «дружба між двома державами не має обмежень». Китай підтримав цю клятву, виголошену перед Олімпійськими іграми 2022 року, одіозною «дипломатією воїна-вовка», яка зумисне посилювала дезінформацію кремля та намагалася пом'якшити фінансові й економічні збитки від упроваджених більшістю вільного світу санкцій проти рф. Ідея, щоб Китай і росія стримували одне одного, чудова, проте наші противники координують спільні дії проти вільного світу. Ці дві країни почергово відіграють ролі то «палія», то «пожежника» в конфліктах повсюди – від Сирії до Пакистану, від Північно-Східної Азії до залів засідань ООН. Тому не варто розділяти Сі й Путіна, вільний світ має розглядати двох диктаторів як єдине ціле. І не лише тому, що вони один одного варті, а й тому, що вигоди від партнерства росії та Китаю великою мірою посилюються через змогу прикривати один одного в заплутуванні, перешкоджанні, примушуванні й саботуванні.

По-третє, російська агресія та українська відвага показують, що хоча війна й не є бажаним способом розв'язання суперечок, вона буває єдиним способом зробити так, щоб хтось інший не розв'язав їх замість вас. Перефразовуючи вислів британського теолога та філософа Ґілберта Кіта Честертона, можна сказати, що потреба зміцнити колективну оборону, щоб відновити політику стримування й підготуватися до реакції на агресію, уже перезріла. США, країни НАТО та держави з-поміж їхніх однодумців на кшталт Японії мусять без зволікань посилити не лише свої військові спромоги, а й допомогти зміцнити оборону Тайваню з огляду на те, що можна було зробити до 24 лютого 2022 року для допомоги Україні запобігти новому російському вторгненню.

По-четверте, покладатися на авторитарні режими щодо енергоносіїв є фатальною помилкою. Для Німеччини стрибок до невідновлюваних джерел енергії в поєднанні з відмовою від ядерної енергетики став кроком у прірву «обіймів» рф. Залежність від російської

нафти й газу на перших порах послабила реакцію Німеччини на чергове жорстоке вторгнення росії в Україну, змусила її спалити більше вугілля та створити більше викидів вуглецю, щоб в оселях не згасло світло. Тому із цього можна дійти висновку, що нам потрібні нові політики, які поєднуватимуть енергетичну безпеку з національною, а також із політикою скорочення вуглецевих викидів.

По-п'яте, навіть поодинокі розриви в ланцюгах постачання, які контролюють агресори, підривають суверенітет й ускладнюють реагування на агресію. Прикладом є не лише залежність Європи від російської нафти та газу, а й залежність Індії від російської зброї. Через це Сі Цзіньпін вибудовує економіку «подвійної циркуляції», яка, з одного боку, мало залежить від закордонних ринків, фінансів і технологій, а з іншого – посилює залежність інших держав від китайських товарів, їхніх базових складників і матеріалів. Наприклад, Китай намагається домінувати в ланцюгах постачання, критично важливих для переходу до чистих джерел енергії.

Таким чином, російсько-українська війна кинула тотальний виклик сучасній глобалізації світу. І нині саме Україна стала тим чинником, що визначив декілька тенденцій світового розвитку [26, 27].

По-перше, сучасний глобалізований світ перетворився на зону перманентного конфлікту між росією і Заходом. Війна консолідувала країни західного світу в боротьбі з неототалітарною росією.

По-друге, Україна стала своєрідним тестом на готовність Заходу, і передусім Європи, знову знайти й виконати свою цивілізаційну місію та сформувати активну зовнішню політику, спрямовану в майбутнє. Виникає й поглиблюється розуміння причетності євроатлантичної спільноти до перемоги України. У прагненні до гідного миру нас підтримує демократичний світ, передусім євроатлантична цивілізаційна спільнота. Трансатлантична співпраця лише активізувалася після вторгнення росії в Україну. Прикметно й те, що НАТО розширилося на порозі росії: Швеція і Фінляндія відмовилися від десятиліть нейтралітету і стали повноправними членами НАТО.

По-третє, відбуваються відродження й розвиток цивілізаційної суб'єктності України в євроатлантичному геополітичному просторі. Маємо визнання світом причетності народу України до євро-

атлантичної цивілізаційної спільноти. Україна продемонструвала готовність вийти з пострадянського стану й перебування в сірій проміжній зоні та обрала європейський вектор розвитку. У дійсності ми відійшли від «руського міра», нас уже прийняли в Європу.

По-четверте, російське вторгнення в Україну продемонструвало деєвропеїзацію росії, її поворот до східного вектору своєї історії. Стан і тенденції розвитку насамперед етно-демографічної структури російського суспільства – серйозний мотив для російської еліти шукати партнерства і в мусульманському світі, і кооперуватися з Китаєм тощо.

По-п'яте, російсько-українська війна оприявнила факт неймовірної історичної ваги: усі лінії історичних протистоянь росії з Європою пролягають культурними теренами України. Нині ми є свідками завершення російської ідеологічної парадигми, яку раніше частково перейняв і Захід: у межах цієї парадигми Україні було відведено маргінальну роль культурної провінції «руського міра». Сьогодні цікавість до України зростає з імперативною швидкістю – і на цей запит потрібно відповідати. Тому необхідно розробити й презентувати саму концепцію української культури й ролі України в європейській історії.

По-шосте, поглиблюється розуміння того, що війна росії проти України – це екзистенціальна й світоглядна війна. Війна не просто за інтереси чи потреби, а за цінності та ідентичність. І не лише для України, а й для всього західного світу. Тому реальна перемога України у війні має глобальний смисл для майбутнього людства. У нинішній російсько-українській війні крім геополітичних та економічних питань вирішується й екзистенціально-політичне питання: хто є аутентичним нащадком Київської Русі – Україна чи росія? Тому однією з причин війни росії проти України є й екзистенціальне бажання з'єднатися зі своїм корінням – Києвом як «матір'ю міст руських». Це й зумовлює позараціональний, екзистенціальний характер війни проти України. Це означає, що росія, всупереч своїм заявам, передусім воює не з колективним Заходом чи НАТО, а з усією військовою жорстокістю вирішує віковічну суперечку з Україною. Завдяки надзвичайному опору, мужності й героїзму народу Україна буквально закарбувалася на ментальній мапі багатьох людей в усьому світі – людей, які до повномасштабного вторгнення

росії не знали, де є Україна на мапі світу. Тому сьогодні важливою є й проблема поширення знання про Україну за кордоном, просування українського культурного продукту та інституційні гарантії цього процесу.

По-сьоме, війна в Україні стала своєрідним каталізатором для нового гуманізму, хвилі якого розходяться по всьому світу, нейтралізуючи неототалітаризм і торуючи шлях до формування нового типу цивілізації – цивілізації подолання війни як способу вирішення конфліктів між народами, державами, країнами та союзами країн. Для цього необхідно викрити й зупинити неототалітаризм як принципово згубний шлях для людства, який заперечує демократію, права людини і, зрештою, розвиток [28].

У свою чергу, за оцінками експертів Центру Разумкова, війна виявила низку проблем у системах глобальної і регіональної безпеки [29]:

1. Практика використання права вето в РБ ООН гальмує, а в гіршому разі унеможливлює ухвалення рішень щодо врегулювання конфліктів, які прямо чи опосередковано зачіпають інтереси постійних членів ради. Неприпустимим є те, що в російсько-українській війні росія, постійний член РБ, є визнаним агресором, який блокує рішення, пов'язані з розв'язанням конфлікту. Це суперечить здоровому глузду й потребує негайного реформування ООН.

2. Система безпеки ООН не продемонструвала ні політичної волі, ні ефективності механізмів розв'язання конфліктів, дотримання міжнародних норм і взятих зобов'язань. З арсеналу РБ практично зникли передбачені Статутом ООН операції щодо примусу до миру через брак політичної волі, фінансових і військово-технічних ресурсів та ветування таких рішень. Натомість практикують більш м'які засоби: операції щодо побудови миру та підтримання миру (так звані операції згідно з главами VI+ або VII–). Намагання ООН та інших безпекових організацій уникати складних проблем призводить до їхнього поглиблення замість розв'язання. Надання пріоритету щодо припинення вогню в політичному врегулюванні збройних конфліктів призводить до їхнього заморожування з наступною ескалацією. Яскравим прикладом є заморожування конфлікту на Донбасі у 2014 році, який прогнозовано переріс у повномасштабну агресію рф проти України.

3. Захід у цілому, його безпекові інститути, системи забезпечення національної безпеки переважної більшості західних держав виявилися неготовими до повномасштабної агресії росії, яка поставила світ на межу Третьої світової війни. З іншого боку, для всього світу стало несподіваним, що такий потужний агресор, як росія, може зазнати не лише опору, але й поразки у протистоянні з країною, народ і влада якої є консолідованими в захисті свободи та територіальної цілісності. Ба більше, Захід міг би й не оговтатися або принаймні зазнав би суттєвих іміджевих втрат після такого нахабного й агресивного «підвищення ставок» кремлем, якби Україна не зірвала російський бліцкриг. Початкова фаза війни росії проти України, висунення рф ультиматумів НАТО, її черговий ядерний шантаж США та європейських країн засвідчили необхідність присутності в арсеналі систем колективної та національної безпеки засобів завчасного виявлення ризиків, запобігання загрозам, адекватного й ефективного реагування не лише безпосередньо на агресію, а й на погрози нею. Підвищилась актуальність як наявності й запасів сил, так і засобів та ресурсів, а також й ефективних, опрацьованих механізмів їх залучення, готовності їх використовувати та надавати допомогу союзникам і партнерам.

4. Зростає ступінь гібридності міжнародних конфліктів і криз, що характеризується появою нетрадиційних видів зброї, таких як енергоресурси, політична корупція, агресивна пропаганда, кіберзброя. Останнім часом до них додалося продовольство. Застосування цієї зброї державою-агресором розкриває її як підступного та жорстокого актора. Головними напрямами та проявами використання цих видів зброї росією наразі є такі:

- тиск на Захід через намагання зганьбити його, закликаючи країни Азії й Африки згадати про їхнє колоніальне минуле, наголошуючи на нерівності між країнами Півночі та Півдня, поширюючи фейки про походження COVID-19 і несправедливий розподіл вакцин;
- підрив єдності Європи через поглиблення енергетичної кризи та посилення невдоволення населення європейських країн напередодні та під час зимового періоду;
- сподівання на зниження стійкості країн ЄС, відволікання їхньої уваги від війни в Україні через вимушене реагування на міграційні хвилі, спровоковані браком зерна, постачання якого з портів України було заблоковано самою росією;

• зміцнення своїх позицій на міжнародній арені через протиставлення росії «загниваючому» Заходу;

• пом'якшення наслідків санкцій способом неприєднання до них окремих країн через запровадження «сірих» і контрабандних схем постачання необхідних російській оборонній промисловості товарів і технологій;

• ослаблення економічного потенціалу України й блокування західної допомоги.

5. Війна висвітлила проблемні питання стосовно ефективності чинних економічних і безпекових союзів. Головними проблемами тут є помилки в оцінюванні ризиків, неспроможність запобігти кризовим явищам, запізнення в реагуванні на них, безвідповідальне ставлення окремих союзників до потреб у ресурсах. На цьому тлі лунають апокаліптичні висновки про кінець глобалізації, завершення епохи крупних союзів та перехід ініціативи до мережевих структур у вигляді автономних регіональних і субрегіональних союзів, альянсів, коаліцій. Ознаки таких процесів справді трапляються, проте їх спрямовано на пошук способів домогтися внутрішньої солідарності та стійкості наявних міждержавних альянсів і коаліцій. Прикладами можуть бути такі:

• уже наявний в Європі Північно-європейський оборонний союз, Вишеградська четвірка, Люблінський трикутник, проєкт Тримор'я;

• ініціатива Б. Джонсона щодо створення поза межами ЄС під егідою Великої Британії нового воєнно-політичного та економічного союзу за участю України, Польщі, Естонії, Латвії, Литви й Туреччини;

• ідея Е. Макрона, що вже почала втілюватися, щодо створення Європейської політичної спільноти із залученням, окрім членів ЄС, усіх країн Західних Балкан, України та Молдови;

• коаліції держав, що склалися навколо допомоги Україні в боротьбі з російською агресією (процеси «Рамштайн» і «Копенгаген»).

На думку експертного середовища, події, які з високою ймовірністю відбуватимуться протягом XXI ст., можуть бути такими [30]:

1. Формування світової коаліції демократичних держав. Перед загрозою гітлерівського поневолення світу Президент США Ф. Рузвельт та Прем'єр-міністр Великої Британії В. Черчілль 14 серпня

1941 року підписали Атлантичну хартію, яка стала основою формування антигітлерівської коаліції держав та забезпечила розгром третього рейху та його союзників. За 80 років 10 червня 2021 року Президент США Дж. Байден і Прем'єр-міністр Великої Британії Б. Джонсон підписали нову атлантичну хартію, метою якої проголошено боротьбу демократичних країн проти авторитарних режимів XXI ст. Такі режими з огляду на їхні глобальні амбіції становлять реальну загрозу для людства, яку слід максимально обмежити. На основі нової атлантичної хартії в умовах ескалації російсько-української війни 22 квітня 2022 року виникло об'єднання «Рамштайн» – серія дипломатичних зустрічей міністрів оборони демократичних країн, які відбуваються задля синхронізації зусиль щодо прискореного надання зброї Україні для протистояння російському широкомасштабному вторгненню, а також задля обговорення питань підтримки України після закінчення війни. Із високою ймовірністю «Рамштайн» є ситуативним демократичним об'єднанням на період російсько-української війни, що в повоєнний час, зважаючи на досвід Великої сімки, Організації Північноатлантичного договору, ЄС, інших організацій та об'єднань, трансформується у світову мережу демократій, спроможних на швидку колективну відповідь авторитарному подразнику.

2. Складання світового блоку авторитарних держав. Ідеться про КНР, рф, КНДР, Іран, Сирію, Білорусь, Венесуелу та деякі інші країни. На лідерські позиції цього блоку неприховано претендує Китай, хоча інституційних форм воєнно-політичної взаємодії із собі подібними режимами (на кшталт альянсів або коаліцій) Пекін традиційно уникає. Із боку КНР вітатиметься економічна взаємодія авторитарних країн, доповнена духовно-психологічною близькістю їхніх лідерів. Посилення африканських позицій Китаю має як суто економічні підстави, так і політичні. На цьому недемократичному континенті відбувається селекція місцевих режимів у пошуках надійних партнерів КНР на тривалу історичну перспективу. Не може не насторожувати намір Китаю до 2049 року (100-річчя проголошення КНР) довести цивілізаційну перевагу автократій над демократіями, навіть якщо для цього доведеться застосувати військову силу за межами своєї країни. У випадку з КНР маємо реставрацію імперського ставлення реально «великої» країни (світової економічної

потуги № 1) до інших країн і народів, які не вписуються в параметри великодержавності по-пекінськи.

3. Створення нової двополюсності світу, принципово відмінної від двополюсності другої половини XX ст., по осі геостратегічний Захід на чолі із США – геостратегічний Схід на чолі із СРСР. Наведені вище пункти 1 і 2 створюють достатні підстави для відмови як від однополюсного сприйняття світу, так і його багатополюсних версій. До середини століття чітко сформується двополюсна модель світоустрою, де проти глобального Заходу на чолі із США буде глобальний Схід з елементами глобального Півдня під проводом КНР.

4. Деімперіалізація росії. На противагу китайським великодержавним приготуванням відбудеться руйнування імперського комплексу рф. Цей процес доцільно розуміти як втрату москвою претензій на світове домінування, виснаження необхідного для цього ресурсного (насамперед економічного) потенціалу. Очікується, що рф втратить частини територій, захоплених у 1945 році (Калінінградська область, Курильські острови), а також, що до Китаю відійде 1,5 млн кв. км, визнаних російськими на основі Айгунського договору 1858 року та Пекінського договору 1860 року. У разі реального повернення цієї території КНР претендуватиме на нові території, незважаючи на міжнародне право. Не менш очікуваним може стати державотворчий ренесанс на Північному Кавказі, заснований на відновленні державності Чечнею-Ічкерією та проголошенні державно-політичної незалежності Інгушетією й Дагестаном. Якщо подібний сценарій буде реалізовано, до нього можуть долучитися волзькі адміністративні одиниці, насамперед Татарстан. У будь-якому разі фактор рф у міжнародних справах слабшатиме порівняно з попередніми епохами.

5. Радикальне оновлення наявних міжнародних організацій ((ООН, Організації з безпеки і співробітництва в Європі (ОБСЄ), Ради Європи (РЄ)) або створення нових. Міжнародні організації XX ст. (насамперед безпекові) у своїй більшості довели недієздатність в умовах суттєвого загострення міжнародної обстановки початку XXI ст. Справедливо критикують РБ ООН та ООН у цілому, які не запобігли ні поширенню COVID-19, ні російському вторгненню в Україну, ні новітній мілітаризації держав і міжнародних відносин загалом. Маємо ситуацію критичної невідповідності старого інструментарію

міжнародної співпраці (зокрема забезпечення міжнародної безпеки) новим загрозам і небезпекам. Як наслідок, політичні лідери висувають ідеї від розпуску ООН до вилучення з організації держав-агресорів. З огляду на інертність процесу трансформації міжнародних організацій демократичні держави вже виступили ініціаторами створення нових міждержавних об'єднань, які здатні перейти від економічних питань до політичних. Прикладами можуть бути Рада з торгівлі та технологій США – ЄС (Trade and Technology Council, TTC), група QUAD (Quad group of nations) – Австралія, Індія, Японія, США, група AUKUS (Австралія, Велика Британія, США), група I2-U2 (Індія, Ізраїль, ОАЕ, Сполучені Штати). Швидкість їх створення дає підстави стверджувати про високу ймовірність поступового витіснення міжнародних структур XX ст. подібними об'єднаннями, які більш тонко відчувають сучасність і пропонують нові рецепти так званого її оздоровлення.

6. Подальше розширення ЄС (нині 27 держав) і НАТО (нині 31 держава). На противагу попередньому процесу ЄС та Організація Північноатлантичного договору (теж політичні продукти попереднього століття) довели свою життєздатність і навіть побудували ескізи подальшого розширення. Наявність цих стійких міжнародних структур, історична перспектива яких виглядає успішною, дає змогу передбачити перемогу великого Заходу в протистоянні зі східними диктатурами принаймні на кількох напрямах – економіко-технологічному, безпеково-політичному, духовно-інформаційному. Україна, хоч і з запізненням, проте зафіксувала свій інтерес долучитися до названих західних об'єднань, що суттєво посилює її шанси на самозбереження й подальший розвиток у конфліктному східно-європейському середовищі.

7. Поширення зброї масового знищення. Іран прагне стати десятою ядерною державою. Із високою ймовірністю ці наміри буде реалізовано, і це радикально послабить глобальну безпеку. Китай як збудник COVID-19 продемонстрував нові можливості розроблення й поширення біологічної зброї. Порогові держави, технологічно здатні на продукування ядерних систем, проте стримані міжнародним законодавством, готові підтримати неідеальну формулу «безпека для себе через наявність власних ядерних засобів». За таких умов реальним стає заволодіння зброєю масового

ураження (насамперед ядерною) терористичних суб'єктів міжнародних відносин, чиї радикальні цілі втрачають ознаки відірваних від життя фантасмагорій.

8. Виникнення та визнання нових держав (їх загальне збільшення до понад 200). Зараз у світі налічується 194 суверенні держави (включно з Ватиканом), рівень суверенітету й впливовості яких коливається в різних межах. Проте процес виникнення (визнання) нових держав триває. Так, Палестину вже визнали 139 держав, Косово – 101 держава, Тайвань – 14 держав. Міжнародні дискусії щодо визнання / невизнання генерують Каталонія, Західна Сахара, Турецька Республіка Північного Кіпру, Придністровська Молдавська Республіка, Південна Осетія, Абхазія, Чечня. Претензії на визнання озвучують навіть «декоративні» державоподібні утворення, якими є Джамму і Кашмір на спірній території Пакистану та Індії; Ва та Шан на території М'янми; Авдалленд, Азанія, Галмудуг, Пунтленд, Сомаліленд, Хіман і Хеб на території Сомалі; Сирійський Курдистан; Кабінда на території Конго; Вазиристан на території Пакистану; Таміл Ілам на Цейлоні; Ісламська держава (Ісламська держава Іраку і Леванту) на території Іраку, Сирії та Лівії. А ще Європа чула про незалежну Шотландію, незалежну Країну Басків, незалежну Паданію. Здебільшого проголошення нових держав створює ситуацію збройно-силового втручання зовнішніх сил, незацікавлених / зацікавлених у виникненні нового гравця на міжнародній арені. Україна це відчула безпосередньо на собі, отримавши досвід конфліктної взаємодії з тимчасовими «ДНР», «ЛНР», а також «ПМР» як частиною Молдови.

9. Посилення релігійного екстремізму, насамперед незаконних збройних формувань ісламського походження. Новітня релігійно-політична історія вже має рухи Хезболла (1982 – сьогодення), Хамас (1987 – сьогодення), Аль-Каїда (1988 – сьогодення), Талібан (1994 – сьогодення), Боко Харам (2002 – сьогодення), ІДІЛ (Ісламська держава Іраку й Леванту) (2014 – сьогодення). Ідея проголошення всесвітнього халіфату, до якого серед інших земель мають увійти Поділля, Північне Причорномор'я та Крим, європейські країни можуть сприйняти критично, проте це матиме й велику кількість прихильників, особливо серед новоутворених ісламістських течій, загальна кількість яких не зменшується.

10. Відновлення території України в міжнародно визнаних державних кордонах 1991 року. Послаблення російської державності матиме множину наслідків, одним з яких стане відновлення територіальної цілісності України, а на цій підставі – її політичне зміцнення. Надалі слід очікувати подальшої інтеграції України й Польщі як лідерів Східної Європи, утворення ними «демократичного запобіжника» проти російського реваншу (на основі нового безпеково-оборонного об'єднання балто-чорноморських країн).

Критично слід відзначити, що лідери демократичних держав (пам'ятаючи про наступні вибори, на яких мають перемогти очолювані ними політичні сили), доволі часто демонструють зайву обережність у ситуаціях, які потребують політичної рішучості. Свідченням цього є небажання приймати рішення, які, з погляду владних західних еліт, відвернуть виборців, а також небажання західних лідерів звузити умовну «зону комфорту», яка стала невід'ємним атрибутом західних суспільств після закінчення Другої світової війни. Більшість західноєвропейських громадян уникає прогнозів щодо війн на їхній території чи власної участі в бойових діях. Сучасна демократія має змінитися, зокрема сформувати в населення готовність до силового блокування авторитарних впливів на права, свободи та людську гідність. Подібна готовність має стати складовою політичної свідомості, яка зараз доволі часто залишається перенасиченою необґрунтованою поблажливістю, невиправданою толерантністю, незрозумілою терплячістю до антигуманних й антидемократичних імпульсів, що генеруються авторитарними силами на адресу Західного світу.

Зважаючи на те, що демократичних держав у системі міжнародних взаємин усе-таки більше, ніж автократичних, світ спроможний спочатку обмежити, а потім й демонтувати світову «вісь зла». Проте подібні процеси ледве започатковано. Для їхнього успішного завершення потрібні як оновлена демократична соціалізація громадян, так і їхня демократична участь.

Альтернативні геополітичні узагальнення, які не суперечать викладеним вище, пропонують фахівці визнаного в Україні та за її межами Українського центру економічних і політичних досліджень (Центру Разумкова). На їхню думку, до глобальних геополітичних трансформацій сучасності потрібно віднести такі [31].

По-перше, відбувається стратегічне утвердження двох цивілізаційних угруповань – демократичного й автократичного. Переважну більшість країн поставлено перед вибором стратегічних орієнтирів розвитку та цінностей, які обстоюються на їхній основі. Паралельно країни визначаються з допустимим рівнем компромісів між проголошуваними ними цінностями та економічними вигодами, необхідними для забезпечення повсякденної життєдіяльності. Переконливою ілюстрацією цих процесів є ставлення держав світу до розпочатої 2014 року російсько-української війни. Маркерами вибору російської чи української сторони в цьому цивілізаційному двобою слугує підтримка / непідтримка іншими державами міжнародної санкційної політики щодо рф, постачання / непостачання Україні зброї та військової техніки, готовність / неготовність «дотиснути» росію до стану поразки, яка означатиме оновлення російського керівництва та трансформацію політичної системи рф на неавторитарних засадах.

По-друге, на основі широкомасштабної агресії рф проти України, за перебігом якої уважно спостерігають в Європі та за її межами, відбувається переусвідомлення державами світу власних державотворчих стратегій. Стає зрозумілим, що соціально-економічний базис будь-якої країни, узятий сам по собі, є надзвичайно вразливим для зовнішньої агресії. Відповідно, на порядку денному більшості держав – оновлення (фактично повторне створення) безпеково-оборонного базису державного розвитку, здатного убезпечити ключові суспільні сфери, насамперед політичну, економічну, інформаційну, на основі використання модернізованого сектору безпеки та оборони. У цих умовах надзвичайно важливого значення набуває інститут стратегічного партнерства держави, її входження (невходження) до міжнародних безпекових структур.

Третій тренд від Центру Разумкова: досвід російсько-української війни дає підстави стверджувати про звуження російського геополітичного проєкту, націленого на підкорення країн і народів не лише на пострадянському просторі, а й за його межами (ідеться про колишні соціалістичні держави Центральної і Східної Європи, а також колишні країни соціалістичної орієнтації). Своїм прикладом боротьби за свободу й незалежність Україна сформувала незворотний процес усвідомлення багатьма країнами світу нових пріоритетів розвитку, базованих на демократичних цінностях. Імперський

потенціал росії деградує. Це додатково засвідчує необґрунтованість російських геополітичних зазіхань на адресу колишніх «історичних» територій та ідеологічних союзників. Складаються об'єктивні передумови розпаду «останньої імперії», у внутрішній динаміці якої відцентрові тенденції посилюються.

Таким чином, маємо відзначити широкий спектр наукових підходів щодо основних геополітичних трендів XXI ст. У їхній загальній палітрі чітко простежується полярність підходів КНР (у взаємодії з рф, іншими автократіями) та США (у тісному спілкуванні зі своїми демократичними союзниками) із стратегічних питань світоустрою та побудови нової системи міжнародних взаємин. Демократичні й цінісно наповнені на основі прав і свобод людини суспільства (до яких належить Україна) протистоять автократичним соціумам, у яких зведена до абсолюту владна воля готова на політичні крайнощі (включно з ядерною війною) заради ілюзорного світового панування.

У найближчій перспективі слід очікувати, що протистояння демократії та автократій посилюватиметься. Цілком можливим вбачається збройне зіткнення сторін за рамками російсько-української війни із залученням нових учасників та урізноманітненням застосовуваних озброєнь. Завершальним етапом такого зіткнення може стати конституювання нової системи міжнародних відносин, принципово відмінної від систем XX ст. – Версальської, Ялтинсько-Потсдамської, Біловезької. Задля цього потрібна перемога демократичної частини людства над авторитарним антиподом. Україна є учасником цих подій, проте її суб'єктний потенціал поки що не дає змоги грати на рівних зі світовими геополітичними лідерами.

Загалом можна визначити такі тенденції формування нового безпекового середовища:

• новий світовий порядок формується двома реальними центрами сили (США і КНР), що мають потенціал як конструктивної, так і деструктивної взаємодії;

• **теми ядерного тероризму, контролю над ядерною зброєю, а також проблеми роззброєння, зміни клімату, застосування штучного інтелекту (ШІ)** стають основними на порядку денному в міжнародному співтоваристві;

• у найближчій перспективі очікують різке зростання витрат на озброєння;

• питання безпеки трансатлантичного простору будуть тісно пов'язані із ситуацією в Індо-Тихоокеанському регіоні, навколо Тайваню та на Корейському півострові. Спостерігається стійка тенденція до формування в Азії системи мікроальянсів безпеки замість створення глобальної структури на кшталт «азійського НАТО»;

• в умовах тривалої конфронтації між США і КНР та агресії росії проти України відносини з middle power (країнами так званого Глобального Півдня) будуть важливим чинником розвитку геополітичної та геоекономічної ситуації;

• перспективи створення економічних блоків, у межах яких держави демократичного табору намагатимуться усувати ризики поставок «чутливих матеріалів» з автократичних країн, а також обмежувати їхні можливості розвивати технології подвійного застосування, стають дедалі більш актуальними.

Висновки до першого розділу

Воєнно-силовий чинник поступово витісняє цивілізаційний та міжнародно-правовий фактори і стає домінантою в новому світовому порядку.

Нові реалії в міжнародних відносинах вимагають розв'язання питань гарантування міжнародної безпеки в глобальному та регіональному масштабі. Ефективність функціонування міжнародних структур безпеки значною мірою залежатиме від механізму застосування насамперед силових заходів. Нова парадигма формування міжнародного безпекового середовища має виходити з усвідомлення принципів єдності світу й неподільності безпеки та можливості протистояти тому, що несе загрозу безпеці.

Крім того, сьогоднішній ландшафт безпеки містить небезпеку прямого військового конфлікту між великими державами. Територіальні претензії Китаю кидають виклик союзникам США від Японії до Філіппін та інших партнерів США в регіонах, таких як Індія та В'єтнам. Давні інтереси США, такі як свобода судноплавства, стикаються з прямим конфліктом із морськими амбіціями Китаю.

Низка переворотів по всій Африці з 2020 року дозволила москві зміцнити свої позиції на континенті, навіть якщо вона спрямовує величезні військові та економічні ресурси на війну в Україні. Збільшення військової, політичної та економічної присутності росії в різноманітних країнах, до яких тепер входять Буркіна-Фасо, Центральноафриканська Республіка, Малі та Судан, також суперечить очікуванням, висловленим держсекретарем США Ентоні Блінкеном, який заявив у червні 2023 року, що повномасштабне вторгнення в Україну «зменшило вплив росії на всіх континентах». Після закінчення цієї війни понад два роки росія, очевидно, залишається здатною скористатися можливостями для розширення свого впливу в Африці та інших частинах світу.

Беручи до уваги демографічну структуру більшості країн Глобального Півдня, зокрема значну частку молодого населення, варто робити окремий трек публічної дипломатії, який сприяв би зростанню підтримки України, роз'яснення причин війни, поточної ситуації та пошук тем, які відгукнулися б серед молоді. Оскільки найближчим часом очікуються вибори в багатьох важливих країнах, це може вплинути на те, яких політиків молодь підтримує у своїх країнах.

Україні варто активно використовувати можливості та майданчики різноманітних міжнародних організацій, окрім ООН, де беруть участь країни Глобального Півдня. На додаток до Асоціації держав Південно-Східної Азії (Association of SouthEast Asian Nations, ASEAN) та Африканського Союзу, де Україна останнім часом демонструє підвищений рівень інтересу, важливим є налагодження сталої комунікації з іншими організаціями, зокрема Економічним співтовариством країн Західної Африки (The Economic Community of West African States, ECOWAS), Азійсько-Тихоокеанським економічним співробітництвом, Організацією американських держав (Organization of American States, OAS), Лігою арабських держав тощо. Ба більше, для багатьох країн цього регіону парламентська дипломатія матиме значний вплив, тому Україні необхідно посилити використання можливостей Міжпарламентського Союзу, де українські парламентарі вже активізували свою діяльність.

Отже, можна із впевненістю констатувати трансформацію світу (відповідно, і системи міжнародних відносин) до вигляду, проаналізувати який на основі попередніх підходів стає фактично неможливим. У сучасних умовах слід брати до уваги складну сукупність чинників впливу на будь-якого суб'єкта міжнародного життя – від ситуативного міжнародно-політичного альянсу, громадської організації, неурядової ініціативи до суверенної держави чи міжнародного об'єднання. З огляду на це висновки та рекомендації, адресовані державним органам із боку інформаційно-аналітичних структур, мають бути надійно верифікованими, багатократно перевіреними й у жодному разі не претендувати на довготривалість практичного використання.

Перелік використаних джерел:

1. Панфілов О. Ю., Петрова Л. О. Фактор воєнної сили в сучасних міжнародних відносинах. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія.* Харків : Право, 2020. № 4 (47). С. 113–126.

2. Бодрук О. С. Фактор сили в сучасному світі. *Політика і час.* 2002. № 3. С. 57–67.

3. Бодрук О. Силова грань безпеки. *Політика і час.* 2005. № 4. С. 47–56.

4. Орлик В., Гриценко А. Основні положення нової Стратегії національної безпеки США**.** URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/osnovni-polozhennya-novoyi-stratehiyi-natsionalnoyi-bezpeky (дата звернення: 25.04.2025).

5. Бєлєсков М. Національна оборонна стратегія США 2022 року: основні положення, оцінки і наслідки для України. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/natsionalna-oboronna-stratehiya-ssha-2022-roku-osnovni (дата звернення: 15.04.2025).

6. Гончар М. Безпекові вакууми як наслідок війни Росії проти України: оцінка впливу і можливі шляхи подолання. URL: https://geostrategy.org.ua/analityka/analitychna-zapyska/bezpekovi-vakuumy-yak-naslidok-viyny-rosiyi-proty-ukrayiny-ocinka-vplyvu-i-mozhlyvi-shlyahy-podolannya (дата звернення: 11.04.2025).

7. Роль і місце України в перспективних європейській та євро-атлантичній системах безпеки. URL: https://razumkov.org.ua/images/2022/11/16/2022_Rolj_i_mistce_Ukr.pdf (дата звернення: 17.01.2025).

8. Рік війни за свободу. Воєнно-історичний нарис російсько-української війни (24.02.2022 – 24.02.2023) у чотирьох книгах / Апарат Головнокомандувача Збройних Сил України, Генеральний штаб Збройних Сил України та Центр досліджень воєнної історії Збройних Сил України. Київ : Видавництво Ліра-К, 2023. Книга І. 270 с.

9. Сологуб І., Федик А. Накласти лапу на критично важливі ресурси Африки: у що інвестують Китай та Росія. URL: https://www.epravda.com.ua/publications/2023/12/4/707291/ (дата звернення: 15.04.2025).

10. Зігль Д. Росія та Африка: розширення впливу та нестабільність. URL: https://www.marshallcenter.org/en/publications/marshall-center-books/russias global-reach-security-and-statecraft-assessment/chapter-10-russia-and-africa expanding-influence-and (дата звернення: 15.04.2025).

11. Надір Тіфлісі. Афро-Російська імперія. Навіщо Москві Сахель? URL: https://www.trtrussian.com/mnenie/afro-rossijskaya-imperiya-zachem-moskve-sahel-17840160 (дата звернення: 15.04.2025).

12. Зігль Д. Розшифровка економічних залучень Росії в Африці. URL: https://africacenter.org/spotlight/decoding-russia-economic-engagements-africa/ (дата звернення: 15.04.2025).

13. The Final Report of the Congressional Commission on the Strategic Posture of the United States. URL: https://www.ida.org/-/media/feature/publications/A/Am/Americas%20Strategic%20Posture/Strategic-Posture-Commission-Report.pdf (дата звернення: 25.06.2025).

14. Statement on the Development of the 2025 National Defense Strategy. URL: https://www.defense.gov/News/Releases/Release/article/4172735/statement-on-the-development-of-the-2025-national-defense-strategy/ (дата звернення: 25.05.2025).

15. Корсунський С. Як Україні завоювати уми Азії. URL: https://zn.ua/ukr/WORLD/jak-ukrajini-zavojuvati-umi-aziji.html (дата звернення: 15.07.2024).

16. Aggression against Ukraine: resolution / adopted by the General Assembly. URL: https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf (дата звернення: 16.07.2024).

17. ERO COMFORT. The Trouble With «the Global South». URL: https://www.foreignaffairs.com/world/trouble-global-south (дата звернення: 25.07.2024).

18. Miliband David. The World Beyond Ukraine. URL: https://www.foreignaffairs.com/ukraine/world-beyond-ukraine-russia-west (дата звернення: 25.07.2024).

19. Городиський А. Що таке Глобальний Південь, чого він хоче і чому про нього стільки говорять? URL: https://www.rfi.fr (дата звернення: 15.07.2024).

20. The Africa Wealth Report 2024. URL: https://www.henleyglobal.com/publications/africa-wealth-report-2024 (дата звернення: 16.07.2024).

21. The Middle East and North Africa Gap. URL: https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621549/bp-mena-gap-prosperity-for-the-rich-austerity-for-the-rest-051023-en.pdf;jsessionid= 30C645BA2DF485B6305EEF8F5EEDE050?sequence=13 (дата звернення: 17.07.2024).

22. Зірки, політики і магнати приїхали з усього світу на розкішне весілля в Індії. URL: https://www.bbc.com/ukrainian/articles/crgevp9d1v9o (дата звернення: 17.07.2024).

23. The Use of the Concept «Global South» in Social Science & Humanities. URL: https://www.academia.edu/7917466 (дата звернення: 25.07.2024).

24. Борділовська О. Глобальний Південь у контексті нових викликів. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/hlobalnyy-pivden-u-konteksti-novykh-vyklykiv (дата звернення: 25.06.2024).

25. Макмастер Г. Поля битв. Боротьба за захист вільного світу. Київ : Наш формат, 2023. 424 с.

26. Смолій В. А., Ясь О. В. Сучасна російсько-українська війна у світлі постколоніалізму. *Вісник НАН України*. 2022. № 6 (36). С. 3–16.

27. Козловець М. А. Світовий порядок XXI століття: вектори трансформації : матеріали XXXV Харківських політологічних читань. м. Харків, 28 квітня 2023 р. Харків : Право, 2023. С. 20–25.

28. Пирожков С. І., Хамітов Н. В. Війна і мир в Україні: шляхи до реальної перемоги і розвитку. *Вісник НАН України*. 2022. № 9 (39). С. 38–49.

29. Роль і місце України в перспективних європейській та євро-атлантичній системах безпеки. URL: https://razumkov.org.ua/images/2022/11/16/2022_Rolj_i_mistce_Ukr.pdf (дата звернення: 17.06.2025).

30. Смолянюк В. Ф., Гунін В. Є. Світовий порядок XXI століття: вектори трансформації : матеріали XXXV Харківських політологічних читань. м. Харків, 28 квітня 2023 р. Харків : Право, 2023. С. 40–44.

31. Геополітичні та геоекономічні зміни, формовані під впливом російської агресії, та оновлення місця України у світовому просторі. Київ : Центр Разумкова, 2022. 102 с.

РОЗДІЛ ІІ
НОВЕ ПОКОЛІННЯ РОСІЙСЬКИХ ВІЙН: ОСНОВНІ ТЕНДЕНЦІЇ ТА КОНЦЕПЦІЇ

2.1. Тенденції розвитку засобів збройної боротьби в сучасних умовах

Війна рф проти України точиться вже більше десяти років. На сьогодні – це найдовша війна, найдовший насильницький конфлікт у Європі після Другої світової війни.

Часи війни спонукають до осмислення її сутності, адже саме переломні періоди дають можливість безпосередньо відчути й зрозуміти явні та приховані смисли подій. Останнім часом численні дослідники та експерти констатують, що стратегічні інтереси сучасних держав нікуди не зникли, а, навпаки, активізувалися. Відповідно, сучасні воєнні конфлікти набули нових властивостей порівняно з минулими, коли ставка робилася на силове домінування.

Досліджуючи питання тенденцій розвитку збройної боротьби в сучасних умовах, доцільно було б спочатку здійснити ретроспективний аналіз еволюції теорії поколінь сучасної війни (Global Modern Wars, GMW).

У 80-х роках XX ст. американські дослідники вводять до наукового та воєнного дискурсу концепцію чотирьох поколінь воєн.

Теорія GMW була вперше представлена Вільямом С. Ліндом та його співавторами в їхній статті 1989 року, опублікованій у «Marine Corps Gazette». У цій статті вони припустили, що історію сучасної війни від Вестфальського договору 1648 року до теперішнього часу можна розглядати як історію чотирьох поколінь війни [1].

Перше покоління (1GW) означає війни ранньомодерного часу та початку індустріальної ери (із середини XVII до першої половини XIX ст.), які характеризувалися використанням лінійної тактики, створенням професійних національних армій і були пов'язані із самою появою сучасної концепції війни як війни між державами, що була сформована навколо ідей Карла фон Клаузевіца. 1GW покладалося переважно на людську силу.

Становлення другого покоління сучасних війн (2GW) було пов'язане з розвитком нових видів транспортних комунікацій, насамперед залізниць, розробленням нових удосконалених видів вогнепальної зброї та артилерії (особливо непрямої артилерії та кулеметів). Головним аспектом, який допоміг виділити друге покоління війн, найважливіший приклад яких становила Перша світова війна, була її спрямованість на досягнення технологічної переваги та переваги в кількості озброєння та мобілізованого війська, що в сукупності мало вилитись у вогневу перевагу на фронтах для виснаження ворога.

Такий підхід поступово призвів до появи концепції «тотальної війни», яку ввів один із видатних полководців Першої світової війни генерал Еріх Людендорф. На відміну від війн першого покоління з дуже жорстким відокремленням військових від цивільного населення, концепція «тотальної війни» пропонує ідею загальної мобілізації та масового залучення цивільного населення до потреб війни.

Війни третього покоління (3GW), найяскравішим прикладом яких є Друга світова війна та тактика блискавичної війни, характеризуються пошуком нових шляхів перемоги в «тотальній війні», яка базувалася б на перевагах стратегічного мислення. Відповідно, основою воєн третього покоління є мобільність і маневреність.

На відміну від описаних у статті Лінда попередніх трьох поколінь війн, які базувалися на історичних прикладах, ідентифікація четвертого покоління була, скоріше, пов'язана з перспективами військової футурології. У часи написання статті Лінда армія США та Корпус морської піхоти лише «намагалися дати собі раду зі змінами третього покоління війн». У цьому світлі Лінд і його співавтори спробували передбачити невизначене майбутнє війни, використовуючи концепцію війни четвертого покоління. Спочатку майбутнє війни, яке було описане в статті, містило аспекти технологічних змін, а також соціальних змін.

З точки зору доктора Роберта Дж. Банкера (1996), який пізніше порівнював ідеї Лінда з ідеями інших військових теоретиків того часу, ставлення до майбутнього війни після закінчення Холодної війни загалом поділялося на два основні підходи, де перший був більш технологічно орієнтованим, тоді як другий – «гуманітарним» і підкреслював роль ідей та соціальних факторів. Перший підхід був

значною мірою пов'язаний з ідеями Елвіна та Хайді Тоффлерів, які запропонували концепцію війни третьої хвилі, що оцінювала переваги високотехнологічної війни, яка, своєю чергою, забезпечувала військову перевагу постіндустріальним країнам. Одна частина концепції війни четвертого покоління Лінда, як це було описано в його статті 1989 року, була технологічно орієнтована, оскільки, подібно до підходу Тоффлерів, також передбачала розвиток військової високотехнологічної зброї, такої як зброя спрямованої енергії та робототехніки, тоді як друга частина була більш «гуманітарною» і передбачала зростання тих видів війни, які відомі як «асиметричні», включаючи зростання тероризму.

Кревельд зосередився на ідеях Карла фон Клаузевіца як на ідеях, які сформували сучасне значення війни. Він описав це значення як «тринітарне», тобто значення, що спиралося на тринітарне бачення війни Клаузевіцем, яке базувалося на трьох основних елементах: «уряд», «армія», «народ». Кревельд стверджує, що новий тип війни, який зараз набирає обертів, стає «нетринітарним», підриваючи давнє уявлення Клаузевіца про війни як такі, що ведуться урядами, які використовують свої армії та підтримуються своїм народом. Навпаки, війни нового покоління стирають кордони між учасниками бойових дій і цивільним населенням та залучають нових акторів, таких як етнічні, соціальні та релігійні рухи, злочинці та транснаціональні бізнес-групи, тоді як уряди поступово втрачають свою монополію на війну. Тому все у військовій історії, здається, повертається до умов, які існували до Вестфальського договору 1648 року, який створив передумови сучасного образу війни. Водночас ці зміни також пов'язані з появою так званих конфліктів низької інтенсивності, які, у свою чергу, пов'язані з неможливістю ведення повномасштабної «тотальної війни» в ядерну епоху та які, незважаючи на власне ім'я, часто характеризуються особливою жорстокістю і кровопроліттям. З іншого боку, ці зміни були представлені зростанням таких явищ, як революційні рухи, національно-визвольні рухи, релігійні рухи, антиколоніальна боротьба, які починали та вигравали асиметричні війни проти значно могутніших ворогів, наприклад, війна в Алжирі, війна у В'єтнамі, війна в Афганістані 1979–1989 років та інші. У таких війнах ці рухи впроваджували абсолютно нові (з точки зору сучасної війни) принципи, що призводили до масового залучення населення

до боротьби, стирання кордонів між комбатантами та некомбатантами, ефективної партизанської війни, деморалізації ворожої сторони (у тому числі всередині країни противника), маніпуляції ставленням світової громадськості до подій.

Таким чином, 4GW насправді не є новим явищем, оскільки в цьому контексті воно виникло як широко розповсюджене явище в історичних умовах розпаду колоніальної системи після закінчення Другої світової війни і дуже часто було пов'язане з позитивними змінами в соціально-політичному житті та боротьбою різних категорій людей за свою свободу, що підривало старі структури влади та гноблення. Проте в останні десятиліття цей спосіб ведення війни також став тісно пов'язаним зі зростанням міжнародного тероризму, який використовує методи, що ніколи не можуть бути виправданими, та який тепер став загальновизнаною глобальною загрозою. У цьому контексті Кревельд (1991) вважає, що сучасні держави не готові до загрози 4GW, оскільки вони не розуміють нових способів ведення війни.

Деякі дослідники, у зв'язку з радикальними змінами в засобах воєнної боротьби, виділяють шість поколінь військових конфліктів, які послідовно змінювали одне одного. У першому поколінні війни головним видом зброї була холодна, а основною метою було знищення противника, заволодіння його зброєю та цінностями. У другому поколінні війна характеризувалася знищенням противника, заволодінням його територією та цінностями, а головним видом зброї була гладкоствольна. У війні третього покоління характерними є знищення збройних сил противника, руйнування його економіки та захоплення території. Основним видом зброї в цьому поколінні є нарізна багатозарядна зброя підвищеної скорострільності, точності та дальності стрільби. Автоматична та реактивна зброя, механізовані війська, танки, авіація, авіаносці та підводні човни замінюють зброю третього покоління. Основною метою війни четвертого покоління є знищення збройних сил противника, руйнування його економічного потенціалу та повалення політичного ладу. Із війною п'ятого покоління пов'язана ракетно-ядерна зброя, за якої цілі не досягаються, але існує загроза загибелі цивілізації або окремих континентів. Війна шостого покоління спрямована на підрив економіки, систем управління та життєдіяльності держави, а також на знищення військових об'єктів. Основними

видами зброї в цій війні є високоточна зброя (ВТЗ), зброя на нових фізичних принципах (НФП), інформаційна зброя, сили та засоби радіоелектронної боротьби.

Тобто феномен війни постійно трансформується разом зі змінами, що відбуваються у світі. І це треба враховувати під час осмислення трендів збройної боротьби в майбутньому. Які ж основні тенденції збройної боротьби майбутнього ми можемо окреслити?

Так, Кобець Ю. пропонує розрізняти сім видів війни, які можуть вестися (відбуватися) у XXI ст. Ці війни значно відрізняються одна від одної за багатьма характеристиками, включаючи критерій ефективності [2].

До загального переліку війн можна віднести:

- класичну техногенно-силову війну;
- економічну війну;
- неоголошений геноцид проти населення держави-суперника;
- організаційну війну (випадки впровадження зовнішніх або ворожих організаційних структур у національну державну систему протилежної сторони, наприклад нелегітимних органів влади або різних фондів);
- інформаційну війну;
- хронологічну війну – спосіб ведення воєн через цілеспрямоване переосмислення «неприємного» минулого країни та постійне маніпулювання історичними фактами на користь замовника;
- духовну війну, що є ще одним способом ведення війни, який передбачає нав'язування небезпечних цінностей народам або державам, які підкорюються. Цей метод має на меті змінити духовні принципи та цінності цих народів або держав для досягнення своїх цілей.

У свою чергу, М. Требін та Т. Чернишова пропонують такі тенденції збройної боротьби майбутнього [3]:

По-перше, ретроспективний погляд на еволюцію військового мистецтва свідчить, що траєкторія його розвитку являє собою освоєння простору, у якому здійснюється постійно розширювана збройна боротьба. Це розширення мало місце від стратегії генеральної битви в одній точці (епоха наполеонівських воєн) до лінійної стратегії (з другої половини XIX ст. до середини 1930-х рр.), а далі – до глибокої операції на континентальному театрі воєнних дій (ТВД) (Друга світова війна) та об'ємної (повітряно-космічної, повітряно-наземної

і наземно-морської) операції початку XXI ст. Тобто на зміну традиційним воєнним діям, суворо розподіленим за фізичними сферами, прийшли об'ємні, що проводяться одночасно в усіх сферах протиборства, у значно розширеному просторово-часовому континуумі. Тут запроваджується принцип «багатосферності», який у перспективі отримає подальший розвиток.

По-друге, до збільшення просторових показників збройної боротьби слід додати зростання значення інформаційного континууму. Це обумовлено тим, що на сучасному етапі розвитку цивілізації інформація відіграє ключову роль у функціонуванні суспільних і державних інститутів та житті кожної людини. Інформатизація спричиняє створення єдиного світового інформаційного простору, у межах якого здійснюються виробництво, нагромадження, обробка, збереження та обмін інформацією між суб'єктами цього простору – людьми, організаціями, державами. Цілком очевидно, що можливості швидкого обміну політичною, економічною, духовною, науково-технічною та іншою інформацією, застосування нових інформаційних технологій у всіх сферах суспільного життя та особливо у виробництві й управлінні є безсумнівним благом. Подібно до того, як швидке промислове зростання створило загрозу екології Землі, а успіхи ядерної фізики спричинили небезпеку ядерної війни, так і інформатизація може стати джерелом цілої низки проблем.

Можна виділити два основних об'єкти впливу інформаційної зброї. Перший – антропогенний (власне людина, її інтелект і масова свідомість соціуму). Реалії сучасного буття свідчать, що вплив безпосередньо на людину дозволяє успішно реалізовувати мету інформаційного протиборства. Як свідчать дослідження, що проводилися наприкінці XX ст., в умовах повсякденної діяльності військ психічне порушення спостерігається у 4–6 % особового складу, під час виконання завдань навчально-бойової діяльності – від 15 до 20 %, у ході бою – від 30 до 86 % (залежно від інтенсивності, кількості поранених та вбитих). Другий об'єкт впливу інформаційної зброї – техногенний (програмне та власне інформаційне забезпечення; програмно-апаратні та телекомунікаційні засоби, канали зв'язку, що забезпечують циркуляцію інформаційних потоків та інтеграцію систем управління тощо). Найбільш вразливими елементами інфраструктури є телекомунікаційні вузли, центри супутникового зв'язку та канали міжнародного інформаційного обміну.

По-третє, зростання значення космічного простору. Основними завданнями бойових космічних засобів під час ведення воєнних дій з космосу з метою завдання втрат супротивнику на континентальних, океанських і морських ТВД, а також у повітряному просторі, на думку американських фахівців, має бути ураження: наземних угруповань космічних сил і засобів (елементів позиційних районів частин запуску та управління, обробки інформації та інших об'єктів); стаціонарних і мобільних угруповань стратегічних ядерних сил (пускових установок, пунктів управління та інших об'єктів); мобільних угруповань надводних кораблів і підводних човнів; літаків стратегічної авіації на аеродромах і в повітряному просторі; важливих об'єктів стратегічного призначення; живої сили, озброєння та військової техніки, а також виставлення активних перешкод радіоелектронним засобам, глобальний вплив на природне середовище території супротивника. Окрім того, військові аналітики вважають, що за допомогою космічних засобів можуть бути вирішені такі завдання, як глобальний і локальний контроль з космосу за станом і динамікою дій угруповань військ (сил флоту) в будь-якому регіоні світу, інформаційний, координатно-метричний та інші види забезпечення їхніх дій; управління ними з єдиного центру, віддаленого на будь-яку відстань від регіону бойових, оперативних або стратегічних дій, при забезпеченні більшої самостійності прийняття рішень усіма ланками органів військового управління.

По-четверте, розширення спектру застосовуваних засобів збройної боротьби, серед яких істотно зростає значення зброї на НФП, а також високоточної, гіперзвукової, кіберзброї, інформаційно-керуючих систем, роботизованих комплексів військового призначення (РКВП), безпілотних літальних та автономних морських апаратів, ШІ в системах підтримки прийняття рішень, управління військами (силами) та озброєнням, військової та спеціальної техніки.

У ході проведення воєнних операцій у війнах майбутнього ставка робитиметься на засоби збройної боротьби, що працюють на НФП. Застосування зброї на НФП передбачає миттєву поразку противника на великій відстані за рахунок перенесення спрямованої енергії. Це може бути лазерна зброя – доставка до об'єкта ураження енергії електромагнітного випромінювання гамма, рентгенівського, ультрафіолетового, видимого чи інфрачервоного діапазонів довжини

хвиль; радіочастотна зброя – доставка до об'єкта ураження енергії електромагнітного випромінювання радіочастотного діапазону довжини хвиль (надвисокочастотна зброя, інфразвукова зброя та ін.); пучкова (прискорювальна) зброя – доставка до об'єкта ураження спрямованих пучків високоенергетичних заряджених або нейтральних частинок, прискорених майже до швидкості світла. Усі ці види зброї забезпечують практично миттєву доставку до цілі вражаючої енергії, причому дальність ураження може вимірюватися багатьма сотнями кілометрів. Реалізація такого принципу ураження об'єктів потенційним супротивником може докорінно змінити характер майбутньої війни. Застосування ним такої зброї дозволить уражати об'єкти без їх фізичного руйнування, обмежити застосування звичайних засобів збройної боротьби, а також скоротити час проведення операції до кількох хвилин. Не вбиваючи людей, така зброя може порушувати роботу телефонів, радіолокаторів, комп'ютерів, інших засобів зв'язку, наведення, навігації та управління. Передбачається також використовувати «інгібітори згоряння», що зупиняють двигуни машин, а також хімікати, що руйнують шини автомобілів і літаків, якщо їх розпорошувати на дорогах та аеродромах. Акцент робиться на те, щоб за допомогою подібних засобів паралізувати війська, не знищуючи їх.

Досвід ведення бойових дій на урбанізованій території (у міських умовах) збройними силами багатьох країн, отриманий у локальних війнах і воєнних конфліктах кінця XX – початку XXI ст., активував розвиток нового виду озброєння – РКВП. Основними завданнями, що покладаються на РКВП, є: вогнева підтримка наступаючого підрозділу, наведення ВТЗ, розвідка місцевості та контроль результатів ураження об'єктів противника, розвідка та спостереження, підвезення боєприпасів, паливно-мастильних матеріалів у зону бойових дій та ін.

У майбутніх війнах характер бойових дій у повітрі кардинально зміниться внаслідок більш широкого застосування таких РКВП, як безпілотні літальні апарати (БПЛА) та засоби зниження помітності.

Завдяки широкому застосуванню БПЛА планується розширити бойові можливості підрозділів сухопутних військ та розвідувально-диверсійних підрозділів. У майбутніх війнах БПЛА будуть застосовуватись і як окремі комплекси, і у вигляді формувань безпілотної

авіації. Залежно від дальності польоту, бойового навантаження та завдань масштаб застосування БПЛА буде різним – від тактичного до стратегічного рівня. Тривалість польоту, як свідчать експериментальні польоти БПЛА США, може вимірюватися роками. Формами застосування безпілотної авіації можуть бути розвідувально-ударні дії, контроль повітряного простору та ін.

Використання технологій ШІ в нових системах управління озброєнням дозволить здійснити прорив під час ведення бойових дій. Такі системи дозволять прискорити прийняття рішень з урахуванням максимальної кількості чинників та значно скоротити цикл управління військами (силами), а також підвищити їхні бойові можливості. На сьогодні найбільших результатів американські фахівці досягли в галузі «глибокого машинного навчання». Це стало можливим завдяки швидкому прогресу в розвитку багаторівневих штучних нейронних мереж. Технології розпізнавання образів та машинне навчання, використовувані в сучасному ШІ, можуть забезпечити високий ступінь автоматизації прийняття управлінських рішень під час аналізу та обробки інформації від різних джерел.

По-п'яте, зміна логіко-часової побудови збройної боротьби: завоювання ініціативи та переваги в інформаційній сфері (в управлінні військами та зброєю); створення переваги в повітряно-космічній сфері; зміна на свою користь співвідношення сил на суші та морях; досягнення загальної кількісно-якісної переваги в силах та засобах; збільшення тривалості підготовчих та зменшення періоду активних дій; посилення дедуктивних та послаблення індуктивних зв'язків і відносин збройної боротьби; використання стратегічних та оперативних засобів для ураження тактичної ланки; організація та ведення збройної боротьби в реальному масштабі часу; перехід від управління військами до управління збройною боротьбою.

Нинішня війна в Україні являє собою абсолютно нове явище у військовій історії. Так, Шон Макфейн зазначає, що російсько-українська війна продемонструвала не лише нові правила війни, а й те, як воювати й перемагати сильніші армії у XXI ст. Він виокремив десять правил [4]:

Правило 1. Традиційна війна відійшла в минуле.

«Традиційна війна» є одним із видів бойових дій – і Друга світова війна тому приклад, – але нині немає нічого більш нетради-

ційного, ніж традиційна війна. З 1945 року лише 6 % війн були традиційними, а останні з них велися сорок років тому. Ніхто вже так не воює, бо це більше не дає перемоги – проте Росія спробувала. У лютому 2022 року вона розпочала першу за 35 років традиційну війну і зазнала поразки. Символом її стратегічної недолугості стала 64-кілометрова російська військова колона, яка в перші тижні війни застрягла на шляху до Києва. Ведення традиційної війни потребує надзвичайного рівня дисципліни, управління й організаційної єдності, а росіяни цього позбавлені. Війна була приречена на провал, а росіяни остаточно змінили свою тактику наприкінці березня, перейшовши до російської нетрадиційної війни, яку ми бачили в Грозному й Алеппо. Це стратегія терору. Це правило пояснює, чому традиційні війни сьогодні закінчуються невдачею, і підказує, що працює краще.

Правило 2. Інвестуйте в людей, а не в технології.

Багато хто уявляє майбутню війну надзвичайно високотехнологічною, але бойовий досвід високотехнологічних збройних сил після 1945 року був жалюгідним – вони регулярно програвали низькотехнологічним арміям. Франція зазнала поразки в Алжирі та Індокитаї, Велика Британія – у Палестині й на Кіпрі, СРСР – в Афганістані, США – у В'єтнамі, Сомалі, Іраку й Афганістані, а росія, схоже, нині в Україні. Кадри скромного українського трактора, який тягне російські танки з поля бою, говорять самі за себе. Це правило пояснює, чому найкраща технологія – це 15 сантиметрів між нашими вухами. Хитрість перемагає високотехнологічну грубу силу.

Правило 3. Немає війни або миру – вони завжди співіснують.

Розумні супротивники використовують простір між війною й миром задля своєї перемоги. У 2014 році росія застосувала «зелених чоловічків», підрозділи спецназу й найманців на кшталт ПВК «Вагнер», щоб здійснити приховану окупацію на Сході України. Українці не дали себе надурити, але Захід – дав. Для нього це не скидалося на традиційну війну, але й не було миром. Поки західні спецслужби все ще намагалися розібратися, що ж росія робить на Донбасі, анексія Криму стала доконаним фактом. Це правило пояснює, чому не буває війни або миру, а лише війна та мир. Від усвідомлення цієї різниці залежить стратегія перемоги.

Правило 4. Завоювання умів і душ не працює.

Завоювання умів і душ місцевого населення не веде до перемоги, як хибно вважала більшість американських генералів в Афганістані й Іраку. І це одна з причин їхньої поразки. Упродовж В'єтнамської війни серед бійців спецназу Армії США побутувала приказка: «Якщо взяти їх за яйця, уми й душі теж будуть вашими». Таким є російський підхід до боротьби з повстанцями, і він передбачає масові вбивства цивільного населення та стирання міст із лиця землі. Саме це вони зробили із Чечнею, Сирією, а тепер і з Україною. Порушення прав людини та супутні втрати є не похибкою, а прикметою російської війни, про що свідчать Буча, Маріуполь та Ізюм. Це аморальний й огидний підхід, який використовували протягом усієї історії, нерідко успішно. Це правило пояснює, чому на війні насильство зазвичай ефективніше, ніж милосердя.

Правило 5. Найкраща зброя стріляє не кулями.

«Бій точиться тут, мені потрібна зброя, а не евакуація». Це була одна із найбільш цитованих фраз під час російського вторгнення в Україну – слова зухвалого українського президента, який відмовився під пропозиції США залишити Київ. Справжня ця цитата чи ні – значення не має. Вона подіяла. Зброя почала надходити, і НАТО заворушилося вперше за 30 років. Україна успішно перетворила соціальні мережі й меми на зброю, легко обійшовши світового лідера з дезінформації – росію. Правило 4 говорить нам, що уми і душі не мають значення на низовому, тобто «тактичному», рівні війни. Та на глобальному, або «стратегічному», рівні завоювання умів і душ є необхідною умовою перемоги. Український народ і влада разом ведуть успішну інформаційну війну, яка перетворила росію на державу-парію, якої цурається навіть Китай. Що ще важливіше – це дало змогу зберегти інтерес Заходу до України, що привело до збільшення кількості зброї, боєприпасів, цінних розвідувальних даних, дипломатичної та народної підтримки. Це правило пояснює, чому в інформаційну добу інформація має більшу силу, ніж летальна зброя, і як саме нею ефективно користуватися.

Правило 6. Найманці знов у грі.

Російські найманці, як-от ПВК «Вагнер», стали синонімом війни. З 2014 року ПВК «Вагнер» стала улюбленою зброєю Путіна, тому що вона дає кремлю можливість правдоподібно заперечувати

свою участь у разі провалу операцій, а росіяни таки провалюються. У 2018 році ПВК «Вагнер» зіткнулася із Силами спеціальних операцій США на сході Сирії та була знищена. І москва, і Вашингтон вирішили знехтувати цим інцидентом, щоб не доводити до Третьої світової війни, ймовірність якої була б реальною, якби то були російські солдати, а не військові найманці. Найманці – друга найдавніша професія, і від них на війні великі проблеми. Це правило пояснює, у чому полягають ці проблеми, як найманці змінюють війну і як найкраще їх використовувати чи перемагати.

Правило 7. З'явилися нові типи світових сил.

Це правило не стосується України тією самою мірою, як інших збройних конфліктів у світі, наприклад нарковійн у Латинській Америці, конфліктів в Африці, релігійних війн на Близькому Сході і в Південній Азії. Національні держави всюди здають позиції, і замінює їх новий клас світових сил – супербагатії. За даними Світового банку, зі 100 найбільших генераторів прибутку у світі 71 – це корпорації і лише 29 – держави. У людському вимірі 1 % найбагатших володіє 45 % світового багатства, а бідніша половина населення планети сукупно володіє менш ніж 1 %. Тепер, коли найманці повертаються, супербагатії можуть стати озброєними й дуже небезпечними. Вони можуть розпочати війну, щоб захистити свої міжнародні інтереси, так само, як це роблять держави. Колись ExxonMobil чи Ілон Маск зможуть мати власну армію. Насправді вони *вже* можуть, якщо захочуть. Це правило пояснює, як це докорінно змінить світовий порядок.

Правило 8. Війни не завжди ведуться між державами.

Ще одне правило, яке менше стосується української боротьби, але зберігає свою важливість для решти світу. Коли супербагатії можуть набирати найманців, тоді вони можуть вести війну, неважливо, наскільки малу. Держави більше не будуть єдиними суб'єктами війни, а можуть навіть стати трофеєм. Уже сьогодні міжнародні наркокартелі воюють один з одним за вплив на вулицях Латинської Америки. Вони захоплюють країни, як-от Гватемалу, і називають їх «наркодержавами». Видобувні галузі, наприклад нафтові, газові та гірничі компанії, дедалі частіше звертаються до найманців, щоб захистити своїх людей, території та майно. Може, колись вони навіть воюватимуть одна з одною за нафтові родовища в слабких державах,

які не здатні себе захистити чи мають корумпованих політиків, ласих до хабарів. Оскільки вогневу міць можна купити за гроші, супербагатії стають новим видом суперсил, а це віщує війни без держав. Це правило пояснює, якими будуть ці війни і які наслідки вони матимуть для міжнародних відносин.

Правило 9. Тіньові війни переважатимуть.

Росія захопила Крим у 2014 році засобами тіньової війни – так здавалося міжнародній спільноті, але не Україні. В інформаційну добу можливість правдоподібного заперечення є більш вирішальним фактором, ніж військова міць на полі бою. Це заганяє війну в підпілля, де вона точиться в тіні. Тіньова війна дає агресорам змогу непомітно розпалювати конфлікти, здобуваючи перемогу ще до того, як жертва зрозуміє, що її атакувало. Росія, Іран й інші довели тіньову війну до досконалості, і їхній приклад наслідують інші держави. Лівія – це одна суцільна тіньова війна: ніхто насправді не знає, хто саме перебуває на полі бою і за що воює. Тим часом Захід не розуміє природи тіньової війни, про що свідчить його млява реакція на дії росії у 2014 році. Сучасним державам, зокрема Україні, необхідно відточувати своє вміння перемагати в тіньових війнах, і це правило пояснює, як саме цього досягти.

Правило 10. Перемоги взаємозамінні.

Половина перемоги – це розуміння того, який вигляд вона має. І це правило пропонує Україні чудову стратегію для перемоги над росією сьогодні – узяти на озброєння час. Мізки важливіші за грубу силу. До питання про мізки: згадайте Троянського коня та Давида проти Голіафа. До питання про грубу силу: згадайте Першу світову війну. Є багато способів «перемогти», і більшість із них не потребуватиме величезної армії, якщо ви маєте розум. Вам потрібна стратегія, яка використовує спосіб ведення війни вашого ворога проти нього самого, подібно до того, як боєць джиу-джитсу використовує вагу свого суперника проти нього. Це правило пояснює, як вигравати в сучасних війнах.

Іншими словами, технологічна революція, яка вже розпочалася, створює ідеальні умови для такого типу війни, як війна на виснаження, а стратегія досягнення політичної цілі війни буде спрямована на виснаження ресурсів та можливостей противника.

Отже, цей висновок дає можливість усвідомити основну та, імовірно, єдину стратегію перемоги в майбутньому – формування системи «життєстійкості» країни.

У свою чергу, Надзвичайний та Повноважний посол України у Великій Британії і Північній Ірландії, Головнокомандувач Збройних Сил України (ЗСУ) В. Залужний (2021–2024) наголошує, що російсько-українська війна повністю змінила характер війни. Розвідувальні, ударні дрони, дрони, що обслуговували вогонь артилерії, об'єднані системою ситуаційної обізнаності, зробили поле бою абсолютно прозорим. Усе це дало необмежені можливості для нанесення високоточних ударів на тактичному рівні. Високоточні удари по шляхах логістики стали сьогодні абсолютно буденним явищем. Ба більше, такі удари вже є частиною тактики видавлення з позицій.

Таким чином, унаслідок абсолютної прозорості перед переднім краєм утворилася 10-15-кілометрова зона суцільної смерті. Уже не дивно, коли дрон полює не за груповою ціллю чи бронеоб'єктом, а навіть за окремим солдатом.

Чому це стало можливим? Причинами цьому є:

по-перше, шалений розвиток засобів РЕБ. Саме завдяки розвитку РЕБ вдалося нівелювати спроможність супутникових технологій, радіо- і GPS-керованих боєприпасів наносити високоточні удари на оперативному рівні. Ефективність дорогих ракет і високоточних снарядів впала до нуля;

по-друге – на полі бою з'явилася велика кількість засобів візуальної розвідки та ударних дронів тактичного й оперативного рівня.

Як наслідок, тактика застосування та оперативне мистецтво зазнали суттєвих змін.

Таким чином, можна з упевненістю сказати, що:

1. Завдяки безпілотним системам та цифровим технологіям традиційні і відомі всім види озброєнь, які десятиліттями визначали характер війни, залишилися в історії. Їх уже немає.

2. Броньована техніка, яка з 1915 року була основою наступальних операцій, стала беззахисною перед дешевими дронами, а отже, її використання і в інших видах бою сьогодні є неможливим.

3. ВТЗ, що використовувала GPS-позиціонування, через розвиток РЕБ втратила свою ефективність.

4. Протиповітряна оборона (ППО) зазнає чи не найбільших трансформацій. Поява великої кількості малих і дешевих дронів зробила економічно недоцільним використання наддорогих ракет до систем ППО.

5. Повітряний простір над полем бою став недоступним для пілотованої авіації і перетворив її на допоміжний засіб ППО. Авіація потребує модернізації й можливості вести розвідку, наносити ураження із зовсім інших відстаней.

6. Морський простір поступово був зайнятий морськими дронами. Тепер могутні кораблі ховаються в захищених портах.

Це не просто технології. Усе це потребує повного переосмислення форм і способів застосування. Як наслідок – перероблення воєнної доктрини.

Очевидно, додає В. Залужний, що Перемога на полі бою тепер повністю залежить від можливостей випереджати противника в технологічному розвитку. Дуже важливо, щоб зміни відбувалися саме в ланцюгу «наука (розроблення) – виробництво – застосування». Саме від ефективного взаємозв'язку між ними буде залежати інноваційний розвиток. Безумовно, необхідно звернути увагу на:

1. Розвиток технологій ШІ та машинного навчання.

Очевидно, що швидкість впровадження технологій ШІ на полі бою, особливо в керуванні складними процесами у сфері розвідки, планування, управління, вогневого ураження, а також автономних бойових систем (без управління людини), надаватиме якісну і кількісну перевагу.

2. Рішення у сфері РЕБ.

Вони є чи не найголовнішими. Адже необхідно, по суті, вирішити два надважливих завдання: створити цифрове поле для застосування і захистити його від впливу противника. А це, звісно, пошук нових технологій зв'язку. Наприклад, когнітивного радіо. Такі розробки вже є. Важливим також є пошук нових способів навігації та донаведення, розроблення нових методів передавання даних, що виходить за межі радіочастотного спектру.

3. Розвиток дешевих високоточних безпілотних систем великої дальності.

Це необхідно для збільшення спроможності систематичного руйнування інфраструктури противника, виснаження його систем ППО та нанесення комбінованих атак по важливих об'єктах.

4. Розвиток і виробництво дронів (роботів) як складової основних бойових спроможностей.

Російсько-українська війна надала країнам важливий урок: війна, що передбачає обмін людських життів на тактичні успіхи, більше не є доступною.

У сучасному бою людина є наддорогим ресурсом. Ресурсом, який відновити неможливо. Саме технології дозволяють зберігати бойову ефективність при радикальному зниженні втрат.

Отже, ми маємо розвивати:

- ударні дрони, які довели свою виняткову ефективність, особливо в умовах дефіциту артилерійських боєприпасів;
- розвідувальні;
- зенітні;
- наземні безпілотні системи;
- універсальні бойові платформи;
- морські безпілотні системи.

5. Цивільні технології або технології подвійного призначення досягли такого рівня складності, що сьогодні вони становлять основу бойових спроможностей. Серед них:

- використання комерційних супутникових систем в інтересах розвідки;
- використання 3D-друку для швидкого виготовлення запасних частин та компонентів військової техніки в «кустарних» умовах;
- використання соціальних мереж для збирання розвідувальних даних;
- створення імпровізованих систем РЕБ із комерційно доступних компонентів для глушіння зв'язку та управління дронами противника;
- використання цивільних месенджерів із наскрізним шифруванням для обміну даними;
- використання хмарних рішень.

В оборонних галузях провідних країн світу сьогодні вже чітко окреслилася тенденція розвитку (на основі принципів та функціональних якостей Четвертої промислової революції) мультиплікаторних зразків, комплексів та систем озброєння та військової техніки (ОВТ), які за своїми можливостями в рази переважають або будуть переважати існуюче озброєння (у деяких країнах – розпочалося прийняття

таких ОВТ на озброєння). Такі зразки, комплекси, системи ОВТ за своїми бойовими характеристиками та наслідками від застосування будуть зіставні з ВТЗ і навіть з ядерною зброєю. Відповідно до цього змінюються погляди на зміст, тактику і стратегію збройної боротьби – вони розглядаються вже не як зіткнення бойових одиниць, що вражають одна одну в ході вогневого протиборства та захоплення території супротивника, а як зіткнення багатофункціональних бойових систем, основною метою якого є позбавлення конфронтуючої системи здатності до дії [6].

Створюються багатофункціональні бойові автономні та дистанційно керовані робото-технічні системи (уніфіковані платформи) зі ШІ різноманітного базування та застосування в режимі реального часу для вибірково-доцільного (селективного) ураження конкретних цілей від тактичного до стратегічного рівня. З'являються принципово нові інформаційно-технічні та інформаційно-психологічні засоби інформаційної боротьби, програмно-апаратні засоби як для проведення кібероперацій, так і для захисту від них. На основі мікромініатюризації створюються малогабаритні та надмалі засоби розвідки та бойового управління тощо.

Усе це призводить до зміни взаємного впливу зброї і способів ведення бойових дій у бік усе більшої залежності останніх від технологічності та ступеня розвитку зброї. При цьому слід зрозуміти, що в основі будь-якого зразка техніки, до яких відносяться і зразки ОВТ, знаходиться технологія його розроблення та виготовлення. Причому початок «народження» новітнього зразка техніки обумовлюється появою та освоєнням нових технологічних принципів обробки сировини, що дозволяють у подальшому створити потрібний зразок. Наявність базових технологій промислового виробництва технічних засобів є визначальним фактором у розвитку озброєнь [7].

Наприклад, до найбільш перспективних напрямів використання нанотехнологій, наноматеріалів і продукції на їхній основі для забезпечення оборони та безпеки держави військові вчені відносять такі:

1. Новітні конструкційні матеріали, які дозволять суттєво розширити показники надійності та експлуатаційний діапазон сучасних і перспективних зразків ОВТ.

2. Засоби зниження помітності зброї різного цільового призначення.

3. Бойове екіпірування військовослужбовців, яке суттєво підвищить захищеність, автономність та ефективність їх дій.

4. Енергетичні системи (матеріали) для озброєнь, насамперед для боєприпасів різного призначення.

5. Компактна та енергоефективна електронна компонентна база військового призначення.

Крім цього, на сьогодні активно застосовується виробництво з використанням 3D-друку у сфері оборони. Адитивне виробництво (Additive Manufacturing, AM), добре відоме як 3D-друк, було визначено Європейською Комісією як одна з ключових технологій, що здатна підвищити конкурентоспроможність промисловості в Європі завдяки її можливостям швидкого, делокалізованого та гнучкого виробництва. AM вже використовується в цивільній промисловості та виробниками оборонного комплексу. Проте збройні сили знаходяться ще достатньо далеко від використання потенціалу цієї технології. Технології AM – шлях до посилення оборонних можливостей. Очікуване зростання ринку AM може генерувати численні переваги для оборонної спільноти: зменшення витрат на виробництво інструментів та деталей, вдосконалення конструкції, скорочення часу на шляху до кінцевого споживача, підвищення технічної та комерційної конкурентоспроможності. Водночас 3D-друк значно вплине на обслуговування військових платформ шляхом виробництва запасних частин та компонентів обладнання. Крім того, технології AM можуть бути перспективними для посилення оборонних можливостей. Ідеться про логістичну підтримку розгорнутих сил у віддалених або ворожих середовищах. Використання цих технологій у проведенні операцій може суттєво вплинути на хід виконання місій. Час між відмовами в роботі та відновленням доступності платформ, транспортування та зберігання значної кількості запасів може зменшитись, із супутнім зменшенням витрат, скороченням логістичного навантаження на операцію.

Використання нових матеріалів для потреб оборони є також сучасним трендом. Озброєння та військова техніка стають дедалі складнішими, як і матеріали, що використовуються для їх створення. У цьому контексті сучасні матеріали викликають чималий інтерес, оскільки їхнє використання може суттєво вплинути на майбутню операційну ефективність військових місій. Новітні матеріали

можуть застосовуватися в широкому діапазоні сфер та ворожих середовищ, де ризики та пошкодження можуть бути зменшені за допомогою захисних рішень. Найбільш проривний ефект планується отримати завдяки інтеграції функціоналів різних нових розробок, таких як зберігання та застосування енергії, камуфляж, моніторинг персонального здоров'я, захист завдяки «суперінтелектуальним» матеріалам для платформ та солдатів. Інші потенційні способи використання новітніх матеріалів, які будуть вивчені в майбутньому, включають потенціал самовідновлювальних матеріалів, матеріалів кіберзахисту (реагування на електромагнітне втручання), конструкції біометричних матеріалів, морфінові аеродинамічні поверхні або інтеграція метаматеріалів.

Широкомасштабна збройна агресія рф проти України засвідчила, наскільки актуальними й навіть пріоритетними для розвитку України стали саме військова справа та воєнна наука. У таких умовах значно зростають роль та місце воєнної науки в забезпеченні національної безпеки, яка має стати одним з основних чинників державного будівництва.

2.2. Концепція ментальної війни російської федерації

Останнім часом набули поширення такі терміни, як когнітивна війна, консцієнтальна війна (КВ), семантична війна, дискурсивна війна та ментальна війна (МВ). Усі ці терміни не є абсолютно взаємозамінними синонімами, хоча описують одне й те саме явище – ураження нематеріальних складників мілітарного чинника: людської волі, духу, свідомості тощо. Термін «ментальна війна» найбільш повно узагальнює сутнісні характеристики всіх наведених визначень і передає їхню семантичну спорідненість.

Згідно з Енциклопедією сучасної України *ментальність* (від лат. mens – розум, спосіб мислення, склад душі) – сприйняття й тлумачення світу в системі духовного життя народу, нації, соціальних суб'єктів [8]. Отже, МВ – це невидиме поле бою, тому що боротьба відбувається насамперед усередині людини, на психофізіологічному рівні.

рф почала МВ проти України задовго до широкомасштабного вторгнення на територію нашої суверенної держави. На думку фа-

хівців, не знаючи мотиваційних механізмів і реальних цілей ворога, не можна побудувати ефективну систему протидії. У такій війні жертва реагує на тактичні кроки агресора, не розуміючи його стратегії. Це призводить до того, що ворог завжди вибиває ґрунт з-під ніг, адже його дії постійні, повторювані, суперечливі, нелогічні.

Упродовж останніх років вітчизняні та зарубіжні експерти приділяють велику увагу дослідженням цілей, механізмів, технологій і засобів російської гібридної (зокрема інформаційної) агресії в Україні та Європі.

Фактично боротьба за ментальність велася протягом усієї історії цивілізації. Однак у сучасних умовах у результаті розвитку інформаційних технологій зміна менталітету людської особистості та її культурної ідентифікації, руйнування національних історичних цінностей суспільства та держави набувають особливої інтенсивності та масштабу.

На думку російських фахівців, боротьбу за ментальність у сучасній війні спрямовано на досягнення основних цілей [9–12]:

- знищення в населення здатності до розуміння місця та ролі своєї країни та її національної стратегії з метою вироблення в подальшому повної байдужості до долі держави та народу;
- руйнування механізмів традиційної самоідентифікації населення та заміщення їх новими ідентифікаційними сурогатами за допомогою залучення людей до різних «груп участі та підтримки», що формуються за допомогою соціальних мереж та ЗМІ;
- зниження загального інтелектуального рівня населення, формуючи «кліпове мислення», яке не передбачає критичного ставлення до інформації, що подається;
- упровадження в суспільну свідомість нової спеціально сконструйованої матриці цінностей і норм суспільної та особистої поведінки як єдино можливих моделей поведінки. Це призводить до знищення родової, культурної та історичної пам'яті людей, а також до психотизації та невротизації суспільства, яке перетворюється на натовп, що легко піддається зовнішньому управлінню з боку політтехнологів;
- вимивання з інформаційного простору свідомості людини питань, що потребують вдумливого та неквапливого осмислення подій для формування сталого особистісного знання.

На сьогодні застосовуються такі прийоми в боротьбі за ментальність:

• приховування критично важливої інформації про стан справ у різних сферах життя соціуму;

• занурення цінної інформації до масиву «інформаційного сміття» відповідно до принципу «сховати листок у лісі»;

• підміна понять чи спотворення їхнього сенсу;

• відвернення уваги на малозначущі події;

• застосування понять, що постійно використовуються в медіапросторі, зміст яких зазнав якісних змін;

• подання аудиторії негативної інформації, яка краще сприймається порівняно з позитивними новинами;

• обговорення подій, які не мають реальної суспільної цінності, використання результатів некоректно проведених соціологічних досліджень для створення спотвореного уявлення про ситуацію в суспільстві;

• запровадження заборон на певні види інформації та розділи новин з метою недопущення широкого громадського обговорення критичних для певних владних структур питань та тем;

• відверта брехня з метою дезінформації населення своєї країни та зарубіжної громадськості.

Деякі російські військові «експерти» безапеляційно стверджують: «Якщо говорити про українську армію, то тут можна виокремити порівняно невелику групу людей, фанатично відданих нинішній київській владі та тій неонацистській ідеології, яка є духовною основою їхнього панування. Але є й інші, які навчались у натовських та американських навчальних закладах. Їхня діяльність добре оплачується київською владою, і вони, отримавши зв'язки з представниками західних еліт та спецслужб, цілком можуть розраховувати в разі потреби на «тепле містечко» на Заході після закінчення служби або в разі виникнення форс-мажорних ситуацій. Але в разі переорієнтації на східний вектор вони можуть отримати надійні гарантії з боку росії і легко змінять свою політичну орієнтацію. Щодо вищих ешелонів військової ієрархії української армії та флоту доцільно наголосити на формуванні в них уявлення про можливість зберегти своє життя та соціальний статус у разі сприяння зміні політичного курсу України. Спираючись на приклади військовослужбовців ЗСУ,

які перейшли на бік росії в ході приєднання Криму до рф, доцільно наголосити, що вище військове керівництво України може зробити більш вдалу кар'єру, зокрема й у лавах ЗС росії. Важливо показати представникам керівництва української армії та флоту, що західна цивілізація, особливо США, переживає важку кризу, що загрожує розпадом провідних країн цієї цивілізації, і як наслідок, – їм зараз не до України. Український чинник вони використовують лише для тиску на росію».

Ці ж «фахівці» з окремим цинізмом зазначають: «Щодо співробітників українських спецслужб, людей у переважній більшості глибоко прагматичних, але здебільшого мало обізнаних у галузі геополітики та міжнародних відносин (за винятком обмеженого прошарку фахівців), основні зусилля доцільно зосередити на доказі простих речей. Насамперед, що для їхніх західних господарів вони просто видатковий матеріал, яким легко пожертвують за необхідності. Прикладів цього достатньо, починаючи з Грузії до Афганістану. Їм необхідно пояснювати, що в разі надання ними практичної допомоги в розвороті України на східний вектор, нехай і в порівняно невеликих обсягах, наприклад, у вигляді бездіяльності чи м'якості щодо проросійськи налаштованих громадян та організацій, то в новій Україні вони не лише не зазнають репресій, але й можуть зайняти вище службове становище, зберігши і покращивши свій соціальний статус.

Приблизно такої ж лінії поведінки має сенс дотримуватися зі співробітниками Міністерства внутрішніх справ України. Їм варто ще нагадати, у якому принизливому становищі вони знаходяться, коли бойовиків націоналістичних організацій, а часом і відвертих злочинців призначають та наближають до нинішньої української влади».

Щодо громадян України російські «експерти» переконані: «Населення України у своїй масі глибоко аполітичне і залякане, щодо нього основний наголос треба робити на зіставленні рівня життя народу в союзі з росією, особливо за часів СРСР. Потрібно демонструвати безперспективність нинішнього курсу, наголошуючи на ймовірному масовому продажу землі іноземцям. Показувати перспективу відродження української економіки, хай навіть незалежної, у співдружності з росією. Доводити, що вбивство їхніх дітей, рідних

та близьких триватиме в будь-якому разі, навіть якщо гіпотетично Донецька Народна Республіка (ДНР) та Луганська Народна Республіка (ЛНР) повернуться до лона української державності, оскільки без війни нинішній режим не може існувати. Важливо, щоб прості українці дійшли висновку, що нинішні київські узурпатори мають на меті не відродження України, а її знищення з фізичним винищенням переважної більшості українського населення».

У підсумку представники рф наголошують, що ефективність інформаційного протиборства вирішальною мірою залежить від різноманітності залучуваних до її ведення зусиль і коштів. Для цього мають залучатися всі основні державні структури та недержавні утворення, зокрема:

• офіційні дипломатичні органи держави, що вирішують властиві їм завдання політико-правового та дипломатичного забезпечення, а також виконують спеціальні дії політико-дипломатичного характеру;

• міжнародні недержавні організації, основним призначенням яких може бути формування сприятливого міжнародного морально-психологічного фону діяльності держави, а також виконання окремих інформаційних акцій;

• державні та недержавні органи та ЗМІ, які мають бути основним засобом інформаційно-психологічного впливу на населення та керівництво України;

• політичні партії та рухи, християнські та ісламські релігійні організації, державні та недержавні організації та установи культури, творчі організації, які мають бути найважливішим чинником ідейно-релігійного та культурного впливу;

• державна інфраструктура (енергетика, транспорт та зв'язок), паливно-енергетичний та сировинний комплекс країни, промисловість є основним інструментом реалізації інформаційних акцій економічними методами;

• державні органи та структури, що забезпечують військову, політичну та внутрішню безпеку держави: різні спецслужби та збройні сили, недержавні воєнізовані формування відіграють головну роль у виконанні спеціальних інформаційних акцій, зокрема, демонстративного характеру;

• мережеві структури та спільноти у світовому кіберпросторі, які мають суттєво впливати на основну частину українського

суспільства, насамперед молодь. Особливо важливими є ті їх компоненти, які територіально розгорнуті поза межами росії і можуть виступати як іноземні представники, демонструючи погляд на Україну з інших країн.

Розглянемо структуру та окремі положення концепції МВ рф, основні її закономірності та принципи.

На думку російських дослідників, нова парадигма війни має такі особливості [10, 15]:

• агресивні дії (напад) починають без оголошення, їх ведуть у сірих зонах, вони мають еволюційний, перманентний характер і нерідко призводять до поразки держави-жертви через її нездатність дати гідну відсіч;

• національні держави, що зазнали поразки, ліквідуються, причому часто без окупації їхньої території, або втрачають не так населення й ресурси, як політичну волю та можливість самоврядування;

• населення країни-жертви нерідко опиняється під керівництвом структур (зовнішніх та внутрішніх) і втрачає змогу впливати на свою долю;

• боротьбу ведуть за розум, знання та волю, за світогляд окремих громадян і суспільства в цілому;

• національну історію, культуру, традиції, устрій та вибір життєвих пріоритетів населення ігнорує та замінює на інші, які нав'язують ззовні нерідко за мовчазної згоди людей;

• абсолютною перемогою вважають окупацію духовного простору та суспільної свідомості, коли переможений не лише втрачає здатність відстоювати свої цінності, а й повністю асимілює чужі та фальшиві настанови, які йому впровадив, нав'язавши свою волю, противник-переможець;

• бліцкриг у цій війні полягає в тому, щоб паралізувати волю противника через вплив на його еліту та ЗМІ, а потім їхніми руками зруйнувати державні інститути, деморалізувати армію та силові структури;

• країну-жертву атакують не лише ззовні, а й зсередини, що радикально відрізняється від традиційного способу ведення військових дій «ззовні всередину»; фронти та битви такої війни різномасштабні, але синхронізовані та системні.

Російські військові експерти зазначають, що безкомпромісне геополітичне протиборство нового типу, якому властиві вказані особливості, дістало відповідний термін – МВ. Вона має тотальний характер, що передбачає комплексний вплив, який спрямовано як на інформаційне поле, так і на сфери почуттів, емоцій і настроїв населення країни – жертви агресії.

Із цього випливає визначення МВ – це сукупність різномасштабних скоординованих дій та операцій, спрямованих на паралізацію волі противника, зміну індивідуальної і масової свідомості населення, деморалізацію армії та суспільства, знищення духовних і моральних цінностей, традицій та культурно-історичних основ держави, руйнування національної ідентичності.

На думку російських фахівців, боротьбу за ментальність у сучасній війні направлено на досягнення таких основних цілей [10–15]:

- позбавлення населення здатності до розуміння місця й ролі своєї країни та її національної стратегії з метою вироблення в подальшому повної байдужості до долі держави та народу;
- руйнування механізмів традиційної самоідентифікації населення та заміщення їх новими ідентифікаційними сурогатами через залучення людей до різних груп участі та підтримки, що формуються за допомогою соціальних мереж і ЗМІ;
- зниження загального інтелектуального рівня населення за допомогою формування кліпового мислення, яке не передбачає критичного оцінювання інформації, що подається;
- упровадження в суспільну свідомість нової спеціально сконструйованої матриці цінностей і норм суспільної та особистої поведінки як єдино можливої моделі поведінки. Це призводить до знищення родової, культурної та історичної пам'яті людей, а також до психотизації та невротизації суспільства, що перетворюється на натовп, який легко піддається зовнішньому управлінню з боку політтехнологів;
- вимивання з інформаційного простору свідомості людини питань, що потребують вдумливого та неквапливого осмислення подій для формування сталого особистісного знання.

Російські експерти [13] вважають, що концепцію МВ необхідно розглядати як важливий складник загальної теорії війни (рис.

2.1). Теоретико-методологічні основи концепції МВ складають соціально-філософські, психологічні, соціальні, політологічні та інші теорії (наприклад, «вікно Овертона»), теорію національної безпеки, стратегію національної безпеки, воєнну науку, закони війни (перебігу та результату війни, що розкривають їхню залежність від економічного, політичного, соціального, наукового, військового потенціалів держави), закони збройної боротьби тощо. Основне місце в концепції займають філософсько-соціологічні положення про походження, сутність, характер, роль МВ, а також про розвиток і діяльність держави та ЗС в умовах ведення такої війни.

Структура концепції МВ включає такі основні розділи: теоретичні основи; понятійний апарат; методологічні основи (основні закономірності МВ, методи й технології психологічної оборони); практичні рекомендації (рис. 2.2). Передбачено, що ключові положення концепції МВ у подальшому мають стати основою для розроблення відповідних підручників, посібників, настанов, програм навчальних курсів, практичних і методичних рекомендацій для органів державного й військового управління різних рівнів та вищих навчальних закладів.

Визначено такі основні закономірності МВ:

- постійне зростання інтенсивності;
- всеохоплюваність і наполегливість, що посилюється;
- ураження всіх сфер суспільства (розростається як ракова пухлина);
- взаємозв'язок і взаємовплив усіх сфер суспільства, соціальних інститутів;
- визначальний характер духовної сфери та значний вплив економічних чинників на трансформацію суспільства;
- відтермінування впливу, зумовлене інерційністю свідомості (складність протидії технологіям МВ, тому що важко, а часом й неможливо домогтися відмови від помилкових переконань, нав'язаних противником), що створює проблеми в «лікуванні» свідомості та трансформацій у духовній сфері суспільства, які стали наслідком застосування технологій МВ.

На основі дослідження досвіду й практики застосування різних форм, способів, методів та прийомів ведення МВ сформульовано деякі її принципи: превентивність, релевантність, адаптивність,

комплексність, індивідуальність, груповий і масовий підходи, наступальний характер, постійне зростання інтенсивності, дзеркальність.

Спотворення реальності – одна з основних стратегій рф та антиукраїнських сил у нашій державі. Важливим складником антиукраїнської політики є маніпуляції з дискурсом історії, які використовують як інструмент нівелювання загальноукраїнської ідентичності, а також дискредитація діяльності ЗСУ та її спеціальних служб.

2.3. Тенденції розвитку інформаційно-психологічних впливів

Проблема онтології війни має давню традицію, що бере початок від античності. Ще з часів давньогрецького історика Фукідіда окреме місце в дослідженнях природи війни відводилося способам ведення війн і поведінці ворога. У багатьох працях поствестфальського періоду, сфокусованих на проблемах війни, головну увагу приділено сутності війни як антагоністичної збройної боротьби держав, що має на меті досягнення певних цілей. Класичне визначення війни як способу досягнення політичних цілей іншими засобами, яке належить прусському теоретику Карлу фон Клаузевіцу, гранично чітко окреслює таке розуміння сутності війни. Принципово не відходячи від цього класичного визначення, сучасні військові теоретики й практики досліджують методи та технології ведення новітніх війн.

Сьогодні одним із найефективніших видів зброї невоєнного характеру є інформаційні ресурси. Війна як засіб комунікації остаточно диджиталізувалася й перетворилася на інструментарій поділу людей. Україна стала першою у світі державою, яка стикнулася з диджиталізованою воєнною агресією.

Г. Почепцов зазначає, що інформаційні війни часто не різняться між собою, але вони чітко поділяються на технічні й гуманітарні. Гуманітарні інформаційні війни можна поділити на два інші типи: інформаційні війни та смислові війни. На думку Г. Почепцова, якщо просто інформаційні війни мають справу з поданням нових фактів, то смислові війни працюють з реінтерпретацією наявних фактів. Смислові війни спрямовано на руйнування картини світу об'єкта, що призводить до таких типів рішень, які б він не прийняв за старої картини світу. Їх інструментарієм можуть бути не лише прямі, а й фонові впливи, не лише інформаційні операції,

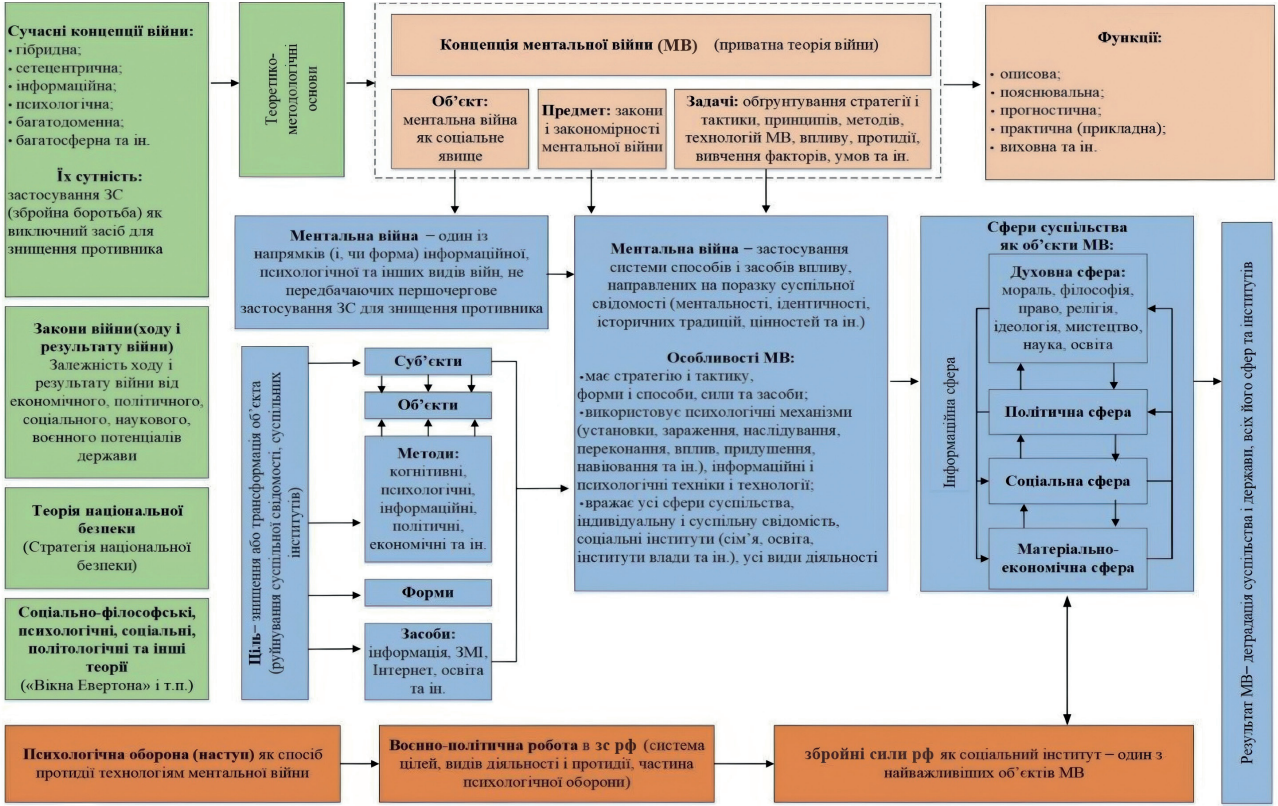

Рис. 2.1. Концепція МВ як важлива складова загальної теорії війни

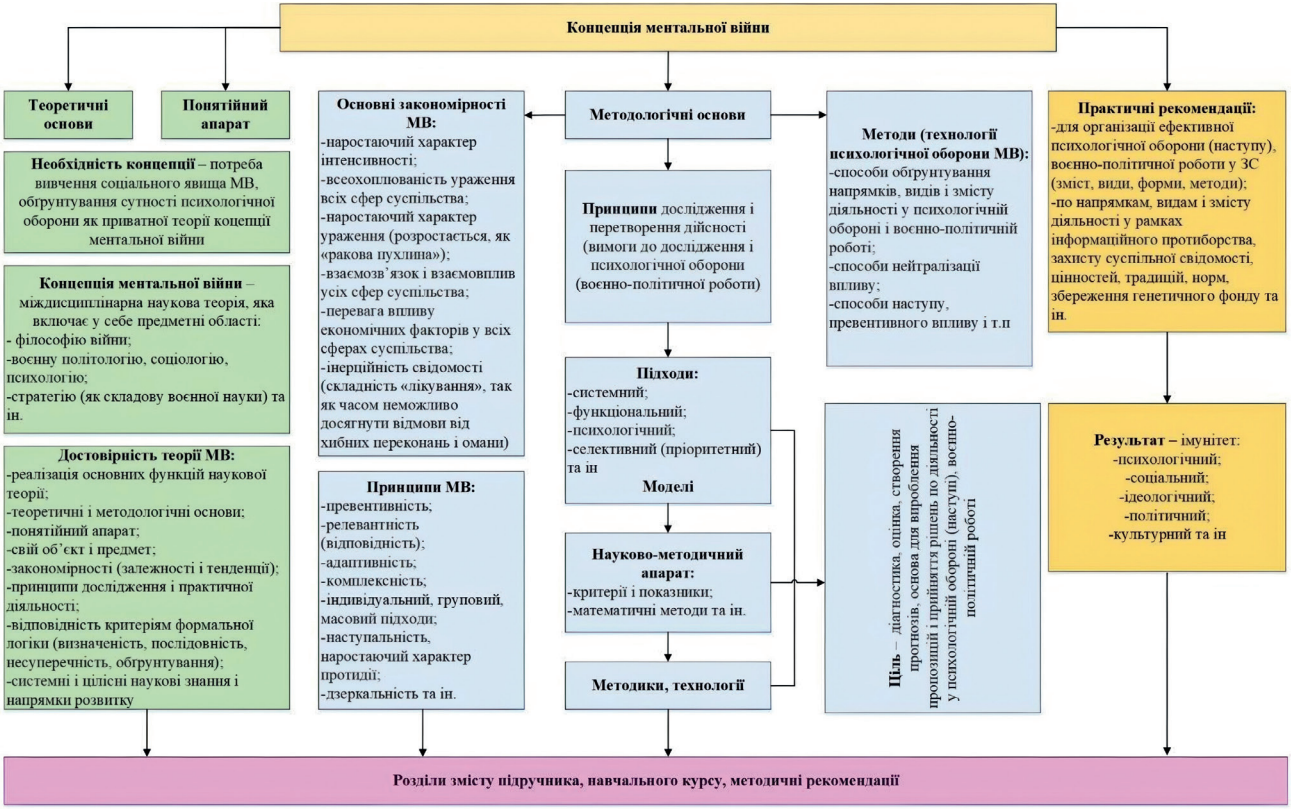

Рис. 2.2. Структура концепції МВ

а й операції впливу. Головною ж відмінністю стає їх довгостроковий характер, тому сьогодні такі дії можуть відбуватися поза увагою об'єкта впливу. Як зазначає Г. Почепцов, усі війни покликані змінити поведінку противника / опонента, і для цього вони мають різний інструментарій. Кожен тип війни спрямовано на певний тип простору: звичайну війну – на простір фізичний, інформаційну – на інформаційний, смислову – на простір когнітивний. Однак саме український досвід показав, що ключовим об'єктом сучасної війни є не кіберпростір, а когнітивна сфера людини.

Якщо Хіросіма і Нагасакі стали символами розуміння людством руйнівної сили ядерної зброї, то війна росії проти України має стати прикладом розуміння небезпеки інформаційної зброї, а саме – інформаційно-психологічної війни.

У науці існує низка тлумачень інформаційно-психологічної війни. Найбільш влучним є визначення дослідниці Т. Бєльської, яка під інформаційно-психологічною війною розуміє вплив, що здійснюється з метою цілеспрямованого поширення спеціальної інформації, яка впливає на психіку і поведінку політичної еліти та громадянське суспільство певної країни або регіону. Тому вищою формою війни майбутнього можна назвати КВ (від латинського conscientia – свідомість) – систему інформаційно-пропагандистських та психологічних заходів, що проводяться із застосуванням ЗМІ, культури, мистецтва та інших (психотропних, психотронних) засобів протягом тривалого часу за ретельно розробленими сценаріями.

Після широкомасштабного вторгнення рф на територію України 24 лютого 2022 року розпочалась і нова фаза КВ, у межах якої використовують широкий спектр консцієнтальної зброї та набутий досвід управління свідомістю за допомогою різних інформаційних кампаній. Вплив таких кампаній рф спрямовано на три основні цільові аудиторії:

- аудиторія країни прямого конфлікту – наразі України (для зміщення ціннісних орієнтирів, насадження необхідної для емоційно-психологічного, а згодом і фізичного підкорення картини світу, формування в населення сприйняття справедливості рішень і планів російського керівництва);
- внутрішня аудиторія рф та аудиторія країн, що її підтримують (для підтвердження правильності дій російського керівництва

та формування якнайбільшої аудиторії, що буде не лише підтримувати рішення кремля, а й стане на бік агітатора й виконуватиме його функції);

• зовнішня аудиторія (для створення інформаційних умов позитивного сприйняття політики рф за кордоном, створення нових агентів впливу, які добровільно, використовуючи специфічні для аудиторії кожної країни важелі, будуть не лише й надалі підтримувати ідеологію кремля, а й підбурювати на конфлікт союзників України).

Д. Кашперська серед головних інструментів ведення КВ у кіберпросторі виокремлює такі [16]:

• SMM-активності (Social Media Marketing);

• астротурфінг;

• deepfake та підміна реальності;

• сугестія на сайтах державних структур тощо.

SMM-активності. З активним розвитком соціальних мереж з'явився ще один майданчик не лише для продажу товарів, але й для продажу ідей. рф активно використовує можливості та засоби SMM для інформаційно-психологічного впливу на широку аудиторію соціальних медіа. Інструменти соціального маркетингу в мережах мають чимало кейсів для управління свідомістю та вибором особою того чи іншого об'єкта. Серед основних принципів SMM, якими послуговується рф у КВ проти України, можна виокремити такі: соціальний доказ, обмін, емоційна пастка, прихильність, авторитетність, дефіцитність.

Астротурфінг. Сучасні кібертехнології дають змогу сугестивно впливати не лише через різнорідний контент, але й за допомогою активного використання кіберсимулякрів. Це віртуальні акаунти, які симулюють репрезентацію реальних людей і завдяки коментарям до певного інформаційного повідомлення можуть змінювати й деформувати його суть. У зв'язку із цим з'явився спеціальний термін «астротурфінг». Активне використання новітніх інтернет-технологій сприяє заміщенню соціальної та політичної реальності комп'ютерними симуляціями [17].

Астротурфінг – це використання сучасного програмного забезпечення або спеціально найнятих оплачуваних користувачів (так званих веббригад) для штучного управління громадською думкою. Цю технологію застосовують для витіснення думки реальних людей

на вебфорумах, для організації підроблених кампаній в Інтернеті, які створюють враження, що велика кількість людей вимагає чогось конкретного чи виступає проти чого-небудь.

Термін походить від назви популярного бренду «AstroTurf», що виробляє синтетичне покриття, яке використовують замість трави на стадіонах. Згодом так стали називати процес створення штучної громадської думки, найчастіше в Інтернеті, у якому беруть участь спеціально найняті на фінансовій основі працівники на численних форумах, сайтах ЗМІ та в блогах. Вони пишуть замовні матеріали, залишають коментарі під постами в соціальних мережах або здійснюють масовий перепостинг необхідної інформації, створюючи в такий спосіб враження спонтанної народної підтримки політика, політичної групи чи партії, продукту, сервісу, події тощо.

Оскільки астротурфінг є однією з форм кіберагресії, його здійснюють не лише найняті користувачі. Серед них можуть бути і так звані тролі (дійові особи, які надають експресивного забарвлення новинам), і боти, фейкові акаунти, вбудовані банери прихованого рекламного змісту, які створено за допомогою складного програмного забезпечення. Троль – креативний, бот – механічний.

Головними функціями астротурфінгу є такі:

- формування помилкового уявлення про події та явища, навіювання хибних спогадів тощо;
- маніпулювання (створювання емоційних та інформаційних пасток, які впливають на прийняття рішень, вибір певної позиції тощо);
- формування певного емоційного фону в аудиторії (почуття паніки, страху, байдужості тощо);
- провокування ворожнечі та агресії (міжнаціональної, расової, релігійної тощо);
- формування масової позаколективної поведінки (стимулювання до дій офлайн).

І якщо бот здебільшого механічно дублює задану алгоритмом інформацію, то троль створює інформаційні повідомлення, які містять емоційно-експресивну лексику та викликають почуття емпатії в реципієнта.

За даними дослідження Принстонського університету (США), росія несе відповідальність за 72 % операцій щодо дезінформації

у світі, включно в соцмережах, обігнавши Китай, Іран і Саудівську Аравію [19]. рф активно використовує астротурфінг як частину гібридної війни з Україною ще з часів Революції Гідності. Послуговування астротурфінгом російською владою відрізняється від традиційних форм пропаганди. Її мета – не переконати чи довести, а підірвати та дискредитувати. За ступенем впливу його можна віднести до категорії зброї масового ураження, але не одномоментного, а прихованого, що прогресує, як інформаційна пандемія. кремль активно використовує ботоферми з метою дестабілізації суспільно-політичного стану України та інших розвинених демократичних країн.

Oxford Internet Institute, який є частиною Оксфордського університету, детально аналізує проблему кіберпропаганди в дев'яти різних країнах, зокрема й в Україні [18]. Учасники цього дослідження Сем Вуллі та Філ Говард стверджують, що після Євромайдану та анексії Криму росією Україна перетворилася у фронт численних кампаній із дезінформації. Більшість із них має інтернет-компонент з активним використанням соціальних мереж, тролів і ботів, із чим пов'язана низка певних внутрішніх та зовнішніх загроз національній безпеці. Згідно з даними дослідження, 21 % українців використовує соціальні мережі як основне джерело новин у той час, коли будь-яка соціальна мережа може бути платформою для активного астротурфінгу, метою якого є дезінформація.

Із початком російської агресії проти України у 2014 році ольгінські тролі активізувалися на просторах укрнету на різних платформах. У 2017 році в Україні було заборонено й заблоковано російську соцмережу «ВКонтакте» (VK). До цього часу вона була другим за популярністю сайтом після Google. Із моменту захоплення Криму, із часів розгортання «руської весни» у східних і південних регіонах було створено багато груп із політичним забарвленням, що підтримували незаконні дії рф на території нашої країни та поширювали антиукраїнську пропаганду. Серед найбільш відомих антиукраїнських груп тих років у VK можна виокремити такі [19]:

- «Сводки от ополчения Новороссии» сумнозвісного Ігоря Стрєлкова, який навесні 2014 року керував операцією із захоплення Слов'янська, а під час широкомасштабної збройної агресії рф із лютого 2022 року є активним YouTube-блогером щодо воєнно-політичних питань;

• «АнтиМайдан» та інші спільноти, які мають це слово у своїй назві;

• «Народное ополчение Донбасса»;

• «Русская весна»;

• «Донецкая республика» тощо.

Аналітична платформа «VoxUkraine» наприкінці 2018 року проаналізувала базу даних із майже 4 тисяч російських акаунтів, оприлюднених Twitter у жовтні того ж року. Було виявлено, що за період із 2010 до 2018 року 1 369 акаунтів російського Агентства інтернет-досліджень згенерували 774 957 твітів про Україну. Сумарна кількість фоловерів у цих профілів – 3,4 млн користувачів. До анексії Криму російські боти у Twitter майже не торкалися української тематики [20]. Поступовий сплеск активності у них розпочався після псевдореферендуму в Криму.

Одним із найпоказовіших кейсів зовнішньої комп'ютерної пропаганди є медіаактивність у відповідь на катастрофу малайзійського Boeing MH17 авіакомпанії «Malaysia Airlines», яка сталася на непідконтрольних територіях Донбасу 17 липня 2014 року і забрала життя 298 людей. За однією з «теорій змови» літак було збито в повітрі українським винищувачем. Ця версія постала з Twitter-повідомлення іспанського авіадиспетчера Карлоса (@spainbuca), який нібито супроводжував політ цього рейсу. Указаний користувач повідомив не лише про те, що спостерігав дві українські ракети коло літака за секунди до його збиття, але й опублікував низку твітів про відповідальність України за катастрофу: «Київ відповідальний», «Нам у диспетчерській загрожують», «Поки в мене не забрали телефон і не розбили мені голову, ще раз: Київ збив літак».

Допис @spainbuca поширило багато користувачів, а потім і медіакомпанії RT і TASS, й інші російські новинні агентства. У липні 2014 року ці повідомлення було використано на пресконференції міністерством оборони росії. Міністерство інформаційної політики України згодом довело, що цей Twitter-акаунт був ботом, діяльність якого було активізовано під час Євромайдану для розповсюдження антиукраїнських гасел. У вересні 2016 року спільне міжнародне слідство довело, що літак було збито російською системою «Бук» із території, контрольованої проросійськими сепаратистами.

2017 року журналісти Radio Free Europe / Radio Liberty і група румунських журналістів-розслідувачів RISE Project зв'язалися з особою на ім'я Хосе Карлос Барріос Санчес, що видавала себе протягом усього часу за користувача цього акаунта [21]. У розмові з ними він визнав, що ніколи не працював диспетчером і не був в Україні під час аварії MH17. Санчес стверджував, що за свої дописи в Twitter він отримував із росії великі суми грошей, а саме 48 тис. дол. від медіакомпанії RT, в ефірі якої згодом після збиття боїнга він з'явився. На телеканалі заперечують, що переводили гроші Санчесу.

Наприкінці 2014 року акаунт знову активували, але вже під іменем Людмила Лопатишкіна. Як й іспанський диспетчер Карлос, вона бореться з «українською хунтою» і ретвітить прокремлівські акаунти, чергуючи це позбавленими сенсу повідомленнями («безстрашна – дивиться», «розмалюю небо», «у 37-му отримав він»). Це підтверджує те, що акаунт «Лопатишкіна» – бот. Станом на 2020 рік акаунта не існує.

Отже, можна дійти висновку, що, як у період існування вказаного акаунта під іменем Карлос, так і після його перейменування, він був штучним кіберсимулякром. Однак у першому разі, найімовірніше, його активністю керувала реальна людина, яка формувала порядок денний і цілеспрямовано доводила до аудиторії свідомо помилкову інформацію. У другому ж – публікації на цій сторінці робили хаотично, часто з граматичними та семантичними помилками, а ретвіти мали тотожний характер із ретвітами попереднього умовного власника користувацької сторінки Twitter. Варто зауважити, що боти в мережі переважно фоловлять та ретвітять одне одного. Вони можуть бути навіть із різних країн, але говорити однією мовою (іспанською, англійською тощо). Наведений приклад активності акаунта @spainbuca підтверджує ефективність астротурфінгу як інструменту політичної та соціальної дестабілізації, що впливає не лише на громадян однієї країни (у цьому разі України), а й породжує фейкові інформаційні приводи для всієї світової спільноти.

На підставі аналізу подібних акаунтів можна виокремити характерні ознаки астротурфінгу, а саме:

- анонімність;
- неабиякий мобілізаційний потенціал, що сприяє високій соціальній самоорганізації громадян;

• низький рівень фінансових витрат на реалізацію інформаційних кампаній, що спричиняють гучний резонанс;

• високий рівень лояльності громадян до створених комунікаторів;

• швидкі темпи розповсюдження фейкової інформації.

Характерною ознакою російської кіберпропаганди є те, що кремль її використовує як для формування відповідної реальності на певній території, так і для забезпечення легітимності дій своїх збройних сил за межами держави й впливу на формування потрібної реакції міжнародної спільноти та світових військово-політичних організацій, як це було продемонстровано на прикладі бот-акаунта @spainbuca у Twitter.

Не менш активно рф використовує астротурфінг й напередодні виборів у багатьох країнах ЄС. Так, у вересні 2023 року віцепрезидентка Європейської комісії Вера Юрова заявила, що соціальні платформи мають діяти напередодні національних та європейських виборів наступного 2024 року задля недопущення розповсюдження дезінформації з боку росії. Натомість вона наголосила, що X, колишній Twitter, який більше не підпадає під добровільний кодекс поведінки у співпраці з ЄС, є платформою з найбільшим співвідношенням публікацій із неправдивою інформацією. А це сприяє російській «війні ідей», про що йшлося в матеріалі Bloomberg [22].

У межах російсько-української війни кремль використовує будь-який інфопривід для консцієнтального впливу. Культурна галузь не є винятком. Twitter (тепер X) дає змогу зручним способом впливати на міжнародну спільноту, нагромаджуючи кількість акаунтів-симулякрів, які утворюють інформаційний шум навколо певного наративу. Так, під час перемоги України на Євробаченні 2022 року, у цій соцмережі ботами, замаскованими під користувачів з Європи, було поширено фото групи «Kalush», фронтмен якої ніби показує жест, що характерний для вітання нацистів. Таке навіювання цілком відповідає цілям КВ рф, яка намагається нав'язати світу й своїм громадянам образ «нацистської» України. Варто зауважити, що ці боти часто підписані на проросійські акаунти в Twitter, зокрема Russia Today.

Під час дослідження журналістів мережі «The Conversation» на початку широкомасштабного вторгнення було виявлено активність 75 офіційних акаунтів російського уряду. Загалом у них понад

7 млн підписників і понад 35 млн ретвітів. Із 25 лютого до 3 березня 2022 року ці акаунти запостили 1 157 твітів, серед яких приблизно три чверті було присвячено фейкам про вторгнення в Україну та спробам його виправдати [23].

Широкомасштабне вторгнення рф в Україну 24 лютого 2022 року спровокувало нову хвилю бот-активності. Так, згідно з аналізом компанії «CASM Technology», яка досліджує дезінформацію в мережі, саме на 24 лютого припав пік реєстрації нових користувачів у Twitter, а це може свідчити про організацію мережі [24]. Також після 24 лютого у Twitter стали виходити в топ пости з хештегами #IStandWithPutin та #IStandWithRussia. Якщо звернути увагу на профілі, які роблять пости з такими хештегами, то можна зауважити, що більшість із них або було створено напередодні вторгнення в січні-лютому, або вже після вторгнення. Варто зазначити, що користувальницька географія з напівпорожніми профілями – це країни Африки та Азії. Виявилося, що пропаганда також ефективно працює в Індії та Туреччині, а найбільша активність сумнівних акаунтів спостерігалася в перші 12 днів вторгнення.

Астротурфери, на відміну від автоматизованих ботів, пишуть осмислені тексти, що підтверджує більшість досліджень аналітичних компаній. Це зазвичай оригінальні замітки з різними формулюваннями. Сама практика астротурфінгу для рф не нова. Коли під час пандемії перед світовою спільнотою постав виклик подолати новий штам коронавірусу COVID-19, астротурфери по всьому світу активізували свою діяльність, генеруючи фейкові твердження та поширюючи дезінформацію серед населення щодо вірусу завдяки соціальним мережам [25]. На початку липня Kings College London оприлюднив дослідження щодо впливу конспірології та соціальних медіа на поведінку людей під час пандемії [26]. У ньому йдеться про те, що люди, які отримують більшість новин із соціальних мереж, таких як Facebook, Twitter, YouTube, частіше вірять теоріям змови про пандемію. Російські ботоферми переважно підхоплюють фейкову новину на російському відомому чи маловідомому медіаресурсі та вдаються до її численних репостів і ретвітів. Бот-акаунт також часто публікує лише вступний абзац статті, який із погляду психолінгвістики обов'язково має містити емоційно-експресивну лексику, що сприяє здійсненню сугестивного впливу на реципієнта. Відповідно до пові-

домлення Служби безпеки України (від 1 червня 2020 року) від початку карантину в Україні було заблоковано понад 2,6 тис. спільнот та акаунтів у соціальних мережах, які розповсюджували фейки про COVID-19, 18 з яких діяли згідно із завданням рф [27]. Головними меседжами бот- і троль-акаунтів були заклики до порушення умов карантину, акцій протестів, силового захоплення влади та підтримки таких неправомірних заходів.

Дослідники з Університету Карнегі-Меллон стверджують, що бот-кампанії домінували в багатьох онлайн-розмовах про коронавірус уже із січня, тобто від самого початку пандемії. Проаналізувавши понад 200 млн повідомлень у мережі Twitter на тему коронавірусу, дослідники з'ясували, що приблизно 82 % із топових 50 впливових ретвітів – це боти, а 62 % із перших 1 000 впливових ретвітів – також боти [28].

Отже, астротурфінг – це спосіб викривлення дійсності за допомогою розставлення необхідних тій чи іншій інформаційній кампанії акцентів у соціальних мережах через велику кількість репостів або публікації постів схожого змісту, сторонні коментарі під публікацією чи в мікроблогах, які змінюють суть самої публікації, новини, події тощо. Основними складниками такого виду кіберпропаганди є боти та тролі. Головними їхніми завданнями є навіювання почуття паніки, страху, байдужості, ненависті чи агресії, трансформація ставлення до фактів і персоналій тощо. В епоху активної інтернет-комунікації маніпуляція свідомістю інструментами інформаційних повідомлень від ботів та тролів є одним із головних способів ведення гібридної війни, а також й інформаційного супроводження широкомасштабної агресії рф проти України. Відповідно до визначення Оксфордського словника маніпуляція (manipulation) – це процес здійснення часто прихованого контролю чи впливу на когось чи на щось [29].

Тролінг – це один із засобів астротурфінгу, коли в агресивній або жартівливій формі подають чи коментують якусь інформацію. Чужа агресія часто сприймається іншими людьми як упевненість у своїй позиції, що найчастіше притупляє пильність слухача / читача та бажання перевірити достовірність інформації. Підвищення ефективності астротурфінгу було реалізовано на основі адаптації до його завдань технології ботів – спеціальних програм, що виконують автоматично або за заданим розкладом / алгоритмом будь-які дії через ті самі інтерфейси, що й типовий користувач.

На рівні з такими найпопулярнішими соціальними мережами українців, як Facebook, Instagram чи YouTube, дедалі більш популярним стає месенджер Telegram, який також має засоби соціальних медіа, зокрема блог-сторінки. Цей застосунок, який створили росіяни Микола та Павло Дурови, має вже пів мільярда користувачів. Він увійшов до 10 найпопулярніших мобільних програм світу. Популярність Telegram підживлювали суперечки з Роскомнаглядом, який намагався отримати доступ до даних чи заблокувати месенджер у росії. Команда Telegram неодноразово публічно давала відсіч російським спецслужбам, що приваблювало нових користувачів. У Telegram можна створювати канали, де їхні власники можуть в односторонньому порядку поширювати контент, який є публічним; інформація в цих каналах відкрита, а бути їхнім підписником може будь-хто. В Україні популярними стали анонімні телеграм-канали, які поширюють дезінформацію та маніпулюють фактами, а також мають чіткі зв'язки з російськими пропагандистськими медіа та спецслужбами [30]. Головними причинами, чому Telegram є сприятливою платформою для ведення КВ, є такі:

- наскрізне шифрування й можливість спілкуватися з необмеженою кількістю людей;
- брак чіткої політики та процедур модерації контенту;
- повна анонімність;
- простота створення й адміністрування каналів;
- налаштована система миттєвих сповіщень тощо.

Як на сайтах соціальних мереж, так і на інформаційних порталах пропагандисти використовують класифікатори – систему розподілу дезінформаційних повідомлень за групами відповідно до заздалегідь визначених ознак. Класифікаторами є ключові слова, до яких підібрано варіанти дезінформаційних повідомлень (наративів).

Наприклад, можна виокремити такі класифікатори:

- «Калібр» (типові варіанти повідомлень у російських новинах: високоточна зброя; крилата ракета, якій немає аналогів; зброя перемоги);
- «Українська влада» (типові варіанти повідомлень у російських новинах: київський режим; влада Зеленського; київська хунта, український Рейх);
- «Патріоти України» (типові варіанти повідомлень у російських новинах: бандерівці; націоналісти; неонацисти; азовці; армія Києва);

• «Himars» (типові варіанти повідомлень у російських новинах: американська реактивна система залпового вогню; неточна та стара зброя; має малу дальність; убиває цивільних).

Для посилення смислового та емоційного ефекту класифікатори супроводжуються в новинах відповідним відеорядом.

Deepfake та підміна реальності. Епоха «глибоких» підробок із множинністю реальностей створила матрицю з інформації, у якій особистість стає не лише споживачем, а й елементом цієї системи. Користувач світової павутини примножує кількість інтерпретацій, а завдяки сучасним цифровим технологіям може створювати й альтернативну реальність, яку одразу розпізнати як фейкову майже неможливо. Зважаючи на максимально швидке споживання інформації в результаті кліпового мислення, технологія deepfake стала продуктом технології ШІ. Це призвело до стрімкого поширення у світі підроблених відео- та аудіозаписів. Чим досконалішим стає ШІ, тим більш переконливо виглядають нові підробки.

Ця технологія поступово змінює правила гри у сфері політтехнологій та інформаційних війн. Deepfake стає проблемою національної безпеки нового покоління. Створення підроблених новин, зловмисні обмани, зокрема компрометації знаменитостей, публічних осіб і знищення політичної репутації – усе це відбувається завдяки цій технології з найбільшою результативністю, оскільки у споживача часу на глибинний аналіз майже немає у швидкозмінному потоці інформації, особливо в часи загострення соціальних настроїв. Можливість поширення інформації, та сама spreadability, про яку писав у 2013 році американський дослідник Генрі Дженкінс у книжці «Spreadable Media» [31], погано впливає на сприйняття та усвідомлення – користувач у середньому схильний натискати на кнопку «поділитися», не замислюючись і спираючись переважно на привабливість, віральність контенту, ніж на його достовірність. Тому deepfake став справжньою шок-технологією, від якої поки що немає абсолютного захисту – лише критичне мислення та фактчекінг.

На світовому ринку вже є чимало додатків, за допомогою яких будь-хто може зробити deepfake. Найвідоміші з них – це Zao, DeepFaceLab, Deepfakes web β. Програмний директор неприбуткової американської організації «Witness» Сем Грегорі зауважує, що deepfake часто використовують для дискредитації жінок-журналістів

і громадських активістів. Однак відповідно до його спостереження політики почали часто використовувати deepfake як виправдання невдалим промовам чи кинутим ненароком фразам у публічному просторі, що викликали резонанс. Вони стверджують: «це deepfake», що відповідає фразі «це фейкові новини» [32].

Перший великий резонанс на політичному підґрунті ця фейкова технологія створила 2020 року. Ситуація стосувалася соціально-політичного руху «Extinction Rebellion» (Бельгія), який технологіями deepfake «змусив» Прем'єр-міністра Бельгії Софі Вільмес розповісти, що причина коронавірусу – екологічні проблеми. Не менш резонансним випадком стала підміна відеовиступу спікера Палати представників США Ненсі Пелосі, на якому було додано ефект стану алкогольного сп'яніння промовиці. Це відео переглянуло в Інтернеті понад 2,5 млн користувачів соціальних мереж. Проте найвідомішим фейковим відео став сфальсифікований виступ Барака Обами, де він лайливо звертався до Дональда Трампа. Мільйони людей переглянули це відео на YouTube і почули слова президента, які той ніколи не говорив. Ніякого скандалу не було, оскільки в кадрі з'явився режисер цього монтажу Джордан Піл і пояснив, що цією творчою витівкою він спробував привернути увагу до цифрової дезінформації.

росія наразі тільки освоює можливості цієї технології. Уже хрестоматійним прикладом глибинного фейку став випадок, коли у 2017 році міноборони рф опублікувало кілька постів у твітері та фейсбуці, у яких містилося «незаперечне підтвердження» співпраці США з бойовиками угруповання ІДІЛ. Натомість, це був обрізаний скріншот із промо до мобільної гри «AC-130 Gunship Simulator», а також відео ліквідації Військово-повітряними силами (ВПС) Іраку бойовиків ІДІЛ у 2016 році.

Від початку широкомасштабного вторгнення рф в Україну Центр стратегічних досліджень та інформаційної безпеки у Facebook попереджав громадян про можливу цифрову провокацію з боку кремля (deepfake), де Володимир Зеленський має оголосити про капітуляцію країни [33]. Мета такого відео – дезорієнтувати, посіяти паніку та почуття зневіри в громадян, деморалізувати спецслужби країни і схилити війська до складання зброї. Якщо такого сценарію не було реалізовано щодо президента, то технологію deepfake було успішно застосовано в червні 2022 року з метою дискредитації мера

Києва Віталія Кличка. Відомо, що кілька європейських столиць отримали з фальшивої поштової скриньки запити на спілкування з ним через додаток «ZOOM». Мери Берліна та Мадрида погодилися на розмову. Завдяки вказаній технології хакери використали зовнішність Кличка для переговорів. У виданні «Deutsche Welle» повідомлялося, що в розмові з бургомістеркою Берліна Франциской Ґіффай фейковий Кличко говорив про соціальні виплати для українських біженців і попросив ужити заходів щодо заохочення молодих хлопців повертатися до України воювати. Також співрозмовник попросив підтримати Київ порадою щодо проведення ЛГБТ-прайду [34]. Ця розмова містила типові кремлівські наративи, які вказують на російський слід у цій фейковій розмові. Але пропагандисти припустилися грубої помилки – побудували розмову винятково на конструктах, що викликають резонанс, а не зробили її більш емоційно / психологічно інтертекстуальною та сугестивною. У результаті згодом сама бургомістерка засумнівалася в достовірності цієї розмови. Варто зауважити, що це перший випадок використання deepfake в живому онлайн-спілкуванні на високому міжнародному рівні, що впливає не лише на репутацію політичної персони, але й усієї країни.

Сугестія на сайтах державних структур. Одним із найбільш прихованих консцієнтальних впливів за своїм механізмом й обраним майданчиком є навіювання настроїв і сприйняття певних фактів суспільно-політичного життя країни через відкриті комунікативні канали сайтів державних установ, зокрема сторінку електронних петицій на сайті Президента України [35].

Однією з рис прямої демократії є вільне право громадян направляти індивідуальні чи колективні письмові звернення до органів державної влади, тим самим брати безпосередню участь у державному управлінні та формуванні політики країни в різних її галузях. Таким інструментом голосу народу (vox populi) є електронні петиції (е-петиції), які було запроваджено на сайті Президента України в серпні 2015 року. Упродовж трьох місяців петиція має набрати не менше ніж 25 тисяч голосів, і тоді президент зобов'язаний протягом 10 днів на неї відреагувати.

Е-петиції виконують декілька функцій. По-перше, вони дають змогу винести ту чи іншу проблему на порядок денний. По-друге, за допомогою петиції можна запропонувати свій варіант розв'язання

порушеної проблеми, завдяки чому громадяни долучаються до процесу ухвалення рішень. По-третє, петиції пожвавлюють горизонтальну комунікацію між самими громадянами, адже для того, аби зібрати необхідну кількість підписів, ініціатори мають схилити на підтримку петиції інших осіб. Отже, актуалізація проблеми, внесення будь-якої авторської ідеї на широкий розгляд, залучення (часто вірусне за допомогою інструментів SMM) великої кількості громадян до обговорення – доволі зручний механізм управління громадською думкою, а завдяки різним текстовим наповненням самих звернень і свідомістю особистості прихованими засобами через канал офіційної комунікації влада-громадянин. Саме тому електронні петиції викликають чималий інтерес з огляду на їх потенціал консцієнтальних впливів у межах війни смислів та інформаційної війни росії проти України.

Попри те, що ст. 23-1 Закону України «Про звернення громадян» [36] регламентовано, що петиція «не може містити заклики до повалення конституційного ладу, порушення територіальної цілісності України, пропаганду війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, заклики до вчинення терористичних актів, посягання на права і свободи людини», лишається велике поле для більш прихованих маніпуляцій. Такі тексти звернень стають активним інструментом просування інтересів росії в Україні через агентів – громадян України (петицію може подати лише громадянин України, який має електронний підпис). На цьому ґрунті можемо виокремити такі типи небезпеки контенту петицій з огляду на аудиторію їх впливу:

- маніпуляція інформацією, деформація інформаційного поля, нав'язування та штучне навіювання громадської думки, створення ілюзії актуальності певного питання завдяки інформаційному шуму та довірі до державних електронних ресурсів, а також просування неукраїнського дискурсу;
- ухвалення деякими силами у владі сумнівних для держави практичних рішень на підставі громадського звернення, що підриває основи національної безпеки.

Інформаційне агентство «Qırım Haber Ajansi» («Кримські новини») у 2020 році зробило контент-аналіз петицій на сайті Президента України на тему Криму і виявило, що після офіційного припинення постачання електроенергії на півострів із 1 січня 2016 року

багато петицій стали писати неякісно, із чималою кількістю орфографічних і стилістичних помилок, без серйозного обґрунтування пропозиції та навіть українською мовою впереміш із російською [37]. Дослідження показало, що доволі велику кількість петицій було присвячено закликам до різного роду способів деокупації Криму, перерізання суходольного зв'язку півострова з материком. Щоразу після появи цих петицій у російських ЗМІ та українському сегменті соцмереж спалахувало активне їх просування й обговорення. А питання «відрізання» Криму росія інтерпретувала як те, що Україна де-факто визнає окупацію Криму навічно.

Під час нового етапу російсько-української війни, який розпочався 24 лютого 2022 року, було зареєстровано низку провокативних петицій, зокрема щодо питань оборонного характеру, а саме:

- запит на підвищення віку мобілізації для чоловіків до 65 років та скасування обов'язкового військового обліку жінок. Така петиція викликала бурхливе неоднозначне обговорення громадян України в соцмережах, а російські ЗМІ використали цей факт для підтвердження двох тез: «в України настав дефіцит живої сили» і «українці не хочуть виконувати злочинні накази київського режиму»;
- запити щодо дозволу на виїзд за кордон чоловіків різних категорій диференціації під час дії воєнного стану. Ці регулярні петиції рф використовує для поглиблення розколу та ворожнечі всередині української спільноти для подолання її консолідації проти спільного ворога;
- множинна кількість петицій, що надходять чи не щодня щодо термінового надання важкої зброї на східний фронт України. Засилля такого контенту створює панічні настрої серед громадян України з постійним нав'язуванням думки про зраду, а також використовується агентами впливу для підкреслення неспроможності України протистояти «міці російської армії»;
- заклики до укладання мирної угоди з рф. Переважно такі петиції не містять конструктиву, а лише емоційно-експресивні звернення, які навіюють стан зневіри та переконують у тому, що війну можна припинити вже зараз, проте комусь це не вигідно, а влада не зважає на народ.

Можна стверджувати, що система фільтрації допущених до публікації петицій є доволі слабкою та потребує перегляду, а сам

контент має стати об'єктом глибокого наукового дослідження, а також пильної уваги з боку уповноважених правоохоронних органів і спеціальних служб України, зокрема розвідувальних органів. Засипання сервісу петиційним спамом, у якому губляться конструктивні ідеї та пропозиції, а механізм взаємодії влади з громадою дискредитується, є прикладом однієї з технологій гібридної війни, яку веде росія проти України. Застосовано технологію рефлексійного управління поведінкою противника, що породжує нівелювання авторитету інституцій влади, інституцій демократії, відбувається псування іміджу інституту президентства як такого, Верховної Ради України, Кабінету Міністрів України тощо. Петиції несуть у собі небезпеку, яка полягає в практичній реалізації: надання підстав для дій російських агентів впливу у владі і дій людей, які не надто заглиблені в певну проблему.

З огляду на вищевикладене можна припустити, що цифрові консцієнтальні атаки на Україну тільки посилюватимуться. Це буде зумовлювати до пошуку нових методів протидії, а також до застосування міждисциплінарних методів роботи з інформацією в мережі, налагодження на державному рівні тісних зв'язків зі світовими IT-компаніями, такими як Google, Meta, Microsoft. Ефективність такої співпраці стала очевидною після звіту цих компаній у вересні 2023 року. На прохання Європейського Союзу, а саме президентки Європейської комісії, вони проаналізували свій інформаційний простір щодо частки в ньому російської пропаганди та дезінформації, пов'язаної з війною рф проти України.

Компанії діють на основі укладеного Кодексу практики (Code of Practice), чотирма новими підписантами якого стали Alliance4Europe, Newtral, EFCSN і Seznam. Підписанти, які є великими онлайн-платформами, зобов'язалися звітувати кожні шість місяців про свої дії. Звіти містять інформацію про дії платформ щодо зменшення дезінформації навколо теми війни росії в Україні. TikTok та Meta розширили зусилля щодо перевірки фактів різними мовами ЄС. Також вони співпрацюють з інформаційними агентствами, серед яких Reuters. Фактчекінг Meta охоплює 22 мови в ЄС, включно на сьогодні із чеською та словацькою. TikTok перевіряє факти в контенті російською, українською, білоруською та 17 європейськими мовами. Він вивчив 832 відео, пов'язаних із війною, після цього було вилучено 211 із них.

Зазначено, що 30 % користувачів скасовують рішення поділитися публікацією, коли бачать напис «неперевірений контент» [38].

Зважаючи на серйозні ризики, пов'язані з дезінформацією для демократій Європи, комісія очікує від підписантів посилення їх зусиль для боротьби з дезінформацією в Україні та навколо європейських виборів. З огляду на це доречно було б, зокрема Міністерству цифрової трансформації України, долучитися як зацікавленій стороні до цих ініціатив й отримати доступ до архіву Центру прозорості, у якому зберігаються вказані звіти, а також працювати разом із цими компаніями над розширенням діапазону перевірки інформації, навіть через залучення українських інформаційних агентств до співпраці. Це дасть змогу на державному рівні взяти під частковий контроль розгалужену інфраструктуру цифрової пропаганди, якнайефективніше використати можливості інформаційно-мережевого метамодерного суспільства, а саме завдяки цифровим технологіям попереджувати інформаційну підміну реального світу, дійсних уявлень, переконань штучними симулякрами агресора.

Висновки до другого розділу

Російсько-українська війна може скоро закінчитися, а може тривати роками. У будь-якому разі вона вже показала, який вигляд матимуть війни майбутнього, так само як громадянська війна в Іспанії стала передвісником Другої світової. Україна може перемогти росію так, як Давид переміг Голіафа. Існує багато способів перемагати, і хитрий стратег знає, як утілити їх у життя.

Україна зруйнувала російські наступальні плани. Дії ЗСУ під час відсічі російської широкомасштабної агресії офіційно позначено як послідовне проведення кількох операцій.

Деталі цих операцій опишуть історики. Проте вже можна вказати на деякі парадокси російсько-української війни, які для більшості країн світу стали реальними несподіванками:

• жодну сучасну армію не було задіяно у війні настільки високої інтенсивності. Війна, яку росія розв'язала проти України, стала найбільш масштабним конфліктом в Європі з часів Другої світової війни. Україна на рівних бореться з ядерною державою та

армією, яку російська пропаганда донедавна визначала як «другу у світі»;

• фронтові успіхи України, яку підтримують численні союзники, спричинили призупинення планів Китаю щодо вторгнення на Тайвань;

• ЗСУ надзвичайно швидко освоїли високотехнологічне ОВТ іноземного походження. Водночас Україна активно відроджує своє оборонне виробництво;

• практично не маючи сучасних Військово-морських сил (ВМС), Україна перемагає Чорноморський флот рф, трансформуючи його оперативно-стратегічні можливості в оперативно-тактичні (на рівні флотилії);

• наступальні дії ЗСУ спростували один із фундаментальних постулатів воєнної науки про необхідність чисельної (у 3–5 разів) переваги в живій силі та озброєнні під час наступу. Українська армія наступає в умовах переваги противника як в озброєнні, так і в кількості особового складу;

• українська логістика, елементи якої частково розміщено за кордоном, забезпечує більшість потреб фронту. Її вдало оптимізовано з огляду на загрози авіаційних і ракетних ударів.

З огляду на реалії сьогодення, воєнна наука має забезпечувати упереджувальне науково-теоретичне обґрунтування актуальних проблем воєнної безпеки держави, відкривати перспективи розвитку воєнної справи та добиватися того, щоб інновації якомога швидше впроваджувались у діяльність ЗСУ – їх підготовку, застосування та забезпечення.

Ставлення до мирних громадян, яке демонструє російська армія, кардинально суперечить уявленням сучасної військової культури, дає підстави стверджувати – керівництво армії росії свідомо відмовляється від гуманних методів ведення війни, передбачених міжнародним правом. Не менш агресивний характер і руйнівні масштаби має інформаційна війна, яку синхронно з конвенційною війною веде росія проти України. Інформаційна та пропагандистська кампанії росії завдають величезної шкоди ментальному здоров'ю українського населення. Сучасні дослідження, які проводяться на досвіді українського соціуму, показують, що рівень психічних розладів, травмувань і захворювань серед населення значно зріс за період російської агресії.

Особливо вразливими до негативного впливу інформаційних операцій та пропагандистських акцій є люди, які мають попередній досвід психічних розладів, а також молодь та люди похилого віку. Агресивні інформаційна та пропагандистська кампанії спричиняють серед українського населення різноманітні психічні розлади, найбільш типовим з яких є посттравматичні стресові розлади, тривожні розлади, депресії та суїцидальні думки. Зростаюча кількість дезінформації, фейків і маніпулятивних інформаційних кампаній є серйозним викликом для збереження ментального здоров'я громадян. Інформаційна агресія, зокрема в контексті сучасної інформаційної епохи, може вплинути на психологічний стан усіх без винятку категорій населення – як військовослужбовців, так і цивільних осіб. У збереженні ментального здоров'я громадянам може допомогти використання різних профілактичних й оздоровчих підходів, методик та технологій.

Інформаційна війна в сучасних умовах є одним із вирішальних факторів перемоги. Особливо це важливо для України, яка веде асиметричну війну проти ядерної держави з переважаючим військовим потенціалом. Від того, як за кордоном сприймають події в Україні, залежить і рівень політичної підтримки, і обсяги допомоги, і масштаби запроваджених проти агресора санкцій.

На сьогодні відбувається процес докорінного переосмислення сформованого образу інформації та сутності інформаційних воєн, її цілей та методів. Особливо гостро це відчувається у складовій зовнішньополітичного курсу рф відносно України та під час повномасштабної російської військової агресії в 2022 році. рф використовує психологічні операції та дезінформацію, яка перетворилася на стандартну та невід'ємну практику «гібридної» війни – зовнішньої політики кремля у глобальному масштабі. Події, що розгорнулися в Україні, є найбільшим випробуванням усієї історії української державності. рф продовжує використовувати проти України активні форми інформаційно-психологічного впливу та явну пропаганду з метою консолідації власного населення, дестабілізації внутрішньої ситуації в нашій державі, а також «легітимізації» своїх агресивних дій на зовнішній арені. Для того щоб зрозуміти, як саме росія веде інформаційну війну, слід розуміти, до яких маніпуляцій вона вдається. Напрямами та способами інформаційних війн рф проти України були й залишаються:

• поступове зниження міжнародного іміджу України з метою послаблення її геополітичного значення;

• відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики «керованого хаосу»;

• формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу;

• домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури.

Перелік використаних джерел:

1. Середін А. Війна в Україні як війна п'ятого покоління: Чому ця війна не переросте у Третю світову. URL: https://politteo.online/materialy/vijna-v-ukrayini-yak-vijna-pyatogo-pokolinnya-chomu-czya-vijna-ne-pereroste-u-tretyu-svitovu/ (дата звернення: 25.07.2025).

2. Кобець Ю. Особливості розгортання та типологізація способів ведення сучасної війни. *Вісник Прикарпатського університету. Серія: Політологія.* Ужгород. Випуск 17, 2024. С. 59–66.

3. Требін М., Чернишова Т. Тренди збройної боротьби у війнах XXI століття. *Світоглядний сенс сучасної війни: соціогуманітарні аспекти: монографія* / за ред. В. А. Кротюка. Харків : Факт, 2024. С. 201–238.

4. Макфейн Ш. Нові правила війни. Перемога в епоху хаосу / пер. з англ. Ігор Бігун. – Київ : Наш Формат, 2023. 256 с.

5. Залужний В. Нова природа війни змінила сутність основ глобальної безпеки: український досвід і майбутній світовий порядок. URL: https://www.pravda.com.ua/columns/2025/04/25/7509135/ (дата звернення: 14.05.2025).

6. Теоретичні засади управління оборонними ресурсами: монографія / В. В. Коваль, О. М. Семененко, Л. В. Скуріневська, С. П. Мокляк, І. М. Ткач, С. В. Ясенко; під ред. О. М. Семененка. Київ : Генеральний штаб Збройних Сил України, 2023. 485 с.

7. 10 трендів майбутнього, які армія України поки що ігнорує. URL: https://defence-ua.com/minds_%20and_ideas/10_trendiv_majbutnogo-2067 (дата звернення: 24.01.2025).

8. Енциклопедія сучасної України. URL: https://esu.com.ua/article-66534 (дата звернення: 12.06.2025).

9. Ильницкий А. М. Ментальная война России. *Военная мысль.* 2021. № 8. С. 19–34.

10. Маричев М. О., Лобанов И. Г., Тарасов Е. А. Борьба за ментальность – тренд современной войны. *Военная мысль.* 2021. № 8. С. 48–56.

11. Сивков К. Технология вразумления. Как убеждать население Украины в неизбежности добрых отношений с Россией. URL: https://vpk-news.ru/articles/64480 (дата звернення: 10.06.2025).

12. Манойло А. Информационные операции разведок эволюционируют и обретают новые формы. URL: https://vpk-news.ru/articles/64291 (дата звернення: 10.12.2025).

13. Караваев И. Н. Концепция ментальной войны как составная часть учения о войне и армии. *Военная мысль*. 2022. № 3. С. 35–42.

14. Ильницкий А. М. Стратегия ментальной безопасности России. *Военная мысль*. 2022. № 4. С. 24–35.

15. Коржевский А. С., Соловьёв И. В. Ментальное противоборство и проблемы формирования целостной системы наступательных и оборонительных действий в нем. *Военная мысль*. 2022. № 11. С. 32–42.

16. Грані агресії: деякі узагальнення досвіду російсько-української війни 2014-2024 років; за ред. д. політ. н. Мироненка П. В., д. політ. н., проф. Мокляка С. П. Київ : Політія, 2024. 395 с.

17. Свідерська О. І. Формування віртуального натовпу шляхом маніпуляції свідомості населення. *Гілея: науковий вісник*. 2019. Вип. 149 (№ 10). С. 62–66.

18. Trends Online Foreign Influence Efforts. URL: https://esoc.princeton.edu/files/trends-online-foreign-influence-efforts (дата звернення: 24.08.2025).

19. ВКонтакте. URL: https://vk.com (дата звернення: 17.08.2024).

20. Как российская «Фабрика троллей» пыталась влиять на повестку дня в Украине. Исследование 755 000 твитов. URL: https://voxukraine.org//longreads/twitter-database/index-ru.html (дата звернення: 27.08.2025).

21. Испанский диспетчер, видевший, как украинцы сбили MH17, превратился в Людмилу Лопатышкину. URL: https://theins.ru/antifake/27246 (дата звернення: 17.07.2023).

22. Musk's X Is Biggest Outlet of Russia Disinformation, EU Says. URL: https://www.bloomberg.com/news/articles/2023-09-26/eu-faults-musk-s-x-in-fight-against-russia-s-war-of-ideas (дата звернення: 30.09.2023).

23. Russian Government Accounts Are Using a Twitter Loophole to Spread Disinformation. URL: https://theconversation.com/russian-government-accounts-are-using-a-twitter-loophole-to-spread-disinformation-178001 (дата звернення: 26.09.2023).

24. #IStandWithRussia #IStandWithPutin. Message-based Community Detection on Twitter. URL: https://files.casmtechnology.com/message-based-community-detection-on-twitter.pdf (дата звернення: 26.09.2023).

25. Кашперська Д. О., Карпенко А. В. Вплив астротурфінгу на національну безпеку під час пандемії коронавірусу COVID-19. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи* : матеріали міжн. наук.-практ. конф. (м. Одеса, 10–11 вересня 2020 р.). Одеса, 2020. С. 278–279.

26. Health-Protective Behaviour, Social Media Usage and Conspiracy Belief During the COVID-19 Public Health Emergency. URL: https://www.cambridge.org/core/journals/psychological-medicine/article/healthprotective-behaviour-social-media-usage-and-conspiracy-belief-during-the-covid19-public-health-emergency/A0DC2C5E27936FF4D5246BD3AE8C9163 (дата звернення: 03.09.2023).

27. У 2020 році СБУ нейтралізувала 600 кібератак і викрила 20 хакерських угруповань. URL: https://ssu.gov.ua/novyny/u-2020-rotsi-sbu-neitralizuvala-600-kiberatak-i-vykryla-20-khakerskykh-uhrupovan (дата звернення: 27.08.2020).

28. Nearly Half Twitter Accounts Discussing May Be Bots. URL: https://www.scs.cmu.edu/news/nearly-half-twitter-accounts-discussing-%E2%80%98reopening-america%E2%80%99-may-be-bots (дата звернення: 27.08.2020).

29. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/american_english/manipulate (дата звернення: 26.09.2023).

30. СБУ викрила агентурну мережу спецслужб РФ, яка дестабілізувала ситуацію в Україні через Telegram-канали. URL: https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly (дата звернення: 12.06.2021).

31. Henry Jenkins, Sam Ford & Joshua Green. Spreadable Media: Creating Value and Meaning in a Networked Culture. New York, USA : New York University Press, 2013. 352 p.

32. Researcher Explains Deepfake Videos. URL: https://www.youtube.com/watch?v=u2lX70U7N0c&t=88s&ab_channel=WIRED (дата звернення: 28.10.2020).

33. Уявіть, що бачите в телевізорі Володимира Зеленського… URL: https://www.facebook.com/protydiyadezinformatsiyi.cpd/posts/131151736100567 (дата звернення: 20.03.2022).

34. Розмова з «Кличком»: мерка Берліна стала жертвою пранкерів. URL: https://www.dw.com/uk/rozmova-z-klychkom-merka-berlina-stala-zhertvoiu-prankeriv/a-62258579 (дата звернення: 28.06.2022).

35. Електронні петиції. Офіційне інтернет-представництво Президента України. URL: https://petition.president.gov.ua (дата звернення: 22.08.2022).

36. Про звернення громадян : Закон України від 02.10.1996 р. № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text (дата звернення: 22.08.2022).

37. Qırım Haber Ajansi / Агентство «Кримські новини». URL: https://old.qha.com.ua/ru/search?t=%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0 (дата звернення: 22.08.2022).

38. Code of Practice on Disinformation: New Reports Available in the Transparency Centre. URL: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-reports-available-transparency-centre*r (дата звернення: 26.09.2023).*

РОЗДІЛ ІІІ

ПРИВАТНІ ВІЙСЬКОВІ КОМПАНІЇ – АСИМЕТРИЧНИЙ ПОТЕНЦІАЛ СУЧАСНОГО ЗБРОЙНОГО ПРОТИСТОЯННЯ

3.1. Становлення й розвиток приватних військових компаній: особливості та класифікація

ПВК мають довгу історію, яка розпочалася ще з найманців середньовіччя. Проте сучасна форма ПВК набула особливого поширення з 1970-х років, коли почали з'являтися перші комерційні військові організації, надаючи державам та приватним особам широкий спектр військових послуг. В українських публікаціях зустрічаються різні їх назви – «приватні військові компанії» або «приватні воєнні компанії». З огляду на наявну в Україні нормотворчу термінологію у сфері оборони автори вважають за доцільне використовувати назву «приватні військові компанії» [1]. Сьогодні ПВК функціонують як невід'ємна частина збройних конфліктів, використовуючи унікальні можливості для ведення операцій в умовах сучасного військового середовища. Особливо помітним є їхній вплив у тих випадках, коли держави намагаються досягти своїх цілей, уникаючи безпосередньої участі регулярних збройних сил.

ПВК відіграють значну роль у сучасних збройних конфліктах і все частіше виступають як ключові учасники на міжнародній арені [2]. Їхнє виникнення та розвиток пояснюються низкою факторів, серед яких геополітичні зміни, економічна вигода та необхідність адаптації до нових типів конфліктів та воєн, що відбулися у світі наприкінці XX ст. та продовжують відбуватися у XXI ст. Однак разом зі зростанням їхнього впливу постають питання правового регулювання, що потребують додаткової уваги з боку міжнародного співтовариства.

Ці організації надають широкий спектр послуг, а саме: реформування та розвиток сил безпеки і оборони; планування та підготовка їх до застосування; розвідка та контррозвідка; навчання особового

складу; застосування, обслуговування та експлуатація ОВТ; матеріально-технічне забезпечення сил безпеки і оборони; гуманітарне розмінування; охорона та безпосередня участь у бойових операціях [3].

Поява ПВК є логічним продовженням історії найманців, які виконували військові завдання для тих, хто мав достатньо коштів, щоб їх найняти. Протягом століть найманці брали участь у конфліктах, починаючи із середньовічних ландскнехтів і до сучасних приватних армій. Однак сучасні ПВК офіційно оформилися як структури у 1960-х роках у Великій Британії, коли з'явилися перші компанії, що надавали військові послуги на контрактних засадах. Засновником першої, у сучасному розумінні ПВК, що має назву «Watchguard International» і створена в 1967 році, був полковник британської армії Девід Стерлінг, який раніше створив SAS (Special Air Service) – спеціальний військовий підрозділ Великобританії, основним напрямом якого була розвідувальна діяльність та проведення спеціальних операцій переважно на території іноземних держав [4]. А компанією, яка одна з перших запропонувала урядам та приватним компаніям рішення у сфері охорони та безпеки, стала Control Risks Group. Цей підхід поступово поширився у світі, і до кінця XX ст. ПВК почали активно використовуватися в різних конфліктах та для захисту інфраструктури в нестабільних регіонах.

Початок активного використання ПВК у сучасному вигляді пов'язаний із кінцем XX ст. та розпадом Радянського Союзу, коли після закінчення Холодної війни країни зіткнулися з необхідністю брати участь у численних регіональних конфліктах, зокрема миротворчих, гуманітарних або суто військових діях у регіонах із високою інтенсивністю конфліктів, а багато урядів скоротили свої регулярні збройні сили. Для таких завдань ПВК стали ідеальним інструментом: вони забезпечували швидку реакцію, високий рівень спеціалізації та відсутність потреби політичного обґрунтування перед громадськістю. Іншим важливим чинником розвитку ПВК є економічна доцільність їхнього використання. Уряди багатьох країн, зокрема США та Великобританії, зіткнулися з проблемою високих витрат на утримання регулярних збройних сил, особливо після закінчення великих військових конфліктів. ПВК стали привабливим варіантом для виконання специфічних завдань, оскільки їх залучення дозволяло державам заощаджувати на витратах на утримання великих військових контингентів. Окрім цього,

багато міжнародних корпорацій, особливо в нафтовидобувній та будівельній галузях, почали активно використовувати послуги ПВК для захисту своїх інвестицій та інфраструктури в зонах конфліктів. Наприклад, охорона нафтових родовищ у таких країнах, як Ірак або Нігерія, часто здійснюється приватними військовими компаніями. Сучасні війни, особливо на початку XXI ст., стали менш формальними, а конфлікти перейшли у формат гібридних війн або конфліктів низької інтенсивності. У таких умовах ПВК виявилися ефективнішими за регулярні збройні сили через свою гнучкість, можливість швидко адаптуватися до нових умов й уникнення публічної уваги. Війна стала бізнесом. Ринок військових послуг виріс, перетворивши ПВК на ключових гравців у цьому бізнесі. Наприклад, у 2009 році річний оборот ринку приватних військових послуг досяг 100 млрд дол. Це підтверджує, що ПВК стали не лише стратегічним інструментом для урядів і корпорацій, але й важливим елементом глобальної економіки.

Також однією з причин швидкого поширення ПВК у цей період стало зростання кількості «конфліктів низької інтенсивності», які вимагали гнучкого підходу до ведення бойових дій, зокрема в регіонах Африки та Близького Сходу. Оскільки ці конфлікти часто не вимагали масових регулярних армій, держави й корпорації все частіше зверталися до послуг ПВК для виконання завдань у таких зонах.

Одним із перших прикладів успішного використання ПВК стала компанія Executive Outcomes, створена в Південній Африці в 1989 році [3]. Її діяльність під час громадянської війни в Анголі та Сьєрра-Леоне продемонструвала здатність невеликих, але добре оснащених і професійно підготовлених приватних військових груп вирішувати завдання, з якими регулярні армії часто не могли впоратися. Ця компанія стала прикладом для наслідування та відкрила шлях до формування цілої індустрії ПВК.

Після цього було створено низку інших відомих компаній, зокрема Blackwater (заснована в 1997 році у США), яка стала однією з найвідоміших ПВК у світі. Її роль під час військових операцій США в Іраку та Афганістані широко обговорювалася в міжнародних ЗМІ. Blackwater, пізніше відома як Academi, тепер відома як Constellis, стала символом не лише високого професіоналізму ПВК, але й контроверсійних ситуацій, пов'язаних із використанням приватних військових формувань.

Функціонування ПВК у міжнародному середовищі залишається суперечливим з юридичної точки зору [2]. Незважаючи на те, що ПВК працюють за контрактами з урядами або корпораціями, їхній правовий статус часто не регулюється на належному рівні. Найманство, заборонене міжнародними конвенціями, не повною мірою застосовується до ПВК, оскільки ці компанії мають офіційний статус і діють у межах закону своїх країн. Проте єдиної міжнародної правової бази, яка б регулювала діяльність ПВК, немає. Деякі країни запровадили внутрішнє законодавство для контролю за діяльністю ПВК, але відсутність глобального регулювання призводить до правових прогалин, що дозволяє ПВК діяти на межі законності. Натомість США стали першою державою, що законодавчо врегулювала діяльність ПВК. Відповідний нормативно-правовий документ було прийнято командуванням армії США 1998 року – інструкція FM 100-21, що регулював взаємовідносини між державою та ПВК, а саме між військовослужбовцями армії США та співробітниками ПВК.

Проте з початком 2000-х років набирають популярності спеціалізовані послуги з логістики, підготовки кадрів служб безпеки, розроблення та впровадження систем безпеки, планування операцій. Фахівців ПВК стали залучати для охорони виробництва, родовищ корисних копалин (в основному нафти та газу), для супроводу вантажів та інше.

Китай, як один із провідних глобальних геополітичних гравців, також розпочав активно використовувати потенціал ПВК для захисту своїх національних інтересів. Хоча ПВК у Китаї ще не мають такої широкої популярності та впливу, як у США чи росії, їхня роль зростає в контексті міжнародної експансії та захисту глобальних проєктів, таких як ініціатива «Один пояс, один шлях». Китайські ПВК діють не лише на території країни, але й за її межами, виконуючи широкий спектр завдань.

Китай, який протягом багатьох років був закритою країною, пережив бурхливий економічний розвиток і завоювання віддалених ринків одночасно з падінням Берлінської стіни, встановленням нового світового порядку, подіями 11 вересня 2001 року та арабськими революціями. Це прискорення історичного розвитку спонукало 10 млн китайців виїхати за кордон у понад 200 країн світу [5]. Сьогодні

ці китайці за кордоном представляють 37 000 китайських компаній і контролюють активи за кордоном на суму 2 трлн дол. [6]. Запуск проєкту «Пояс і шлях» (Belt and Road Initiative, BRI) у 2013 році, який є найбільшим геоекономічним і геостратегічним проєктом XXI ст., безпосередньо пов'язаний із діяльністю Пекіна в 70 країнах, головним чином у Центральній Азії, Південній Азії, Східній Африці, Північній Африці та Східній і Центральній Європі, у рамках 900 структурних проєктів на суму 800 млрд дол. [7].

За іронією долі, у період з 2002 по 2019 рік 140 000 терористичних атак торкнулися країн у регіонах BRI, що призвело до 234 000 смертей [8]. За даними Міністерства торгівлі Китаю, у період з 2010 по 2015 рік 345 терористичних інцидентів були пов'язані з китайськими або китайськими компаніями за кордоном, що призвело до загибелі понад 1 000 осіб [9]. Протягом цього періоду китайська влада розвивала свою доктрину зовнішньої безпеки відповідно до розвитку своїх економічних і геостратегічних амбіцій. Результатом цього стали аутсорсинг безпеки китайських економічних інвестицій, приватизація безпеки в країні та за кордоном, а іноді й спокуса використовувати цю дискретну силу, розкидану по всьому світу, в інших цілях.

До 1984 року лише чотирьом китайським компаніям було дозволено працювати за кордоном. Усі вони були пов'язані з урядовими установами. У 1980 році президент Ден Сяопін розпочав економічні реформи та створив чотири спеціальні економічні зони на південно-східному узбережжі Китаю. Перший експеримент охоплював тодішні невеликі міста Шеньчжень, Чжухай і Шаньтоу в провінції Гуандун та Сямень у провінції Фуцзянь. У 1984 році китайський уряд вирішив поширити його на 14 великих прибережних міст, включаючи Шанхай. Того ж року в Шеньчжені в одному з відділень Бюро громадської безпеки було створено першу китайську компанію, аналогічну приватній охоронній компанії (ПОК). У 1986 році було створено Пекінську генеральну охоронну компанію, яка існує донині і нараховує 77 000 співробітників. Її діяльність зосереджена переважно на внутрішньому ринку Китаю. У 1994 році була створена Shandon Huawei Security Group – перша китайська охоронна компанія, яка працювала за кордоном і супроводжувала китайські компанії в їхньому експорті. Вона існує й досі, переваж-

но в Африці, де забезпечує захист гірничодобувних і нафтових проєктів та інфраструктурних проєктів. Через рік була створена China Security and Protection Group, яка згодом стала головним захисником BRI.

У вересні 2009 року Державна рада Китаю видала «Положення про управління безпековими та охоронними послугами» (Baoan Fuwu Guanli Tiaoli). Цей захід був першою спробою уряду встановити нормативно-правову базу для приватної охоронної галузі та де-факто легалізувати ПОК. Положення визнає дві основні категорії ПОК. По-перше, «охоронні компанії» (baoan fuwu gongsi), що мають завдання з навчання, охорони та консультування з питань оцінки та зменшення ризиків. Їхній персонал оснащений нелетальною оборонною зброєю. По-друге, «охоронні компанії, що надають послуги збройного супроводу» (congshi wuzhuang shouhu yayun fuwu de baoan fuwu gongsi). Таким компаніям дозволено оснащувати своїх сертифікованих співробітників бойовою зброєю, але не важким військовим обладнанням або транспортними засобами. Ця правова база не визначала характер діяльності цих компаній за кордоном, але дозволила відкрити сотні малих компаній і зміцнити більші.

Запуск BRI у 2013 році виявив нові виклики й повністю змінив парадигму зовнішньої безпеки Китаю. Поява масового тероризму після 11 вересня занурила Близький Схід у війну, зробивши нафтові компанії вразливими. 2004 рік, кошмарний рік для китайців за кордоном, ознаменував зміну у сприйнятті людьми обов'язку захищати китайських громадян за кордоном.

Вплив китайських охоронних компаній дуже різниться і, як правило, залежить від готовності держав захищати китайських громадян та засобів, які вони мають у своєму розпорядженні. Їхня робота в цій сфері буде більш-менш помітною залежно від країни, у якій вони знаходяться, та від того, чи дозволяє місцеве законодавство іноземцям інвестувати в охорону. Наприклад, в Алжирі, де ця діяльність суворо зарезервована для громадян країни, китайські охоронні компанії працюють, інтегруючись зі своїми клієнтами або в рамках консультаційних та логістичних офісів. Під виглядом управління флотом та нерухомістю китайської компанії, яку необхідно захищати, вони контролюють зв'язки з місцевими органами безпеки, супровід, конвої, захист важливих об'єктів або в чутливих районах

(від імені кінцевого замовника) та керують партнерами з місцевої безпеки та охорони [10].

В інших регіонах Африки китайські ПОК діятимуть так:

• Єгипет, Туніс, Алжир, Марокко: співпраця з місцевими ПОК та урядовими силами безпеки для захисту посольств, охорони портів та інфраструктури, а також реагування на викрадення з метою викупу (Kidnap and ransom, K&R). Навчання для китайських замовників проводиться заздалегідь на материковому Китаї. Особливістю Єгипту є наявність морської безпеки проти піратів.

• Лівія, Сахель та Південний Судан: діяльність ПОК прирівнюється до діяльності ПВК із залученням озброєних агентів, якщо це можливо. Такі компанії зазвичай використовуються для охорони шахт та нафтових родовищ.

Коли в 2013 році було оголошено про запуск BRI, стало зрозуміло, що Китай буде направляти мільйони своїх громадян, мільярди доларів, тисячі компаній у сотні країн, де безпека не завжди була гарантована. Ерік Принс, засновник американської ПВК Blackwater, розглядав це як унікальну можливість суттєво розширити свій бізнес. Він мав необхідні знання, місцеві зв'язки та план військового внеску в умиротворення країн, що перебували в кризі, шляхом надання людей і важкої техніки (броньованих транспортних засобів, літаків, човнів тощо) та програми підготовки, яка могла дуже швидко створити сучасну армію.

Тож того ж року Принс об'єднав зусилля з однією з найбільших економічних груп Китаю, CITIC, вартість якої становить трильйон доларів, щоб створити ПВК під назвою Frontier Services Group (FSG) (Xianfeng Fuwu Jituan). Принс обіймав посаду голови ради директорів FSG до 2021 року (після чого його замінив ізраїльтянин Доріан Барак, його власний фінансовий радник) і володів 25 % акцій компанії. CITIC – це фінансовий конгломерат, що належить китайській державі, тож це справжній союз між китайською державою та засновником Blackwater. FSG брала безпосередню участь у громадянській війні в Лівії на боці Халіфи Хафтара. Ерік Принс за рахунок фінансування Еміратів надав ліванській національній армії сільськогосподарські літаки, переобладнані під бомбардувальники [11]. У 2019 році він намагався створити вертолітний загін і «команду вбивць», але зазнав невдачі [12]. Для своїх операцій у Північній Африці Ерік Принс і FSG обрали Мальту як логістичну та командну платформу [13]. У Китаї,

у співпраці зі службами безпеки, він побудував навчальний центр із безпеки та міської партизанської війни в Сіньцзяні.

Згідно із заявою FSG, угода була підписана на церемонії 11 січня 2019 року, на якій були присутні чиновники Сіньцзяну та представники CITIC Guoan Construction. Угода передбачає, що FSG інвестує 600 000 дол. у центр, який зможе навчати 8 000 осіб на рік. У 2017 році китайська дочірня компанія Еріка Принса відкрила в Пекіні Міжнародний коледж безпеки та оборони, який мав на меті стати «найбільшою приватною школою підготовки фахівців з безпеки в Китаї» та навчати персонал китайських компаній, що ведуть діяльність в Африці та Центральній Азії. У 2018 році джерела повідомили Arabi21, що охоронна фірма Frontier Services Group, очолювана Еріком Принсом, який раніше керував охоронною фірмою Blackwater, нещодавно відправила бійців із курдського регіону Іраку до Лівії, щоб вони воювали на боці Хафтара, згідно з таємною угодою [14]. Окрім своєї діяльності в Північній Африці, FSG захищає інтереси китайських гірничодобувних і нафтових компаній у кількох регіонах Африки, маючи своїх співробітників і логістику в Нігерії, Мозамбіку та Південному Судані.

Серед відомих китайських ПОК можна назвати такі:

DeWe Security – одна з найбільших китайських ПОК, яка активно працює за кордоном. Компанія забезпечує охорону китайських дипломатичних представництв, корпоративних об'єктів і проєктів ініціативи «Один пояс, один шлях». DeWe Security бере участь в охороні інфраструктурних проєктів у Південній та Південно-Східній Азії, а також в Африці, де Китай має значні економічні інтереси;

China Security & Protection Group (CSPG) – ця компанія є одним із ключових гравців на ринку ПВК Китаю. CSPG забезпечує охорону не лише китайських об'єктів за кордоном, але й надає послуги консультування та навчання для місцевих сил безпеки. Компанія активно працює в Африці, зокрема в Судані та Нігерії, де Китай має стратегічно важливі інвестиції у видобутку нафти;

Shandong Huawei Security Group – ця компанія також спеціалізується на наданні охоронних послуг у міжнародних проєктах, пов'язаних з ініціативою «Один пояс, один шлях». Основна діяльність компанії зосереджена в Африці та Південній Азії, де китайські корпорації потребують захисту від збройних груп та екстремістів.

Останніми роками Китай усе більше використовує ПВК для підтримки своєї глобальної стратегії, особливо в рамках проєктів, що стосуються ініціативи «Один пояс, один шлях». Цей масштабний проєкт передбачає створення інфраструктурних коридорів, які з'єднають Китай з Європою, Африкою та іншими частинами світу, і забезпечення їхньої безпеки є критично важливим завданням. Китайські ПВК надають уряду можливість забезпечувати захист інтересів країни за кордоном, не залучаючи регулярні збройні сили, що дозволяє зберегти дипломатичний нейтралітет у багатьох конфліктах. Це також дає Китаю змогу залишатися активним учасником міжнародної політики, уникаючи безпосередніх військових втручань. ПВК Китаю продовжують розвиватися, і їхня роль у глобальній безпеці стає все більш помітною. Хоча вони поки що не мають такої бойової спроможності, як західні або російські ПВК, їхні функції охорони та захисту інфраструктурних проєктів є важливим елементом китайської стратегії розширення свого впливу у світі.

Незважаючи на швидке зростання, китайські військові та охоронні компанії стикаються з багатьма викликами [5]. Перший з них – низька якість підготовки охоронців, мовний бар'єр і відсутність відкритості до інших національностей. Наразі неможливо (за винятком FSG) знайти китайську ПВК з такими оперативними можливостями, як Blackwater / Academi або Wagner Group. Ці можливості вимагають збільшення логістики та підготовки, чого поки що немає у китайських компаній.

Другий виклик пов'язаний із заробітною платою персоналу. Занадто низька, вона не сприяє появі еліти світового рівня та не заохочує професіоналів у цій галузі приєднуватися до китайських компаній.

Третій виклик пов'язаний із китайським законодавством, яке погано адаптоване до глобального контексту ПВК (статус не визнається законом у Китаї). Законодавство щодо зброї є дуже обмежувальним, навіть для компаній, що мають ліцензії (Закон КНР про контроль над вогнепальною зброєю (Zhonghua Renmin Gongheguo Qiangzhi Guanli Fa), прийнятий у 1996 році, дозволяє володіти зброєю лише Народно-визвольній армії Китаю (НВАК), поліції та міліції).

Нарешті, за відсутності чіткої стратегії приватні військові та охоронні компанії не мають гнучкості, підкоряються лише розпорядженням своїх китайських клієнтів і не виходять на міжнародний ринок безпеки на користь інших компаній або інтересів.

Тому спроможності китайських ПВК, як правило, мають більш обмежений спектр функцій порівняно зі своїми західними аналогами. Вони не беруть активної участі в бойових діях, але забезпечують охорону об'єктів і персоналу, особливо в зонах підвищеного ризику. Ураховуючи високий рівень контролю з боку уряду, китайські ПВК зосереджені на виконанні завдань, які дозволяють захистити національні інтереси Китаю за кордоном, не залучаючи до конфліктів регулярні збройні сили.

Ключовими напрямами діяльності китайських ПВК є [5]:

• охорона об'єктів інфраструктури – Китай має великі економічні інтереси в Африці та Азії, і китайські ПВК забезпечують безпеку цих проєктів. Зокрема, вони охороняють будівельні майданчики, транспортні шляхи, нафтові та газові родовища, а також інші важливі об'єкти;

• захист персоналу – китайські компанії та уряд потребують захисту свого персоналу за кордоном, особливо в країнах, де існує загроза викрадення або нападу. Китайські ПВК забезпечують охорону співробітників китайських корпорацій, дипломатів та інших представників держави;

• консультативні послуги та навчання – деякі китайські ПВК надають послуги з навчання місцевих сил безпеки, особливо в країнах, де політична нестабільність створює загрозу для китайських проєктів. Передбачає також навчання методам охорони, використанню сучасних систем безпеки та проведення аналітичної роботи з оцінки ризиків.

Отже, порівняно з іншими країнами, становлення ПВК у Китаї проходило більш повільно й контрольовано державою. Це пов'язано з традиційним ставленням Китаю до приватних військових структур, які часто сприймаються як потенційна загроза для державної монополії на застосування сили. Китайський уряд має жорсткий контроль над безпековим сектором, і ПВК, які працюють у Китаї, строго підпорядковуються регуляціям, щоб запобігти неконтрольованій діяльності. З початку 2000-х років Китай почав активно залучати ПВК для охорони своїх об'єктів та інфраструктури за кордоном, особливо в Африці, де китайські корпорації здійснюють великі інвестиції у видобуток природних ресурсів. Поява китайських ПВК стала відповіддю на необхідність захисту економічних інтересів Китаю в умовах нестабільних

політичних режимів у багатьох країнах. Китайські ПВК, як правило, працюють у тісному контакті з урядом та державними корпораціями.

Незважаючи на те, що в рф офіційне право на застосування збройних сил має лише держава, інші дії прирівнюються до найманства й заборонені на території рф під загрозою кримінального покарання, однак ПВК існують неофіційно, позиціонуючи себе на російському ринку як приватні охоронні підприємства, а спектр послуг ПВК надають лише у «європейському напрямку», де це дозволено. У сучасних умовах дані організації є дуже ефективними, мобільними та універсальними інструментами вирішення певних державних завдань [15].

Одним із таких завдань ПВК рф виконували під час бойових дій у Грузії (2008 рік), військовому перевороті в Сирії, у бойових діях на території України та в багатьох інших військових конфліктах та війнах. Саме застосування ПВК у війні або збройному конфлікті дозволяє приховати безпосередню участь країни, зокрема рф, що особливо проявилося в гібридній війні рф проти України та на сучасному етапі повномасштабної російсько-української війни.

На жаль, у XXI ст. пальма першості в практичному застосуванні концепції гібридної війни з використанням ПВК належить рф. Збройна агресія проти України створила ідеальне середовище для використання ПВК, адже воно дало можливість проведення різноманітних «операцій», не звертаючи увагу, а по суті, нехтуючи міжнародним гуманітарним правом, міжнародними конвенціями та угодами про припинення вогню – від знущання над полоненими до обстрілів житлових кварталів. Найбільшого розголосу під час російсько-української війни набула ПВК «Вагнер», яка була створена Євгеном Пригожиним і походила від позивного її командира, російського неонациста Дмитра Уткіна – «Вагнер», обраного ним через захоплення «естетикою та ідеологією Третього Райху» на честь відомого німецького композитора Ріхарда Вагнера [16].

Тобто ми бачимо, що ПВК в усьому світі набули значного поширення й виконують різноманітні послуги для різних замовників – приватних осіб, держав і міжнародних організацій.

За результатами аналізу типу послуг, які надають ПВК, відповідних документів міжнародних організацій та публікацій можна здійснити таку класифікацію ПВК [1, 17–19]:

1. Оборонні військові компанії

Основна функція оборонних ПВК полягає в забезпеченні охорони об'єктів та людей, а також наданні логістичних послуг і військових тренувань. Ці компанії зазвичай виконують завдання, пов'язані з охороною критичної інфраструктури, включаючи дипломатичні представництва, промислові підприємства, нафтові та газові об'єкти. Оборонні ПВК також забезпечують навчання місцевих військових та поліцейських сил, виконують логістичну підтримку військових операцій, зокрема транспортування вантажів або медичне забезпечення в зоні конфлікту.

2. Наступальні військові компанії

Наступальні ПВК беруть участь у бойових діях та спеціальних операціях. Вони виконують завдання з безпосередньої участі у війнах і конфліктах. Такий тип ПВК найчастіше виконує завдання для держав, що не бажають відкрито втручатися в конфлікт через політичні або правові ризики. ПВК «Вагнер» є яскравим прикладом наступальної ПВК, що бере участь у різних конфліктах по всьому світу, зокрема на сході України та у країнах Близького Сходу. Ці компанії часто використовуються для проведення таємних операцій або виконання завдань, які уряди не можуть виконати відкрито.

3. Розвідувальні, контррозвідувальні компанії

Особливістю розвідувальних та контррозвідувальних ПВК є те, що вони випереджають спеціальні служби у створенні та використанні новітніх технологій, які застосовують у відповідній діяльності, а їхня мережа є практично закритою. За різними інтернет-джерелами, з державними розвідувальними органами співпрацюють, зокрема, американські компанії «Strategic Forecasting Inc», «Booz Allen Hamilton», британські – «Aegis» і «Haklyut & Company». Вони можуть бути використані для проведення різних форм політичної боротьби, а також бути не лише виконавцями замовлень державних органів (включно зі спецслужбами) і корпорацій, а й набувати статусу об'єкта, що становить розвідувальний інтерес для інших країн задля отримання інформації, якою ПВК володіють.

4. Гібридні військові компанії

Гібридні ПВК виконують як оборонні, так і наступальні завдання. Вони можуть забезпечувати логістику та охорону, одночасно виконуючи бойові операції. Такий тип компаній є найбільш

універсальним і застосовується як державами, так і приватними компаніями для досягнення своїх цілей у нестабільних регіонах.

5. *Компанії бойового забезпечення*

ПВК, які надають своїм клієнтам послуги з підтримання бойових дій їхніх сил безпеки та оборони (за термінологією НАТО – тактичну підтримку), включно з безпосередньою участю в бойових операціях. Утім, остання зі згаданих послуг сучасними ПВК не надається, принаймні офіційно.

6. Військові консалтингові компанії

ПВК, що спеціалізуються на наданні послуг із планування, створення, реформування й розвитку сил безпеки та оборони, зокрема органів розвідки й контррозвідки, їхньої бойової та спеціальної підготовки тощо.

7. Військові логістичні компанії

Сфера діяльності цих ПВК охоплює: обслуговування й експлуатацію складних систем озброєння, військової техніки та комп'ютерних систем; матеріально-технічне забезпечення військ; будівництво військових об'єктів.

8. Приватні охоронні компанії

До таких відносять компанії, які працюють в умовах воєнного конфлікту або в зоні підвищеного ризику, зокрема на території країн із нестабільною обстановкою. Хоча зазвичай вони здійснюють захист об'єктів та фізичних осіб, а не бойові дії, однак у районах воєнного конфлікту чітке розмежування між цими видами діяльності відсутнє. Наприклад, під час захисту аеродромів, нафтопроводів та інших об'єктів інфраструктури охоронні компанії можуть проводити бойові операції проти незаконних військових формувань, терористів тощо.

9. Морські військові компанії

Останніми роками ПВК почали активно залучатися до боротьби з піратством, забезпечуючи при цьому супроводження та збройний захист суден, ведення переговорів із нападниками тощо. Нині тільки в Аденській затоці й у районі Африканського Рогу діють понад 20 таких ПВК. Річні витрати судноплавних компаній на їхній найм становлять близько 100 млн дол. США [19]. Правові питання діяльності таких ПВК розглядалися в Лондоні у травні 2012 року на 90-й сесії Комітету з безпеки на морі Міжнародної морської ор-

ганізації ООН. Крім іншого, під час сесії був затверджений проєкт Тимчасового порадника для приватних компаній з морської охорони, які надають послуги приватної збройної охорони на суднах у зоні високого ризику [20].

Отже, ПВК – це військово-політичний феномен XXI ст., який є серйозним викликом міжнародного права; вони працюють як на урядові замовлення, так і на приватні корпорації. Із часу утворення в 1967 році у Великій Британії першої в новітній історії ПВК «Watchguard International» простежується стійка тенденція до зростання попиту на послуги таких компаній, збільшується кількість їх замовників та розширюється спектр самих послуг. ПВК посіли особливе місце в сучасній військово-політичній сфері, стратегіях та практиці держав. Цей та багато інших фактів говорять про пряму зацікавленість держав в існуванні таких компаній та такого бізнесу. На сучасному етапі державам, у першу чергу західним, які в основному і є державами походження таких компаній, вкрай зручно використовувати ПВК не лише з економічної точки зору, але й з метою збереження своєї політичної репутації. Наразі ПВК стали невід'ємним інструментом збройних протистоянь та конфліктів, що призвело до виникнення різних проблем, починаючи з прав людини і закінчуючи участю бойовиків у військових операціях та війнах.

3.2. Спроможності приватних військових компаній в умовах дестабілізації міжнародного середовища безпеки

В ієрархії основних учасників міжнародної взаємодії, які формують систему міжнародних відносин і визначають головні тренди її розвитку, недержавні суб'єкти відіграють усе більш значущу роль. При цьому їхнє коло помітно розширилося і за загальним визнанням охоплює сьогодні неурядові організації (НУО), міжнародні неурядові організації (МНУО), ЗМІ, великі політичні партії, транснаціональні компанії, міжнародні терористичні організації та ін.

Характерно, що недержавні суб'єкти виступають, з одного боку, як активна сила, що впливає на загальну динаміку міжнародних процесів, а з іншого, є об'єктом зовнішнього впливу й маніпулювання з боку традиційних, перш за все державних, суб'єктів світової політики.

Практика спілкування з громадами в інших державах існувала й раніше. Зокрема, вона була відпрацьована в період Холодної війни як в СРСР, так і в США. Уже тоді стали виникати не лише державні структури, які опікувалися роботою з громадськими структурами інших держав, але і громадські структури в іноземній державі. Прикладами можуть служити товариства дружби із зарубіжними країнами в СРСР.

Відповідно до традиційного підходу, недержавні суб'єкти, зокрема НУО та МНУО, розглядаються як «групи інтересів» і «групи тиску», які швидше досягають результату шляхом зміни політики урядів, ніж шляхом прямих дій. Так, впливаючи на суспільну думку всередині тієї чи іншої держави, МНУО здійснює тиск і на уряд тієї чи іншої держави в ході прийняття зовнішньополітичних рішень.

Крім того, держави часто залучають МНУО для збирання інформації та надання експертних оцінок. В обмін МНУО розраховують отримувати від держав підтримку, у тому числі інформаційну. Зростаюча взаємозалежність між державами та МНУО – лише один із прикладів їхньої взаємодії.

Надаючи інформацію й мобілізуючи громадську думку, МНУО отримують можливість впливати на процес прийняття рішень, прийнятих у рамках міжнародних міжурядових організацій (ММУО), висловлюючи свою думку з потрібних питань. Останніми роками масштаби співробітництва ММУО та МНУО постійно зростають, що веде до посилення впливу МНУО на міжнародні процеси.

Водночас слід серйозно переосмислити значення недержавного сектору в питаннях забезпечення національної безпеки. Навіть зараз ці структури надзвичайно багато роблять для допомоги державі (як у військовій сфері, так і в багатьох інших, у тому числі в інформаційній). Однак це співробітництво все ще побудоване на базі консервативного ставлення державних структур до будь-яких зовнішніх гравців, які тією чи іншою мірою намагаються долучитися до реалізації його функцій. Утім, слід визнати, що держава ніколи не зможе бути настільки ж високомобільною та гнучкою у своїх діях, як недержавні структури, що не стримуються формальними бюрократичними правилами та приписами.

До речі, використання росією своїх ПВК та інших парамілітарних структур (наприклад, «Вагнер» та козачі об'єднання) на території України певною мірою показало ефективність подібної мо-

делі. Війна на сході України, яку розпочала рф у 2014 році, за своїм географічним масштабом мала локальний характер, та деякі вітчизняні політики називали цей конфлікт гібридною війною рф проти України, у якій ПВК «Вагнер» використовувалася як основний елемент цієї війни. Вона брала участь в анексії Криму, а пізніше – у бойових діях у Донецькій і Луганській областях. Дану ПВК можна назвати класичною моделлю найманців, армією засуджених осіб за тяжкі кримінальні злочини, завербованих у колоніях й інших місцях позбавлення волі. Під час повномасштабного вторгнення росії на територію України значну частину військового потенціалу агресора в цій війні становили підрозділи ПВК (у тому числі ПВК «Вагнер»), діяльність яких є прикладом сучасного найманства та направлена на повалення уряду й конституційного ладу.

Нижче ми розглянемо спроможності найвідоміших ПВК та їхню участь у різних умовах дестабілізації міжнародного середовища безпеки, включаючи російсько-українську війну.

Blackwater (зараз відома як Constellis). Blackwater стала однією з найвідоміших ПВК завдяки своїй діяльності під час війни в Іраку та Афганістані. Заснована у 1997 році, компанія Blackwater спеціалізувалася на наданні послуг охорони, тренуванні військових та забезпеченні безпеки дипломатичних місій. Її основною метою була підтримка збройних сил США у конфліктах після терактів 11 вересня 2001 року. Найбільш відомий епізод, що привернув увагу міжнародної спільноти, стався в Багдаді; у 2006 році в зеленій зоні Багдада сталася автомобільна аварія. Позашляховик, керований співробітниками «Blackwater», врізався в Хамві армії США. Співробітники «Blackwater» роззброїли військовослужбовців і змусили їх лежати на землі під дулом пістолета доти, доки вони не відігнали свій позашляховик від місця аварії. Увечері 24 грудня 2006 року співробітник компанії, зловживаючи алкоголем, застрелив охоронця віцепрезидента Іраку, влучивши в нього з пістолета тричі. Найманця, який вчинив цей вчинок, звільнили з компанії та депортували з країни – більше жодних санкцій до нього не застосовували.

Через рік, у 2007 році, американські медіа раптово почали говорити, що «блеквотерівці» в Іраку займаються стратою цивільного населення. Говориться насамперед про випадок, коли колона броньованих авто найманців супроводжувала машини посадовців

Держдепартаменту США. Того дня співробітники «Blackwater» відкрили вогонь по цивільному населенню на площі Нісур. Інцидент призвів до загибелі 17, поранення 20 мирних жителів та викликав міжнародний скандал. За справу одразу ж узялися у Федеральному бюро розслідувань (ФБР). Їхні висновки були об'єктивними: мовляв, цивільні мертві, адже теж стріляли в найманців.

Однак уряд був не на боці «блеквотерівців». Їхні контракти відкликали, чотирьох членів заарештували і позбавили ліцензії на діяльність в Іраку. З одного боку, це не суворе покарання, з іншого – мінус десятки мільйонів доларів. Ліцензію поновили наприкінці 2008 року. Однак за «Blackwater» почали пильно стежити урядові організації. У всіх їхніх броньованих авто зобов'язали поставити апаратуру для прослуховування. Радіопереговори та переписки членів ПВК теж стали відкритими для спецслужб. І хоча компанія стверджувала, що її співробітники діяли у відповідь на загрозу, подія посилила критику ПВК і підкреслила проблеми з регулюванням їхньої діяльності в зонах конфлікту.

Після ситуації з цивільними в 2007 році в компанії почалися погані часи. Удар по репутації відомства був настільки сильним, що їм довелося повністю реорганізувати структуру своєї організації. У 2009 році компанію перейменували в «Xe Services» LLC, а вже в 2011 році вона мала назву «Academi». Однак їх і надалі всі знають як «Blackwater». Ерік Принс відійшов від справ, й управління та контроль перейняли різні спецпризначенці.

«Blackwater» також брала участь у військових операціях в Афганістані, надаючи послуги охорони та логістики американським військовим та дипломатам. Незважаючи на критику, компанія продовжила свою діяльність під новими назвами**.** Та у 2014 році «Academi» об'єдналася з «Triple Canopy», дочірньою компанією Constellis Group. Пізніше «Academi» була повністю інтегрована в материнську компанію і тепер працює під назвою «Constellis», яка надає охоронні послуги за контрактом федеральному уряду США.

«Blackwater» пройшла довгий шлях – від звичайної охоронної компанії до елітного підрозділу найманців, який готовий вирушити в будь-яку гарячу точку планети. Для них немає неможливих завдань, табу чи співчуття – усе вирішують гроші.

DynCorp International. DynCorp – одна з найбільших американських ПВК, яка бере участь у численних конфліктах і миротворчих операціях. Її діяльність охоплює надання логістичних послуг, охорону, навчання місцевих сил безпеки та гуманітарні операції. Однією з головних сфер діяльності DynCorp є забезпечення охорони урядових об'єктів і дипломатичних місій у таких країнах, як Ірак та Афганістан. Крім того, компанія активно співпрацює з ООН та іншими міжнародними структурами у виконанні миротворчих місій. DynCorp також забезпечувала охорону президента Афганістану Хаміда Карзая. DynCorp відома своєю участю в процесах післявоєнної стабілізації, зокрема тренуванням іракських поліцейських сил після падіння режиму Саддама Хусейна. Вона також надає послуги з підтримки збройних сил США та інших країн, допомагаючи з матеріально-технічним забезпеченням і навчанням військових кадрів. Однак діяльність DynCorp не завжди проходила без скандалів. Наприклад, у 1999 році компанія була залучена до миротворчої операції в Боснії та Герцеговині, де виникли звинувачення в причетності до торгівлі людьми, що спричинило серйозну критику на міжнародному рівні.

Triple Canopy. Triple Canopy – одна з провідних американських ПВК, що надає широкий спектр військових послуг, включаючи охорону, тренування та розвідувальні завдання. Компанія активно діє в конфліктах на Близькому Сході, Африці та Латинській Америці. Triple Canopy забезпечує безпеку для дипломатичних місій, урядових установ та приватних компаній, особливо в Іраку та Афганістані. Її роль у конфліктах передбачає не лише охоронні функції, але й підтримку розвідувальних операцій, забезпечення логістики та консультування.

GardaWorld. GardaWorld є однією з найбільших канадських ПВК, яка надає охоронні послуги та забезпечує безпеку в різних регіонах світу, зокрема в небезпечних зонах конфліктів. Компанія спеціалізується на захисті дипломатичних місій, урядових установ та комерційних об'єктів. Одним із прикладів діяльності GardaWorld є охорона дипломатичних місій та об'єктів в Афганістані, Іраку та Лівії. Компанія також активно надає логістичні послуги в зонах конфліктів, забезпечуючи безпечний рух вантажів і персоналу через небезпечні регіони. GardaWorld відома своєю ефективністю в

забезпеченні безпеки для приватних корпорацій, які працюють у нестабільних регіонах, включаючи нафтові та газові компанії. Вона також бере активну участь у гуманітарних операціях, надаючи підтримку міжнародним організаціям та урядам.

Aegis Defence Services. Aegis Defence Services – британська ПВК, заснована в 2002 році, яка спеціалізується на наданні послуг безпеки, зокрема в конфліктах на Близькому Сході та в Африці. Її основна діяльність зосереджена на забезпеченні безпеки під час миротворчих місій та операцій стабілізації. Aegis Defence Services відома своєю участю в конфліктах в Іраку, де вона забезпечувала охорону та логістику для урядових установ США і Великобританії, а також приватних компаній. Компанія активно співпрацює з урядами та міжнародними організаціями, забезпечуючи безпеку в небезпечних регіонах.

ПВК «Вагнер». Протягом останніх років спостерігається активне застосування ПВК у воєнних конфліктах за участю рф, хоча їхня діяльність не передбачена діючим законодавством і є протиправною, що можна побачити на прикладі застосування ПВК «Вагнер». «Вагнерівців» використовували як основну ударну силу, доповнювану підрозділами повітрянодесантних військ, які вже зазнали серйозних втрат і значно втратили боєздатність.

ПВК «Вагнер» є яскравим прикладом сучасної російської ПВК, що бере участь у конфліктах по всьому світу, виконуючи як офіційні, так і неофіційні замовлення російського уряду. Уперше ПВК «Вагнер» з'явилася на полі бою у 2014 році під час анексії Криму та війни на сході України, де її бійці підтримували проросійські сили. ПВК «Вагнер» стала одним із головних інструментів зовнішньої політики росії, оскільки дозволяє уряду здійснювати військові операції за межами країни, зберігаючи можливість «правдоподібного заперечення». Це дозволяє росії уникати прямої відповідальності за дії «вагнерівців», що є важливим елементом у рамках гібридної війни. Одним із найбільш показових епізодів участі ПВК «Вагнер» став конфлікт у Сирії, де вона підтримувала уряд Башара Асада. За даними різних джерел, бійці «Вагнера» брали участь у битві за нафтові родовища в провінції Дейр-ез-Зор у 2018 році. Тоді відбулося зіткнення між силами коаліції на чолі із США та бойовиками «Вагнера», унаслідок якого загинули десятки росій-

ських найманців. Цей епізод став підтвердженням того, що «Вагнер» діє як непрямий інструмент росії в конфліктах на Близькому Сході. Також відомо про участь «Вагнера» у військових операціях у Центральноафриканській Республіці, Лівії, Судані та інших африканських країнах, де їхні бійці беруть участь у захисті урядів і стратегічних об'єктів. Це дозволяє росії отримувати політичний та економічний вплив у регіоні без прямого втручання регулярної армії.

Отже, зі зростанням кількості регіональних конфліктів та глобальної нестабільності роль ПВК як інструменту ведення війни суттєво зросла. Вони здатні надавати швидкі, гнучкі та адаптовані рішення для військових і геополітичних завдань у таких умовах, де регулярні збройні сили можуть бути неефективними або непотрібними. Тому на сьогодні попит на послуги ПВК у сучасних воєнних конфліктах стрімко збільшується, а обсяг світового ринку послуг ПВК оцінюється в різних дослідженнях у сотні мільярдів доларів США.

За оцінкою Global Growth Insights, ринок приватних військових послуг (Private Military Services) у 2024 році становив близько 236,33 млрд дол. США. Прогнозується, що у 2025 році він досягне 254,15 млрд дол. США, до 2026 року – приблизно 273,32 млрд дол. США, а до 2034 року зросте до 488,9 млрд дол. США. Це стійке зростання відображає середньорічний темп зростання на рівні 7,54 % протягом 2025–2034 років [21].

За даними The Market Intelligence, розмір світового ринку приватних військових послуг оцінювався в 212,34 млрд дол. США у 2024 році і, за прогнозами, досягне 221,69 млрд дол. США у 2025 році, збільшившись до 312,86 млрд дол. США до 2033 року, із середньорічним темпом зростання 4,4 % протягом прогнозованого періоду [22].

Дослідники Custom Market Insights очікують, що з 2025-го по 2034 рік світовий ринок приватних послуг військової безпеки зафіксує середньорічний темп зростання на рівні 5,68 % (рис. 3.1).

Прогнозується, що у 2025 році обсяг ринку досягне оцінки в 274,53 млрд дол. США. Очікується, що до 2034 року оцінка досягне 451,18 млрд дол. США [23].

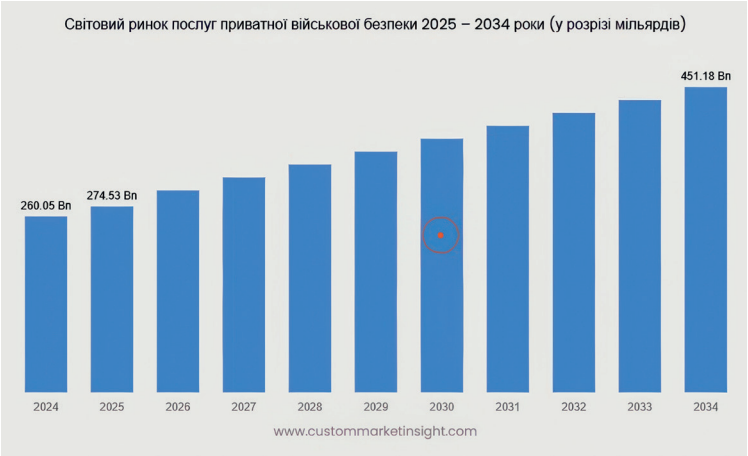

Рис. 3.1. Світовий ринок послуг приватної безпеки з 2025-го по 2034 рік

Отже, можна констатувати, що обсяг світового ринку послуг ПВК наразі становить приблизно 200–260 млрд дол. США щорічно, з очікуваним зростанням до 400–450 млрд дол. у найближчій декаді.

Крім того, на думку галузевих експертів Custom Market Insights, впровадження виробниками нових стратегій і технологій відкриває вигідні можливості для гравців на ринку послуг приватної військової охорони протягом прогнозованого періоду (рис. 3.2).

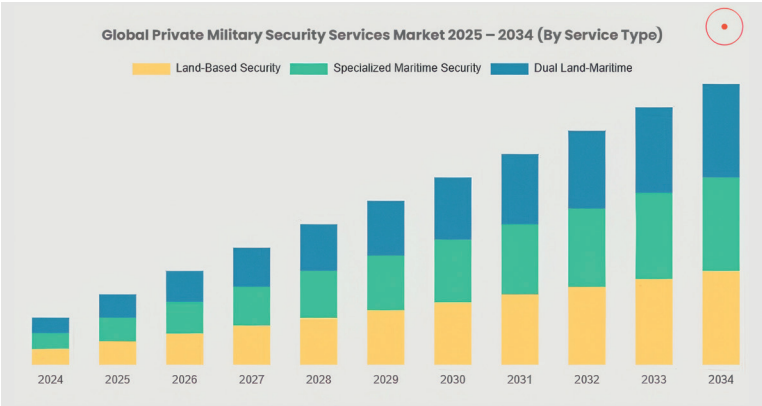

Рис. 3.2. Світовий ринок послуг приватної безпеки (за видами послуг) за 2025–2034 роки

Експерти виокремлюють такі ключові тенденції та драйвери розвитку ПВК:

1. *Зростання попиту на інтегровані рішення безпеки.* Очікується, що зростання попиту на інтегровані рішення безпеки, де фізична та цифрова безпека поєднуються, сприятиме зростанню ринку. Клієнти шукають загальні послуги, які надають озброєних осіб, спостереження, аналітику ризиків та кіберзахист в одному пакеті. Це забезпечує ефективність і зменшує залежність від ряду обслуговуючих суб'єктів. ПВК зараз пропонують моделі гібридного типу, у яких сходяться класична оборона та моніторинг на основі ШІ, безпілотники та цифрова розвідка загроз. У міру того, як глобально зростають складні та багатовимірні загрози, інтегровані рішення стають необхідністю часу, а приватні гравці у сфері безпеки стають універсальними партнерами для захисту наступного покоління та управління ризиками.

2. *Збільшення використання новітніх технологій*. Завдяки новітнім технологіям на ринку приватних військових та охоронних послуг відбулися значні зміни. Компанії впроваджують спостереження на основі ШІ, біометричний контроль доступу, прогнозну аналітику та спостереження за допомогою дронів для підвищення операційної ефективності та виявлення загроз. Робототехніка та автономні системи розглядаються для охорони периметра та розвідки зон підвищеного ризику. Безпека на кіберрівні також стає критично важливим компонентом з огляду на зростання кількості гібридних воєн. Впровадження передових технологій знижує ризики для ПОК, дає їм можливість надавати розвідувальну інформацію в режимі реального часу та оперативно реагувати на виникаючі загрози. Ця тенденція робить компанії більш конкурентоспроможними та краще підготовленими для задоволення динамічних потреб бізнес-будинків та урядів.

3. *Аутсорсинг оборонних функцій.* Уряди почали передавати на аутсорсинг оборонні функції, які не лежать в основі оборонної діяльності, для ПВК із метою економії коштів та підвищення гнучкості. Логістика, охорона конвоїв, безпека будівель та аналіз загроз є поширеними функціями, які були передані на аутсорсинг, щоб офіційні збройні сили зосереджувалися на веденні бойових дій. Ця тенденція набрала обертів у країнах, що беруть участь у міжнародних

місіях або діяльності з підтримання миру, у яких приватні компанії відіграють життєво важливу допоміжну роль. Поряд із забезпеченням швидкого розгортання та доступу до спеціальних навичок, аутсорсинг також є економічно вигідною пропозицією. Зростаюче використання ПВК для підтримки оборонних функцій генерує стабільний потік замовлень, посилюючи тенденцію зростання ринку.

4. ***Зростаюча потреба в безпеці критичної інфраструктури.*** Безпека критичної інфраструктури, такої як нафтові родовища, енергетичні заводи, порти та транспортні мережі, є зростаючою тенденцією на ринку. Критична інфраструктура опиняється в центрі уваги терористів, піратів і саботажу в політично нестабільних або зонах підвищеного ризику. Приватна військова фірма пропонує озброєні групи охорони, спостереження та швидкого реагування 24/7 для захисту таких об'єктів. Оскільки інвестиції в енергетику та інфраструктуру зростають у всьому світі, попит на ефективні рішення для безпеки продовжує зростати. Корпорації все частіше віддають перевагу приватним структурам через здатність негайного розгортання та універсальність у складних операційних середовищах, забезпечуючи таким чином безперервність критично важливих ліній постачання та національної економічної інфраструктури.

5. ***Експансія на ринки, що розвиваються.*** Розширення приватних служб військової безпеки неухильно зростає в нових регіонах, особливо в Африці, на Близькому Сході та в Південно-Східній Азії. Регіони потерпають від постійних проблем, таких як політична нестабільність, повстання, піратство, слабо розвинені інститути державної безпеки. Транснаціональні гірничодобувні, будівельні та нафтові корпорації покладаються на приватні охоронні фірми для захисту персоналу та обладнання. Це створює шанси для міжнародних гравців та нових місцевих учасників, що створює можливості для співпраці, яка відповідає світовому досвіду та місцевим знанням. Проникнення в ці регіони триватиме за умови збереження нестабільності та зростання економічних проєктів і призведе до значного розширення приватних військових корпорацій.

6. ***Зростаюча увага до прозорості та етичних стандартів***. Зараз галузь більше інвестує в етичну поведінку та прозорість для вирішення питань порушення прав людини та притягнення до відповідальності. Скандали змусили ПВК погодитися на більш суворі

кодекси поведінки, кращу підготовку та написання звітів. Деякі із цих організацій переходять до міжнародного узгодження та створення внутрішніх механізмів нагляду, намагаючись завоювати довіру урядів, неурядових організацій та бізнес-клієнтів. Цей фокус не лише допомагає компаніям вигравати контракти на дуже політизованих ринках, але й покращує репутацію у всьому світі. Прозорість та етичні практики як виграшні фактори сприяють розширенню ринку, забезпечуючи довгострокову стійкість та довіру клієнтів.

На рис. 3.3 показано кілька вражаючих тенденцій у розподілі країн базування компаній, що працюють у різних регіонах світу.

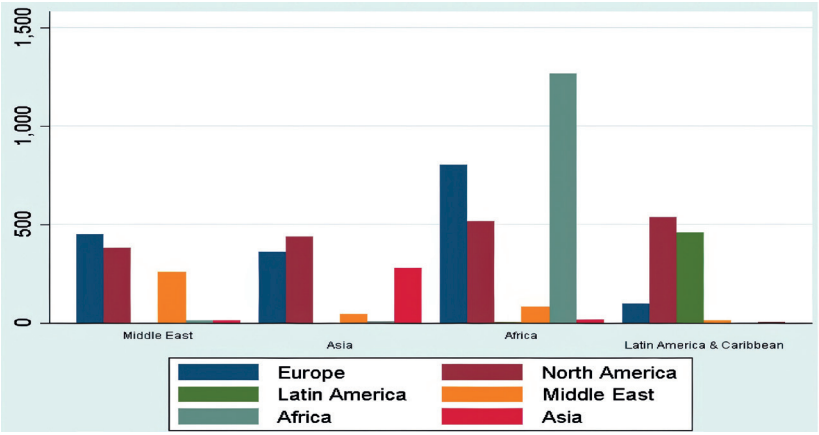

Рис. 3.3. Загальна кількість ПВК, що оперують у певних регіонах світу

По-перше, світовий ринок силової техніки, здається, переважно заповнений європейськими та північноамериканськими компаніями, які є єдиними, що працюють у всіх регіонах. У той час як північноамериканські компанії продемонстрували подібний рівень підрядної діяльності у всіх регіонах, європейські здебільшого були активні в Африці, далі йдуть Близький Схід, Азія та, значно меншою мірою, Південна Америка. По-друге, азійські, південноамериканські та близькосхідні компанії, навпаки, переважно працювали у своїх регіонах базування, а підрядна діяльність африканських компаній в Африці була надзвичайно високою, лише трохи меншою, ніж активність усіх компаній з усіх інших регіонів разом узятих [24].

Головною перевагою застосування ПВК є те, що державна влада різних країн може застосувати їх в обхід обмежень, які регулюють чинні механізми контролю

Наприклад, законодавча база обмежує чисельність військового персоналу за кордоном, а ПВК не входить до тієї кількості. Також їх можна включити до складу будь-якої операції як підрозділ, адаптований до виконання специфічних (спеціальних, тайних) функцій. У багатьох країнах ПВК не зобов'язані надавати інформацію щодо своєї діяльності або своєї статті прибутку. Їхні працівники в основному виконують діяльність як фахівці з консалтингу, а не військовослужбовці. Також перевага ПВК полягає в тому, що повністю відсутнє незадоволення серед населення місцевості, де саме проводиться операція, тому що це не регулярні збройні сили іншої країни, а мультинаціональні компанії для охорони важливих об'єктів (суб'єктів). Крім того, немає незадоволення власного населення, тому що не буде офіційних поранених та втрат серед збройних сил, державі не треба виплачувати рідним кошти за загибель їхнього родича. Ще один важливий аргумент на користь ПВК – те, що вони можуть перебувати у так званій сліпій зоні юрисдикції всіх держав та виконувати спеціальні (приховані) операції. Саме режим прихованості та змога вести латентну політику цікавлять більшість держав. Законодавча база, яка регулює діяльність ПВК, не є доопрацьованою, особливо за кордоном, що призводить до неможливості їх контролювати. Конвенцію ООН про боротьбу з вербуванням, використанням, фінансуванням і навчанням найманців ратифікувало лише 35 країн, і вона значною мірою залишається непридатною для протидії новим викликам. Здебільшого в національному законодавстві окремих країн також немає ефективних механізмів притягнення найманців до відповідальності за їхні злочини. Тому заперечення будь-яких зв'язків ПВК із державою та національними і відомчими спецслужбами є вагомим аргументом для їх застосування.

Тож в умовах зростання міжнародної напруженості і появи осередків нестабільності, пов'язаних із міграційною кризою, політичним популізмом і тероризмом, на перший план виходять завдання з реалізації національних інтересів у будь-якій точці світу. ПВК являють собою поширені в міжнародній практиці структури, уповноважені державами для вирішення спеціальних завдань.

Фахівці стверджують, що історія використання найманців для підсилення воєнного потенціалу тягнеться тисячоліттями, а перші згадки про них з'явилися ще задовго до нашої ери. Сьогодні наймати людей у воєнних цілях – це непоганий бізнес, до того ж практику використання таких «комерційних воїнів» можна спостерігати в багатьох державах світу. Цікавим є те, що найбільш відомі приклади використання послуг ПВК в районах ведення бойових дій відносяться навіть не до Росії, а до США.

На думку О. Дахно, зростання популярності ПВК розпочалося із середини 70-х років XX ст. [25]. Тоді були підписані перші контракти ПВК з урядом США. У 1970 році з'явилася перша ПВК США. «Vinnell Corp» підписала багатомільйонний контракт з Урядом США на надання спеціалізованих послуг із підготовки та створення національної гвардії в Саудівській Аравії. Пізніше дані організації стали створюватися в країнах Африки (ПАР), Ізраїлі, і їх чисельність різко зросла в США та Великобританії. Велика кількість ПВК і їх активна діяльність привели в 1980 році до першого у світі з'їзду «найманців» (США).

У цілому період кінця 1980-х – початку 1990-х рр. також став досить значущим для розвитку діяльності ПВК. Закінчення Холодної війни спровокувало зміну геополітичної ситуації.

По-перше, почалася тенденція скорочення фінансування військової сфери, що призвело до скорочення солдат, офіцерів і фахівців із цієї сфери. Найчастіше єдиним виходом для даних людей був перехід під керівництво приватників.

По-друге, те саме скорочення відбилося і на діяльності уряду. Для держави стало більш вигідним залучати для вирішення тимчасових геополітичних завдань ПВК, ніж утримувати власні збройні сили.

По-третє, змінилася геополітична ситуація на світовій арені. Почалися активні процеси «перероблення» сфер впливу, що вимагають підтримки збройних сил, тож ідеальним інструментом для цього стали ПВК.

Також варто зазначити, що США увійшли в історію як перша держава, яка законодавчо врегулювала функціонування ПВК. Відповідний нормативно-правовий документ був прийнятий командуванням армії США в 1998 році, який регулював взаємовідносини між

державою і ПВК, а саме між військовослужбовцями армії США і співробітниками ПВК.

Ще однією знаменною датою в історії ПВК є квітень 2001 року, коли була створена перша міжнародна організація, яка регулює діяльність ПВК на світовій арені – «Peace Operations Association» (POA). З 2000-х рр. послугами ПВК зацікавилися величезні міжнародні компанії, корпорації та організації.

Основними факторами, які посилили активність розвитку ПВК, є:

1. Поглиблення проблем підтримки національної безпеки та оборони деяких держав, які за офіційною термінологією ООН називаються «найменш розвиненими країнами», або тих, яких вважають «державами, що не відбулися». Їхні уряди в епоху глобалізації часто зіштовхуються з надто складними для себе проблемами в багатьох сферах.

2. Існування для багатьох держав, які розвиваються, проблеми освоєння нових видів озброєння та підготовки армій до протидії нинішнім загрозам. Відсутність фахівців у цих державах обумовлює потребу в певній допомозі. Для цього залучаються корпорації, які виробляють озброєння, та збройні сили розвинених держав, проте переважно надання зазначеної допомоги проводиться із залученням ПВК.

3. Скорочення чисельності збройних сил деяких країн та зниження обсягів їхнього державного фінансування. Це примусило переходити на аутсорсинг.

4. Збільшення потреб транснаціональних корпорацій у гарантуванні безпеки власної діяльності в нестабільних регіонах світу.

5. Збільшення попиту на послуги ПВК зі сторони міжнародних безпекових та гуманітарних організацій, зокрема щодо матеріально-технічного забезпечення миротворчих операцій, гуманітарного розмінування, охорони гуманітарних вантажів тощо.

6. Економічні аспекти функціонування ПВК. Ринок таких послуг визначається високою динамікою зростання. За перше десятиліття XXI ст. він перетворився з невеликої спеціалізованої ніші у глобальну сферу військових послуг.

7. Розширення пропозиції на ринку військових спеціалістів, що дає змогу ПВК отримувати високопрофесійні кадри, не вкладаючи коштів у їхню підготовку.

З початку XXI ст. ПВК стали вельми популярними. Послугами цих організацій користуються як уряди багатьох держав, так і міжнародні корпорації. Даний сегмент ринку досить активно і стабільно розвивається. Справжній бум для діяльності ПВК стався, коли американські війська вторглися на територію Іраку та Афганістану. Багато фахівців військової сфери стверджують, що досі там знаходиться досить велика кількість «приватних військових».

Активну участь ПВК брали і в грузинській агресії 2008 року, і у військовому перевороті в Сирії, і у військових діях на території України, і в багатьох інших військових конфліктах.

Наразі ж прослідковується стійка тенденція до збільшення попиту на послуги таких компаній, зростає чисельність їх замовників та розширюється діапазон самих послуг. Цілком очевидно, що в сучасних військових конфліктах ПВК фактично становлять різновид підрозділів спеціального призначення регулярних збройних сил.

Загалом ПВК є структури, які займаються вирішенням спеціальних завдань у регіонах зі складною військово-політичною обстановкою на замовлення держави. ПВК здатні виконувати такі функції:

- воєнізована охорона людей та об'єктів, зокрема посольств або нафтопроводів; охорона гуманітарних місій;
- участь у миротворчих цілях, у т. ч. під егідою ООН;
- розмінування;
- розвідувальна діяльність й оцінка ситуації безпеки в регіоні;
- технічне обслуговування та використання бойових комплексів і техніки;
- боротьба з піратством;
- евакуація населення з територій, де точаться збройні конфлікти;
- професійна підготовка сил місцевої поліції або військових;
- здійснення функцій поліції там, де не працюють правоохоронні органи;
- утримання під вартою і конвоювання затриманих або ув'язнених;
- підготовка цивільних осіб до роботи в надзвичайній обстановці;
- повноцінна участь у бойових операціях – спільно з кадровими частинами або окремо.

ПВК також служить і росії потужним інструментом впровадження експансіоністської політики як на території Співдружності Незалежних Держав (СНД), так і різних регіонах світу.

О. Івасечко та Т. Бондар стверджують, що перші ПВК на території росії почали утворюватися майже одразу після розпаду Радянського Союзу. Причиною цього слугувало те, що після розпаду СРСР без роботи залишилися сотні тисяч колишніх військовослужбовців, працівників Комітету державної безпеки, міліції тощо. Неофіційно вважається, що першим міжнародним конфліктом, де було залучено російські ПВК з метою забезпечення національних інтересів, є Придністровська війна [26].

Проте активним періодом формування ПВК стали 2014–2015 рр., коли росія одночасно розпочала інтервенцію до Сирії, анексувала півострів Крим та окупувала частини Донецької та Луганської областей. Особливістю російських ПВК є те, що вони реєструються за кордоном та офіційно не мають жодного юридичного стосунку до рф. Саме це допомагало російській владі майже 10 років використовувати ПВК як таємний інструмент для втілення геополітичних інтересів.

І якщо в інших державах ПВК є окремими комерційними формуваннями, то в росії вони перебувають під контролем владної верхівки та майже повністю фінансуються міністерством оборони рф. Отже, можна стверджувати, що російські ПВК перетворилися на гібридну форму ПВК, оскільки вони не є незалежними від держави комерційними структурами.

Близький Схід та Африка були тими регіонами, на які Радянський Союз спрямовував значні ресурси, що дозволяло йому зберігати свій вплив та виступати проти Заходу та Америки. Проте після 1991 року конфігурація сил змінилася, через розпад СРСР країни Африки та Близького Сходу почали тяжіти до проєвропейського вектора. Уже на початку 2000-х років російська влада усвідомила, що може втратити цей регіон, а разом із ним – значну частину впливу на міжнародній арені, тому вона поступово почала змінювати свою зовнішню політику. Відповідно до Концепції зовнішньої політики рф від 2016 року посилення могутності росії, конкурентоспроможність її економіки та зміцнення міжнародного іміджу є основною метою зовнішньополітичної діяльності.

Крім цього, 2015 року керівництво рф затвердило Морську доктрину рф до 2020 року, відповідно до якої Середземне море входило до стратегії регіонального морського панування та було однією з важливих стратегій рф у зовнішньополітичній діяльності.

Свою активну діяльність в Африці російська влада розпочала з 2010 року, а вже з 2014–2015 рр. вона залучає ПВК до конфліктів, які відбувалися на території регіону. Російські ПВК були помічені на території Лівії, Алжиру, Судану, Малі, Мавританії, ЦАР, Конго, Анголи, Зімбабве, Мозамбіку, Ботсвани та Мадагаскару.

Для того щоб продемонструвати діяльність російських ПВК, ми можемо описати їх залучення в Лівії. Використання російських ПВК у Другій громадянській війні в Лівії розпочалося ще у 2015 році, коли туди відправили перші групи бійців «Групи Вагнера». Спочатку «вагнерівці» займалися в основному охороною стратегічних об'єктів або тренуванням лівійських військових, проте вже у 2019 році відбулась офіційна зустріч головнокомандувача лівійської армії Х. Хафтара з міністром оборони рф С. Шойгу та очільником «Групи Вагнера» Є. Пригожиним, під час якої було погоджено, що росія надає пакет військової допомоги та забезпечує державу підтримкою в РБ ООН. Проте натомість влада Лівії мала погодитися на те, що «Група Вагнера» здійснюватиме контроль за нафтовими родовищами, двома військовими базами, мережею залізниць та автомагістралей. Така угода дозволила російській владі розширити свій вплив на території Африки та продемонструвати свою силу на міжнародній арені.

Найбільш болючим та складним питанням є використання ПВК в Україні, адже росії вдалося їхніми руками підірвати територіальну незалежність та розв'язати тривалу війну проти українського народу. Найважливішою метою зовнішньої політики щодо країн, які раніше входили до СРСР, є бажання збереження своєї зони впливу, домінування російських інтересів у політиках цих держав та економічний контроль.

У зверненнях президента росії до федеральних зборів у 2003 та 2004 роках зазначається, що росія розглядає простір СНД як сферу своїх стратегічних інтересів, а «Концепція зовнішньої політики» 2008 року визначає так звану межу, де перетин інтересів росії, США та Європи буде вважатися загрозою національній безпеці. Україна ж

має вигідне геополітичне розташування, і контроль над цією територією дозволить росії впливати на Захід, отримати повний контроль Чорного моря та підвищити свій вплив на міжнародній арені.

Зрештою, втрата України означала б недостатню силу рф та повний провал імперської політики. Використовуючи ПВК під час анексії Криму та окупації Луганської та Донецької областей, росія ставила такі завдання:

- унеможливити вступ України до НАТО та ЄС;
- створити нові точки впливу на українську владу та Європу;
- мінімізувати можливість перетворення України на регіонального лідера;
- виснажити українську економіку веденням бойових дій;
- заблокувати значну частину торговельних шляхів, які були важливими для існування держави в цілому.

Фактично ці дії стали підтвердженням того, що зовнішня політика росії повернулася до імперіалізму. Цікаво, що у 2016 році в «Концепції зовнішньої політики рф» Україна згадується як недружня держава, а вже в новій концепції 2023 року про неї немає жодної згадки.

Отже, на сьогоднішній день ПВК набули значного розповсюдження у всьому світі. Вони виконують найрізноманітніші види послуг для різних замовників, якими можуть виступати як приватні особи, так і держави. Найбільше ПВК зареєстровано в країнах Заходу. При цьому діють вони в різних регіонах світу. В основному там, де відбуваються конфлікти: Близький Схід, Африка, Латинська Америка та інші.

Зарубіжний досвід указує на те, що спектр використання ПВК у різних регіонах є досить широким. Їм доручається будівництво військової інфраструктури, охорона вантажів та дипломатичних установ, підготовка та навчання військових кадрів, впровадження військових технологій та виробництво зброї, реалізація розвідувальних або контррозвідувальних заходів, а також участь у бойових діях та контртерористичних операціях, реалізація певних «специфічних» доручень, у яких держава не може офіційно залучити представників правоохоронних органів та збройних сил.

3.3. Особливості розвідувальної діяльності приватних військових компаній

Деякі великі ПВК мають спеціалізовані розвідувальні підрозділи, що виконують професійні розвідувальні операції на замовлення урядів або корпорацій. Такі підрозділи мають високу технічну підготовку та використовують сучасне обладнання для збирання інформації. Вони також взаємодіють із національними розвідувальними органами для координації дій.

Розвідувальна діяльність ПВК є важливим аспектом їх операцій у зонах конфліктів. ПВК мають можливості виконувати стратегічні й тактичні розвідувальні завдання, що надає їм перевагу у швидкому збиранні інформації про противника або про умови проведення операцій. Ці можливості активно використовуються як на полях бою, так і в інформаційній війні.

Розвідувальна діяльність ПВК може включати збирання та аналіз інформації, необхідної для забезпечення безпеки та виконання контрактів, які вони виконують. Ця діяльність може охоплювати як відкриті, так і приховані методи збирання даних, спрямовані на виявлення загроз, оцінку ситуації та надання розвідувальних даних для підтримки операцій ПВК.

Важливою особливістю є те, що ПВК мають більше свободи в порівнянні з регулярними арміями в методах збирання розвідувальних даних, що робить їх надзвичайно корисними для прихованих операцій та гібридної війни. Такі компанії, як ПВК «Вагнер», часто виконують складні розвідувальні завдання в умовах високого ризику, використовуючи нелінійні методи ведення війни, зокрема радіоелектронну боротьбу, аналіз відкритих джерел та впровадження агентів у ворожі структури [16]. Розглянемо основні напрями розвідувальної діяльності ПВК.

Тактична розвідка. ПВК часто залучаються до збирання тактичної інформації в рамках безпосередніх операцій у зоні конфлікту. Це може передбачати:

- збирання інформації про розташування противника, його озброєння, логістику та комунікації;
- аналіз місцевості, кліматичних умов та інфраструктури для планування операцій;

• оцінку загроз для персоналу та об'єктів, які охороняються, включаючи потенційні атаки або диверсії.

Наприклад, ПВК, що працюють у зонах конфліктів, таких як Афганістан або Ірак, збирають інформацію про терористичні групи, їхні маршрути пересування та методи атак. Це дозволяє забезпечити безпеку об'єктів і планувати дії для мінімізації ризиків.

Стратегічна розвідка. Окрім виконання тактичних завдань, ПВК також беруть участь у стратегічній розвідці. Це передбачає довгострокове спостереження за політичною та військовою ситуацією в регіоні. ПВК здійснюють аналіз регіональної безпеки, політичних ризиків та економічних умов, щоб допомогти замовникам ухвалювати обґрунтовані рішення. Наприклад ПВК, що працюють в Африці, де Китай чи росія мають стратегічні економічні інтереси, часто збирають інформацію про політичну ситуацію, настрої серед місцевого населення та діяльність інших акторів, включно з повстанцями чи конкуруючими державами [16].

Контррозвідувальна діяльність. У рамках охорони об'єктів і персоналу ПВК також здійснюють заходи з контррозвідки для запобігання проникненню ворожих агентів або диверсантів. Це може охоплювати:

• виявлення шпигунських дій та моніторинг комунікацій;

• збирання інформації про можливі диверсійні групи та їхні плани щодо об'єктів ПВК;

• захист від кіберзагроз і спроб проникнення у внутрішні системи безпеки.

Збирання інформації з відкритих джерел (Open Source Intelligence, OSINT). Сучасні ПВК широко використовують методи збирання інформації з відкритих джерел, включаючи Інтернет, соціальні мережі, новинні платформи та спеціалізовані аналітичні видання. Це дозволяє оперативно отримувати інформацію про події в регіоні, моніторити зміни в поведінці різних груп, включаючи терористичні або повстанські угруповання, а також прогнозувати можливі загрози для замовників. Наприклад, ПВК «Вагнер» активно використовує OSINT для збирання інформації про політичні настрої в країнах Африки та Близького Сходу, де вони діють [16]. Це допомагає аналізувати можливі загрози для інтересів росії та планувати подальші операції з урахуванням ризиків.

Технологічна розвідка та радіоелектронна боротьба. Багато ПВК мають у своєму арсеналі технологічні засоби для радіоелектронної розвідки (Signals Intelligence, SIGINT), зокрема моніторинг радіокомунікацій противника, перехоплення даних та ведення радіоелектронної боротьби. Це дозволяє отримувати важливу інформацію про плани противника або його розташування, а також порушувати комунікації між ворожими підрозділами. Так, наприклад, ПВК «Вагнер» під час операцій у Сирії використовувала радіоелектронні засоби для моніторингу комунікаційних ліній між опозиційними угрупованнями [16]. Це дозволяло не лише отримувати інформацію про плани противника, але й ефективно порушувати їхню координацію.

ПВК можуть займатися розвідкою для захисту своїх інтересів, забезпечення безпеки персоналу та об'єктів, а також для підтримки операцій, які вони проводять. При цьому використовувати різні методи збирання розвідувальної інформації, включаючи відкриті джерела, спостереження, аналіз відкритих даних, а також негласні методи, якщо це дозволено законом та умовами контрактів. До основних методів і засобів проведення розвідувальних операцій ПВК можна віднести:

• *агентурні операції.* Одним із традиційних методів збирання інформації є робота агентів, які діють на місцях. ПВК можуть використовувати місцеве населення, колишніх військових або політично зацікавлених осіб для отримання внутрішньої інформації про ворожі плани, структуру, постачання та інші важливі аспекти. Агенти можуть працювати під прикриттям або під виглядом цивільних осіб, щоб знизити ризик викриття;

• *БПЛА та дрони*. Сучасні ПВК все частіше використовують БПЛА для збирання розвідувальних даних. Дрони дозволяють проводити розвідку на великих площах без залучення наземних підрозділів і зниження ризику для життя співробітників ПВК. Вони використовуються для моніторингу території, збирання візуальної інформації та виявлення руху противника. Наприклад ПВК, що працюють в Африці, часто використовують дрони для моніторингу транспортних шляхів та забезпечення безпеки конвоїв, що перевозять цінні вантажі, такі як нафта або мінерали;

• *аналіз соціальних мереж та інформаційна розвідка*. ПВК також активно використовують інформаційні технології для моніторингу соціальних мереж, де можуть бути доступні дані про наміри

противника, плани атак або зміни в політичній ситуації. Інформаційна розвідка дозволяє відстежувати не лише місцеві події, але й глобальні тренди, що можуть впливати на регіон безпеки.

Отже, ПВК можуть проводити розвідку в різних сферах, таких як політична, економічна, військова та інші, залежно від потреб своїх клієнтів та специфіки контрактів. Розвідувальна діяльність ПВК відрізняється від розвідки державних спецслужб тим, що вона обмежена завданнями, які ставить перед собою ПВК, та умовами контрактів, які вони укладають. Діяльність ПВК у сфері розвідки може регулюватися національним та міжнародним законодавством, що стосується приватної військової діяльності та збирання інформації.

Висновки до третього розділу

У розділі досліджуються ПВК та їхнє застосування й роль у сучасних збройних конфліктах. Розглянуто причини появи ПВК, історію їх виникнення та розвитку. Проаналізовано специфіку, особливості та напрями діяльності найвідоміших ПВК Великої Британії, США, Китаю, рф. Показано, що ПВК можуть надавати державам та приватним особам широкий спектр військових послуг. Доведено, що сьогодні ПВК функціонують як невід'ємна частина збройних конфліктів, використовуючи унікальні можливості для ведення операцій в умовах сучасного військового середовища, коли держави намагаються досягти своїх цілей, уникаючи безпосередньої участі регулярних збройних сил. За результатами аналізу типу послуг, які надають ПВК, відповідних документів міжнародних організацій та публікацій їх можна поділити на: оборонні військові компанії; наступальні військові компанії; розвідувальні, контррозвідувальні компанії; гібридні військові компанії; компанії бойового забезпечення; військові консалтингові компанії; військові логістичні компанії; ПОК; морські військові компанії.

Перелік використаних джерел

1. В. Горовенко, В. Тютюнник. Приватні воєнні компанії: міжнародний досвід і можливі шляхи його реалізації в Україні. Наука і оборона. 2013. № 3. С. 32–39.

2. Семенюк Ю. В., Мокляк С. П., Лисецький Ю. М. Розвідувальна діяльність і міжнародні відносини. Нові реалії та підходи: монографія; за заг. ред. Ю. М. Лисецького. – Київ : ЛАТ&К, 2021. 160 с.

3. Автушенко І. Б. Автушенко О. С. Приватні військові компанії як один із інструментів ведення сучасних війн. Військово-науковий вісник. 2024. № 41. С 120–132.

4. Приватна військова компанія. URL: https://uk.wikipedia.org/wiki/Приватна_військова_компанія#Бойові_операції_і_участь_у_збройних_конфліктах_XX—XXI_ст (дата звернення: 04.05.2025).

5. China's Discreet Game in North Africa – Private Military Companies. URL: https://rosaluxna.org/publications/chinas-discreet-game-in-north-africa-private-military-companies/ (дата звернення: 07.06.2025).

6. Bartlett David. The Political Economy of Dual Transformations: Market Reform and Democratization in Hungary. University of Michigan Press. 1997. p. 280.

7. Chatzky, A., & McBride, J. (2020, January 28). China's Massive Belt and Road Initiative. Council on Foreign Relations. URL: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative (дата звернення: 07.06.2025).

8. Global Terrorism Index 2020: Measuring the Impact of Terrorism. Institute for Economics & Peace. Sydney. 2020. p. 106.

9. Jingdong Yuan. China's private security companies and the protection of Chinese economic interests abroad. 2021. PP. 173–195.

10. Security Officer Interview questions in Oran. URL: https://www.glassdoor.co.in/Interview/departement-d-oran-security-officer-interview-questions-SRCH_IL.0,18_IS3581_KO19,35.htm (дата звернення: 07.06.2025).

11. Erik Prince's Mercenaries Are Bombing Libya. URL: https://medium.com/war-is-boring/erik-princes-mercenaries-are-bombing-libya-88fcb8e55292 (дата звернення: 07.06.2025).

12. Des mercenaires occidentaux ont aidé Haftar dans son offensive contre Tripoli en 2019. URL: https://www.middleeasteye.net/fr/actu-et-enquetes/libye-haftar-mercenaires-occidentaux-emirats-prince (дата звернення: 07.06.2025).

13. Frontier Services Group Sets Up Operations in Malta. URL: https://www.globenewswire.com/new-selease/2014/11/17/1236402/0/en/

Frontier-Services-Group-Sets-Up-Operations-in-Malta.html (дата звернення: 07.06.2025).

14. Libya: Foreign mercenaries recruited for Haftar by Security Company. URL: https://northafricapost.com/30417-libya-foreign-mercenaries-recruited-for-haftar-by-security-company.html (дата звернення: 07.06.2025).

15. Приватні військові компанії та їх роль у сучасних регіональних конфліктах. Виступ представника Міністерства оборони України генерал-майора Вадима Скібіцького на 949-му засіданні Форуму ОБСЄ з безпеки співробітництва, 17 червня 2020 року. URL: https://webcache.googleusercontent.com/search?q=cache:sll663tpmBkJ:https://vienna.mfa.gov.ua/en/news/vistup-na-temuprivatni-vijskovi-kompaniyi-ta-yih-rol-usuchasnih-regionalnihkonfliktah&cd=3&hl=uk&ct=clnk&gl=ua. (дата звернення: 28.05.2025).

16. Приватна військова компанія «Вагнер»: від створення до сьогодення : монографія / А. В. Слюсаренко, І. І. Фурман, І. С. Печенюк та ін.; за заг. ред. М. В. Коваля. Київ : НУОУ. 2023. 136 с.

17. R. Uesseler. Servants of War: Private Military Corporations and the Profit of Conflict. New York, Soft Skull Press. 2008. P. 146.

18. Валецкий О. Частные военные компании, их создание, развитие и опыт работы в Ираке и других регионах мира. URL: http://www.vrazvedka.ru/main/analytical/valeckiy.html (дата звернення: 04.05.2025).

19. Небольшая статистика по морским ЧВК. URL: http://ir-ingr.livejournal.com/883373.html (дата звернення: 04.05.2025).

20. Информационное агентство INFOLine. 31.05.2012. URL: http://www.advis.ru/php/view_news.php?id=3E9550FB-EADD-5840-901F-0023FFEB14E1 (дата звернення: 04.05.2025).

21. Private Military Services Market Size, Share, Growth, and Industry Analysis, By Types (Local Company, International company), Applications (Government, Private, Military, International Organization, Other) and Regional Insights and Forecast to 2034. URL: https://www.globalgrowthinsights.com/enquiry/request-sample-pdf/private-military-services-market-104457 (дата звернення: 06.08.2025).

22. Private Military Services Market Size, Share, Growth, and Industry Analysis, By Type (Guard Services, Armored Transport, Others), By Application (Government, Commercial and Industrial, & Others) and

Regional Forecast to 2033. URL: https://www.themarketintelligence.com/ market-reports/private-military-services-market-1809 (дата звернення: 06.08.2025).

23. Global Private Military Security Services Market Size Likely to Grow at a CAGR of 5.68 % By 2034. URL : https://www.custommarketinsights.com/press-releases/private-military-security-services-market-size/?utm_source=chatgpt.com (дата звернення: 06.08.2025).

24. The Commercial Military Actor Database. URL: https://journals.sagepub. com/ (дата звернення: 06.08.2025).

25. Дахно О. Світовий досвід створення та розвитку приватних військових компаній як інструмента реалізації національних інтересів. URL: https://fip.dp.ua/index.php/FIP/article/view/1037/1156 (дата звернення: 06.08.2025).

26. Івасечко О., Бондар Т. Приватні військові компанії у зовнішній політиці росії: 2014–2023 роки. URL: https://science.lpnu.ua/sites/default/files/journalpaper/2024/jun/34851/ivasechko.pdf (дата звернення: 06.08.2025).

РОЗДІЛ IV

ТРАНСФОРМАЦІЯ МІЖНАРОДНИХ ВІДНОСИН ЯК ЧИННИК ВПЛИВУ НА РОЗВІДУВАЛЬНУ ДІЯЛЬНІСТЬ

4.1. Національні інтереси як мотиваційна основа діяльності розвідувальних органів

Цілеспрямована людська діяльність заснована на потребах та інтересах, детермінованих певними станами особистості, що залежать від оточуючого середовища: матеріального, соціального, духовного.

Потреби й інтереси – поняття не тотожні. Потреби виражають ставлення будь-якого суб'єкта життєдіяльності до необхідних умов свого існування, оскільки без задоволення низки базових потреб неможливе існування ні біологічного, ні соціального організму. Однак не всяка потреба повною мірою може стати стимулом до того чи іншого виду життєдіяльності. Потреба, виражаючи взаємозв'язок між суб'єктом та умовами його життєдіяльності, проявляє себе в неусвідомлених потягах і досить усвідомлених мотивах поведінки. Істинною причиною та рушійною силою соціального розвитку є інтерес. Інтереси – це усвідомлені потреби, сформовані суспільством, соціальними групами, особистостями.

У 1935 році термін «національні інтереси» був уперше внесений до Оксфордської енциклопедії соціальних наук. Відтоді дослідження даної проблематики незмінно зберігає свою актуальність, оскільки є однією з підвалин концептуальної розробки проблеми демократії.

В англомовній літературі це поняття вживається у значенні «державний інтерес». Під національними інтересами розуміють переважно інтереси держави, оскільки західні країни в соціально-політичному аспекті є мононаціональними державами. Нація являє собою єдність громадянського суспільства і держави, тому національний інтерес стає узагальнюючим інтересом, який знімає суперечність між інтересами держави та громадянського суспільства.

Національний інтерес у демократичних країнах – це передусім узагальнений відповідно до існуючих процедур інтерес людей, що формують політичну націю. Формування національного інтересу передбачає узгодження інтересів усіх громадян країни, хоча іноді це зводиться до врахування думки найбільш численних соціальних груп.

В. Смолянюк акцентує увагу, що з двох основних підходів щодо нації (політичного та етнічного) у даному випадку вибір падає на політичну націю як політичну спільноту громадян певної держави, як «сукупність громадян, що здійснюють колективні й національні інтереси через механізм власної політичної організації – національної держави» [1]. Нація визначається як основний державотворчий елемент, носій державного суверенітету, джерело державної влади та національних інтересів. Додамо – і як висхідна позиція щодо визначення національної безпеки.

Національні інтереси є наслідком властивого нації «ставлення до власних потреб у внутрішньополітичному і зовнішньополітичному плані, що викликає негативну або позитивну зумовленість її діяльності, активності вибору шляхів розвитку і перетворюється на мотиви і стимули історичної творчості» [2]. Дані інтереси формуються на основі системи національних потреб, які, у свою чергу, визначаються суспільною (національною) необхідністю створення держави, захисту суверенітету, розвитку економіки, політичної системи, системи права, моралі, підтримки відповідного рівня життя населення тощо.

Законодавче визначення терміна «національні інтереси України» прозвучало у 2003 році [3]. Водночас нормативно-правового акта, який би давав вичерпний перелік національних інтересів, влада протягом усього періоду державно-політичної незалежності України не запропонувала. Як правило, державні документи обмежуються «пріоритетами національних інтересів», «життєво важливими національними інтересами», «пріоритетними національними інтересами», «фундаментальними національними інтересами». Подібна різноманітність значно розширює простір пояснення національних інтересів, проте позбавляє необхідної в даному випадку чіткості їх вербального оформлення. Ситуацію, що склалася, свого часу описав М. Михальченко: національні інтереси в Україні все ще перебувають на етапі становлення, тому не становлять збалансовану систему.

У внутрішньому контексті дається взнаки гостре ідеологічно-ціннісне, політичне, економічне протистояння різних соціальних сил, політичних партій, соціально-політичних лідерів із приводу ієрархії національних інтересів, їх змістовного наповнення та механізмів реалізації [2]. У зовнішньому сенсі неможливо не враховувати європейський вибір української нації та активну протидію рф із цього приводу, що отримало практичний вияв в окупації у 2014 році частини території України (Автономної республіки Крим та міста Севастополя), розв'язанні воєнної агресії на Сході нашої держави, а після 24.02.2022 р. – у здійсненні широкомасштабного вторгнення в Україну. Ці та інші чинники посилюють складність загальноприйнятного формулювання національних інтересів, які були б підтримані усіма категоріями населення на всій території України. Доводиться обмежуватися «рамковими» принципами формулювання національних інтересів, що має як своїх прихильників, так і критиків. Ще більш складною є ситуація з визначенням національних цінностей, які взагалі не представлені в національному законодавстві як окрема нормативно-правова розробка. Деякі автори до загального переліку національних цінностей України відносять релігійність, поліконфесійність, поліетнічність, мультикультуралізм, сімейні вартості, територіальну цілісність, природне середовище, науково-освітній та науково-технічний потенціали, державний суверенітет, культурні та матеріальні надбання народу (зокрема, економічний потенціал), демократичні інститути як передумову забезпечення рівноправності народів, що населяють Україну, прогресивний суспільно-політичний розвиток, а також визначальні риси національного характеру (волелюбство, працелюбність, толерантність, доброзичливість, миролюбність, самовідданість при захисті Батьківщини, загострене відчуття соціальної справедливості, демократизм, схильність зберігати традиції) [4]. Унаслідок екстраполяції національних цінностей на конкретно-історичні умови розвитку нації формуються відповідні національні інтереси. Найбільш пріоритетні з них (життєво важливі, фундаментальні), як це було зазначено вище, проголошуються на офіційному (державному) рівні.

Деструктивними впливами на національні інтереси та діяльність щодо їх захисту є виклики, загрози та небезпеки, які в західній політичній культурі здебільшого об'єднуються терміном «ризики».

Майже завжди слід очікувати непередбачені впливи (ризики) на систему національної безпеки, що можуть бути вербально позначені як «невизначеність» [5].

Феномен невизначеності має підтвердження у вигляді політичного досвіду більшості сучасних країн. Розглянемо різні варіанти її прояву, які прямо чи опосередковано впливають на національну безпеку.

Невизначеність 1. Національна безпека з моменту публічної артикуляції її засад на початку XX ст. традиційно сприймалася як стан захищеності життєво важливих інтересів особистості, суспільства, держави, за якого забезпечувалися їх поступальний розвиток та мінімізація контрспрямованих ризиків. Майже завжди «життєво важливі інтереси» варіативно представлялися як «національні інтереси», підживлювані «національними цінностями». Як національні інтереси, так і національні цінності отримували нормативно-правову фіксацію на сторінках відповідних нормативно-правових розробок – законів, стратегій, доктрин. Беззаперечною виглядала категорія «нації» як висхідний момент формулювання національних інтересів і цінностей.

Соціально-політичні трансформації останнього часу ставлять під сумнів вищість нації в загальному спектрі суспільних відносин. Нації не є константою соціогенезису, їхні статичні ознаки зміщуються, трансформуються, іноді зникають. Інтенсифікація міграційних потоків у вигляді рухів заробітчан, біженців, шукачів політичного притулку ставить під сумнів виключне становище націй як усталених одиниць соціально-політичного аналізу, що було властиве минулому століттю. Політична, етнічна, культурологічна теорії походження нації стають лише «частково справедливими», не відбиваючи всієї повноти соціальної динаміки. Доволі часто формальне проживання індивіда на території певної країни аж ніяк не засвідчує його повноцінну належність до місцевої нації. Індивідом можуть не сприйматися (відторгатися) інтереси й цінності нового соціального оточення, які (з точки зору формальних керівників держави перебування) визначаються як національні. Відбувається розмивання фундаментальних основ національної безпеки, до захисту якої умовний «мігрант X» аж ніяк не готовий.

Виникає така суперечлива ситуація: на території конкретної держави-нації, яка довела свою стійкість у попередніх історичних

випробуваннях, зараз дедалі частіше з'являються індивіди (соціальні групи), які не відчувають повноцінної належності до «нової батьківщини» та сфери її національної безпеки. У кількісному вимірі подібні групи невпинно зростають, опираючись на власні соціокультурні, мовні, релігійні, побутові та інші особливості. Як результат, у суспільно-політичних реаліях умовної «країни N» маємо національну безпеку «не для всіх». У неї не вписуються численні варіації індивідуальної (сімейної, родинної, кланової) життєдіяльності мігрантів, які не збігаються з державними підходами щодо забезпечення національної безпеки або спрямовуються проти них.

Невизначеність 2. Проглядається в недостатній готовності правлячих еліт регулювати національну безпеку на основі «сферного» підходу. В Україні раніше звучали законодавчі приписи щодо забезпечення національної безпеки в усталених сферах – політичній (внутрішній та зовнішній), економічній, соціальній, воєнній, інформаційній, технологічній, духовно-культурній, екологічній, гуманітарній, у сферах безпеки державного кордону, цивільного захисту населення та ін. Останніми додатками до переліку сфер забезпечення національної безпеки стали сфери кібернетичної та міграційної безпеки, значення яких у конфліктних взаєминах сучасності невпинно зростає. Попри намагання законотворців прописати максимальну кількість сфер на сторінках певного державного документа залишалися суспільні ніші (сфери), які не потрапляли до визначеного переліку. Ними, зокрема, були сфери конфесійної, морської, етнонаціональної, продовольчої безпеки тощо.

Отже, «сферна» диференціація феномену національної безпеки не враховує всього різноманіття соціального буття та необхідності його багатостороннього моніторингу. У сучасних умовах будь-який фрагмент фізичного, кібернетичного або духовного простору, де присутня людська діяльність, може стати середовищем виникнення різноманітних загроз та державних і суспільних контрдій відносно них. Відповідно, вузьке тлумачення небезпечних ситуацій у визначених законодавством сферах хоча й застосовується на практиці, проте поступається місцем комплексному баченню різнопланових загрозливих впливів, здатних проявитися в широкому діапазоні та підірвати заздалегідь створену «сферну» конструкцію безпеки.

Невизначеність 3. Проглядається в різночитанні природи імпульсів, спрямованих проти неї. Задля конкретизації таких впливів у деяких країнах (зокрема пострадянських) широко використовуються терміни «виклики», «загрози», «небезпеки». Вважається, що їх основною відмінністю є інтенсивність деструктивного впливу на предмет національної безпеки: виклик може призвести до його часткової деформації, загроза – до руйнування, небезпека – до повного знищення без можливості наступного відновлення. Проте вичерпного змістовного роз'яснення цих термінів національні правові системи не наводять. У безпекових реаліях відбувається довільне змішування вказаних термінів. Зокрема, деградація середовища безпеки різними авторами описується через довільно побудовані парні констатації: виклик – небезпека, загроза – виклик, загроза – небезпека тощо. Подібні вербальні конструкції додатково заплутують розуміння національної безпеки, посилюють непозначений (ірраціональний) компонент її еволюції. У діяльності з питань національної безпеки подібна вербальна недисциплінованість створює додаткові умови її суб'єктивного розуміння та практичного втілення.

Для виправлення ситуації останнім часом більш широко вживається західний термін «ризик» як універсальний змістовний еквівалент викликів, загроз та небезпек. Це допомагає більш адекватно окреслювати безпекову ситуацію, проте розширює межі суб'єктивізму в безпековій діагностиці.

Невизначеність 4. В інструментальному забезпеченні національної безпеки є надмірна суб'єктивність процесу визначення структури, функціонального призначення та ресурсного забезпечення сектору безпеки і оборони як основного інструменту здійснення націєбезпечної діяльності в суспільних сегментах, де фізична (збройно-силова) активність людини поки що залишається домінантною.

Максимально лаконічно сектор безпеки і оборони описується як «всі силовики», створені демократичною державою та орієнтовані на убезпечення національних інтересів. Насамперед ідеться про збройні сили (армію), поліцію, національну гвардію, пенітенціарні органи, служби безпеки, прикордонного захисту, надзвичайних ситуацій, розвідувальні органи та центри управління ними, деякі інші державні органи спеціального призначення. Окремі країни до цього

переліку додають структури воєнно-промислового комплексу, а також громадські об'єднання, що опікуються безпековими й оборонними питаннями.

Отримуємо доволі розгалужений формат державних та громадських утворень, націлених на забезпечення національної безпеки. При цьому правлячий політикум одноосібно визначає «запас міцності» сектору безпеки і оборони, який залежить від кількості віднесених до нього збройних формувань (служб) та способів їх підготовки й застосування. Вимоги щодо уніфікації сектору безпеки і оборони в політично інтегрованих країнах (наприклад, у НАТО) є доволі приблизними. Кожна країна, що входить до Альянсу, здатна проявити «безпеково-організаційну творчість» з метою створення силових структур, які, на погляд держави, оптимально відповідають поточним ризикам. Як наслідок, виникає ситуація підвищеної складності в процесі налагодження взаємодії між секторами безпеки і оборони різних держав, оскільки формальна подібність силових структур різних країн розмивається специфікою національного мислення з безпекових і оборонних питань та національними пересторогами щодо потрібності / непотрібності віднесення того чи іншого органу до системи забезпечення національної безпеки.

Ситуація ускладняється з огляду на стійку симпатію автократичних систем до воєнної організації держави (ВОД) – аналога сектору безпеки і оборони в демократичних країнах. За поданням російського керівництва ідеологія домінування ВОД у політичних відносинах усередині країни та за її межами підтримується державами, які симпатизують російському режиму. Принципова різниця між секторами безпеки і оборони та воєнними організаціями держав полягає в наявності / відсутності всеохоплюючого демократичного контролю над силовими структурами та унеможливленні одноосібного використання державним лідером силових ресурсів держави. У демократичних країнах такий контроль є даністю, ознакою безпеково-оборонної культури нації. На противагу цьому в автократичних державах демократичний контроль є або формальним, або відсутнім. Виникає додаткова суспільна невизначеність: яким чином можливо налагодити взаємодію (тим більше співпрацю) секторів безпеки і оборони та воєнних організацій держав, які за своєю природою були й залишаються цивілізаційними антиподами? Одного разу це ста-

лося (у виключних воєнно-політичних умовах Другої світової війни при формуванні антигітлерівської коаліції держав). Наступні 80 років світової історії, стержнем яких стала Холодна війна між геостратегічним Заходом і Сходом, засвідчили неможливість відтворення подібного формату міждержавних взаємин. В умовах сьогодення суспільна невизначеність як фактор впливу на безпекову й оборонну політику загострюється до політичної неможливості британсько-російської, американсько-китайської або білорусько-польської співпраці у сфері посилення міжнародної безпеки шляхом формування та практичного застосування змішаних військових контингентів.

Невизначеність 5. У контексті позадержавної підтримки безпекової і оборонної політики є неможливість завчасного визначення оптимуму державно-громадянської взаємодії з питань забезпечення національної безпеки в умовах мирного та воєнного часу. Суспільний досвід неодноразово продемонстрував здатність зацікавленої громади вирішальним чином впливати на політичну владу – коригувати державний курс, змінювати політичний режим, досягати персональних змін у правлячій еліті. Проте особливої чутливості державно-громадянська взаємодія набуває під час військових конфліктів (війн). Тут можливими стають два варіанти розвитку подій.

У випадку апелювання легітимної влади до необхідності збройного захисту національних інтересів і цінностей відбувається продержавна поляризація патріотично налаштованих структур громадянського суспільства з метою всебічної допомоги владі. Суспільство виступає ресурсом стійкості держави. За його ініціативою у форс-мажорних умовах стрімко виникають сили самооборони, добровольчі батальйони, підрозділи та частини територіальної оборони, які захищають державу разом зі збройними силами. До інших важливих проявів безпекової (оборонної) активності громади слід віднести волонтерські рухи, аналітичні осередки, медійні структури, значення яких було й залишається надзвичайно суттєвим. У такий спосіб проявляється потенціал національної стійкості, здатності суспільства до самоорганізації.

У випадку ліквідації (знищення) ворогом держави громада пропонує власні варіанти суспільного виживання включно з висуванням нових політичних лідерів та налагодженням альтернативних форматів політичної активності (включно зі збройною боротьбою проти ворожої сторони). Іншими словами, держава у випадку

критично-руйнівного збройного впливу ворога тимчасово може не існувати. Проте суспільство залишається. Навіть суспільний фрагмент демонструє завидну живучість та орієнтується спочатку на відновлення якості власного існування, а потім – і на відновлення державності. Це доводить, що зріле громадянське суспільство, якому властиве глибинне розуміння національних цінностей та інтересів, в історичному часі стає основним замовником державотворчого проєкту. Відбувається відродження нації включно з реалізацією нею на зрілому етапі розвитку державно-громадянського субпроєкту «національна безпека».

Проте детально визначити наперед алгоритм громадянського впливу на державу в контексті спільного відстоювання безпекових й оборонних характеристик соціуму неможливо. Збройно-силовий експромт громадянського суспільства із цих питань завчасному плануванню не підлягає. Отримуємо додатковий різновид суспільної невизначеності з питань залучення громадянського суспільства в діяльність із питань національної безпеки.

Невизначеність 6. Ступінь делегування суверенною державою безпекових повноважень міжнародним структурам, у назві яких присутнє слово «безпека». Широкомасштабна агресія рф проти України унаочнила вражаючу слабкість більшості безпекових органів міжнародного рівня, які виявилися неспроможними запобігти російському вторгненню або мінімізувати його перебіг. Ідеться про РБ ООН та ОБСЄ, міжнародно-регулятивний потенціал яких залишився в минулому столітті. Якщо взяти до уваги державу-агресора, то вона опинилась у схожій ситуації: у війні з Україною їй мало чим допомогла завчасно створена за російською ініціативою Організація Договору про колективну безпеку. Єдиний виняток – спрацювали механізми НАТО, заблокувавши перенесення бойових дій на територію Альянсу та запустивши процес його дев'ятого розширення шляхом вступу Фінляндії і Швеції.

Новітня історія України збагатила перелік невизначеностей, що стосуються національної безпеки і оборони, невизначеністю гібридної війни, яка у структурному, функціональному, ресурсному та інших вимірах є доволі складною імпровізацією. Мета гібридної війни нічим не відрізняється від мети гарячої війни – послаблення або знищення держави-ворога. Сутність гібридного

різновиду війни полягає в цілеспрямованому створенні (гібридизації, схрещуванні) нестандартних ударних форматів – традиційно-збройних, інформаційних, дипломатичних, економічних, екологічних, мережевих, кібернетичних, громадянських, партизанських, терористичних, їх вибірковому або масованому використанні [6]. Відбуваються: поєднання конвенційних та неконвенційних бойових дій, мілітарних, квазімілітарних, дипломатичних, санкційно-обмежувальних, фінансових, енергетичних, торговельних, технологічних, кібернетичних та інших форм боротьби; розширення кола учасників (військовослужбовці, учасники приватних армій, найманці, партизани, ополченці, терористи тощо); «розмитість» моменту початку (без вручення ноти про оголошення війни) та закінчення (без підписання акта про капітуляцію). Особливого значення набуває інформаційна (інформаційно-психологічна, пропагандистська) боротьба із застосуванням усіх доступних способів впливу на індивідуальну й групову свідомість тих, з ким ця війна ведеться.

Стає зрозумілим, що кількість невизначеностей у заплутаному форматі гібридної війни є надмірною, не підлеглою лінійному аналізу на кшталт «фронт – тил», «друг – ворог», «невтручання – колабораціонізм» тощо. Конче потрібним стає нове безпекове мислення, побудоване на обробці астрономічних масивів інформації та виокремленні з них раціональної складової, здатної відповісти на гострі поточні питання щодо національної безпеки та збройної боротьби як її складової.

Комбінація невизначеностей та залежних від них загроз, з якими людство зіткнулося на початку XXI ст., сприймається як унікальна, раніше невідома й особливо небезпечна. Сучасна наука з метою розуміння природи соціальних ситуацій, ознаки яких є не- або малозрозумілими, а наслідки спроможні стати особливо руйнівними, пропонує нові концептуальні підходи до осмислення суспільних відносин в умовах невизначеності. Одним із них є концепт VUCA-світу, де Volatility означає мінливість, Uncertainty – невизначеність, Complexity – складність, Ambiguity – багатозначність [7]:

• Volatility (мінливість, нестабільність, нестійкість) – ситуація змінюється швидко й хаотично; на основі наявних даних не можна передбачати наступну ситуацію або планувати подальші дії;

• Uncertainty (невизначеність) – відсутні передбачуваність, планомірність та розуміння причинно-наслідкових зв'язків між причинами, проблемами та подіями, формально рознесених у просторі й часі; майбутнє стає непередбачуваним через неможливість / обмеженість використання попереднього досвіду; зростає ймовірність руйнівних змін соціального середовища;

• Complexity (складність) – спостерігається лавиноподібне накопичення суперечливих фактів, оцінок, пропозицій; наслідками змішування різнопланових духовних утворень (позицій, оцінок, пропозицій) стають хаос, плутанина, безлад у соціальних взаєминах, які протидіють впорядкованим структурам та суттєво ускладнюють управлінську діяльність;

• Ambiguity (багатозначність) – домінують суб'єктивне тлумачення ситуації та некоректне сприйняття проблеми, наслідком чого стає поверховість у ставленні до неї; різними авторами довільно змішуються вербальні формули, що описують проблему; як наслідок просторово-часовий фрагмент соціальної еволюції не підлягає лінійному моніторингу на основі однозначних суджень.

Попри важливість кожного з названих елементів основним складником VUCA-світу вважається невизначеність, яка трактується як неоднозначність, неповнота, нечіткість, непередбачуваність розвитку ситуації, управління якою з боку зацікавленого суб'єкта можливе лише на частковій основі або взагалі неможливе. Будучи складником більшості соціальних систем і процесів, невизначеність відбиває обмеженість свідомої участі людини в надперсональних процесах та існує незалежно від поточного розуміння їхньої сутності й наслідків прояву. При цьому невизначеність слід відрізняти від помилковості та недетермінованості. Яскравим прикладом формування політики на основі помилковості є військова кампанія росії проти України, розпочата у 2014 році та розрахована на короткий час. Кампанія базувалася на основі низці припущень, непродуманих та надто оптимістичних для російського керівництва. Ігнорування можливості таких помилок створило невизначеність, яка призвела до недооцінки з боку і російських, і західних політиків та експертів потенціалу стійкості та опірності України напередодні російського вторгнення. Якщо узагальнити, то невизначеність у більшості випадків

є результатом відсутності інформації, необхідної для прийняття рішень, або відсутності довіри до такої інформації та джерел її походження.

Відповідями на виклики VUCA-світу, здатними допомогти суб'єкту соціального управління (державі) подолати невизначеності та ефективно діяти в недостатньо зрозумілих ситуаціях, пропонується віднести протилежну версію VUCA-концепту [8], де:

• бачення (Vision) – чітке сприйняття та розуміння довгострокового напрямку руху, що дозволить організації пережити «струс». Бачення є важливим кроком до стабілізації ситуації, яке здатне надихнути всі зацікавлені сторони до перетворень. Похідними від бачення опціями стають чіткість поставленої мети; віра, яка підкріплена фактами та доказами; узгодженість та зосередженість щодо знаходження взаємозв'язків, трендів та закономірностей впливу сторонніх факторів;

• розуміння (Understanding) – постійний моніторинг очікувань з боку об'єктів впливу; дослідження нових ідей та їхнє відображення в практичній діяльності; здатність до співпраці; уміння реагувати на конструктивну критику; володіння новими IT-технологіями; розуміння поведінки людей у ситуації стресів і навантажень; розуміння мотивів індивідуальної діяльності;

• креативність / ясність (Creativity / Clarity) – уміння спрощувати; застосування системного мислення, заснованого на глобальному баченні результату, розумінні взаємодії і взаємозалежності елементів системи; використання інтуїції; застосування міждисциплінарних знань; критичність сприйняття подій; гнучкість до впровадження змін; націленість на інновації в будь-якій галузі та готовність втілювати в життя інноваційні підходи;

• гнучкість, спритність, рішучість, швидкість, жвавість (Agility) – швидкість і гнучкість виконання процесів, що сприяє підвищенню ефективності функціонування організації; упевненість у необхідності інновацій, пошуку нових оригінальних шляхів вирішення всіх питань, поліпшення процесів; рішучість у прийнятті рішень; інноваційність, формування мережевих зв'язків; постійне вдосконалення.

У даному випадку теж звучить акронім VUCA. Проте тут він пропонує відповіді на запитання, продиктовані невизначеністю. Чинник VUCA може й має бути врахований у теорії і практиці на-

ціональної безпеки. Його використання не має стримуватися ні «сферними» кордонами, ні «паспортами загроз», ні іншими статичними елементами сприйняття середовища національної безпеки.

Зараз пропонуються три основні способи управління невизначеністю:

• кількісний аналіз ситуації, яка містить компонент невизначеності; раціональне сприйняття відомого, зрозумілого, прорахованого, що звужує простір об'єктивації невідомого або невизначеного. Ratio має переважати irratio, що є умовою прийняття зважених політичних рішень;

• локалізація невизначеності. Її повне вилучення з державно-управлінської діяльності є неможливим. Проте владні центри цілком спроможні пояснити свої дії на основі зрозумілої суспільно-політичної логіки, страхуючись при цьому від імовірних «чорних лебедів»;

• планування заходів щодо зменшення невизначеності. Зокрема, пропонується: контролювати інформацію з метою підвищення її достовірності, а також недопущення маніпуляцій; чітко визначати проблеми, цілі й наслідки перед прийняттям рішення, у ході його виконання та після завершення; формувати ширшу та більш активну дослідницьку спільноту; залучати додаткові (альтернативні) наукові, науково-аналітичні та медійні установи до опрацювання безпекової проблеми з елементами невизначеності.

На основі цього можна зробити такі висновки щодо доцільності внесення принципових змін до формування й реалізації політики національної безпеки з урахуванням впливу невизначених чинників [9]:

• раптові й непередбачувані зміни безпекового середовища вимагають більшої гнучкості під час формування й реалізації державної політики; шаблонність мислення, побудована на минулому досвіді, обмежує цю гнучкість;

• необхідність реагування на ситуацію невизначеності потребує уточнення значення нації як об'єкта захисту, перегляду ієрархії національних інтересів, пошуку нового балансу між національними цінностями та потребами забезпечення національної безпеки і стійкості;

• доцільним є впровадження більш гнучких, але зрозумілих підходів до визначення напрямів забезпечення національної безпеки, з урахуванням особливостей трансформації ризиків у сучасних умовах;

• продовжується пошук оптимального складу сектору безпеки і оборони на національному рівні та шляхів оптимізації державно-громадської взаємодії в мирний і воєнний час;

• зростає потреба в перегляді повноважень, делегованих національними урядами міжнародним безпековим організаціям, а також пошуку ефективних механізмів кризового врегулювання на міжнародному рівні;

• формування та реалізація державної політики має здійснюватися на засадах адаптивного управління, що передбачає постійний моніторинг ситуації, виявлення нових трендів, ризиків і загроз, регулярний аналіз відповідності цілей і завдань державної політики змінам у безпековому середовищі;

• з огляду на поширення нелінійних зв'язків у системі суспільних відносин потребують оновлення концептуальні підходи до оцінювання ефективності державної політики у сфері національної безпеки та розроблення інструментів оцінювання її відповідності принципам стійкості;

• доцільним є інвестування в розвиток науки. Нової якості має набути безпекова прогностика, насамперед розроблення нових способів (методик) прогнозування змін у сфері міжнародних взаємин та їх впливу на конкретні держави з метою зменшення потенціалу невизначеності в їхньому економічному, політичному, екологічному, духовно-культурному та іншому поступі.

Хоч би в якому контексті ми розглядали нинішній хаос у міжнародних справах, **важливо усвідомлювати, що ледь не кожна держава, навіть та, що є простим спостерігачем, бачить ситуацію по-своєму.** Показово, що з початком XXI ст. дослідники розвідки, узявши до уваги «революційні зміни» в безпековому середовищі, у природі загроз і природі миру, як і зміни в характері воєн, наголосивши мінливість характеру інформації, швидкість технологічних змін, варіативність очікувань не лише споживачів розвідувальної інформації, але й громадськості, заговорили про необхідність «революції в розвідці».

У липні 2023 року директор ЦРУ США В. Бернс під час лекції виступив у Фундації Дічлі (Велика Британія) та в січні 2024 року в статті для «Foreign Affairs» виклав своє стратегічне бачення розвитку основних тенденцій у сучасному світі та у сфері розвідки [10, 11]. На думку В. Бернса, період безперечного домінування США закінчується, тому Вашингтон має покладатися на співпрацю з партнерами та дружніми альянсами. У розвідувальній сфері основними партнерами США є Велика Британія та інші члени розвідувального альянсу «П'ять очей» (стратегічне партнерство США, Великої Британії, Австралії, Нової Зеландії та Канади у сфері розвідки).

За оцінкою В. Бернса, у сучасному світі спостерігаються такі три ключові тенденції.

По-перше, це виклик стратегічної конкуренції з боку зростаючого та амбітного Китаю та з боку росії, яка постійно нагадує нам, що занепадаюча сила може бути принаймні такою ж руйнівною, як і та, що зростає. На думку В. Бернса, основною довгостроковою загрозою для США є Китай – найбільш серйозний противник Сполучених Штатів у геополітичній і розвідувальній сферах. Китай, на відміну від рф, має економічні, дипломатичні, військові й технологічні спроможності для переформатування світового порядку. У зв'язку із цим у ЦРУ США створено Центр місій з питань Китаю, діяльність якого спрямована виключно на спостереження за цією країною та забезпечення координації з усіма іншими підрозділами американської розвідки в частині, що стосується КНР. Упродовж останніх двох років витрати ЦРУ США на китайському напрямі збільшено вдвічі. Як зауважив В. Бернс, американська розвідка, з одного боку, посилює свої спроможності для конкуренції з КНР у всіх точках земної кулі, а з іншого – намагається підтримувати комунікацію з Китаєм, щоб уникнути небезпечного непорозуміння та випадкових інцидентів.

В. Бернс наголосив, що проблема не в підйомі Китаю як такому, а в діях, які його супроводжують. Президент Сі починає свій третій термін із більшою владою, ніж будь-який китайський лідер після Мао. І замість того, щоб використовувати цю силу для зміцнення, оживлення та оновлення міжнародної системи, яка уможливила трансформацію Китаю, він прагне переписати її.

Також він підкреслив, що найбезпосереднішим і найгострішим геополітичним викликом для міжнародного порядку сьогодні

є повномасштабне вторгнення володимира путіна в Україну. Хоча, як зауважив пан Бернс, російська агресія – важке випробування, але єдиною країною, яка має намір змінити міжнародний порядок, є Китай, і, що більше, має економічну, дипломатичну, військову та технологічну силу для цього.

В. Бернс вважає, що путінська війна стала стратегічним провалом росії – її військові вразливості стали очевидними; її економіка зазнала руйнівного впливу; її майбутнє – це статус «молодшого партнера» та «економічної колонії» Китаю; її реваншистські амбіції зазнали відсічі з боку Північноатлантичного альянсу, який зріс кількісно і став ще сильнішим.

По-друге, це проблеми без громадянства, такі як кліматична криза та глобальні пандемії, які поза межами досяжності будь-якої однієї країни, і вони стають дедалі екстремальнішими екзистенціально.

COVID показав кожному уряду небезпеку бути залежним від однієї країни в питанні життєво необхідних медичних товарів, так само як агресія путіна в Україні ясно показала кожному уряду ризики бути залежними від однієї країни в постачанні енергії. У сучасному світі жодна країна не хоче опинитися на милості картелю однієї з важливих корисних копалин і технологій, особливо країна, яка продемонструвала волю та спроможність поглибити цю залежність і використовувати її як зброю. Відповідь на це запитання полягає не в тому, щоб від'єднатися від такої економіки, як китайська, що було б безглуздо, а в розумному зменшенні ризиків і диверсифікації шляхом забезпечення стійких ланцюжків поставок, захисту нашої технологічної переваги та інвестування в промислові потужності.

І по-третє, це революція в технологіях, яка змінює те, як ми живемо, працюємо, боремося і конкуруємо, з можливостями та ризиками, які ми ще не можемо повністю зрозуміти.

Із цього приводу В. Бернс наголошує, що прогрес у пов'язаних із комп'ютерами технологіях – від чіпів до квантового та ШІ – веде до проривів надзвичайного масштабу та розмаху. Лише за кілька місяців із моменту появи першої публічної версії ChatGPT у листопаді минулого року ми побачили, що новіші моделі перевершують людей на вступних іспитах до аспірантури та в оцінюванні взаємодії лікаря з пацієнтом у програмах медичного навчання.

Лідерство в технологіях та інноваціях стало основою нашого економічного процвітання та військової сили. Це також було критично важливо для встановлення правил, норм і стандартів, які захищали б наші інтереси та наші цінності. Наші китайські суперники розуміють це так само, як і будь-хто інший, і тому не дивно, що вони інвестують значні кошти в новітні технології як центральний вимір нашої стратегічної конкуренції.

Показово, що в щорічній доповіді Розвідувального співтовариства (РС) США про світові загрози національній безпеці (Annual threat assessment of the U.S. intelligence community. March 2025) зазначається: «…Росія, Китай, Іран і Північна Корея – індивідуально і колективно – кидають виклик інтересам США у світі, нападаючи або погрожуючи іншим у своїх регіонах, застосовуючи як асиметричну, так і традиційну тактику жорсткої сили, а також просуваючи альтернативні системи, щоб конкурувати зі Сполученими Штатами, насамперед у сфері торгівлі, фінансів і безпеки. Вони прагнуть кинути виклик Сполученим Штатам та іншим країнам за допомогою цілеспрямованих кампаній, щоб отримати перевагу, водночас намагаючись уникнути прямої війни. Зростаюча співпраця між цими супротивниками посилює їхню стійкість проти Сполучених Штатів, збільшує потенціал воєнних дій з одним із них, які можуть втягнути в них іншого, і чинить тиск на інших глобальних гравців, змушуючи їх ставати на чийсь бік…» [12].

Крім цього, у вищезазначеній доповіді наголошується, що КНР, імовірно, продовжуватиме позиціонувати себе як країну, що має перевагу в потенційному конфлікті із США. КНР і надалі намагатиметься тиснути на Тайвань щодо об'єднання і продовжуватиме проводити широкомасштабні кібероперації проти американських об'єктів як з метою шпигунства, так і для отримання стратегічної переваги. Китай, імовірно, буде намагатися достатньо обмежити діяльність китайських компаній і кримінальних елементів, які забезпечують постачання і незаконний обіг прекурсорів фентанілу і синтетичних опіоїдів до США, якщо не будуть вжиті більш активні заходи з боку правоохоронних органів.

Пекін продовжуватиме зміцнювати свій звичайний військовий потенціал і стратегічні сили, посилюватиме конкуренцію в космосі і підтримуватиме свою індустріальну й технологічно інтенсивну

економічну стратегію, щоб конкурувати з економічною потужністю і глобальним лідерством США.

Китай становить найбільш комплексну і потужну військову загрозу національній безпеці США. НВАК розгортає об'єднані сили, здатні вести війну повного спектру, щоб протистояти втручанню Сполучених Штатів у регіональні конфлікти, поширювати свою владу в глобальному масштабі і захищати те, що Пекін вважає своєю суверенною територією. Значна частина зусиль Китаю з військової модернізації зосереджена на розвитку сил і засобів протидії інтервенції, пристосованих до всіх аспектів військових операцій США і їхніх союзників у Тихоокеанському регіоні. Пекін зосередиться на досягненні ключових етапів модернізації до 2027 і 2035 років, спрямованих на перетворення НВАК на армію світового класу до 2049 року.

На окрему увагу заслуговує те, що Китай використовує агресивний загальнодержавний підхід у поєднанні з державним управлінням приватним сектором, щоб стати глобальною науково-технічною наддержавою, перевершити США, сприяти самодостатності та досягти подальших економічних, політичних і військових переваг. Пекін визначив пріоритетними такі технологічні сектори, як передова енергетика, ШІ, біотехнології, квантова інформатика і напівпровідники, кидаючи виклик зусиллям США щодо захисту критично важливих технологій, пристосовуючи обмеження вузько для вирішення проблем національної безпеки. Китай прискорює свій науково-технічний прогрес за допомогою цілого ряду законних і незаконних засобів, включаючи інвестиції, придбання і крадіжку інтелектуальної власності, кібероперації, залучення талантів, міжнародну співпрацю та ухилення від санкцій.

У свою чергу, 19 березня 2025 року Європейська комісія представила «Білу книгу з питань європейської оборони – Готовність 2030» [13].

Міжнародний порядок змінюється. Уже в другій половині нинішнього десятиліття постане новий. Європа повинна брати активну участь у цих процесах, щоб уникнути небезпеки стати «пасивним отримувачем» наслідків нового порядку, включно з перспективою повномасштабної війни. Виклики європейській безпеці мають стратегічний характер і вимагають стратегічної відповіді. Стрімко

розширюється традиційний спектр різних типів загроз безпеці, посилюються взаємозв'язки між ними, про що свідчать неодноразові випадки тероризму та насильницького екстремізму, гібридні атаки, дії міжнародних організованих злочинних груп та мереж кіберзлочинців. Наявні докази зв'язків між злочинними групами та ворожими державними акторами, що завдяки новим технологіям легко долають кордони. Європейські держави через близькість географічного положення постійно зіштовхуються з міграцією, спричиненою наслідками воєн та зміною клімату, яких зазнають країни Північної Африки та Близького Сходу. Арктика стає новою ареною геополітичної конкуренції на півночі континенту.

росія становить серйозну стратегічну загрозу на полі бою, змусивши Європу і партнерів стикнутися з реальністю інтенсивної масштабної механізованої війни на Європейському континенті, якої не було вже 80 років. рф, яка є найбільш озброєною європейською державою, будує військову економіку, зосереджену на досягненні своїх воєнних цілей через промислову мобілізацію й технологічні новації. Крім того, масштабує свою військову економіку за підтримки Білорусі, КНДР та Ірану. рф чітко дає зрозуміти, що залишається в стані війни із Заходом. І якщо їй дозволити досягти цілей в Україні, її територіальні амбіції виходитимуть за межі цієї країни.

Посилюються гібридні загрози, як-от: кібератаки, саботаж (зокрема, у Балтійському та Чорному морях), електронні перешкоди в глобальних навігаційних і супутникових системах, кампанії з дезінформації та політичне й промислове шпигунство, використання міграції як зброї. Геополітичне суперництво призвело не лише до нового етапу гонки озброєнь, а й спровокувало глобальну технологічну гонку. Технології стануть основною характеристикою конкуренції в новому геополітичному середовищі. Низка критично важливих та базових технологій (ШІ, біо- та квантові технології, робототехніка, гіперзвукові технології) є ключовими компонентами як довгострокового економічного зростання, так і військової переваги.

З огляду на кардинальні зміни у стратегічному середовищі Європі необхідно наростити достатній потенціал стримування для запобігання можливій агресії. ЄС визнає відповідальність держав-учасниць за власні збройні сили: від розроблення доктрини до особливостей розгортання та потреб. ЄС має значний потенціал для

підтримки та координації зусиль у зміцненні оборонної промислової бази та загальної оборонної готовності ЄС через:

• сприяння тіснішій співпраці та ефективному масштабуванню європейської оборонної промисловості в розробленні, виробництві та просуванні систем озброєння;

• підвищення ефективності, взаємозамінності та взаємосумісності озброєнь, зменшення витрат шляхом уникнення конкурентних закупівель та покращення купівельної спроможності держав-членів, а також забезпечення стабільності та передбачуваності завдяки довгостроковим промисловим замовленням;

• підтримку інфраструктури подвійного призначення для мобільності, космічного зв'язку, навігації та спостереження;

• сприяння різним формам партнерства.

Таким чином, можемо констатувати, що стратегічна конкуренція, загальні транснаціональні імперативи та безпрецедентна в історії людства технологічна революція створюють надзвичайно складний міжнародний ландшафт. Це, безперечно, загострює увагу на зміні підходів до ролі розвідки в цьому трансформованому світі.

4.2. Концепт «розвідувальна діяльність» у сучасних умовах

Сучасний світ стрімко й безповоротно змінюється. Турбулентність і напруга в глобальній політиці та економіці продовжують наростати. Звичний міжнародний порядок відходить в історію. Існуюча система міжнародних відносин і безпековий простір, не витримавши гібридних викликів і загроз XXI ст., переживають нині трансформації фундаментального характеру. Це дало додаткове прискорення процесу формування нової глобальної архітектури простору безпеки і середовища міжнародних відносин.

В умовах сучасних глобальних викликів та загроз міжнародній і національній безпеці відбулася трансформація міжнародного простору, що виявила низку політичних, безпекових, економічних, гуманітарних проблем, які неможливо адекватно оцінити й подолати виключно на рівні окремо взятої держави. Їхнє вирішення лежить у міжнародній політичній площині та у сформованому державами-глобалізаторами міжнародному просторі безпеки.

Реальністю XXI ст. стала реставрація великодержавного, імперського типу геополітичної свідомості, який, опираючись на досвід історичного минулого, пропонує ідеал державного розвитку у вигляді створення «великих імперій» та механізмів їхнього домінування над «середніми» та «малими» державами, а також недержавними політичними силами. Насамперед це властиво рф та КНР, які в умовах XXI ст. у різний спосіб намагаються практично реалізувати задум «великодержавного ренесансу». При цьому слід ураховувати, що в постмодерних умовах великодержавницька геополітична свідомість зазнала змін: її орієнтація на максимально можливе територіальне домінування приховується інформаційним шумом щодо необхідності конструювання «великих політичних просторів», здатних створити кращі умови задля задоволення соціально-економічних, політичних, культурних та інших потреб упокорених народів і націй (останнім не забороняється мати власну «декоративну» державність, межі якої мають регулюватися новітньою метрополією).

Неспровоковане широкомасштабне вторгнення росії в Україну підкреслило, що ера міжнаціонального / міждержавного змагання та конфліктів не відійшла в минуле, а натомість стала визначальною характеристикою нинішньої епохи.

Стратегічне змагання між США та їхніми союзниками, Китаєм і росією щодо того, який світ виникне, робить наступні кілька років критично важливими, зокрема в контексті дій росії в Україні, які загрожують перерости в ширший конфлікт між росією та Заходом.

«Українське питання» продовжує домінувати в оцінці безпекового середовища, залишаючись у пріоритеті порядку денного та прямо чи опосередковано впливаючи на більшість сфер та напрямів забезпечення міжнародної, регіональної безпеки.

У такому контексті увагу привертає новітній імператив НАТО – імператив когнітивної першості, що має забезпечити стратегічні переваги Альянсу. Когнітивні переваги – один із вагомих акцентів, який так чи інакше присутній у новітніх документах Альянсу. Зокрема, прикметною особливістю «Концепції воєнних дій НАТО» (The NATO Warfighting Capstone Concept – NWCC, 2021) [14], є те, що «Концепція…» стосується майбутнього – аж до 2040 р. І в ній, з-поміж іншого, зазначається низка важливих речей: новітнє (і, відповідно, майбутнє) оперативне середовище вимагає від Альянсу нового

способу мислення, організації та дії, а серед його основних завдань – концентрація уваги на військовій перевазі та активному формуванні «оперативного» середовища з обов'язковим урахуванням особливостей процесу його «постійного розширення» та діяльністю як традиційних, так і нетрадиційних акторів. Пізнання оперативного / безпекового середовища вимагає безперервного сканування горизонтів – отримання інформації, вивчення стратегій його учасників, їхніх підходів до ведення війни, оцінювання планів та намірів, сили та розвитку спроможностей заради можливої зміни способів дій усіх акторів середовища. Ураховуючи базову настанову NWCC, згідною з якою майбутні бойові дії Альянсу – «багаторегіональна, багатовимірна (фізична, віртуальна, когнітивна) і багатодоменна робота» (тобто на суші, у повітрі, на морі, у кібернетичній сфері та у космосі) в умовах, коли «виклик кордонам» буде лише зростати, коли кордони між «доменами» фактично будуть стертими, ідея когнітивних переваг набуває неабиякої ваги.

Когнітивний вимір дій НАТО, як можна зробити висновок, ознайомившись із NWCC, передбачає:

• щодо ворога – краще знання, а отже, і розуміння стратегічного середовища, що буде «більш вимогливим»;

• щодо членів НАТО – не лише прагнення учасників Альянсу до досконалості й маневреності (що спираються на унікальність армії НАТО, етос, культуру, різноманітність, бажання ініціативності та перемоги за будь-яких обставин над будь-яким супротивником), але й насамперед володіння інформацією та, відповідно, мисленням, що перевершує супротивника у швидкості (знаходиться «поза темпом») розпізнавати, ризикувати, приймати рішення та діяти швидше (ніж потенційний супротивник). Багатоаспектний когнітивний вимір – підґрунтя забезпечення здатності членів НАТО «сприяти і використовувати взаємопідтримуючі і звичні стосунки та можливості партнерства»; здатність думати, планувати, прогнозувати, адаптуватися заради можливості «терпіти стільки, скільки потрібно» у ході стратегічної конкуренції і за будь-якої конфліктної ситуації.

Когнітивна перевага в документі оголошена пріоритетом Альянсу та витлумачується як «розуміння оперативного середовища та потенціалу супротивника, можливостей Альянсу та цілей», як «критична здатність», спрямована на «поліпшення ситуаційної обізнаності та

стратегічного прогнозування», на «розширення знань і розуміння» заради досягнення, кінець кінцем, цілей.

Імператив когнітивної переваги розглядається не осібно, а в контексті – у тісному зв'язку з іншими імперативами розвитку воєнних дій, такими як:

• «багатошарова стійкість», що передбачає здатність поглинати удари та боротися на всіх рівня – «військовому, цивільно-військовому та військово-цивільному»;

• «проєкція впливу та влади», суттю якої є «формування позитивного середовища з урахуванням сильних сторін Альянсу, включаючи створення варіантів і нав'язування дилем противнику»;

• «інтегрована мультидоменна оборона» – розуміння командирами багатодоменного операційного середовища заради швидких та ефективних дій;

• «міждоменна команда», яка має забезпечувати єдність Альянсу в ході прийняття рішень і протидії загрозам «у будь-якому домені, незалежно від їхнього походження чи природи» і яка володітиме гнучким та асиметричним мисленням у ході командування місією у 2040 році, що постійно підкріплюватиметься надійними та постійно оновлюваними комунікаційними та інформаційними системами.

Характеризуючи «лідерів і штаби», NWCC наголошує на потребі таких із них (можна сказати, суперлюдей), які «здатні вправитися зі швидкістю, складністю, бути зорієнтованими на дані та технології» безпекового середовища майбутнього. Крім того, цікавий наголос стосується гендеру та поколінь: НАТО і його союзники повинні використовувати «переваги гендеру та багатоманітність як мультиплікаторів сили» та уникати ризиків, пов'язаних із «розривом поколінь». Таким чином, досягнення когнітивних переваг НАТО та союзників фактично виключає дискримінацію на основі гендеру чи віку. Утім, у кожному випадку до уваги беруться інтелектуальні чи пізнавальні здатності / здібності особи (разом з її ціннісними чи культурними пріоритетами), а не, наприклад, її гендерна специфіка (тобто, чи є особа трансгендерною, лесбійкою, гомосексуалом, небінарною, кроссдрессером і т. ін.), попередній досвід персони, який у XXI ст., в умовах появи і розвитку нових технологій, що використовуються / використовуватимуться в «день-нуль», значною мірою і досить швидко фактично втрачає свою актуальність. Тож «широта

різноманітності» (мовою «Концепції…») – важлива, але, як можна припустити, із суттєвими застереженнями.

Особлива роль, як зазначено в NWCC, відводиться підготовці осіб, потрібних для виконання актуальних для НАТО завдань (у т. ч. у когнітивній сфері), зокрема під час їхнього навчання в Оборонному коледжі НАТО (NATO Defense College, NDC) у Римі та в Школі НАТО в німецькому Обераммергау, які, вочевидь, і розглядаються як надійне підґрунтя для огранки (формування та розвитку) мізків тих, хто вже сьогодні забезпечує й забезпечуватиме (після 2040 року) когнітивні переваги НАТО та їхніх союзників, керуючись при цьому настановою творця NDC генерала Дуайта Д. Ейзенхауера: «Розвивайте осіб як з військової, так і з цивільної сторони, щоб вони мали повне розуміння багатьох складних факторів у ході участі у створенні адекватної оборонної позиції для зони Північноатлантичного договору».

Успіх майбутніх військових дій, як передбачалося в документі, буде «повністю спиратися на дані». Тож, за задумом стратегів, в Альянсі має відбуватися широкий обмін якісними даними, обробка яких має невпинно покращуватися. Передбачено об'єднання «усіх джерел інформації та розвідки», розширення аналітики в рамках процесів прийняття воєнно-стратегічних рішень, досягнення «цілісності та послідовності інформаційних потоків». Крім того, NWCC орієнтує членів Альянсу на обмін даними технологічної розвідки, на сканування горизонтів нових наукових і промислових розробок як усередині, так і поза межами НАТО, щоб «визначити сфери потенційних переваг» (зокрема технологічних).

Важливим у NWCC є і акцент на своєрідному механізмі навчання (задля досягнення когнітивних переваг), який передбачає «постійну підготовку» на основі «вкоріненої у збройних силах Альянсу культури». Саме постійна підготовка кадрів з опорою на культуру, що склалася, є тим, як переконані стратеги Альянсу, надбанням, яке дозволить перевершити інших. Воно містить два важливих компоненти: перший – здатність розробляти складні сценарії, другий – практикувати розроблення низки варіантів таких сценаріїв та, відповідно, низки варіантів прийняття рішень. Вимога до процесу навчання дуже конкретна: у навчальних вправах повинні використовуватися «живі і просунуті моделі та симулятивні конструкції», які згодом і забезпечать «виявлення сфер, що вимагатимуть

покращення, зміцнюватимуть довіру до нових можливостей і планів», підтримуватимуть керівництво розробленням воркгеймінгу, експериментування, як і виключне – реалістичне (!) у своїй основі – навчання з урахуванням чинника «день-нуль», що може наступити (до чи після 2040 року).

Хоч би в якому контексті ми розглядали нинішній хаос у міжнародних справах, **важливо усвідомлювати, що ледь не кожна держава, навіть та, що є простим спостерігачем, бачить ситуацію по-своєму.** Показово, що з початком XXI ст. дослідники розвідки, узявши до уваги «революційні зміни» в безпековому середовищі, у природі загроз і природі миру, як і зміни в характері воєн, відзначивши мінливість характеру інформації, швидкість технологічних змін, варіативність очікувань не лише споживачів розвідувальної інформації, але й громадськості, заговорили про необхідність «революції в розвідці».

Так, колишній головний технічний директор та заступник директора Національного агентства геопросторової розвідки США Ентоні Вінчі у статті «Майбутня революція в розвідувальних справах. Як штучний інтелект та автономні системи трансформують шпигунство» (2020) зазначив: «Протягом усієї історії людства люди шпигували один за одним, щоб дізнатися, що роблять або планують робити інші. Люди стежили, контролювали та підслуховували, використовуючи інструменти, які постійно вдосконалювалися, але ніколи не витісняли своїх господарів-людей. ШІ та автономні системи змінюють усе це. У майбутньому машини шпигуватимуть за машинами, щоб знати, що роблять або планують робити інші машини. Розвідувальна діяльність усе ще полягатиме в добуванні та захисті секретів, але те, як ці секрети здобуваються, аналізуються та поширюватимуться, буде принципово іншим» [15].

Крім того, у праці «Аналіз розвідки в епоху цифрових технологій» (2021) [16] у рамках концепції «цифрової ери» відзначається збільшення змін та ускладнень (у площині «викликів–загроз–ризиків»), які впливають на темпи поширення інформації: нові технології скоротили час поширення інформації фактично до нуля. Такий стан речей призводить до того, що рішення ухвалюються в дедалі несприятливіших умовах, коли неухильно зростає попит на своєчасну, релевантну та надійну розвідку, а час для ухвалення адекватних рішень

мінімізується, і, відповідно, розроблення адекватної часу політики у вкрай мінливому світі стає також викликом для лідерів, держав, спільнот.

Інший виклик часу для розвідок та безпосередньо роботи з інформацією пов'язаний із проблемою «великих даних», зібраних в умовах сьогодення в дифузному, багатополярному середовищі. У книзі 2024 року авторства Мії Хаммонд-Ереї «Великі дані, нові технології та розвідка: підрив національної безпеки» [17] доводиться, що великі дані трансформують виробництво знань розвідкою, як і взаємини РС із громадськістю, а також ставлять під сумнів окремішність (відокремленість) збирання внутрішніх та зовнішніх розвідданих. А це, зрозуміло, вимагає постійної зміни конфігурації РС держави / держав.

«Великі дані» є результатом інтеграції даних розвідки з багатьох джерел. Американські аналітики ще у 2015 році, відтворюючи різноманіття даних, які залучалися до аналізу, указували на використання інформації із численних генераторів даних: зокрема, «бойових повітряних патрулів» MQ1 Predator, гіперспектральних датчиків з інтенсивним об'ємом даних, датчиків виявлення світла чи визначення дальності, інформація з яких, своєю чергою, доповнювалася датчиками розвідки сигналів (SIGINT), інформацією з датчиків індикаторів рухомої цілі, інфрачервоних та датчиків нетрадиційних вимірювань і сигнатур (Measurement and Signature Intelligence, MASINT). Головоломка «великих даних» базується не лише на безлічі джерел, але й цілому спектрі дисциплін, що інтегрують як згадані SIGINT і MASINT, так і «людську» (чи «агентурну») розвідку (Human Intelligence, HUMINT) та геопросторову (Geospatial Intelligence, GEOMINT) і, безумовно, розвідку з відкритих джерел (OSINT).

Таким чином, уже сьогодні викликом у ході збирання, інтеграції та аналізу інформації може бути неспроможність відійти від традиційних лінійних підходів до збирання та обробки даних (слабке місце яких – ненавмисне знецінення інформації та, як наслідок, постання «стратегічних несподіванок»), як і до подальшого оцінювання та прогнозування, що й може зумовити специфічний «збій розвідки».

Таким чином, можна виділити такі особливості розвідувальної діяльності в сучасних умовах:

1. Упровадження та використання нових технологій та інновацій.

Революція у сфері цифрових технологій має більший вплив, ніж індустріальна революція чи можливість застосування атомної енергії свого часу. З огляду на це в ЦРУ США створено Спеціальний технологічний центр, який активно співпрацює з приватним IT-сектором, та введено вперше в історії нову посаду головного технічного директора ЦРУ США.

Однією з найбільш революційних технологій збирання розвідувальної інформації військового характеру сьогодні стала інтеграція безпілотників і супутників. Застосування цих інноваційних технологій дало змогу збройним силам не лише отримати низку суттєвих переваг стратегічного й тактичного характеру, а й трансформувати ландшафт військової розвідки. Упровадження сучасних алгоритмів уможливило аналіз зібраних даних у режимі реального часу, а отже, швидше й ефективніше виявляти загрози на полі бою.

Супутникові технології вже кілька десятиліть є важливим компонентом розвідки. Супутники, що обертаються на орбіті високо над Землею, забезпечують широке покриття, збирання даних і можливості зв'язку, що робить їх незамінними в сучасній війні. Синергія, що виражається в інтеграції безпілотників та супутників для збирання розвідувальних даних, ознаменувала нову еру в розвитку розвідувальної діяльності.

Значну роль у трансформації її систем відіграє впровадження технологій на основі ШІ, що дає змогу аналізувати значні обсяги даних, генеруючи важливу інформацію для прийняття управлінських рішень. Використовуючи технології ШІ для розвідувального аналізу, можна виявляти потенційні загрози, картографувати ворожу діяльність та оцінювати геополітичну ситуацію, а також швидко приймати виважені рішення.

Основними перевагами аналізу даних у розвідці на основі ШІ є поглиблена ситуаційна обізнаність, удосконалені можливості прогнозування, точна оцінка загроз.

Оборонні розвідувальні системи можуть використовувати когнітивний ШІ для підтримки прийняття рішень військовим керівництвом, допомагаючи у складному стратегічному плануванні та оцінці ризиків. Застосування когнітивних обчислень у військовій розвідці може відбуватися за такими напрямами:

• обробка природної мови (Natural Language Processing, NLP) – алгоритми NLP можуть обробляти текстові дані, даючи змогу системам оборонної розвідки отримувати інформацію зі значних обсягів неструктурованих документів;

• ШІ – віртуальні помічники на основі ШІ допомагають військовому керівництву упорядковувати інформацію, робити запити та приймати рішення в режимі реального часу, заощаджуючи цінний час у критичних ситуаціях;

• сценарне моделювання – когнітивні системи ШІ аналізують різні параметри та моделюють упровадження різних сценаріїв, допомагаючи збройним силам прогнозувати результати і розробляти ефективні стратегії.

Інтеграція ШІ з автономними системами та робототехнікою зумовлює суттєві зміни в розвідувальній діяльності. Серед найбільш значущих переваг упровадження ШІ до автономних систем можна навести такі:

• вони значно ефективніше здійснюють візуальне спостереження, збирають та аналізують дані, мінімізуючи ризик для персоналу;

• ці системи можуть виявляти, відстежувати та ідентифікувати потенційні цілі з більшою точністю, мінімізуючи можливі невиправдані руйнування цивільної інфраструктури;

• автономні системи, оснащені ШІ, оптимізують логістику та ланцюги поставок, забезпечуючи своєчасну доставку ресурсів на лінію фронту.

2. Співпраця з приватним сектором та використання соціальних мереж.

Сьогодні нові технології дозволяють недержавним суб'єктам й окремим особам також збирати та аналізувати розвідувальні дані іноді краще та швидше, ніж державні органи. Комерційні структури щороку запускають сотні супутників. Більше половини світу перебуває в Інтернеті, виробляючи та одержуючи розвідувальні дані з відкритим кодом, навіть якщо вони цього не знають. Згідно зі звітом Всесвітнього економічного форуму 2019 року, користувачі Інтернету щодня публікують близько 500 мільйонів твітів у Twitter і 350 мільйонів фотографій у Facebook [18, 19].

Зокрема, у ЦРУ США створено підрозділ, який зосереджений на розбудові партнерських відносин із приватним (недержавним)

сектором з метою отримання інновацій, що надають конкурентну перевагу.

Крім цього, активно використовуються соціальні мережі. Так, у рамках протидії росії спецслужби США активізували вербувальну роботу (зокрема, з використанням Telegram) серед невдоволених політикою кремля громадян рф.

3. Контрольоване розсекречення чутливої інформації.

«Стратегічне розсекречення», навмисне публічне розкриття певних секретів, щоб підважити позиції конкурентів і згуртувати союзників, стало потужним політичним інструментом. Використовувати його – не означає необачно поставити під загрозу джерела чи методи добування розвідувальної інформації, проте означає розсудливий опір рефлексивному бажанню тримати все засекреченим.

4. Партнерські відносини та особисті контакти з представниками спецслужб інших держав.

Особисті контакти та партнерські відносини – своєрідна розвідувальна дипломатія, яка сприяє зближенню інтересів, підтримці зусиль політиків і дипломатів досягати необхідних результатів.

Ці зустрічі є важливим засобом захисту від непотрібних непорозумінь і ненавмисних зіткнень, а також доповнюють і підтримують канали формування політики, такі як контакти керівників держав.

5. Інвестиції в людей (особовий склад РС).

Фахова підготовка особового складу в сучасних умовах набуває все більшої важливості і є ключовим фактором посилення розвідувальних органів (служб).

Необхідно залучати та утримувати технологічні таланти, покращувати пакети оплати праці та заохочувати більш гнучкі моделі кар'єри, щоб офіцери могли перейти до приватного сектору, а потім повернутися назад.

Показово, як свідчить сайт Офісу директора національної розвідки США, що з-понад 165 вакансій (восени 2024 року) величезна їх кількість (крім лікаря, юриста чи перекладача) стосувалася фахівців, здатних працювати безпосередньо у сфері розвідки. Аналіз посад та, відповідно, констатованих ЦРУ напрямків роботи (на тій чи іншій посаді) дозволяє виокремити певну специфіку «бажань» ЦРУ в умовах сьогодення. Тож своєрідними акцентами в знаннях, уміннях та навичках фахівців-претендентів, затребуваних ЦРУ, були:

• володіння знаннями, уміннями, навичками з різноманітних сфер (наприклад, вакансія адвоката передбачала роботу «на стику права і передових технологій», тоді як методолог-аналітик повинен уміти «розробляти методи для підвищення точності аналізу та збирання розвідувальних даних за допомогою статистичних, економетричних і математичних оцінок», здійснювати геопросторове моделювання та ін.);

• наявність обов'язкового бакалаврського ступеня (зокрема, для бухгалтерів, картографів, поліграфологів чи case-офіцерів, які «таємно виявляють, оцінюють, розробляють, вербують та обслуговують неамериканських громадян, що мають доступ до даних іноземної розвідки, життєво важливих для органів зовнішньої політики та національної безпеки США»);

• наявність обов'язкового магістерського чи вищих ступенів (для «методолога-аналітика», для «науковців із питань життя та експертів у галузі біотехнологій; для адвоката – «доктор юриспруденції» виключно від акредитованих Американською асоціацією юристів правничих шкіл; для психолога -наявність бакалаврського чи магістерського диплома для «агентів – виконавців захисту», які «є частиною команди, що забезпечує озброєний захист лідерів РС в усьому світі 24/7/365»;

• наявність диплома доцента (для ІТ-фахівців корпоративної системи, які «надають партнерам місії агентства консультації, аналіз і вирішення проблем щодо технологічних продуктів, програм, доступу до даних і системи, а також проблем із програмним забезпеченням»; для офіцерів «фізичної та технічної безпеки»);

• багатопрофільність (тобто не лише вакансія «розвідник», але й «багатопрофільний офіцер розвідки» чи «DST Data Scientists» у сфері збирання та використання даних», які здатні збирати дані «з багатьох систем і типів даних» заради отримання «ключової інформації про місію»; або «DDI Data Scientists», які «вирішують критичні проблеми з даними, створюючи оптимальні конвеєри даних, аналізуючи та перетворюючи дані, а також доставляючи дані в системи для просування розвідувальної місії ЦРУ»);

• аналітичні здібності (вакансії для військових і цивільних: аналітик з кадрів; аналітик з персоналу; аналітик розвідки; військовий аналітик; політичний аналітик; лідер-аналітик; аналітик зі збирання

даних; аналітик даних; аналітик людських ресурсів; аналітик таргетування; технічний аналітик таргетування; офіцер бізнес-аналітики; економічний аналітик; аналітик кіберзагроз; програмний аналітик; аудитор IG / аналітик програм; IG-IT-аудитор / аналітик програм; наглядовий IT-аудитор / аналітик програм IG та ін.);

• яскраво виражена наукова спроможність (наукова складова в здібностях / здатностях фахівців для вакансій: аналітик науки, технологій і зброї; науковий дослідник матеріалів; «інженери та науковці з джерел живлення»; «науковий дослідник у галузі мікроелектроніки»; науковці в галузі розвідки, які «досліджують, пишуть і викладають усі аспекти історії ЦРУ... мають доступ до вихідного матеріалу. Їхні твори включають короткі есе чи історії довжиною в книгу» та ін.);

• володіння найсучаснішими технологіями («спеціаліст зі штучного інтелекту»; «спеціаліст із розширеної реальності», який використовує «свій досвід для розроблення можливостей для віртуальних, доповнених і сенсорно покращених середовищ за допомогою ігрових механізмів, тактильних пристроїв та/або окулярів з ефектом занурення»).

6. Бюджет.

Пріоритети не є реальними, якщо за ними не стоїть бюджет.

Незважаючи на революцію у сфері цифрових технологій і бурхливий розвиток технічних видів розвідки, агентурна розвідка залишається пріоритетним напрямом діяльності будь-якої розвідки. Це пояснюється тим, що завжди залишатимуться таємниці, про які ми зможемо дізнатися лише за допомогою агентурних джерел, і таємні операції, які зможе проводити лише людина. Це потребує від співробітників агентурної розвідки інтенсивної підготовки, командної роботи, вражаючої креативності та жаги ризику.

Вищенаведені тези тісно переплітаються з положеннями Національної розвідувальної стратегії США, яку опубліковано в серпні 2023 року [20]. У документі визначено шість основних напрямів розвитку РС США, а саме:

• посилення ролі розвідки у зв'язку із загостренням стратегічної конкуренції між США, Китаєм та росією. Означено, що лише КНР має і наміри, і спроможності для того, щоб конкурувати із США, а рф – це джерело постійної загрози регіональній безпеці

в Євразії, а також дестабілізаційний чинник глобального рівня. У контексті стратегічної конкуренції основним завданням РС США є забезпечення лідерства Сполучених Штатів у сфері технологій та інновацій, насамперед це розвідка з відкритих джерел, робота з біг-дата, ШІ і поглиблена аналітика. Для цього РС США має активізувати співпрацю із союзницькими і партнерськими розвідками, а також із громадським і приватним сектором;

• пошук, професійний розвиток та утримання на службі талановитих співробітників РС США. Найбільш цінними є технічно підготовлені та обдаровані кадри, які через організаційно-бюрократичні та інші обмеження або не можуть працевлаштуватися в розвідці, або звільняються після нетривалого періоду служби. Щоб пришвидшити приймання на роботу, планується модернізувати систему відбору та працевлаштування співробітників РС США, а щоб підвищити рівень професійного розвитку, вважається за доцільне й далі практикувати спільні місії для представників різних розвідувальних органів, які братимуть у них участь на ротаційній основі;

• розроблення інтероперабельних та інноваційних рішень для формування нових спроможностей РС США. Результатом реалізації таких рішень має бути створення уніфікованих підрозділів, які відповідають за закупівлю необхідного майна та обладнання; запровадження централізованої автоматизованої системи постановки запитів на закупівлю та єдиної системи укладення контрактів на виконання робіт. Запорукою успіху вважається формування у РС США корпоративної культури, яку буде спрямовано на пошук нових інструментів, процесів та стандартів, що допоможе виконувати трудомісткі завдання завдяки продуктивній взаємодії людини з машиною (ШІ). Основоположним є принцип датацентричності, який передбачає суттєве підвищення доступності й стандартизації розвідувальної інформації, а також спроможностей пошуку й добування конкретних даних з уже наявних обсягів інформації. Це потребує більш глибокої інтеграції науково-дослідних, технічних, аналітичних і добувних підрозділів РС США;

• розширення, диверсифікація та посилення партнерства у сфері розвідки. Створення мережі союзників і партнерів суттєво підвищує операційні та аналітичні спроможності РС США. Важливою умовою є активізація обміну розвідувальною інформацією на

регіональному та локальному рівнях. Водночас РС США має переосмислити й удосконалити процедури обміну інформацією з недержавними й субнаціональними установами, оскільки їхня роль суттєво зросла, особливо у сфері захисту критичної інфраструктури від кіберзагроз;

• підвищення рівня експертизи щодо транснаціональних викликів, таких як кліматичні зміни, контрабанда наркотиків, фінансова криза, порушення ланцюжків поставок, корупція, невідомі хвороби, проривні технології. У цьому контексті РС США планує залучати до роботи кращих експертів, які мають високий рівень обізнаності у сферах своєї діяльності та здатні формувати пропозиції для прийняття керівництвом держави відповідних стратегічних рішень;

• забезпечення стійкості функціонування РС США. Для цього планується модернізація та розширення розвідувальної інфраструктури, що має поліпшити спроможності раннього виявлення та попередження найбільш небезпечних загроз, таких як пандемії, масовані кібератаки, кліматичні зміни й терористичні акти. Водночас розвідувальна інфраструктура має забезпечувати не лише стійке функціонування розвідки, а й можливість завдання ударів у відповідь та швидкого відновлення в разі нападу.

У контексті цифровізації розвідувальної діяльності також заслуговує на увагу прийнята в липні 2023 року Дата-стратегія РС США на 2023–2025 роки, у якій висвітлено основні напрями політики цифровізації РС США [21]. Згідно з документом нова епоха характеризується датацентричністю світу. У зв'язку із цим американська розвідка має впроваджувати досвід провідних комерційних компаній, які організовують свою роботу за принципами agile2 та безперервного навчання. На цьому тлі зростає значення поглибленого аналізу даних в інтересах максимально швидкого прийняття рішень керівництвом держави. Одним із найважливіших завдань є вдосконалення формату розвідувальної інформації для того, щоб дані однаково ефективно могла сприймати як людина – споживач інформації, так і машина.

До цього часу власне дані не вважалися ключовим інструментом розвідувальної діяльності ні на стратегічному, ні на оперативному рівнях. Основна проблема полягає в тому, що американські розвідувальні органи надто повільно розвивають такі дата-спроможності,

як комплексне збирання та аналітика даних, насамперед за допомогою ШІ. Для поліпшення ситуації РС США вважає за доцільне впроваджувати датацентричний підхід, що дасть можливість удосконалити процеси інтеграції, транспортування, розподілу, використання та супроводу розвідувальних даних.

Основні напрями реалізації Дата-стратегії РС США:

• застосування принципу E2E (віч-на-віч) у дата-менеджменті передбачає детальне планування, розроблення та реалізацію єдиних процедур збирання, обробки, розподілу та використання інформації. Для цього буде впроваджено єдиний у РС США формат розвідувальних даних (тегів чи міток), для їх подальшої обробки за допомогою ШІ, а також стандарти генерування, обміну, розподілу, доведення та захисту інформації;

• забезпечення інтероперабельності (взаємосумісності) даних для своєчасного доведення їх до потрібного споживача передбачає зміну парадигми управління розвідкою із системно-центричної на датацентричну. Якщо раніше основною метою управління розвідкою було створення інформаційної архітектури (комп'ютери, сервери, мережі тощо), то нині фокус управління спрямовано на процедури збирання, аналізу та розподілу інформації з використанням ШІ. Датацентричний підхід має поліпшити якість розвідувальної інформації, поглибити її інтеграцію, підвищити точність інтерпретації та інтероперабельність. Застосування ШІ має скоротити час збирання й обробки необхідної інформації з тижнів / днів до годин / хвилин;

• розвиток партнерства у сфері цифрових інновацій передбачає активну співпрацю РС США з іноземними розвідками та цивільними установами й академічними колами для кращого розуміння інформаційних технологій та реагування на зміни в їхньому розвитку. Варто наголосити на тому, що досі співпраця РС США з приватним сектором та науковцями не мала такого важливого значення з огляду на стрімкість цифрової революції, насамперед у сфері ШІ;

• підвищення дата-грамотності співробітників розвідки. Перехід до датацентричної моделі розвитку РС США неможливий без зміни системи освіти, курсової та професійної підготовки співробітників розвідки в контексті усвідомлення ними того, що робота з даними – це основа успішного виконання будь-якої місії (завдання).

Дата-грамотність визнається однією з ключових професійних компетентностей як пересічних виконавців, так і старших керівників розвідки.

4.3. Місце і роль недержавних суб'єктів розвідувальної діяльності в контексті забезпечення національних інтересів

Нині зовнішня політика будь-якої держави базується на відомій їй інформації суспільно-політичного характеру, дослідженні ключових проблем у політичній та соціальній сфері, аналізі стратегій і тактик, здійсненні політичних та соціально-економічних перетворень. Одними з головних здобувачів та обробників цієї інформації є РО, за допомогою яких держава дізнається про своє зовнішнє оточення та усвідомлює власні завдання в цій сфері. Відповідно цивільні та військові РО зосереджуються на пошуку, аналізі, використанні інформації, як секретної, так і одержаної з відкритих джерел (OSINT).

Упродовж тривалого часу держави прагнули зберігати за собою монопольне право на ведення розвідувальної діяльності. Проте впродовж першої половини 1990-х років з'явилися приватні структури, які надавали інформаційно-аналітичні послуги, що виходили за межі бізнес-розвідки, не лише великим корпораціям та приватним особам, а й державним структурам. Такі організації отримали назву «приватні розвідувальні компанії» (ПРК), і в цій специфічній сфері діяльності почало розвиватися державно-приватне партнерство. За приблизними даними, у понад 50 державах світу діють близько кілька сотень ПРК [22].

Вагомою причиною залучення ПРК до забезпечення зовнішньої складової частини національної безпеки було те, що приватні структури переважно еластичніші та ефективніші, ніж державні, зокрема в економічних відносинах. Крім того, такий «підряд» ПРК давав можливість знижувати державні видатки на утримання спеціальних служб, а також вирішувати деякі чутливі питання, приховуючи безпосередню причетність держави до них. ПРК пропонують свої послуги не лише державним органам, а й великим корпораціям та окремим споживачам [23].

Родоначальником у системі державно-приватного партнерства у сфері національної безпеки вважаються США, а першої ПРК

– американський дослідницький центр глобальної політики RAND Corporation (Research ANd Development, RAND) [24]. Він був заснований 14 травня 1948 року в Санта-Моніка (Каліфорнія) Генрі Харлі Арнольдом, Дональдом Віллсом Дугласом та Кертісом Лемеєм як партнерство між американськими ВПС та компанією Douglas Aircraft для конструювання літаків, ракетної техніки та супутників. RAND Corporation вважається одним із перших у світі «мозковим центром», чи «інститутом політики» (think tank, policy institute), який надавав військові поради керівництву держави, міністерству оборони.

Історія виникнення RAND Corporation починається з часів Другої світової війни, коли в США була створена велика група переважно вчених та інженерів для реалізації війни на «технологічному фронті». У відносно короткий термін ця група створила такі новинки, як атомна бомба, радар, неконтактний підривач тощо. Також був розроблений і вдало застосований аналітичний метод дослідження операцій, що дозволило підвищити ефективність ППО, бомбометання і військово-морських операцій.

Наприкінці війни, коли цей колектив став розпадатися, військові вирішили зберегти деяких із найбільш талановитих співробітників для продовження розвитку військових технологій. Генерал Генріх Г. Арнольд, командувач ВПС Армії США, створив проєкт RAND із фінансуванням 10 млн дол. з метою довгострокового планування майбутньої зброї. У березні 1946 року компанія Douglas Aircraft отримала контракт на дослідження міжконтинентальної війни, використовуючи дослідження операцій. У травні 1946 року був випущений попередній проєкт експериментального космічного корабля, що облітає світ. 14 травня 1948 року RAND був зареєстрований як некомерційна корпорація відповідно до законів штату Каліфорнія, а 1 листопада 1948 року контракт Project RAND був офіційно переданий від Douglas Aircraft Company до корпорації RAND. Таким чином, проєкт RAND перетворився на незалежну некомерційну організацію RAND Corporation, початковий капітал для якої був наданий Фондом Форда (Ford Foundation).

Першою значною роботою RAND було дослідження, опубліковане як Preliminary Design of an Experimental World-Circling Spaceship (попередній проєкт експериментального космічного

корабля, який обертається навколо Землі). Незважаючи на те, що штучні супутники Землі на той час вважалися науковою фантастикою, у цьому документі 1946 року було вказано: «Супутниковий транспортний засіб із відповідною апаратурою можна вважати одним із найпотужніших наукових інструментів XX століття. Досягнення супутникового судна призведе до наслідків, порівнянних із вибухом атомної бомби...». Вдале пророцтво зміцнило престиж RAND Corporation. У середині 1957 року було спрогнозовано дату запуску першого супутника Землі, з помилкою лише у два тижні.

До кінця 50-х років наукова література визначає різницю між системним аналізом і дослідженням операцій, системним аналізом і системною інженерією, теорією рішень і дослідженням операцій тощо. Широко розглядаються проблеми застосування наукової методології до таких «неточних» сфер, як керівництво, прийняття рішень людиною, організація. Прикладом важливого досягнення RAND Corporation у розв'язанні цих науково-прикладних проблем є розроблення й широке застосування Systems analysis (системного аналізу). Фахівці RAND Corporation виконали низку фундаментальних досліджень і розробок щодо системного аналізу, орієнтованих на вирішення слабо структурованих проблем Міністерства оборони США. Створення у 1952 році надзвукового бомбардувальника B-58 було першою розробкою, що поставлена як система. Усе це вимагало випуску наукової та навчальної літератури.

Перша книга із системного аналізу вийшла у 1956 році. Її видала RAND (автори А. Кан і С. Манн). Методологія системного аналізу була детально розроблена і представлена у I960 році у книзі Ч. Хітча і Р. МакКін «Військова економіка в ядерне століття». У ній також наводиться додаток до методів кількісного порівняння альтернатив для вирішення проблем озброєння. Пізніше Дж. Хітч (помічник Міністра оборони США, Президент Каліфорнійського університету) описав системний підхід до вибору зброї у США.

У 1965 році з'явилася вельми ґрунтовна книга Е. Квейда «Аналіз складних систем для вирішення військових проблем». У ній представлено основи нової наукової дисципліни – аналізу систем. Книга спрямована на обґрунтування методів оптимального вибору при вирішенні складних проблем в умовах високої невизначеності. Ця книга є переробленим викладом курсу лекцій з аналізу систем,

прочитаних працівниками корпорації RAND для керівних фахівців Міністерства оборони та промисловості США.

Цього ж року вийшла книга С. Оптнера «Системний аналіз для вирішення ділових і промислових проблем», яка насичена великою кількістю нових ідей, дає повне й чітке уявлення про системний аналіз із характеристикою проблем ділового світу, сутності систем і методології вирішення проблем. Книга стала однією з перших виданих у нас праць, які висвітлюють стан цієї сфери в США. Навчальні дисципліни з теорії систем і системного аналізу є нормативними та важливими елементами системи навчання в багатьох вищих навчальних закладах світу й України.

Як видно з назв книг, під час розроблення методів системного аналізу для військової сфери з'ясувалося, що проблеми цивільні – проблеми фірм, маркетингу, аудиту та інші теж потребують обов'язкового застосування методології системного аналізу, системного підходу. Системний підхід перетворився на важливий метод пізнання, на відміну від спеціальних прийомів, характерних для розробленя техніки XVI-XIX ст. Це був другий етап історичного розвитку системного підходу в техніці. Розроблено цілу низку вельми складних і тонких математичних методів, зокрема: лінійне програмування, динамічне програмування, визначення черговості проблем, нелінійне програмування, метод Монте-Карло, теорія ігор тощо. У 1957 році в США видана книга System Engineering. An introduction to the design of large-scale systems (Системна інженерія. Вступ до розроблення великих складних систем) Г. Гуда і Р. Макола.

RAND Corporation провела значну роботу з вивчення проблем розповсюдження ядерної зброї, у ході якої здійснювався аналіз економічних, політичних і технічних аспектів створення ядерного потенціалу в різних країнах. RAND Corporation перша серед американських установ почала розробляти науку Холодної війни з використанням методів, які передбачають інтенсивне вивчення потенційного противника «з певної відстані». Також RAND Corporation є розробником концепцій «гнучкого реагування», «контрсили» та інших. Найбільш помітним внеском можна вважати Доктрину взаємного гарантованого знищення (Mutually Assured Destruction, MAD), розроблену під керівництвом тодішнього міністра оборони Роберта Макнамари на основі теорії ігор.

MAD – військова доктрина, згідно з якою застосування двома протиборчими сторонами зброї масового ураження призведе до повного знищення обох сторін, що робить безглуздими будь-які спроби застосування доктрини першого удару. Слово «mad» також означає «божевільний», «несамовитий», а термін MAD ввів Джон фон Нейман – геніальний математик, консультант корпорації RAND. Доктрина взаємного гарантованого знищення є наочним прикладом Рівноваги Неша, за якої жодна озброєна сторона не може ні розпочати безкарно конфлікт, ні роззброїтися в добровільному порядку.

У 1971 році група математиків з RAND Corporation на чолі з Ендрю Маршаллом розробила першу математично обґрунтовану «національну розвідувальну оцінку» (National Intelligence Estimates, NIE), яка містила систематизовані результати обробки розвідувальних та публічних даних, що отримані з різних джерел. Тепер NIE розробляє Національна рада з розвідки для федерального уряду. Це узгоджені судження всіх 18 складових РС США. Видатний аналітик Міністерства оборони США Ендрю Маршалл, який передбачив низку важливих змін у світі, включаючи розпад СРСР, підвищення геополітичної ролі Китаю і широке використання робототехніки у військових операціях, у 1973 році був призначений керівником Управління загального аналізу Пентагону. На цій посаді він пережив Холодну війну, незліченні військові конфлікти і 10 президентських виборів.

Істотний внесок зробила RAND Corporation також у галузі Artificial Intelligence (ШІ). Дослідники RAND розробили багато принципів, що використовувалися для побудови Інтернету. Досвід RAND Corporation у воєнній сфері привів до створення у США відомого у всьому світі Агентства передових оборонних дослідницьких проєктів США (Defense Advanced Research Projects Agency, DARPA). У свою чергу, вдалий досвід DARPA дав змогу створити відповідну структуру для Національної розвідки США (Intelligence Advanced Research Projects Activity, IARPA), а також подібну структуру в цивільних міністерствах (держагенціях), наприклад, Агентство передових досліджень США у сфері освіти (Advanced Research Project Agency for education, ARPA-Ed). Системний підхід привів до відкриття у 2018 році Державного Агентства передових дослідницьких проєктів (Government Advant Research Development Agency, GARDA).

Нині RAND Corporation є одним із найавторитетніших дослідницьких центрів світу в усіх сферах державної політики та управління, національної безпеки та розвідки, від оборони та міжнародних відносин до освіти, охорони здоров'я, містобудівного планування та інфраструктури, транспорту, енергетики, охорони навколишнього середовища, права, демографії, зайнятості тощо. Водночас RAND підтримує тісні неафішовані зв'язки зі своїм основним замовником – ЦРУ. Корпорація має близько 1 700 працівників із 50 країн, які є фахівцями в найрізноманітніших галузях (економіка, психологія, медицина, освіта, інженерія, математика, комп'ютерні технології, міжнародні відносини тощо). Серед співробітників корпорації були таки відомі особи, як професор Френсіс Фукуяма, Державний секретар США Генрі Кіссінджер, міністр оборони і директор ЦРУ Джеймс Шлезінгер, заступник радника президента США з національної безпеки Джеймс Стейнберг, а до складу Ради директорів RAND входили колишні Державний секретар США Кондоліза Райс та міністр оборони США Дональд Рамсфельд. До реалізації різних проєктів корпорації долучалися 30 лауреатів Нобелівської премії.

RAND Corporation має офіси США: Санта-Моніка (штат Каліфорнія), де розташована штаб-квартира та Вища школа Фредеріка С. Парді; Арлінгтоні (штат Вірджинія; Пітсбург, штат Пенсільванія); Бостоні (штат Массачусетс) і Вашингтоні. RAND також має американських дослідників, які живуть і працюють у понад 35 інших штатах та окрузі Колумбія. Крім того, вона має офіси в Кембриджі (Великобританія), Брюсселі (Бельгія); Роттердамі (Нідерланди) та Канберрі (Австралія). Замовниками досліджень RAND виступають уряди та урядові підрозділи різних країн, громадські організації, приватні компанії.

Rand Corporation яскраво характеризує книга, видана у 2008 році під назвою «Soldiers of Reason: The RAND Corporation and the Rise of the American Empire» («Солдати розуму: RAND Corparation і піднесення американської імперії»). Корпорація має за мету міждисциплінарне та кількісне вирішення проблем шляхом переведення теоретичних концепцій із формальної економіки та фізичних наук у нові застосування в інших галузях, використовуючи та розробляючи прикладні наукові дослідження. Значна частина досліджень RAND включає проблеми національної безпеки. Багато подій, у яких RAND

відіграє певну роль, ґрунтуються на припущеннях, які важко перевірити через відсутність деталей роботи RAND для оборонних та розвідувальних органів.

Після розпаду СРСР, уже в нових геополітичних умовах, у 1992 році в штаті Флорида колишніми співробітниками ЦРУ була створена CTC International Group. Імовірно, кадровий склад групи й спричинив обмежену відкриту інформацію про цю ПРК. У короткій рекламі на вебсайті зазначено, що компанія працює у сфері забезпечення безпеки та проведення розслідувань і надає практичну інформацію, щоб навчати клієнтів і допомагати їм приймати обґрунтовані рішення [25]. Очолювана колишніми офіцерами ЦРУ, CTC використовує цикл розвідки, щоб надати приватним клієнтам високоякісні розвідувальні дані, які уряд США використовує для прийняття рішень. Цілеспрямоване дослідження в поєднанні з професійним аналізом дає інтелект, а не просто «інформацію», яка відокремлює «приємно знати» від «необхідності знати». CTC надає розвідувальні дані генеральним директорам, юристам та іншим особам, які приймають рішення і яким потрібна точна, прогнозована та дієва розвідка. Адже знання справді є силою.

Спеціалізація CTC International Group – бізнес-аналітика, конкурентна розвідка, незалежна перевірка компаній, перевірка минулого, стратегічна розвідка, підтримка складних судових розглядів. Штат компанії налічує від 50 до 100 співробітників.

Однією з найбільш відомих та авторитетних ПРК є Strategic Forecasting, Inc. (Stratfor), заснована 1996 року політологом Джорджем Фрідманом [25]. Він на початку 1980-х років почав проводити дослідження з проблематики радянсько-американських відносин. У 1994 році при Університеті штату Луїзіана він заснував Центр геополітичних досліджень, який спеціалізувався на стратегічному прогнозуванні. Протягом 1996–2015 рр. – очолював Stratfor.

На матеріали Stratfor посилаються авторитетні ЗМІ, зокрема CNN, Bloomberg, Associated Press, Reuters, The New York Times, Time та BBC. У 2001 році газета «Barron's» назвала Stratfor «тіньовим ЦРУ». Поступово за своєю впливовістю серед корпорацій і державних організацій та популярністю серед журналістів ця ПРК витіснила RAND. Принципова відмінність Stratfor від RAND полягає в тому, що Stratfor першою створила загальносвітову агентурну

мережу, яка зорієнтована насамперед на корпорації та корпоративний підхід.

Співробітники Stratfor збирають та аналізують інформацію про події у світі, акцентуючи на безпекових питаннях та геополітичних ризиках. Інформацію вони отримують не лише зі ЗМІ та інших відкритих джерел, а й з власних джерел. Фактично це агентурна розвідка (HUMINT). На підставі зібраних відомостей аналітики Stratfor роблять економічні та геополітичні прогнози. Штат компанії налічує близько 100 співробітників.

Крім дослідників різних наукових галузей, Stratfor залучає до роботи експертів із відповідним практичним досвідом. Так, у 2004–2020 рр. віцепрезидентом компанії з питань антитероризму та корпоративної безпеки був Фред Бартон, колишній співробітник Секретної служби США, а пізніше – заступник начальника відділу боротьби з тероризмом Служби дипломатичної безпеки Державного департаменту США. У 2013–2018 рр. віцепрезидентом з питань митної розвідки був Брет Бойд, колишній офіцер Командування спеціальних операцій США.

У 2012 році Stratfor опинилася в центрі скандалу, організованого міжнародною організацією WikiLeaks, яку заснував австралійський журналіст Джуліан Ассанж. Він виклав у відкритому доступі понад 5 млн електронних повідомлень цієї компанії і звинуватив її у відстеженні діяльності міжнародних активістських організацій за дорученням клієнтів ПРК, зокрема компаній «The Dow Chemical Company» та «The Coca Cola Company», а також спецслужб США. У викрадених хакерами матеріалах були згадки й про контакти Stratfor з ізраїльською національною розвідслужбою Моссад. Після скандального витоку даних компанія була змушена запевняти своїх клієнтів, що посилить заходи безпеки, також запропонувала двотижневу безкоштовну передплату на нові розсилки. Зважаючи на напівпублічний характер агентурної мережі компанії, її часткове розкриття не призвело до великих втрат цієї мережі чи до втрати репутації ПРК.

У 2015 році Дж. Фрідман став засновником і керівником нової ПРК –Geopolitical Futures (GPF). Аналіз відкритих публікацій компанії та висловлювань цього провідного експерта свідчить про певні зміни в його політичних симпатіях, що, можливо, і спонукало Дж. Фрідмана піти зі Stratfor, а також про непослідовність у стратегічних прогнозах [26].

У травні 2000 року була створена The Arkin Group LLC (TAG) [27]. Засновники цієї ПРК – колишній начальник глобальних операцій ЦРУ та відомий нью-йоркський юрист Стенлі Аркін. TAG спеціалізується на міжнародному кризовому управлінні, стратегічній розвідці, слідчих дослідженнях та вирішенні бізнес-проблем, що здійснюється у спосіб використання стратегічної інформації, прогностичного аналізу й даних (HUMINT).

Джек Девайн – партнер-засновник та президент TAG є 32-річним ветераном ЦРУ. Він обіймав посади виконувача обов'язків директора та заступника директора з операцій ЦРУ за межами США з 1993 по 1995 рік, де здійснював нагляд над тисячами співробітників ЦРУ, які брали участь у секретних місіях по всьому світу. Крім того, у 1992-1993 рр. Девайн обіймав посаду начальника Латиноамериканського відділу і був головним менеджером секретних проєктів ЦРУ в Латинській Америці. У період із 1990 по 1992 рік Девайн очолював Центр боротьби з наркотиками ЦРУ, який відповідав за координацію та побудову тісної співпраці між усіма основними правоохоронними органами США та інших країн у відстеженні світових наркоторговців та злочинних організацій. З 1985 по 1987 рік очолював Афганську оперативну групу ЦРУ, яка успішно протистояла радянській агресії в регіоні. 1987 року за це досягнення був відзначений нагородою ЦРУ «Заслужений офіцер».

Міжнародний досвід Девайна в уряді США охоплював відрядження до Латинської Америки та Європи. За більш як 30 років роботи в ЦРУ він брав участь в організації, плануванні та виконанні великої кількості секретних проєктів практично у всіх галузях розвідки, включаючи аналіз, операції, технології та управління. Девайн нагороджений медаллю «За видатні заслуги в розвідці» Агентства та кількома почесними нагородами. Він визнаний експерт у питаннях розвідки і писав статті-огляди для The Washington Post, The Wall Street Journal, The Financial Times, Foreign Affairs Magazine, The World Policy Journal, Politico та The Atlantic Monthly. Він також виступав як гість у National Press Club, CNN, CBS, NBC, MSNBC, Fox News, CSPAN, Bloomberg News, а також на каналах History та Discovery, PBS, NPR та ABC Radio.

У приватному секторі Девайн раніше працював у Kohl's Cyber Security Advisory Group, SAP National Security Services (NS2) Advisory

Board, CyberCore Advisory Board та Secretary of Navy Advisory Board. Він проживає в Нью-Йорку і є членом Ради з міжнародних відносин, володіє іспанською та італійською мовами. Книга Девайна «Good Hunting! An American Spymaster's Story», бестселер New York Times, була опублікована в червні 2014 року. Вона присвячена його кар'єрі в Агентстві та ролі таємних операцій у минулому та майбутньому.

Команда TAG об'єднує фахівців із найкращих американських університетів та аспірантських програм і має досвід роботи в ключових державних установах США, міжнародних організаціях і провідних консалтингових фірмах. У своїй діяльності ПРК спирається на широкі національні та міжнародні мережі регіональних і функціональних експертів, у тому числі спеціалістів із розвідки, правоохоронних органів, дипломатів і політиків, промислових, бізнес- і фінансових аналітиків, провідних науковців, журналістів і спеціалізованих експертів із судової експертизи та безпеки. Спеціалізація TAG: бізнес-аналітика, незалежна перевірка компаній, криміналістичні розслідування, стратегічне кризове консультування, аналіз політичних ризиків, безпека та готовність. Місія ПРК – використовувати стратегічну розвідку та прогнозний аналіз, щоб дозволити клієнтам мінімізувати ризики та максимізувати виплати під час прийняття важливих бізнес-рішень. Вона виконала сотні завдань у кожному регіоні Земної кулі. TAG відрізняється індивідуальним підходом та послугами. Для кожного завдання ПРК створює унікальний план гри для досягнення конкретних цілей клієнта. Незважаючи на те, що вона покладається на широкий спектр слідчих, криміналістичних, комунікаційних і безпекових інструментів, відмінними рисами методології TAG є обґрунтований аналіз і добре отримані людські дані.

У лютому 2009 року з'явилася ще одна американська ПРК – The Chertoff Group [28]. Це спеціалізована консалтингова компанія, яка є світовим лідером у сфері безпеки та управління ризиками. Засновниками та основними співробітниками стали колишні високопосадовці США: Майкл Чертофф, міністр внутрішньої безпеки (2005–2009); Майкл Вінсент Хейден, чотиризірковий генерал, директор Агентства національної безпеки (АНБ) (1999–2005), перший заступник директора національної розвідки (2005–2006), директор ЦРУ (2006–2009); Чед Світ, керівник штабу Міністерства внутрішньої безпеки (2005–2009), колишній співробітник

ЦРУ; Чарльз Аллен, заступник міністра внутрішньої безпеки з питань розвідки та аналізу (2005–2009), колишній помічник директора ЦРУ; Джей Коен, контрадмірал, заступник міністра внутрішньої безпеки з питань науки і технологій (2006–2009). Команда визнаних експертів The Chertoff Group із різноманітним досвідом у сфері безпеки в приватному та державному секторах допомагає організаціям керувати кібернетичними, фізичними, регуляторними та геополітичними ризиками. Завдяки практиці розвитку бізнесу вона допомагає своїм клієнтам отримати конкурентну перевагу та прискорити зростання.

До складу Chertoff Group входять:

- інвестиційно-банківська дочірня компанія Chertoff Capital, яка надає консультації щодо злиття та поглинання (M&A, Mergers and Acquisitions) компаніям у сфері оборонних технологій, державних послуг і ринків кібербезпеки;
- Merchant Banking Practice, що має підтверджену історію консультування щодо майже 8 млрд дол. у закритих транзакціях M&A, надає інтегровані інвестиційні банківські послуги та інвестиції капіталу для швидкозростаючих, орієнтованих на місію компаній у сфері національної безпеки, кібербезпеки тощо;
- дочірня компанія MC2 Investment Management, LLC, яка пропонує капітал для зростання через фонд прямих інвестицій MC2 Security Fund, що здійснює інвестиції в акціонерний капітал компаній, котрі швидко розвиваються та мають високий потенціал у сфері кібербезпеки, національної безпеки, оборонних технологій та державних послуг. Фонд безпеки MC2 здійснює інвестиції безпосередньо або через компанії спеціального призначення, такі як MC2 Titanium, LLC.

The Chertoff Group обслуговує підприємства зі списку Fortune 500 у різних секторах, а також малий і середній бізнес зі спеціальними потребами. Робота експертів і фахівців ПРК ґрунтується на передбаченні того, що буде далі, застосуванні передового досвіду та демонстрації цінності. Її досвідчена команда допомагає організаціям керувати кібернетичними, фізичними, транспортними та геополітичними ризиками; розвивати стійкість; орієнтуватися в змінних нормативних вимогах і вимогах відповідності; відкривати можливості для ведення бізнесу та створення цінності.

The Chertoff Group є однією з небагатьох професійних компаній у світі, яка отримала статус БЕЗПЕКИ відповідно до Закону Міністерства внутрішньої безпеки США за перевірену методологію консультування з управління ризиками безпеки. Вона розробила власну методологію, щоб дати можливість організаціям оцінювати, пом'якшувати та контролювати ризики фізичної та кібербезпеки для своїх людей, об'єктів і технологічних активів, а також для бізнес-операцій, які вони підтримують.

Місія The Chertoff Group полягає в застосуванні свого досвіду у сфері безпеки, технологій і політики, щоб допомагати клієнтам створити стійкі організації, отримати конкурентну перевагу та прискорити зростання. Для цього вона має такі можливості:

- 360-градусний огляд ризиків безпеки:
  - глобальне середовище ризиків безпеки;
  - бізнес-ринки та інвестиційні можливості технологій безпеки та безпеки;
  - політична та нормативна взаємодія;
- інтегрована консультативна модель повного життєвого циклу:
  - управління ризиками безпеки;
  - стратегії органічного та неорганічного зростання;
  - події транзакційної ліквідності;
  - інвестування в акціонерний капітал.

Конкурентними перевагами The Chertoff Group є: перевірена методологія консультування з управління ризиками безпеки; продемонстрований успіх у зниженні загального ризику безпеки; надання клієнтам можливості вимірювати та повідомляти про ефективність своїх програм управління ризиками; прагматичний підхід, заснований на досвіді операторів безпеки та розробників політики; можливість перетворити знання безпеки на створення цінності для клієнтів; наявність міцної глобальної мережі стратегічних відносин і надійних партнерів: доступ до великих обсягів капіталу зростання та синдикатів інвесторів.

Оскільки використання ПРК у розвідувальній діяльності США мало й деякі побічні ефекти, то в серпні 2009 року в Національному пресклубі відбулася експертна дискусія, учасники якої обговорили цю проблему з керівниками The Chertoff Group та The Arkin Group.

Експертів насамперед цікавили відповіді на два запитання: чи загрожує інтересам національної безпеки та майбутньому РС така приватизація; а також проблема «переманювання» значної кількості співробітників розвідки до приватних фірм, де вони використовують свої професійні знання та навички. Під час дискусії наводилися дані про те, що розвідувальні служби США передоручають виконувати частину своїх традиційних функцій «підрядникам», на оплату роботи яких витрачаються значні кошти. Зокрема, ЦРУ витрачає понад 30 % річного бюджету. Крім того, ПРК «переманили» дві третини високопоставлених співробітників Міністерства внутрішньої безпеки, які мають широкі контакти в різних колах, значний професійний досвід та знання про механізм роботи державних органів.

Особливо напружені дискусії точилися навколо проблеми секретних програм ЦРУ, у рамках яких, наприклад, ПВК Blackwater USA (із січня 2010 року – Academi) 2004 року отримала контракт на фізичну ліквідацію лідерів Аль-Каїди. За даними американських ЗМІ, метою такого кроку було виведення співробітників ЦРУ з-під можливої кримінальної відповідальності в разі провалу операції чи інших непередбачених обставин.

Учасники дискусії дійшли висновку, що дії «підрядників», яких наймають федеральні органи, повинні відповідати таким же жорстким моральним та юридичним нормам, що й дії співробітників РС. Вирішальним чинником під час наймання ПРК чи окремих осіб є їхня унікальна кваліфікація або навички, на оволодіння якими може піти багато часу. Крім того, до «підрядників» звертаються зазвичай тоді, коли виникає тимчасова потреба в знаннях і вміннях у певній сфері. У цих випадках наймання спеціалістів заощаджує час і ресурси, оскільки «підрядники» не є постійними співробітниками, їх можна легко замінити за потреби. Це особливо актуально, коли законодавці ставлять перед РС завдання, що потребують значних витрат, але при цьому скорочують бюджет.

Як зазначив керівник The Arkin Group Дж. Девін, наприкінці 1990-х років Конгрес скоротив бюджет ЦРУ на 25 %. Це означало, що на момент терактів 11 вересня 2001 року людські та матеріальні ресурси цього розвідувального органу були недостатніми для швидкого й ефективного виконання його функцій. Задля вирішення проблеми керівництво вдалося до масового використання «підряд-

ників». Проте їм передавалися не всі функції, відповідно всередині ЦРУ розроблялися концепції завдань та здійснювався менеджмент і контроль за їхнім виконанням. Водночас Дж. Девін заперечив, що американська розвідка практикувала наймання ПРК для ліквідації терористів (принаймні за час його 32-річної служби в ЦРУ).

Генерал М. Хейден (The Chertoff Group) закликав не проводити межу між державними органами та представниками приватного бізнесу, значна частка яких готова ризикувати без грошової винагороди, щоб допомогти забезпечувати національну безпеку. Він також наголосив, що відсутність вичерпних даних про осіб та компанії, які працюють за урядовими контрактами у сфері розвідки та безпеки, зумовлена необхідністю захисту джерел інформації. Такий підхід має бути зрозумілий, зокрема, представникам ЗМІ, котрі виявляють до цього питання підвищений інтерес.

Нині Велика Британія є лідером у наданні приватних послуг розвідувального характеру на Європейському континенті. За оцінками експертів, кілька років тому бюджет галузі ПРК, розташованих лише в Лондоні, наближався до 20 млрд дол. США. Варто охарактеризувати роботу деяких відомих ПРК, що діють на теренах Великої Британії.

SCL Group (Strategic Communication Laboratories) – приватна британська компанія поведінкових досліджень та стратегічних комунікацій, була зареєстрована в Companies House 20 липня 2005 року Найджелом Оуксом, який був її генеральним директором [29]. Компанія позиціонувала себе як «глобальне агентство з управління виборами». Керівники та власники компанії мали тісні зв'язки з Консервативною партією, британською королівською сім'єю, британськими військовими, Міністерством оборони США та НАТО, а серед її інвесторів були деякі з найбільших спонсорів Консервативної партії.

У 1990 році Найджел Оукс, який мав досвід роботи у сфері телевиробництва та реклами, заснував Behavioral Dynamics Institute (BDI) – Інститут поведінкової динаміки як дослідницький центр для стратегічної комунікації [30]. Оукс вважав, що для зміни громадської думки слід застосовувати академічні ідеї, отримані психологами та антропологами в BDI, і це буде успішнішим, ніж традиційні методи реклами. Вивчення масової поведінки та того, як її змінити, призвело до створення Strategic Communication Laboratories – Лабораторій стратегічної комунікації, а

BDI став її некомерційною філією SCL Group. Серед інвесторів у SCL Group був банкір Пол Девід Ешбернер Нікс, чий син Олександр Нікс мав стати близьким соратником Оукса. Одним із колишніх директорів є лорд Івар Маунтбеттен. Серед інвесторів компанії були Джонатан Марланд, Барон Марланд і Роджер Габб, великий спонсор Консервативної партії, який був зареєстрований як такий, що має значний контроль над компанією станом на 2018 рік.

Після початкового комерційного успіху SCL Group розширила свою присутність на військових та політичних аренах. Вона стала відома передбачуваною участю у військових дезінформаційних кампаніях із брендингу в соціальних мережах та таргетування виборців. SCL Group почала фокусуватися на виборах у країнах, що розвиваються, залучалася їхніми військовими та політиками для вивчення та маніпулювання громадською думкою та політичною волею. Для цього ПРК використовувала те, що називалося «психологічними операціями», щоб отримати уявлення про мислення цільової аудиторії. Вона проводила інтелектуальний аналіз даних та аналіз даних про свою аудиторію. Ґрунтуючись на результатах, націлювала комунікації спеціально на ключові групи аудиторії, щоб змінити поведінку відповідно до вимог своїх замовників. На початок 1990-х років ПРК брала участь у психологічній війні у військових контекстах як підрядник для американських і британських військових під час війни в Афганістані та війни в Іраку.

У 2005 році на виставці Defence and Security Equipment International (DSEI) – найбільшій виставці військових технологій у Сполученому Королівстві, SCL Group продемонструвала свої можливості в «операціях впливу», показавши, як можна допомогти організувати складну кампанію масового обману громадськості такого великого міста, як Лондон. SCL Group стверджує, що її методологію було схвалено, серед іншого, агентствами уряду Сполученого Королівства та федерального уряду США.

Згідно з інформацією на її вебсайті, з 1994 року SCL Group взяла участь у понад 25 міжнародних політичних та виборчих кампаніях та впливала на вибори в Італії, Латвії, Україні, Албанії, Румунії, Південній Африці, Нігерії, Кенії, Маврикії, Індії, Індонезії, Філіппінах, Таїланді, Тайвані, Колумбії, Антигуа, Сент-Вінсенті та Гренадінах, Сент-Кітсі та Невісі, Тринідаді та Тобаго.

У 2013 році SCL Group заснувала дочірню компанію Cambridge Analytica (CA), яка спеціалізується на наданні консалтингових послуг у політичній сфері, використовуючи при цьому технології глибинного аналізу даних, зокрема із соціальних мереж, для розроблення стратегічної комунікації в мережі Інтернет під час виборчих кампаній [31]. Ці технології засновані на алгоритмах, опрацьованих співробітником Кембриджського університету Міхалом Косінським, які дозволяють створювати психологічні портрети користувачів вебресурсів. Ця ПРК була створена для участі у виборчому процесі у Сполучених Штатах та брала участь у 44 виборах до Конгресу США, Сенату США та виборах на рівні штатів на проміжних виборах 2014 року. У 2015 році компанія брала участь у попередніх виборах президента Республіканської партії на виборах 2016 року, насамперед на підтримку Теда Круза.

CA значною мірою фінансувався мільярдером-хедж-фондом Робертом Мерсером, основним прихильником Круза, а потім Дональда Трампа. За повідомленням газети The Guardian, Cambridge Analytica сформувала глобальну мережу своїх джерел, «пустивши коріння» в 68 країнах світу.

Вважається, що саме Cambridge Analytica 2016 року допомогла урядові переконати населення Великої Британії проголосувати на референдумі за вихід із ЄС. В опублікованому через кілька років «Звіті про Росію», підготовленому Комітетом з питань розвідки та безпеки парламенту, ішлося про факти можливого втручання Росії в референдум щодо Брекзиту. У розслідуванні фігурувала й Cambridge Analytica. Варто зазначити, що у 2017 році до послуг цієї компанії звертався російський Сбербанк задля покращення системи оцінювання кредитоспроможності (кредитних ризиків) клієнтів.

У 2018 році Cambridge Analytica опинилася в центрі міжнародного скандалу: стало відомо, що компанія незаконно отримала доступ до даних 87 млн користувачів Facebook, працюючи на виборчу кампанію президента США Дональда Трампа. Крім того, британський телеканал «Channel 4» оприлюднив запис розмов із менеджерами ПРК, з яких можна дійти висновку, що співробітники Cambridge Analytica вдаються до хабарів для дискредитації політичних діячів. Скандал призвів до того, що мережа Facebook закрила доступ до будь-яких послуг для Cambridge Analytica, а сама

компанія опинилася під слідством урядів Великобританії та США. Відтоді компанія була розформована та куплена Emerdata Limited. У 2019 році Федеральна торгова комісія (Federal Trade Commission, FTC) подала адміністративну скаргу на Cambridge Analytica за неправомірне використання даних, одночасно уклавши мирові угоди з її колишнім генеральним директором Олександром Ніксом та розробником додатків Олександром Коганом, у яких вони погодилися видалити незаконно отримані дані.

У 2020 році Олександр Нікс підписав дискваліфікаційне зобов'язання, ухвалене Алоком Шармою, державним секретарем з бізнесу, енергетики та промислової стратегії 14 вересня 2020 року. Починаючи з 5 жовтня 2020 року Олександр Нікс дискваліфікований на 7 років від виконання обов'язків директора або прямої чи непрямої участі без дозволу суду в просуванні, формуванні або управлінні британською компанією.

ПРК Emerdata Limited була заснована в серпні 2017 року групою людей, пов'язаних із Cambridge Analytica: директором за даними та головою материнської компанії Cambridge Analytica SCL Group, яка припинила свою діяльність 1 травня 2018 року [32]. Її штаб-квартира в Лондоні знаходиться в тій самій будівлі, що й Cambridge Analytica. Було зазначено, що компанія пропонує аналогічні послуги, що й SCL Group та Cambridge Analytica.

До ради директорів Emerdata увійшли співробітник Frontier Services Group Джонсон Чун Шун Ко, гонконзький бізнесмен, пов'язаний з Еріком Прінсом (засновником Blackwater), інвестор Cambridge Analytica Ребекка Мерсер і генеральний директор Cambridge Analytica Олександр Нікс. У січні 2018 року Emerdata Limited залучила 19 млн дол. від міжнародних інвесторів і широко обговорювалася в ЗМІ. Її зображували як потенційного наступника Cambridge Analytica. У травні 2018 року Найджел Оукс, засновник SCL Group, британської філії Cambridge Analytica, визнав, що наміром Emerdata було придбати Cambridge Analytica і SCL, але сказав, що ці плани були покинуті, що Emerdata та її частка, що належить дочірній компанії Firecrest Technologies Ltd, яка була створена колишнім генеральним директором Cambridge Analytica Олександром Ніксом, будуть ліквідовані.

У липні 2019 року з'ясувалося, що Emerdata повністю придбала ці компанії, сплачувала юридичні рахунки компаній SCL в

умовах процедур банкрутства, розслідувань та судових позовів по обидва боки Атлантики, а також заплатила мільйони, щоб придбати те, що залишилося від компаній, доки вони перебували в процесі ліквідації.

У контексті дослідження інтерес становить діяльність кількох ізраїльських ПРК. Psy-Group була заснована у 2014 році Рої Бурштейном – колишнім підполковником ізраїльської армії, який очолював спеціальний підрозділ розвідки при уряді країни та згодом став генеральним директором цієї ПРК [33]. Власником був Джоел Замель – австралійський єврей, який розбагатів на видобутку корисних копалин. Серед радників – колишній заступник директора Моссада Рам Бен-Барак, а також Яаков Амідрор – колишній голова Ради національної безпеки при канцелярії Біньяміна Нетаньяху. Юридичний радник компанії – Даніель Рейзнер.

Psy-Group займалася управлінням сприйняттям в Інтернеті, кампаніями із впливу / маніпулювання в соціальних мережах, дослідженнями опозиції, «медовими пастками» та таємними заходами на місцях для клієнтів. Psy-Group інколи називали «приватною службою Моссад».

У 2016 році ПРК запустила проєкт «Метелик», покликаний боротися з BDS на території американських університетів. Psy-Group запропонувала своїм спонсорам підірвати зсередини стабільність організацій, які просувають бойкот Ізраїлю. Співробітники компанії шукали в соціальних мережах та у відкритому доступі, а також у так званій темній мережі (Dark Web) інформацію, що могла б зганьбити активістів BDS або посіяти розбрат у лавах BDS-рухів.

Як приклад журналісти The New Yorker наводять публікації фотографії мусульман, які розпивають алкоголь або змінюють своїх дружин. Результати роботи Psy-Group завжди публікувалися таким чином, щоб їх не можна було пов'язати ні з фірмою, ні з її замовниками. Загалом у проєкт, за даними The New Yorker, було вкладено 2,5 млн дол., і боротьба з BDS поширилася на 10 великих американських університетів.

Psy-Group була фінансово пов'язана з Групою компаній «Метрополь», керівником якої є російський мільйонер Михайло Сліпенчук, колишній депутат Державної думи рф від партії «Єдина Росія». Свого часу Psy-Group надавала послуги російським олігархам Олегу

Дерипасці та Дмитру Риболовлєву, заступникові керівника Служби загальної розвідки Саудівської Аравії генерал-майору Ахмеду аль-Ассірі (причетному до вбивства журналіста Джамаля Хашоґджі) та корумпованому президентові Габону Алі Бонго Ондімбі. Крім того, у червні 2016 році Дж. Замель брав участь у Петербурзькому міжнародному економічному форумі, який проводиться за участю президента рф.

У 2016 році ця ПРК співпрацювала з британською Cambridge Analytica під час виборчої кампанії президента США Дональда Трампа. Джоел Замель зустрічався з Дональдом Трампом-молодшим та Джаредом Кушнером, пропонуючи їм розпочати інтернет-кампанію зі знищення політичної репутації суперників Трампа (співробітники Psy-Group як мінімум один раз провели таку операцію напередодні парламентських виборів в одній з європейських країн). У рамках цієї кампанії використовувалися такі методи: проникнення в цільову аудиторію в соціальних мережах спеціально створених фейкових учасників; поширення оманливої інформації через вебсайти, що імітували новинні портали; дискредитація політичних опонентів завдяки організації вручення хабарів чи звинувачень у сексуальних домаганнях. Діяльність Psy-Group пізніше стала частиною розслідування ФБР та Спеціального комітету в справах розвідки Сенату щодо можливого втручання росії в президентські вибори у США.

У 2017 році ПРК провела кампанію з дезінформації проти українського Центру протидії корупції (ЦПК), спрямовану проти голови правління Віталія Шабуніна та виконавчої директорки організації Дар'ї Каленюк. Організована Psy-Group кампанія з дискредитації членів ЦПК призвела до того, що як мінімум два відео на YouTube поширювали неправдиву інформацію про українських активістів. Два повністю фейкові «випуски англомовних новин» були розміщені на каналі Storozh Ukraina і мають понад 20 000 переглядів, що свідчить про розкручування відео через рекламу. Storozh Ukraina – ще одне анонімне об'єднання громадян, які «викривають» антикорупціонерів.

У березні 2017 року високопосадовці Саудівської Аравії, близькі до наслідного принца Мухаммеда бін Салмана, пропонували кільком ПРК за 2 млрд дол. організувати низку замовних убивств. Зокрема, ішлося про командувача спецпідрозділом «Аль-Кудс» Корпусу стражів Ісламської революції Ірану генерала Касема Сулеймані.

На зустрічі були присутні вищезгадані заступник керівника Служби загальної розвідки Саудівської Аравії генерал-майор Ахмед аль-Ассірі та Дж. Замель, який нібито відмовився від такої пропозиції. Але слід зазначити, що К. Сулеймані був ліквідований 3 січня 2020 року точковим авіаударом ВПС США. За деякими даними, інформацію про місцезнаходження генерала американській стороні надала служба Моссад.

У 2018 році, після того, як діяльністю Psy-Group зацікавилася комісія спеціального прокурора Роберта Мюллера, Дж. Замель був змушений її закрити, і окремі співробітники перейшли до компанії Black Cube, діяльність якої пов'язана зі справою Харві Вайнштейна та зі збиранням компромату на Барака Обаму. Натомість сам Дж. Замель залишається керівником Групи компаній «Zamel», до складу якої входить ПРК Wikistrat, заснована 2010 року в США [34]. У 2014–2017 рр. її директором зі стратегічного розвитку був колишній співробітник ізраїльської розвідки Шая Гершковіц. Напрям діяльності Wikistrat: геостратегічний консалтинг із використанням краудсорсингу (залучення широкого кола осіб для використання їхніх творчих здібностей, знань та досвіду на кшталт субпідрядної роботи на добровільних засадах із застосуванням інформаційних технологій).

ПРК White Knight Group, яка фактично є правонаступницею Psy-Group, була заснована у 2017 році [35]. Спеціалізація цієї ПРК: кампанії в соціальних мережах, акції впливу, управління виборчими кампаніями. Група також є активним інвестором у транснаціональні інфраструктурні проєкти, включно зі сферою розвитку ШІ та сектором кібербезпеки, особливо для компаній Центральної та Східної Європи. Подібні до Psy-Group методи: онлайн-управління сприйняттям, вплив через соціальні мережі, маніпулятивні кампанії, стратегічна дезінформація (наприклад, підготовка фейкових новин чи пропагандистської продукції), політичні кампанії з використанням соціальних медіа та ШІ. Те саме використовують інші ізраїльські ПРК – Archimedes Group та Black Cube [36, 37].

Тактика діяльності Archimedes Group, орієнтованої на низку африканських держав, Латинську Америку та Південно-Східну Азію, дуже нагадує тактику інформаційної війни, яку часто використовують уряди окремих країн, зокрема росії. Зі свого боку, Black

Cube прослуховувала неурядові організації Угорщини напередодні виборчої кампанії навесні 2018 року з метою зібрати компромат для передання штабу прем'єр-міністра країни Віктора Орбана.

Деякі ПРК спеціалізуються на технічному забезпеченні розвідувальної діяльності. Однією з них є ізраїльсько-американська Verint Systems Inc., яка існує з 1994 року, штат оцінюється у 5–10 тис. співробітників [38]. 2017 року вона купила невелику ПРК «Terrogence», створену в 2005 році колишнім офіцером контррозвідки «Шин Бет» Шаєм Арбелем [39]. Обидві компанії активно укладають контракти з урядом США щодо забезпечення АНБ та інших спецслужб новітніми шпигунськими технологіями. Серед таких технологій – сервіс «Face-Int», призначений для розпізнавання облич, заснований на базі даних багатьох тисяч осіб, які підозрюються в протиправній діяльності. ПРК «Terrogence» активно відстежувала та збирала в Інтернеті інформацію про терористів та інших осіб, які становили загрозу національній безпеці (зокрема, у сфері безпеки авіаперевезень, імміграції тощо). Джерелами таких даних називалися мережі YouTube, Facebook, а також різні відкриті та закриті форуми. У квітні 2018 року інформація про сервіс «Face-Int» зникла із сайту Terrogence, проте можна вважати, що компанія й досі продовжує надавати такі послуги, а як джерела інформації використовує більше ресурсів, ніж офіційно було відомо. Точно невідомо, на базі якої технології сервіс «Face-Int» отримує зображення облич, але опис програми нагадує один із проєктів АНБ США (National Security Agency, NSA), розкритий Едвардом Сноуденом у 2014 році. Ця спецслужба за три роки існування проєкту зібрала 55 тис. якісних знімків розпізнаних облич. Схоже, що Terrogence порушує політику Facebook, згідно з якою заборонено використання для стеження за користувачами даних, отриманих із соціальної мережі. Не дозволяється також використання будь-яких автоматизованих методів збирання інформації, наприклад ботів.

Немає свідчень про те, що американський уряд може використовувати сервіс «Face-Int», проте відкриті дані свідчать про наявність у компанії «Terrogence» принаймні двох державних контрактів із ВМС США на загальну суму майже 150 тис. дол. Ця сума еквівалентна річній передплаті на два сервіси цієї ПРК – «Mobius» та «TGAlertS». Сервіс «Mobius» є добіркою матеріалів із різних соці-

альних мереж та платформ про останні тренди щодо вибухових пристроїв, створених терористами, та способів їхнього застосування, а «TGAlertS» містить оперативну інформацію про деякі важливі події, отриману співробітниками Terrogence з Інтернету.

Хоча основним напрямом діяльності Terrogence є співпраця з розвідслужбами та правоохоронними органами для боротьби з тероризмом, проте у профілях колишніх співробітників компанії у LinkedIn можна знайти згадки про «роботу з громадською думкою для урядових клієнтів» та використання «методів роботи в соціальних мережах для вивчення політичних та соціальних груп».

Ще одним напрямом діяльності ПРК, подібних до Terrogence, що викликає занепокоєння громадськості, є створення різних «чорних списків». У 2018 році Verint запустила іншу програму розпізнавання облич – «FaceDetect», яка уможливлює ідентифікацію людини, незважаючи на її національність, будь-які перешкоди, старіння об'єкта, маскування, і миттєво вносить дані до реєстру осіб, які розшукуються. Основною проблемою подібних реєстрів, котрі створюють держави, є алгоритм потрапляння до них конкретних людей та сфера застосування зібраних даних.

У лютому 2021 року Amnesty International повідомила, що Verint Systems надала Службі національної безпеки Південного Судану обладнання для перехоплення каналів зв'язку. Цю спецслужбу звинувачують у переслідуванні, залякуванні, свавільному затриманні та, у деяких випадках, насильницькому зникненні, навіть убивствах політичних противників режиму.

Об'єднані Арабські Емірати (ОАЕ) також мають свою ПРК DarkMatter Group (DarkMatter), яка заснована в 2014 році еміратським бізнесменом Фейсалом аль-Баннаі, засновником постачальника мобільних телефонів Axiom Telecom и сином генерал-майора поліції емірату Дубая [40]. Ця ПРК позиціонувала себе як компанія з комп'ютерної безпеки, що займається виключно оборонними заходами, але деякі експерти стверджують, що DarkMatter причетна до «наступальних» заходів, тобто зламу комп'ютерних мереж, кібернетичних атак, незаконного отримання доступу до даних у мережі Інтернет, зокрема в інтересах уряду ОАЕ. У тому ж 2014 році розпочала свою діяльність у Фінляндії дочірня компанія DarkMatter – Zeline 1. Свій штат вона формувала з колишніх співробітників АНБ

та офіцерів технічних підрозділів Армії оборони Ізраїлю, пропонуючи їм до 1 млн дол. на рік.

Публічний старт DarkMatter відбувся у 2015 році на 2-му щорічному саміті Arab Future Cities. На той час компанія рекламувала такі можливості, як мережева безпека та усунення помилок, а також обіцяла створити новий «захищений» мобільний телефон і позиціонувала себе як «цифрова оборонна та розвідувальна служба» для ОАЕ.

У 2016 році з'явилися повідомлення про те, що компанія CyberPoint, яка працювала на уряд ОАЕ, уклала контракт з італійською компанією – розробником шпигунського програмного забезпечення Hacking Team, що підірвало репутацію CyberPoint як фірми, що займається кібербезпекою. ОАЕ, незадоволені тим, що покладаються на американського підрядника, замінили CyberPoint на DarkMatter, яка стала підрядником проєкту Raven замість компанії CyberPoint. Цей проєкт був конфіденційною ініціативою, покликаною допомогти владі ОАЕ стежити за урядами інших країн, терористами та політичними противниками. До його команди входили колишні агенти розвідки США, які застосовували свою підготовку для зламання телефонів та комп'ютерів, що належать жертвам проєкту Raven. Операція проводилася в переобладнаному особняку в передмісті Абу-Дабі в Халіфа-Сіті, яке називалося «Вілла». Проєкт Raven виник у 2008 році як Відділ досліджень, експлуатації та аналізу розвитку (Department of Research, Exploitation, Analysis and Development, DREAD), створений Річардом А. Кларком через його консультативну групу з безпеки Good Harbor Consulting як підрозділ королівського двору ОАЕ Мохамеда бін Заїда Аль Нахайяна. До кінця 2010 року Good Harbor відійшов від DREAD, поступившись контролем Карлу Гамтоу, співзасновнику та генеральному директору CyberPoint. З 2014 до 2016 року CyberPoint постачала проєкту Raven підрядників, навчених у США. Після цього проєкт Raven розширив своє стеження, включивши до неї американців, що потенційно залучали її американських співробітників до протиправної поведінки. Наприклад, DarkMatter зламав електронне листування між першою леді Мішель Обамою та колишнім міністром Катару щодо поїздки Мішель Обами та Конана О'Браєна до Катару в листопаді 2015 року. Обама та О'Брайєн відвідали ави-

абазу Аль-Удейд, на якій розміщується передова штаб-квартира Центрального командування США та 83-тя експедиційна авіагрупа Королівських ВПС. Крім того, авіабаза служила штаб-квартирою Центрального командування ВПС США під час воєн в Іраку та Афганістані. DarkMatter був дуже зацікавлений у зламі комп'ютерів Катару, щоб отримати та прочитати його електронні повідомлення, оскільки вважалося, що Катар підтримує братів-мусульман. Після публікації статті The Intercept від 24 жовтня 2016 року, де розкривається стеження DarkMatter, Самер Халіфе, фінансовий директор DarkMatter, перевів деяких громадян США з DarkMatter до нової компанії Connection Systems.

Того ж року проєкт Raven купив інструмент під назвою Karma. Karma могла віддалено експлуатувати Apple iPhone у будь-якій точці світу, не вимагаючи жодної взаємодії з боку власника iPhone, доки було вказано ім'я користувача, таке як Apple ID, адреса електронної пошти, пов'язана з телефоном, або номер телефону. Оперативники проєкту Raven могли переглядати паролі, електронні листи, текстові повідомлення, фотографії та дані про місцезнаходження зі скомпрометованим iPhone. Серед людей, чиї мобільні телефони були навмисно зламані за допомогою Karma, були Емір Катару шейх Тамім бін Хамад Аль Тані, Хамад бін Халіфа Аль Тані, а також його брат та кілька інших наближених; Надя Мансур, дружина ув'язненого активіста з прав людини з ОАЕ Ахмеда Мансура; британський журналіст Рорі Донагі; прем'єр-міністр Лівану Саад Харірі; Лауреат Нобелівської премії з Ємену Тавакуль Карман (лідер Арабської весни); сотні інших користувачів айфонів у Європі та на Близькому Сході, включаючи уряди Катару, Ємену, Кувейту, Оману, Сербії, Лівану, Ірану та Туреччини.

Також у 2016 році DarkMatter шукала експертів із розроблення смартфонів в Оулу (Фінляндія) та найняла кількох фінських інженерів. Вона розробила модель смартфона під назвою Katim, що в перекладі з арабської означає «тиша». У 2021 році кіберактивність DarkMatter була передана компанії Digital14 із штаб-квартирою в Абу-Дабі, яка поширювала захищену систему зв'язку «Katim». Digital 14 позиціонує себе як одна з провідних компаній із кібербезпеки на Близькому Сході, що обслуговує клієнтів із державних, енергетичних, транспортних, фінансових та медичних секторів.

На початку 2018 року оборот DarkMatter становив сотні мільйонів доларів. Відомо, що 80 % контрактів ПРК припадає на урядові структури ОАЕ, включно з Агентством радіотехнічної розвідки (Radio Intelligence Agency, RIA), раніше відомим як Національне управління електронної безпеки (National Electronic Security Authority, NESA). Ця спецслужба є розвідувальною агенцією ОАЕ – аналогом АНБ, яка створена в 2011 році за допомогою США у відповідь на ймовірне кібершпигунство з боку Ірану.

У 2018 році Фейсал аль-Баннаї підтвердив, що DarkMatter дуже тісно співпрацювала з урядом ОАЕ та була конкурентом ізраїльської фірми NSO Group. Із січня 2016 року по листопад 2019 року завдяки своїм експертам – колишньому співробітнику АНБ Марку Байєру, а також Райану Адамсу та Деніелові Геріці, які працювали у військових та розвідувальних колах США, значно покращило послуги, які DarkMatter надавала уряду ОАЕ.

У січні 2020 року, на підставі матеріалів розслідування ФБР, зокрема щодо DarkMatter, за такими злочинами, як послуги цифрового шпигунства, участь у вбивстві Джамаля Хашоггі та позбавлення волі іноземних дисидентів Конгрес США ухвалив закон, запропонований у 2019 році конгресменом Максом Роузом із Нью-Йорка. Закон вимагає від РС щорічно оцінювати загрози національній безпеці, що можуть виникати через діяльність колишніх співробітників розвідки, які після звільнення зі служби працюють на іноземні фірми, організації та уряди.

У 2021 році Луджайн аль-Хатлул подала позов до окружного суду США в Орегоні проти трьох колишніх офіцерів розвідки та армії США, які проводили хакерські операції від імені ОАЕ. Згідно з позовом троє чоловіків – Марк Байєр, Райан Адамс і Деніел Геріке – працювали на DarkMatter і допомагали співробітникам служби безпеки Еміратів витягувати дані з її iPhone. Злам призвів до арешту аль-Хатлул в ОАЕ та видачі до Саудівської Аравії, де її затримали, ув'язнили і катували.

14 вересня 2021 року Марку Байєру, Райану Адамсу та Денієлу Геріке були пред'явлені звинувачення в порушенні законів США, пов'язаних із комп'ютерним шахрайством та неналежним експортом технологій. Вони погодилися на відстрочення судового переслідування в обмін на: сплату штрафів у розмірі 750 000, 600 000 та

335 000 дол. США протягом трьох років відповідно на загальну суму 1,68 млн дол. США; підтримку розслідувань ФБР та Міністерства юстиції; розрив зв'язків із будь-якими розвідувальними та правоохоронними органами ОАЕ; підпорядкування заборони на послуги, включаючи оборонні статті, що підпадають під Міжнародні правила торгівлі зброєю (International Traffic in Arms Regulations, ITAR), та майбутню роботу з експлуатації комп'ютерних мереж; відмова від своїх допусків до секретної інформації у США та будь-якої іноземної організації; прийняття довічної заборони майбутніх допусків до секретної інформації із США.

У грудні 2021 року американські законодавці закликали Міністерство фінансів та Державний департамент увести санкції проти DarkMatter, NSO Group, Nexa Technologies та Trovicor. У листі, підписаному головою фінансового комітету Сенату Роном Уайденом, головою комітету з розвідки Палати представників Адамом Шиффом та 16 іншими законодавцями, містилося прохання про запровадження глобальних санкцій Магнітського, оскільки компанії звинувачували у сприянні порушенням прав людини.

Підсумовуючи, можна зробити висновки, що для будь-якої держави стратегічно важливою є обізнаність із подіями та процесами, які відбуваються поза її межами, але можуть становити інтерес для вироблення тактики та побудови стратегії для відповідного реагування. Діяльність ПРК є вагомою із цієї точки зору. ПРК часто випереджають спецслужби у створенні та застосуванні новітніх технологій у своїй діяльності. Ці організації виступають не лише виконавцями замовлень державних структур, а й об'єктами, котрі становлять розвідувальний інтерес для інших країн для отримання інформації, якою вони володіють. ПРК можуть бути використані для ведення політичної боротьби. Тому їхня діяльність повинна здійснюватися під контролем із боку держави на основі спеціально створеного законодавства. Україні варто вивчати зарубіжний досвід функціонування ПРК та використовувати його для зміцнення національної безпеки держави.

Висновки до четвертого розділу

Аналіз останніх подій свідчить про трансформацію поглядів на завдання та функціонування розвідки.

Ключовими перевагами проривних технологічних інновацій у розвідувальній діяльності є такі:

БПЛА та супутники, які забезпечують ефективний та економний моніторинг у режимі реального часу, зменшуючи ризики для військовослужбовців;

нові розробки в галузі сенсорних технологій, які розширюють можливості добування інформації розвідкою для виявлення, ідентифікування та відстеження потенційних загроз;

наземні радари спостереження із вбудованими сучасними алгоритмами обробки сигналів, які дають можливість виявляти переміщення особового складу і транспортних засобів на великих відстанях, забезпечуючи системи раннього попередження;

застосування алгоритмів ШІ, що дає можливість обробляти значні обсяги даних, зібраних системами спостереження, виявляючи закономірності й аномалії, які аналітики можуть пропустити;

використання алгоритмів машинного навчання, що дає змогу в автоматичному режимі виявляти та класифікувати загрози, допомагаючи збройним силам ефективно реагувати на ситуацію;

проведення аналітики великих даних, щоб, проаналізувавши результати моніторингових спостережень, отримати цінну інформацію, яка дасть змогу прийняти оптимальні рішення та планувати майбутні військові операції.

Аналітичні дискурси та безпосередні розвідувальні практики західних країн дозволяють твердити про те, що сучасна розвідка мислиться як складний, багатопрофільний, наукоємний процес, що вимагає постійної трансформації «педагогіки розвідки» задля підготовки ефективних – мультипрофільних – фахівців, стійких психологічно та фізично, науково та фахово спроможних до збирання, розуміння, інтеграції та передавання даних із багатьох джерел, як і проведення стратегічної розвідки, здійснення прогнозування (узявши до уваги виклики з майбутнього), спираючись на можливості ШІ та ін.

Положення «Білої книги з питань європейської оборони – Готовність 2030» свідчать про те, що ЄС, зважаючи на випадки вторгнення рф в інші країни та її нинішню політику експансії, сприймає росію як «екзистенційну загрозу для Євросоюзу». Зміни в підходах США до безпеки Європи визначаються як реальність, яку необхідно враховувати, однак НАТО, як і раніше, «залишається наріжним каменем колективної оборони». Загальна політична рівновага, що встановилася після завершення Другої світової війни, «незворотно порушена». Формування нового світового порядку – це нова реальність, яка постане в короткостроковій перспективі, відповідно Європа повинна стати активним його творцем, а не пасивним «споживачем наслідків».

Дослідження державно-приватного партнерства у сфері розвідувальної діяльності на прикладі найвідоміших ПРК США, Великої Британії, Ізраїлю, ОАЕ показало, що вони виступають виконавцями замовлень державних структур як здобувачі та обробники розвідувальної інформації, за допомогою якої держава дізнається про своє зовнішнє оточення та усвідомлює власні завдання в цій сфері. Також ПРК можуть бути використані для ведення політичної боротьби, тому їхня діяльність повинна здійснюватися під контролем із боку держави на основі спеціально створеного законодавства.

Перелік використаних джерел:

1. Стратегічні пріоритети політико-правового розвитку України в контексті європейської інтеграції: монографія / кол. авт.; за ред. І. О. Кресіної. Київ : Інститут держави і права імені В. М. Корецького; Київ, Норма права, 2024. 858 с.

2. Михальченко М. Інтереси національні. Політична енциклопедія. редкол. : Ю. Левенець, Ю. Шаповал та ін. Київ : Парламентське вид-во, 2011. 808 с.

3. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV. URL: http://zakon2.rada.gov.ua/laws/show/964-15 (дата звернення: 10.04.2025).

4. Глобальна та національна безпека / за заг. ред. Г. Ситника. Київ : НАДУ при Президентові України, 2016. 784 с.

5. Olga Reznikova, Volodymyr Smolianiuk. Konceptual Issues of National Security Policy-Making Under Uncertainty. Vilnius University Press. Politologia. 2023/3. Vol. 111, pp. 41–73.

6. Крутій В. О. Трансформація політичної системи суспільства в умовах гібридної війни : автореферат дис. … к. політ. н. 23.00.02. Київ : Інститут держави і права ім. В. М. Корецького НАН України, 2018. 19 с.

7. Цимбал І. В., Жовтун А. А., Ліманська О. Л. Світ VUCA як сучасний контекст інформаційних і суспільно-політичних змін. Науковий часопис НПУ ім. М.Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. 2015. Вип. 17. С. 43–47.

8. Догадайло Я. В., Лаптєва У. Д. Передумови виживання у VUCA-світі. URL: https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/84eefdbd-cc81-4de7-a728-80cfa34781cf/content (дата звернення: 20.03.2024).

9. Штучний інтелект як чинник забезпечення національної безпеки: монографія / Алєксєєнко І. В., Дзядук Д. О., Кармазіна М. С., Лисецький Ю. М., Мокляк С. П., Смолянюк В. Ф., Ткач І. М.; за заг. ред. С. П. Мокляка. – Київ : Видавець Бихун В. Ю., 2025. 228 с.

10. Burns William J. A World Transformed and the Role of Intelligence. 59th Ditchley annual lecture. URL: https://www.ditchley.com/sites/default/files/ Ditchley%20 Annual%20Lecture%202023%20transcript.pdf (дата звернення: 20.03.2024).

11. Burns William J. Spycraft and StatecraftTransforming the CIA for an Age of Competition. URL: https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns?fbclid=IwAR2eojU8rT8_C_uoLwvD6YXGBCWZIStTorpkiuB4QDLkC_xfVC4ZTMNVJA4 (дата звернення: 20.05.2025).

12. Annual threat assessment of the U.S. intelligence community. March 2025. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf (дата звернення: 20.05.2025).

13. JOINT WHITE PAPER for European Defence Readiness 2030. Brussels, 19.03.2025. URL: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf (дата звернення: 20.05.2025).

14. Концепція завершення бойових дій НАТО. URL: https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/ (дата звернення: 20.05.2025).

15. Вінчі Е. Майбутня революція в справах розвідки. Як штучний інтелект і автономні системи змінять шпигунство. URL: https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs (дата звернення: 20.05.2025).

16. Intelligence Analysis in the Digital Age. 1st Edition, Kindle Edition / Stig Stenslie (Editor), Lars Haugom (Editor), Drigt H. Vaage. Routledge, 2021. 194 p.

17. Hammond-Errey M. Big Data, Emerging Technologies and Intelligence: National Security Disrupted. 1st Edition, Kindle Edition. Routledge, 2024. 212 p.

18. Private Eyes in the Sky. How Commercial Satellites Are Transforming Intelligence. URL: https://www.foreignaffairs.com/world/private-eyes-sky?check_logged_in=1 (дата звернення: 20.05.2025).

19. Spies, Lies, and Algorithms. Why U.S. Intelligence Agencies Must Adapt or Fail. URL: https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms (дата звернення: 20.05.2025).

20. National Intelligence Strategy 2023. URL: https://www.dni.gov/-index.php/newsroom/reports-publications/reports-publications-2023/3713-2023-national-intelligence-strategy (дата звернення: 15.09.2024).

21. IC Data Strategy 2023-2025. URL: https://www.dni.gov/files/ODNI/-documents/IC-Data-Strategy-2023-2025.pdf (дата звернення: 15.09.2024).

22. Приватні розвідувальні компанії: іноземний досвід залучення приватного сектору до виконання завдань розвідки. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/pryvatni-rozviduvalni-kompaniyi-inozemnyy-dosvid-zaluchennya (дата звернення 20.05.2025).

23. Семенюк Ю. В., Лисецький Ю. М. Державно-приватне партнерство у сфері національної безпеки. Держава і право. 2025. Випуск 97. С. 118–146.

24. Погляд з України на американську корпорацію «солдатів розуму» RAND Corporation. URL: https://dss-bi.blogspot.com/2019/01/rand-corporation.html. CTC International Group. URL: https://ctcintl.com/ (дата звернення: 20.05.2025).

25. Strategic Forecasting Inc. URL: https://stratfor.com/ (дата звернення: 25.05.2025).

26. Geopolitical Futures (GPF). URL: https://geopoliticalfutures.com/welcome/ (дата звернення: 25.05.2025).

27. The Arkin Group. URL: https://thearkingroup.com/ (дата звернення: 27.05.2025).

28. The Chertoff Group. URL: https://thearkingroup.com/ (дата звернення: 27.05.2025).

29. Strategic Communication Laboratories. URL: https://www.devex.com/organizations/strategic-communication-laboratories-41754 (дата звернення: 29.05.2025).

30. Behavioral Dynamics Institute. URL: https://behavioraldynamicsinc.com/ (дата звернення: 29.05.2025).

31. Cambridge Analytica. URL: https://uk.wikipedia.org/wiki/Cambridge_Analytica (дата звернення: 05.06.2025).

32. Emerdata Limited. URL: https://en.wikipedia.org/wiki/Emerdata_Limited (дата звернення: 06.06.2025).

33. Psy-Group. URL: https://en.wikipedia.org/wiki/Psy-Group (дата звернення: 08.06.2025).

34. Wikistrat. URL: https://en.wikipedia.org/wiki/Wikistrat (дата звернення: 10.06.2025).

35. White Knight Group. URL: http://www.whiteknight.asia (дата звернення: 12.06.2025).

36. Archimedes Group. URL: https://en.wikipedia.org/wiki/Archimedes_Group (дата звернення: 14.06.2025).

37. Black Cube. URL: https://www.blackcube.com/ (дата звернення: 16.06.2025).

38. Verint Systems Inc. URL: https://en.wikipedia.org/wiki/Verint_Systems (дата звернення: 18.06.2025).

39. Terrogence Ltd. URL: https://www.bloomberg.com/profile/company/1251707D:IT (дата звернення: 20.06.2025).

40. DarkMatter Group. URL: https://en.wikipedia.org/wiki/DarkMatter_Group (дата звернення: 20.06.2025).

Наукове видання

Семенюк Юрій Володимирович, Мокляк Сергій Петрович,
Лисецький Юрій Михайлович

НОВА ГЕОМЕТРІЯ МІЖНАРОДНИХ ВІДНОСИН ТА РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

Монографія

За загальною редакцією Мокляка Сергія Петровича

Літературний редактор, коректор – А. В. Галушкіна
Комп'ютерна верстка, макетування – В. Ю. Бихун
Дизайн обкладинки – О. О. Старовойтенко

Підп. до друку 10.12.2025. Формат 64х90/16.
Папір крейдований. Друк офсетний.
Ум. друк. арк. 14,17. Тираж 500 прим. Зам. № 12/2

Видавець Бихун В. Ю.
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./ факс: +38 044 235 75 28
моб.: +38 050 310 22 04
e-mail: lk@ukr.net