Інформаційно довідкові матеріали до лекції “Війна за незалежність у контексті нової генерації гібридних воєн”

Тривалість: 1 академічна година (60 хв — 80 хв).

1. Мета лекції

Пояснити сутність гібридної та багатодоменної війни у Війні за незалежність.

Сформувати у слухачів розуміння того, як Війна за незалежність України виходить за межі суто військових дій.

Показати роль інформації, технологій та українського суспільства у захисті державності.

2. Основні питання для розкриття

а) **Поняття “гібридна” та “багатодоменна” війна**.

Поняття гібридної війни увійшло у науковий і військово-політичний дискурс на початку XXI століття, коли стало очевидно, що класичні підходи до війни — з чітким фронтом, формальним оголошенням, воєнним і мирним станом — перестали описувати реальність. “Гібридна війна” означає конфлікт, у якому держава або недержавний актор застосовує поєднання традиційних і нетрадиційних засобів впливу: військових, політичних, економічних, інформаційних, кібернетичних, культурних та релігійних.

Її суть полягає не у тотальному знищенні противника, а у контролі над свідомістю, ресурсами і простором впливу, що досягається без офіційного стану війни. Традиційна армія у такій моделі лише один з інструментів — поряд із пропагандою, дезінформацією, економічним тиском, диверсіями, кібератаками, підривом політичної єдності та довіри до інститутів держави.

Теоретично цей тип війни окреслив генерал Френк Гоффман у 2007 році, описавши “гібридні загрози” як одночасне використання конвенційних та неконвенційних методів, коли ворог діє “під порогом” прямої війни, але з ефектом повномасштабного конфлікту. На практиці ці принципи чітко проявилися під час російської агресії проти України у 2014 році: анексія Криму без формального вторгнення, створення “внутрішнього повстання” у Донбасі, масовані інформаційно-психологічні операції та атаки на українські IT-інфраструктури.[https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf]

Сучасне розуміння гібридної війни еволюціонувало у концепцію багатодоменної війни (Multi-Domain Warfare). Цей термін використовується у стратегіях НАТО та армії США і означає ведення бойових дій одночасно у п’яти взаємопов’язаних просторах — доменах: наземному, повітряному, морському, космічному та інформаційно-кібернетичному.

У класичній війні перевага визначалася кількістю військ і техніки; у багатодоменній війні вирішальним стає швидкість інтеграції — здатність поєднати розвіддані із супутників, роботу безпілотників, кібероперації, психологічні кампанії та дії на полі бою в єдину систему. Тобто поле бою більше не обмежується географією — воно охоплює інформаційний простір, кібермережу, суспільну думку і навіть економічні ланцюги.

Українсько-російська війна 2014–2025 років стала наочним прикладом такого типу конфлікту. Вона ведеться не лише на фронті, а й у сфері енергетики, культури, міжнародного права, цифрової безпеки. росія використовує багатодоменність для підриву української державності — від атак на енергетичні мережі до спроб дискредитації України в медіа, водночас застосовуючи ракети, безпілотники, найманців і пропагандистські кампанії.

Для України багатодоменна війна означає новий рівень синхронізації військових, ІТ, дипломатичних і громадських структур, коли ефективність визначається не лише кількістю зброї, а здатністю координувати дії у різних середовищах.

Отже, гібридна війна — це спосіб ведення конфлікту, де межа між миром і війною стирається; багатодоменна війна — це технологічне і стратегічне продовження цієї ідеї, де боротьба відбувається у всіх просторах одночасно. Обидві моделі вимагають від суспільства не тільки військової сили, але й інтелектуальної, моральної та психологічної стійкості, бо вирішальна битва у XXI столітті відбувається не лише за території — а за свідомість. Приклад: дії ЗСУ у 2022–2023 рр., коли оборона фізичної території супроводжувалася кіберзахистом, протидією фейкам, боротьбою за інформаційну ініціативу.

[https://www.act.nato.int/activities/multi-domain-operations/?utm_source]

б) **Відмінність від класичних воєн**.

Класичні війни, як їх розуміли у XX столітті, мали чітку логіку та структуру: оголошення війни, мобілізація армій, фронт, бойові дії, перемир’я, мирний договір. Конфлікт відбувався у визначеному просторі, між двома або більше державами, і мав зрозумілу мету — захоплення території, ліквідацію противника, зміну уряду або встановлення контролю над ресурсами. Такі війни мали форму “зіткнення армій”, де успіх залежав від чисельності, технічного переважання, дисципліни та логістики.

Сучасні гібридні та багатодоменні війни суттєво відрізняються від цього зразка. Вони не мають чітких меж у просторі, часі чи навіть у визначенні “ворога”. Головна мета — не знищення противника, а деморалізація, дестабілізація, підрив суспільної єдності та руйнування політичної волі до спротиву. У таких війнах перемога — це не лише військовий результат, а насамперед контроль над інформаційним простором і сприйняттям реальності.

У класичній війні фронт був фізичним — лінія зіткнення між арміями. У сучасній війні фронт став розмитим і багатовимірним: він проходить через

телеефір, соціальні мережі, економіку, енергетичні системи, міжнародні організації. Сьогодні “удар по тилу” може означати кібератаку на державні реєстри або масовану інформаційну кампанію, яка послаблює довіру до влади чи армії.

Ще одна принципова відмінність — участь недержавних акторів. Якщо у класичній війні діяли регулярні війська, то у гібридній — важливу роль відіграють приватні військові компанії, терористичні угруповання, медіаструктури, хакерські спільноти, впливові бізнес-групи. Ворог більше не завжди одягнений у військову форму, а його атака може бути спрямована на фінансову систему чи суспільні настрої.

Класична війна передбачала певну “чесність правил” — дотримання Женевських конвенцій, обмін полоненими, захист цивільних. У гібридній війні межі моралі розмиті: ворог може заперечувати свою участь, використовувати цивільне населення як прикриття, а пропаганду — як зброю. Російська агресія проти України стала яскравим прикладом цього: “зелені чоловічки” без розпізнавальних знаків, “народні республіки”, фейкові референдуми — усе це елементи, несумісні з класичною моделлю війни, але ефективні в умовах інформаційної асиметрії.

Ще один ключовий момент — зміна часу реакції. Класичні війни дозволяли стратегічне планування на місяці чи роки. У гібридних конфліктах рішення приймаються в реальному часі: одна публікація у соцмережі, одне відео з фронту або одна кібератака можуть змінити перебіг операцій. Тому головним ресурсом стає не лише озброєння, а швидкість комунікації, аналітична спроможність і технологічна інтеграція.

Крім того, сучасна війна ведеться не лише проти армії, а проти суспільства як системи. Класичний ворог атакував військові об’єкти; новий ворог б’є по ментальних, культурних і духовних орієнтирах — підриває довіру, сіє апатію, змушує людей сумніватися у власній державі. Це робить боротьбу складнішою, бо вона вимагає не лише зброї, а й психологічної, моральної та інформаційної готовності всього населення.

Таким чином, відмінність гібридних і багатодоменних воєн від класичних полягає у тому, що війна більше не має початку і кінця у традиційному розумінні. Вона триває постійно — у формі змагання за вплив, інформацію, ресурси й довіру. У XXI столітті переможе не той, хто має більше танків, а той, хто краще координує дії у всіх доменах — від кіберпростору до свідомості людини.

в) **Взаємодія п’яти доменів: сухопутного, повітряного, морського, космічного та інформаційно-кібернетичного**.

Багатодоменна війна — це не просто одночасне використання різних видів збройних сил, а синхронізована взаємодія всіх середовищ ведення бойових дій, де успіх у кожному домені підсилює інші. Такий підхід змінив саме уявлення про

поле бою: воно більше не обмежується землею, морем чи небом, а охоплює кіберпростір, орбіту та інформаційну сферу.

1. Сухопутний домен. Це класична основа війни, де відбувається фізичне зіткнення противників. У сучасних умовах сухопутні війська залишаються ключовим чинником контролю території, однак їхня ефективність тепер залежить від інтеграції з технологіями спостереження, розвідки, навігації та зв'язку. Український досвід показує, що навіть невелика група на землі може діяти з високою точністю, якщо має доступ до розвідувальних даних із безпілотників або супутників. Таким чином, класичне "панування на полі бою" замінилося поняттям "мережево-центричної взаємодії".

2. Повітряний домен. Повітряний простір залишається критичним для мобільності, вогневої підтримки й розвідки. Але сучасна війна перетворила його на середовище безпілотних систем і високоточної зброї. Дрони різних класів — від розвідувальних "Лелек" до ударних "Байрактарів" і FPV-дронів — змінили тактику ведення бою. Вони стали "очима" для артилерії, інструментом швидкої реакції та навіть носієм інформаційного ефекту: відео з ураженням техніки противника має не лише тактичну, а й психологічну цінність. Повітряна перевага тепер досягається не лише кількістю літаків, а ефективністю взаємодії повітряних і кіберсистем управління.

3. Морський домен. Море традиційно вважалося сферою великих флотів, але багатодоменна війна радикально змінила баланс сил. Україна продемонструвала, що навіть без повноцінного флоту можливо досягати значних результатів за рахунок інновацій і асиметричних рішень — морських дронів, крилатих ракет, цілевказання через супутники. Удар по крейсеру "Москва" став символом переходу до нової морської стратегії, де вирішальне значення мають точність, інформаційна координація та інтеграція з іншими доменами. Морський простір перетворився з "океану бойових кораблів" на мережу мобільних платформ, зв'язаних з інформаційною інфраструктурою.

4. Космічний домен. Космос сьогодні — це не лише сфера наддержав, а життєво важливий шар сучасної війни. Супутникові системи забезпечують навігацію, зв'язок, спостереження й передачу розвідувальних даних у реальному часі. Для України співпраця з компаніями типу Maxar або використання Starlink стали фактично елементами оборони. Без супутникових даних неможливо ефективно координувати артилерію, відстежувати пересування противника чи забезпечувати стійкий зв'язок під час кібератак. Космос більше не є абстрактним простором — це плацдарм інформаційної переваги, що з'єднує всі інші домени в єдину систему.

5. Інформаційно-кібернетичний домен. Цей домен став центральним у сучасній війні. Саме тут вирішується, хто контролює реальність і наратив. Кібератаки на енергетичні об'єкти, інформаційні операції у соцмережах, поширення фейків, "зливи" розвідданих — усе це частини однієї стратегії. Інформаційно-кібернетичний домен не існує окремо від фізичного: він підсилює

або паралізує інші середовища. Наприклад, кібератака може вивести з ладу системи управління ППО, а інформаційна кампанія — посіяти паніку в тилу.

У межах багатодоменної операції дані з усіх джерел — супутників, дронів, наземних сенсорів, аналітичних платформ — об'єднуються в єдину інформаційну мережу. Це створює "цифровий фронт", де головна зброя — швидкість ухвалення рішень і точність даних.

Сутність взаємодії доменів. Ключова ідея полягає в тому, що жоден домен не діє ізольовано. Успіх сухопутних військ залежить від розвідки з повітря й космосу. Ефективність повітряних операцій визначається кіберживучістю систем управління. Морські дрони діють завдяки супутниковій навігації. Інформаційна кампанія може підкріпити або зруйнувати військовий ефект на полі бою. Така інтеграція перетворює сучасну війну на динамічну систему взаємопов'язаних середовищ, де фізичні дії та інформаційні впливи відбуваються одночасно. Український досвід довів: перевагу здобуває не той, хто має більше ресурсів, а той, хто здатен координувати п'ять доменів у єдиному темпі, з єдиною метою і спільним інформаційним полем.

г) **Підготовка рф до агресії (інформаційна, політична, енергетична, культурна експансія до 2014 року).**

Російська агресія 2014 року не стала раптовим актом, а була результатом багаторічної системної підготовки, що охоплювала всі сфери суспільного життя — від політики й економіки до інформаційного простору та культури. Москва цілеспрямовано вибудовувала багаторівневу систему впливу, створюючи умови для гібридної війни задовго до її відкритої фази.

1. Політична експансія: мережа впливу та "контроль через залежність". Починаючи з початку 2000-х, Кремль активно використовував "м'яку політичну інфільтрацію" — підтримку проросійських партій, лідерів громадської думки, бізнес-груп, орієнтованих на москву. Через енергетичні угоди, спільні економічні проєкти, а також дипломатичні формати (як-от СНД або "русскій мір") Росія поступово інтегрувалася у внутрішню політику України. Ключовим інструментом стало використання корупційних і олігархічних зв'язків, що дозволяли впливати на рішення національного рівня. Через політичні угруповання та проросійські медіа просувалися тези про "нейтралітет України", "позаблоковий статус", "братські народи". Це створювало враження, ніби російська присутність є природною частиною української державності.

2. Інформаційна експансія: формування наративів і контроль над медіа. До 2014 року російські інформаційні кампанії вже системно працювали в Україні.

Основна мета — підрив української ідентичності та дискредитація західного курсу. Через телеканали, соціальні мережі, "експертні клуби", культурні фонди поширювалися такі меседжі: Україна — "штучна держава"; НАТО — "загроза миру"; росія — "захисник православ'я та слов'янської єдності"; Майдан — "хаос, інспірований Заходом". Ці наративи формували інформаційне середовище

подвійної лояльності, у якому велика частина населення Сходу та Півдня сприймала Україну як частину “спільного простору з росією”. Паралельно велася інформаційна деморалізація армії — поширювалися фейки про “недієздатність ЗСУ”, “зраду командування”, “застарілість озброєння”. Це була частина гібридної доктрини, спрямованої на руйнування довіри до власних інститутів.

3. Енергетична залежність як інструмент шантажу. Енергетика стала основною важелем політичного тиску. Газові угоди 2006 та 2009 років, залежність від російського імпорту нафти та ядерного палива створили для Кремля реальний інструмент впливу на економічну стабільність України.

росія використовувала постачання енергоносіїв не як комерційний, а як стратегічний ресурс, нав’язуючи вигідні для себе умови в обмін на політичні поступки — наприклад, продовження базування Чорноморського флоту в Севастополі (Харківські угоди 2010 р.).Таким чином, енергетична залежність стала формою “геоекономічного контролю”, коли економічний тиск створює умови для політичного шантажу.

4. Культурна експансія: “русскій мір” як ідеологічна зброя. Одним із найнебезпечніших напрямів була культурно-ідеологічна експансія, що діяла під гаслом “спільної історії” та “єдиного духовного простору”. Через освітні програми, релігійні інституції, пропаганду “Великої Вітчизняної війни” росія послідовно розмивала українську національну ідентичність. Церковні структури Московського патріархату, мережі культурних центрів, спільні телепроєкти створювали ментальну основу для прийняття російського впливу. Так формувалася “гібридна окупація свідомості”: ще до появи військових у Криму та на Донбасі частина населення вже була підготовлена психологічно.

5. Військово-стратегічна підготовка: “маскування під партнерство”. У військовій сфері росія діяла приховано, використовуючи співпрацю в межах СНД та двосторонніх угод. Через спільні навчання, кадрові обміни, програми підготовки офіцерів вона отримувала доступ до українських систем оборони та розвідки. У той же час проводила модернізацію власних сил за принципом гібридної війни — розвиток ССО, кіберпідрозділів, приватних військових компаній, інформаційних операцій. Ключова ідея полягала у створенні “керованого хаосу”: коли перед військовим вторгненням держава-жертва вже ослаблена інформаційно, політично та економічно. Саме тому агресія 2014 року виглядала блискавичною — бо ґрунт для неї готувався понад десятиліття.

Підготовка рф до агресії була комплексною гібридною операцією, що поєднала інформаційно-психологічні, економічні, політичні та військові методи. Її мета — не лише захопити територію, а зруйнувати ідентичність, довіру та спроможність України чинити опір. Від 2000-х до 2014 року Росія формувала поле, на якому мала відбутися “операція впливу”, — і коли настав момент, використала всі домени одночасно.

Напрям впливу	Ключові дії Російської Федерації	Мета / Наслідок для України

Політична експансія	• Підтримка проросійських партій і політиків (“Партія регіонів”, КПУ) • Використання корупційних зв’язків і бізнес-груп для просування кремлівських інтересів • Просування ідеї “позаблокового статусу” України • Участь у проросійських міждержавних об’єднаннях (СНД, ЄЕП)	Формування політичної залежності, нейтралізація проєвропейського курсу, підрив державного суверенітету
Інформаційна експансія	• Контроль і фінансування медіа (телеканали, онлайн-платформи, газети) • Пропаганда наративів “спільної історії”, “братських народів”, “захисту російськомовних” • Дискредитація НАТО, ЄС і демократичних реформ • Поширення фейків, маніпуляцій, антиукраїнських меседжів	Підрив національної ідентичності, створення двоякої лояльності, деморалізація суспільства
Енергетичний тиск	• “Газові війни” 2006 і 2009 рр. • Політичні умови енергетичних угод • Маніпуляції тарифами та постачанням енергоносіїв • Харківські угоди (2010): продовження базування ЧФ рф у Севастополі	Енергетична залежність як форма шантажу, контроль над стратегічною інфраструктурою
Культурна та ідеологічна експансія	• Просування концепції “русского міра” • Домінування російського продукту у ЗМІ, кінематографі, книговиданні • Вплив через церкву Московського патріархату • Маніпуляції навколо “спільної історичної пам’яті” (Друга світова війна, “Антифашизм”)	Розмивання української культурної ідентичності, створення “ментальної залежності” від рф
Військово-стратегічна підготовка	• Спільні навчання у межах СНД • Агентурна робота, проникнення у структури безпеки • Нарощення присутності ЧФ у Криму • Створення сучасних Сил спеціальних операцій (ССО), кіберпідрозділів, ПВК • Нарощення військових баз поблизу кордонів України	Підготовка до швидкої окупаційної операції, створення умов для “керованого хаосу”
Кібернетичний та інформаційно-психологічний вплив	• Хакерські атаки на держустанови (зокрема 2007–2013 рр.) • Випробування методів кібератак на інфраструктуру (енергетика, зв’язок)	Відпрацювання сценаріїв гібридної війни, формування системи впливу на громадську думку

	• Запуск фабрик тролів та ботоферм • Тестування ІПсО на прикладі Грузії (2008 р.)	

д) **Еволюція бойових дій: від анексії Криму до повномасштабного вторгнення (20014—2025).**

Еволюція бойових дій у протиріччі між рф і Україною пройшла кілька чітко відокремлених, але взаємопов'язаних етапів. Кожен з них підкреслював зміну способів застосування сили, поєднання гібридних інструментів та адаптацію сторін до нових умов війни.

1. Початковий етап — "Низькоінтенсивна" гібридна операція (2014).

Анексія Криму (лютий–березень 2014) і події на Донбасі показали нову модель: використання безпозначених підрозділів, інформаційних кампаній і політичних провокацій задля швидкого захоплення критичної інфраструктури. Це була операція "під порогом": відсутність офіційного оголошення війни, маніпуляції з місцевим населенням, створення маріонеткових формувань. Тактика характеризувалася швидкими, локальними операціями, мінімальним застосуванням масової військової сили і широким використанням інформаційних та політичних інструментів.

2. Період позиційної війни і "фіксації фронту" (2014—2021). На Донбасі сформувалися стабільні лінії зіткнення, де гострі бої перемежовувалися тривалими періодами позиційної протидії. Характерною стала статика — траншеї, укріплення, артилерійські дуелі. Водночас противник вдався до постійних ІПСО (інформаційно-психологічних операцій) і кібератак, що підривали критичну інфраструктуру та мораль. Українські підрозділи вивчали тактику контрбатарейної боротьби, розвідки, адаптувалися до роботи у складних умовах "сірого" фронту.

3. Підготовчий та тактичний розвиток (2018—2021). Обидві сторони модернізували підготовку: росія розвивала ССО, ПВК, кіберпотенціал; Україна — мобілізаційні механізми, волонтерські мережі і "нові" моделі постачання (приватні поставки, міжнародна технічна допомога). Також відбувся перехід до більш інтегрованого застосування БПЛА (розвідка, корегування вогню, удари).

4. Повномасштабне вторгнення (лютий 2022) — від масованого наступу до адаптивної оборони. Вторгнення 2022 року ознаменувало повернення до масштабного застосування сили, але з урахуванням усіх набутих гібридних практик. Характерно: масовані ракетні удари по інфраструктурі, авіація, бронетанкові угруповання на кількох напрямках. Однак українська оборона виявилася здатною до швидкої адаптації: використання мережевої розвідки, мобільних ракетних і артилерійських підрозділів, високоефективна робота безпілотників. Багато бойових дій набули маневреного, імпульсивного характеру — дрібні штурми, контрудари, рейдові операції на тилах ворога.

5. Техніко-тактична трансформація (2022—2025). У цьому періоді війна стала по-справжньому багатодоменною: синхронне використання супутникових даних, дронів, контрбатарейних радарів, артилерії високої інтенсивності та кібероперацій. Безпілотники стали не лише розвідувальним інструментом, а й ефективною ударною силою (малокаліберні FPV, ударні "розвідувально-ударні" комплекси). Артилерія й далекобійні засоби зросли в ролі — рішення бою все частіше ухвалюється на основі точності виявлення цілей та швидкості передачі даних. Логістика стала критичним фактором: руйнування опорних пунктів постачання, атаки на мости й депо змінювали темп кампаній.

6. Асиметричні та спеціальні операції, інформаційна війна. Окрім суто військових дій, розгорнуто широкомасштабну інформаційну кампанію, кібератаки на держсервіси та енергетику, цілеспрямовані операції щодо підриву громадського порядку. Водночас Україна розвинула потенціал цивільного спротиву: волонтерські ланцюги, народна мобілізація, швидкі ремонти інфраструктури та системи гуманітарної допомоги.

Еволюція бойових дій у Війні за незалежність демонструє перехід від прихованих гібридних операцій до відкритих багатодоменних кампаній, де технологія й суспільний настрій стають такими ж важливими, як і чисельні сили.

е) **Приклади взаємодії кібер- і військових операцій** кіберпростір став одним із ключових театрів сучасної війни — невидимим, але вирішальним. Його взаємодія з класичними бойовими діями дедалі тісніша: кібератаки готують або супроводжують удари по фізичних цілях, впливають на командування, зв'язок, логістику, мораль населення. В умовах російсько-української війни (2014—2025) ця інтеграція набула безпрецедентної глибини і стала прикладом того, як військові та кібероперації зливаються в єдину багатодоменну систему.

1. Початок — кіберудари як елемент гібридної агресії (2014–2016). Під час анексії Криму рф уперше комплексно застосувала кіберзасоби разом із фізичними діями. До початку захоплення адмінбудівель у Сімферополі було зафіксовано збої в українських телекомунікаційних мережах, атаки на урядові сайти та спроби паралізувати зв'язок між Києвом і півостровом. Паралельно велися інформаційно-психологічні операції (ІПСО): російські ресурси поширювали дезінформацію про "масові переходи українських військових на бік РФ", створюючи ефект хаосу й деморалізації. Усе це дозволило окупанту діяти швидко і без офіційного оголошення війни — класичний приклад "кіберрозм'якшення" перед захопленням території.

2. Перші масштабні кібератаки проти критичної інфраструктури. У грудні 2015 року росія здійснила першу у світі кібератаку, яка спричинила фізичне знеструмлення частини українських регіонів. Хакери групи Sandworm (підконтрольної ГРУ) зламали системи енергокомпаній і віддалено вимкнули підстанції. Цей інцидент став прецедентом — кібератака фактично виконала функцію артилерійського удару, не руйнуючи об'єкти, але виводячи їх із ладу.

У 2016 році повторний удар по енергомережі (“Industroyer”) засвідчив розвиток російських можливостей — кібератаки почали плануватися в координації з військовими навчаннями поблизу кордонів.

3. NotPetya (2017): кіберзброя стратегічного масштабу. У 2017 році РФ провела одну з наймасштабніших у світі кібератак — NotPetya, яка спочатку націлювалася на українські компанії, але згодом вийшла за межі країни. Вона паралізувала роботу державних установ, банків, транспортних компаній, портів, лікарень. За задумом — це була кіберпідготовка до можливого загострення бойових дій: удар по економіці, управлінню та логістиці. NotPetya показала, що кіберзасоби можуть виконувати стратегічні цілі, аналогічні ракетним ударам — але без прямої видимості.

4. Початок повномасштабного вторгнення (2022): синхронізація ударів. 24 лютого 2022 року, за кілька годин до вторгнення, Україна зазнала серії масштабних кібератак: зламано сайти уряду, банків, медіа; атаковано супутникові комунікації Viasat, які забезпечували зв’язок військових; розповсюджено фальшиві повідомлення про “здачу влади”; спроби зламати системи управління енергетикою та транспортом. Це була координація кібер- і кінетичних операцій: кібератаки мали дезорганізувати управління, ускладнити комунікацію між підрозділами, а також створити паніку серед цивільних. Такий підхід повністю відповідає концепції “багатодоменної війни”, де кібероперації є рівноправним інструментом збройної боротьби.

5. Українська кібероборона і кіберконтрнаступ. На противагу цьому, Україна розвинула потужну систему кібероборони та кіберрозвідки. Було створено Кіберкомандування Збройних Сил, Державну службу спецзв’язку, ініційовано “ІТ-Армію України” — спільноту волонтерів і фахівців, які здійснюють контркібератаки проти російських урядових структур, банків, пропагандистських ресурсів. [https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf?utm_source]

Важливим стало також використання OSINT (відкритих джерел розвідки): дані з соцмереж, супутникові знімки та відео дозволяли швидко виявляти позиції противника.

Кібервплив поєднувався з військовими діями: наприклад, виявлення координат складів боєприпасів через цифрові сліди користувачів у Telegram чи “Яндекс.Картах” призводило до точкових ударів артилерії або ракет.

6. Кібератаки як доповнення до артилерійських і ракетних ударів. З 2022 по 2025 рік спостерігається тенденція попереднього кіберприглушення перед ударами. Наприклад, перед атаками на енергетичну систему восени 2022 року відбувалися хакерські вторгнення у мережі “Укренерго” та обленерго. Мета — сповільнити реакцію диспетчерів, ускладнити перерозподіл навантаження після ударів ракетами. Таким чином, кібердія стала частиною “пакету ураження” —

подібно до роботи радіоелектронної боротьби, але на рівні цифрової інфраструктури.

7. Громадянський вимір і психологічні операції. Кібервплив поширюється й на інформаційно-моральну площину. Злами державних і медіасайтів супроводжуються публікацією фейкових “звернень” або “наказів”, покликаних деморалізувати суспільство. У перші дні війни такі фальшивки мали створити відчуття неминучої поразки, але згодом українська аудиторія стала значно більш стійкою до таких маніпуляцій.

Взаємодія кібер- і військових операцій сьогодні — це не допоміжна функція, а повноцінний бойовий домен. Вона забезпечує: розвідку і наведення для ударів; руйнування логістичних і комунікаційних систем противника; інформаційно-психологічний вплив на населення і військових; підтримку оборони критичної інфраструктури. Український досвід став світовим прикладом ефективної інтеграції кібер- та кінетичних дій. Війна майбутнього вже відбувається не лише на полі бою, а й у мережевих середовищах, де перемогу визначають не лише ракети й гармати, а швидкість коду, алгоритмів і рішень.

є) Інформаційний фронт та кібербезпека.

Інформаційний фронт у сучасній війні давно перестав бути другорядним полем боротьби — він став центральним компонентом загальної стратегії, на якому вирішується, як сприйматимуться події, хто контролюватиме наратив і наскільки стійкою буде суспільна підтримка оборони. Ще до відкритої фази агресії проти України московська пропаганда системно формувала сприятливе інформаційне середовище: через теле- та інтернет-платформи просувалися наративи про “загрозу Заходу”, “історичну спорідненість” і сумніви в легітимності проєвропейського курсу. Таке інформаційне підготування створювало ґрунт для подальших дій — анексії, дестабілізації та локальних окупацій — ілюструючи, що інформація може виконувати роль підготовчого “м’якого удару”, який значно полегшує застосування фізичної сили. Кібербезпека при цьому не є лише технічним захистом мереж: це захист економіки, державного управління та довіри громадян, бо кібератаки на енергетику, банківські системи чи державні реєстри мають прямий вплив на здатність держави функціонувати і на упевненість людей у завтрашньому дні. Український досвід показав, що кібероперації супроводжують і готують кінетичні удари: перед масштабними ракетними атаками чи ударами по енергосистемі відбувалися вторгнення в мережі, спроби вивести з ладу диспетчерські системи або паралізувати комунікацію, що значно посилювало ефект від фізичного ураження. Водночас інформаційні кампанії, фейкові “заявлення” й масові вкиди в соцмережах мали на меті посіяти паніку, дискредитувати владу або викликати внутрішні розколи — отже, інформація та кібердії працюють у єдиному комплексі. Реакція України була комплексною: державні установи налагодили оперативні комунікації, журналісти та OSINT-

спільноти почали документувати злочини й оперативно верифікувати факти, волонтерські ІТ-спільноти й державні структури формували потужну систему кібероборони. У відповідь на кібератаки виникли нові форми протидії — координація військових, цивільних експертів і волонтерів, використання відкритих джерел і супутникових даних для швидкого виявлення цілей і коригування дій. Це показало, що успіх у кібер- та інформаційному просторі залежить не лише від технологій, а й від організаційної здатності держави та суспільства діяти в унісон: швидка, прозора і правдива комунікація значно знижує ефективність ворожих ІПсО (інформаційно-психологічних операцій). Наративна перевага, яку забезпечують чесні й зрозумілі повідомлення, сприяє мобілізації підтримки, зменшує паніку й уповільнює поширення фейків. Крім цього, медіаграмотність і цифрова гігієна населення в умовах гібридної агресії стають елементом національної оборони: перевірка джерел, уважність до неперевіреної інформації, відмова від поширення сумнівних повідомлень — усе це практичні кроки, які рятують життя. [https://www.president.gov.ua/documents/472017-21374]

ж) Як формується громадська думка під час війни.

Формування громадської думки під час війни — складний і динамічний процес, у якому емоції, довіра до джерел інформації та вплив лідерів думок відіграють важливу роль. На відміну від мирного часу, коли люди схильні аналізувати події раціональніше, у період збройного конфлікту суспільство живе в умовах постійної невизначеності, небезпеки та інформаційного тиску. Це створює середовище, де емоції часто стають головним чинником сприйняття реальності, а не факти.

Емоції під час війни мають потужний мобілізаційний ефект. Вони перетворюються на інструмент управління поведінкою мас — як із боку держави, так і з боку ворога. Почуття страху, болю, ненависті або гордості впливають на те, як громадяни сприймають події на фронті, дії політичного керівництва, а також власну роль у суспільному процесі. Ворог свідомо намагається викликати відчай, зневіру й втому — через інформаційно-психологічні операції, фейки, маніпуляції, спрямовані на розкол суспільства. Натомість українські комунікації мають протилежну мету — зміцнювати віру в перемогу, підтримувати стійкість, консолідувати громадян навколо спільних цінностей і захисту державності.

Довіра до джерел інформації стає ключовим елементом інформаційної безпеки. У час, коли кількість повідомлень вимірюється мільярдами на день, а штучно створені акаунти поширюють маніпуляції, громадяни мають навчитися розпізнавати надійні джерела. Український інформаційний простір із 2022 року пережив суттєву трансформацію: традиційні медіа поступово поступилися місцем онлайн-платформам і соціальним мережам, де інформація поширюється миттєво, але часто без перевірки. Це породжує феномен "інформаційних

бульбашок" — коли користувачі отримують лише ту інформацію, яка підтверджує їхні власні переконання. Саме тому держава, журналісти, аналітики й волонтери активно працюють над створенням системи перевірених комунікацій — офіційних каналів, які формують довіру та задають стандарти достовірності.

Не менш важливою є роль лідерів думок — військових, волонтерів, журналістів, митців, науковців, які здатні достукатися до емоцій і свідомості аудиторії. Під час війни лідери думок перетворюються на комунікаторів між фронтом і тилом, між подією й суспільством. Їхня щирість, досвід і послідовність створюють те, чого не може дати жодна офіційна структура — емоційну довіру. Люди схильні сприймати інформацію через особисті історії, тому розповіді ветеранів, волонтерів чи журналістів із зони бойових дій мають значно більший вплив, ніж сухі зведення.

російська федерація, своєю чергою, використовує принципи інформаційної війни для підриву довіри до українських джерел — поширює фейки, дискредитує військове керівництво, створює фальшиві "альтернативні" медіа. Її мета — посіяти сумнів і страх. Українська ж стратегія полягає у зміцненні інформаційного імунітету суспільства — навченні критичного мислення, формуванні звички перевіряти факти, підтримці відкритості й чесності у комунікації.

Таким чином, громадська думка під час війни — це не просто сукупність переконань. Це жива система, в якій кожна емоція, слово, фото чи історія впливають на стійкість держави. Там, де люди довіряють своїм захисникам, державі й правді, інформаційна зброя ворога втрачає силу. Емоції, довіра та авторитет лідерів думок у цей час стають не слабкістю, а щитом — тим, що допомагає суспільству вистояти й не дати ворогу перемогти у свідомості, перш ніж він буде розбитий на полі бою.

з) Приклади російських ІПсО.

Типові наративи, які використовує росія, — це не просто слова, а готові сценарії для дії: наприклад, "війна США руками України" має на меті показати, що Україна нібито лише ширма для іноземних інтересів; "Захід втомився" покликаний посіяти сумнів у довготривалості підтримки західних партнерів; теза про "ТЦК буціфікацію" працює як жахастик про втрату свободи. Ці меседжі часто виглядають по-різному — в телевізорі, у соцмережах, у коментарях — але завжди мають одну мету: підірвати довіру, посіяти паніку або розколоти суспільство.

Як створюються фейки — механіка по кроках. По-перше, ідея: інформаційні служби формулюють "наратив" — просту емоційну тезу, яку легко поширити. По-друге, фабрика контенту: професійні копірайтери, дизайнери, відеомонтажери готують "докази" — скриншоти, "витоки", відео з відредагованим контентом, підроблені документи. По-третє, запуск через

мережу джерел: замість одного повідомлення створюють багато ілюзійних підтверджень — фейкові сайти, "альтернативні" телеграм-канали, сторінки у соцмережах. По-четверте, розкрутка: бот-мережі й "фабрики тролів" координовано поширюють матеріал, купують рекламу, вкидають хештеги, піднімають тему у тренди. По-п’яте, ескалація: коли тема набирає охоплення, пропагандистські телеканали й авторитетні для цільової аудиторії ресурси підхоплюють її, надаючи "весомість". Нарешті — поступове "закріплення" наративу через повторення, меми, імітацію громадського обговорення.

Фабрики тролів (контент-центри) працюють за відпрацьованою схемою: сотні чи тисячі акаунтів, керованих людьми або напівавтоматично, публікують узгоджені меседжі, відповідають на протилежні думки, посилюють поляризацію. Бот-мережі (автоматичні аккаунти) допомагають зробити ілюзію масової підтримки — лайки, репости, коментарі за кілька секунд після публікації. Комбінація людей і ботів дає потрібний ефект: живий тон коментарів + швидке штучне розповсюдження.

Фальшиві джерела — окрема категорія: підроблені новинні сайти (з доменами, схожими на авторитетні), псевдоекспертні блоги, "громадські організації" з вигаданими контактами. Вони виглядають правдиво: мають логотип, шапку, надають "електронні копії документів". Щоб збільшити правдоподібність, застосовують техніки: SEO-просування, купівлю банерів на місцевих сайтах, перепост у локальних чатах. Часто підробка супроводжується "витоком" — нібито внутрішньою перепискою чи аудіозаписом, змонтованим так, щоб видати бажаний зміст.

Технічні прийоми: масова реєстрація акаунтів, використання проксі та VPN для маскування географії, генерація фальшивих фото/відео (статичні кадри вирізаються й монтуються у нові сюжети), deepfake для підробки голосу чи обличчя, маніпуляція метаданими файлів, "сейв-фото" з чужих подій, підміна заголовків у цитованих повідомленнях. Соціальні платформи використовують алгоритми, які підсилюють віральний контент: достатньо первинного імпульсу від ботів — і алгоритм саме розкрутить матеріал як популярний.

Координація й тактика: кампанія ретельно таргетує аудиторії — наприклад, мовні та регіональні групи, ветеранів, молодь, батьків. Для кожної групи готують свою форму меседжу: прагматична риторика для бізнесу, емоційні історії для сімей, "експертні" доповіді для політично підкованих. Одночасно працюють "підсилювачі": коментатори, лідери думок (інколи куплені), які створюють видимість незалежної підтримки.

Навіть якщо фейк розвінчують, шкода може бути зроблена — довіра до інституцій падає. Тому важливі контрзаходи: швидка й прозора офіційна комунікація, проактивний моніторинг соцмереж, розкриття механіки фейків, підвищення медіаграмотності населення.

Механіка ІПсО — це поєднання творчості (контент), техніки (боти, deepfake), соціальної інженерії (таргетинг) і технологічних можливостей

(алгоритми платформ). Ефективна протидія вимагає не тільки технічного блокування, а й системної інформаційної політики: правдива, швидка, локалізована комунікація; навчання громадян; прозоре розслідування інцидентів.

и) Ветеран як носій досвіду нової війни.

Ветеран Війни за незалежність — це не просто учасник бойових дій, а носій унікального досвіду, який поєднує реалії фронту, технологічних і психологічних викликів, а також глибоке розуміння суті державності під тиском гібридних загроз. Він є живим свідком епохи, коли війна вже давно не обмежується лінією зіткнення, а проходить крізь інформаційний простір, економіку, культуру, щоденне життя. Його роль — це роль медіатора між тими, хто воює, і тими, хто живе у відносному спокої. Саме через ветеранів суспільство отримує чесну, нефільтровану картину війни, зв'язок із тими, хто щодня ризикував життям заради держави.

На відміну від традиційного уявлення про ветерана як "учасника минулого", ветеран Війни за незалежність — це учасник теперішнього. Його досвід не завершується демобілізацією. Він несе у собі системні знання про нову форму конфлікту — багатодоменну, де реальний і віртуальний фронти злиті воєдино. Він бачив, як рішення у соцмережах можуть коштувати життів, як інформаційний вкид паралізує тил, як точність дронів чи цифрових карт змінює тактику бою. Цей досвід є унікальним і спілкування з носієм такого досвіду є важливою складовою у підготовці до національного спротиву.

Ветеран стає посередником між військовими і цивільними. Він пояснює, що означає "стійкість", не як гасло, а як умови виживання. Через його наратив формується колективне розуміння війни — не як "далекої події", а як реальності, у якій держава і кожен громадянин мають свою відповідальність.

Його роль у суспільстві багатовимірна. Він може бути волонтером, політиком, аналітиком, підприємцем чи митцем, але у кожній сфері несе головне — практичний досвід шляхетності, який не купується і не вивчається теоретично. Саме тому ветеран є природним носієм національної пам'яті, морального авторитету та референтної точки для молодших поколінь. Він вчить, що держава — це не абстракція, а люди, які в критичний момент не відступили.

В умовах гібридної війни, де основною зброєю стає інформація, а метою — злам духу, ветеран — це також носій психологічної стійкості. Його історії руйнують фейки, його впевненість розвіює паніку, його приклад формує імунітет проти зневіри. Водночас цей зв'язок — двосторонній. Суспільство також впливає на ветеранів не лише у дні пам'яті, а щоденно — у спілкуванні, у підтримці та у своєму відношенні.

і) Моральна та психологічна стійкість як фактор перемоги.

Моральна та психологічна стійкість — це невидимий, але визначальний фронт сучасної війни. У гібридному конфлікті, де ворог б'є не лише артилерією, а й інформацією, емоціями, страхом та втомою, саме внутрішня сила людини — її здатність тримати удар, не втратити ясність думки і віру — стає чинником, що вирішує долю бою, спільноти й держави.

На відміну від матеріальних ресурсів — техніки, зброї, логістики — моральна стійкість не вимірюється у цифрах. Вона проявляється у здатності продовжувати діяти, навіть коли умови безнадійні. Це — те, що дозволяє військовому на позиції не зламатися під обстрілами, волонтеру — не опустити руки після втрат, громадянину — не піддатися апатії від новин про війну. Психологічна витривалість — це фундамент довіри до себе, до побратима, до суспільства. І саме ця довіра формує середовище, де можлива перемога.

Під час повномасштабної війни стало очевидно, що моральна перевага може переважити технічну слабкість. росія мала більші запаси зброї, більше солдатів, але не мала внутрішньої єдності та сенсу. Українське суспільство ж продемонструвало неймовірний рівень самоорганізації, довіри, жертовності — від цивільних, що плели сітки, до медиків, які рятували під обстрілами. Це приклад того, як моральна стійкість перетворюється на силу, що змінює хід історії.

Однак важливо усвідомлювати: підтримувати цю стійкість потрібно постійно. Ворог цілеспрямовано б'є у моральні точки — через інформаційно-психологічні операції, дезінформацію, нав'язування безсилля та зневіри. Мета таких атак — не зруйнувати армію фізично, а зламати її дух. Саме тому боротьба за моральну стійкість — це не абстракція, а питання виживання.

Моральна і психологічна стійкість також тісно пов'язана з культурою пам'яті. Люди, які знають свою історію, не стають жертвами чужої пропаганди. Вони усвідомлюють, що свобода не є даністю, а виборюється щодня. Звідси — гідність, здатність не миритися з несправедливістю, розуміння цінності кожного життя.

Перемога у XXI столітті — це не лише про озброєння, але і про свідомість. Держава може втратити територію, але не програє, якщо не втратить дух. І навпаки — навіть найсильніша армія не врятує націю, якщо в ній панує байдужість. Тому моральна та психологічна стійкість — це не метафора, а реальний щит, без якого неможлива ні свобода, ні майбутнє.

Наприклад після війни Судного дня (1973 р.) Ізраїль зробив ставку на створення системи тотальної оборони — де кожен громадянин розуміє свою роль у кризовій ситуації. Понад 70% дорослого населення проходило військову підготовку. Ветерани активно були залучені до громадського життя, бізнесу, освіти. Під час атак "Хамасу" у 2023 році суспільство миттєво самоорганізувалося: добровольці забезпечували евакуацію, тилову підтримку, психологічну допомогу. Це не лише дисципліна, а внутрішня установка — "держава виживе, якщо триматимемося разом".

Після кожної війни ізраїльські школи проводять уроки психологічної стійкості, тренінги з реагування на небезпеку. Це приклад системного підходу до ментальної готовності ще з дитинства.

У Фінляндія — концепція "тотальної оборони суспільства" (Total Defence). Після Зимової війни 1939–1940 рр. Фінляндія розробила концепцію, за якою кожен громадянин є частиною оборонної системи. У школах викладають основи цивільного захисту. Засоби масової інформації узгоджено діють під час криз — без паніки, без хаосу. Держава готує населення до інформаційних атак: тренінги з медіаграмотності, інструкції у кожному домі на випадок війни. Основний акцент: психологічна єдність і довіра до держави є такою ж зброєю, як артилерія.

Під час війни в Україні (з 2022 р.) Фінляндія оперативно зміцнила інформаційну безпеку: створено Центр протидії гібридним загрозам у Гельсінкі (Hybrid CoE), який аналізує пропаганду, дезінформацію та розробляє методи "ментальної оборони". Ізраїль і Фінляндія — приклади суспільств, де стійкість стала частиною національної ідентичності.

Україна нині проходить подібний шлях — формується власна культура витримки, самоорганізації та взаємної підтримки.

ї) Відповідальність громадян у час війни.

В умовах повномасштабної війни поняття "оборона держави" давно вийшло за межі фронту. Сучасна війна — це не лише про зброю, бронетехніку та лінії зіткнення. Це війна за свідомість, єдність і здатність суспільства діяти як цілісний організм. Тому сьогодні оборона України — справа не лише армії, а всіх громадян, незалежно від професії, віку чи місця проживання.

У гібридній війні ворог атакує не тільки військові об'єкти, а й інформаційний простір, моральну витривалість, економіку, систему освіти, культуру. Кожен громадянин стає мішенню — через новини, соцмережі, чутки, пропаганду. Саме тому першим обов'язком цивільного у час війни є інформаційна гігієна. Не поширювати неперевірену інформацію, не піддаватися паніці, не бути ретранслятором ворожих наративів — це сучасна форма відповідальності, еквівалентна збереженню бойового секрету. Одна неправдива новина може завдати більше шкоди, ніж ворожий снаряд.

Другою формою громадянської оборони є волонтерство. Це не просто допомога армії чи переселенцям — це доказ того, що держава тримається на горизонтальних зв'язках довіри. Волонтери — це тил, який компенсує вразливість системи, і водночас моральний фундамент суспільства. Їхня діяльність під час війни демонструє, що українці вміють самоорганізовуватися, діяти без наказу, брати на себе відповідальність. Така культура солідарності — це те, чого не може зрозуміти і відтворити жоден авторитарний режим.

Ще одна форма сучасного спротиву — критичне мислення. росія програє не лише на полі бою, а й у сфері смислів. Її зброя — це дезінформація, спотворення фактів, маніпуляції емоціями. Тому громадянин, який уміє ставити запитання,

перевіряти джерела, аналізувати інформацію — це вже боєць інформаційного фронту. Освічене суспільство важче деморалізувати, посварити або змусити сумніватися у власній правоті.

Важливо усвідомити, що під час війни пасивність теж має наслідки. Той, хто мовчки споживає ворожі наративи або ухиляється від участі у спільних зусиллях, фактично допомагає противнику. Натомість активна громадянська позиція — це спосіб захистити себе і своїх близьких. Навіть маленькі дії — донат, підпис під петицією, участь у волонтерському зборі, допомога сусіду — складаються у велике колективне зусилля, що тримає країну.

У цій війні кожен має свій фронт: військовий — на позиціях, медик — у шпиталі, журналіст — у правді, вчитель — у вихованні свідомих дітей, айтішник — у кіберзахисті. Коли кожен виконує свою частину роботи чесно і відповідально — система стає непохитною. Саме така взаємозалежність створює стійкість держави до будь-яких викликів.

росія намагається зруйнувати не лише наші міста, а й відчуття спільності, нав'язати українцям байдужість. Протидією цьому є усвідомлення власної ролі. Бути громадянином — означає не лише мати права, а й брати участь у спільній справі.

Тому сьогодні, як ніколи, актуально звучить теза: "Кожен громадянин — елемент національної безпеки."

й) Війна за незалежність як приклад нової генерації воєн.

Війна, яку веде Україна проти російської федерації з 2014 року, є не лише боротьбою за територію чи політичний суверенітет. Це війна нового типу, яка демонструє зміну самої природи збройних конфліктів у XXI столітті. Вона стала прикладом переходу від класичних міждержавних воєн до багатодоменної гібридної війни, у якій переплетені військові, інформаційні, економічні, політичні та психологічні методи впливу. Саме тому українська війна за незалежність — не просто епізод у світовій політиці, а зразок нового формату протистояння, який визначатиме правила безпеки в Європі на наступні десятиліття.

У класичному розумінні війна — це зіткнення армій на полі бою. Проте з розвитком технологій і глобалізацією центр ваги перемістився з фронту на рівень управління інформацією, комунікаціями, логістикою, енергетикою, суспільними настроями. Тепер перемога не завжди вимірюється зайнятими територіями — вона вимірюється контролем над реальністю, здатністю змусити противника сумніватися, суспільство — роз'єднатися, союзників — втратити довіру.

Україна опинилася у центрі цієї нової моделі. росія розпочала агресію не з танків і авіації, а з інформаційної інтервенції. Ще до 2014 року формувалися наративи про "спільну історію", "братні народи", "захист російськомовних", через які в український простір впроваджувалися моделі залежності — культурної, економічної, політичної. Це був підготовчий етап, який дав змогу у

потрібний момент швидко перейти до активних дій — анексії Криму та війни на Донбасі.

Таким чином, росія не просто порушила міжнародне право — вона практично зруйнувала традиційні уявлення про межі між війною і миром. Її агресія стала лабораторією нової генерації воєн, де бойові дії поєднуються з інформаційними кампаніями, кібератаками, диверсіями, економічним тиском, політичним підкупом і використанням соціальних мереж як інструментів маніпуляції.

З 2014 року світ уважно спостерігає за тим, як Україна стала полігоном для тестування гібридних технологій. Уперше на практиці відбулося масштабне поєднання кібервпливу, політичної дестабілізації та прямого військового втручання.

В 2015–2016 роках фіксувалися кібератаки на енергетичну систему України — частково успішні, із тимчасовими відключеннями електроенергії в низці регіонів. Паралельно російська пропаганда через медіа, соцмережі та релігійні структури формувала ідею “зовнішнього управління” Україною. У політичному полі працювали мережі проросійських партій, громадських організацій і медіахолдингів, що створювали ілюзію “альтернативної правди”. Це не випадковий набір дій — це єдина стратегія впливу, яка має на меті розхитати державу без повномасштабної війни. Саме тому дослідники НАТО та ЄС розглядають російсько-українську війну як “case study” нової генерації гібридних воєн — тобто, конфліктів, де немає чіткої лінії фронту, а всі сфери життя стають полем бою.

24 лютого 2022 року стало точкою переходу від “гібридної підготовки” до багатодоменної війни у повному сенсі. росія одночасно застосувала всі п’ять доменів: Сухопутний — масштабне вторгнення бронетехніки та живої сили. Повітряний — атаки з використанням авіації та дронів. Морський — блокада портів, обстріли узбережжя, мінування акваторії. Космічний — використання супутникових розвідданих, спроби втручання у супутникові канали зв’язку. Інформаційно-кібернетичний — атаки на урядові системи, кампанії дезінформації, фейки про “здачу Києва”, “біженців, які все зруйнують”, “нелегітимність влади”.

Вперше у світовій історії всі ці складові діяли синхронно, як частина єдиного операційного середовища. Тому цю війну можна назвати конфліктом нового типу, де фізичні удари супроводжуються інформаційними хвилями, спрямованими на деморалізацію населення, зниження довіри до влади й союзників.

Україна, зі свого боку, показала іншу модель реагування. Замість класичної оборони по фронту вона створила асиметричну систему спротиву, у якій поєднані зусилля армії, добровольчих формувань, волонтерів, айті-спільноти та дипломатів. Саме ця горизонтальна модель — без централізованого контролю,

але з високим рівнем самоорганізації — стала новим форматом оборони XXI століття. [https://nuou.org.ua/assets/documents/mnpk-vseob-2023.pdf]

Українська війна продемонструвала, що технології та ресурси — важливі, але не визначальні. Ключовим чинником стає сміливість і рішучість суспільства. Саме людський фактор — здатність діяти автономно, не чекаючи наказу, — зруйнував початковий план блискавичної окупації. російська федерація розраховувала на слабкість інституцій, паніку серед населення, відсутність координації між військовими й цивільними. Проте українці довели, що сучасна війна — це не тільки зіткнення армій, а зіткнення волі. Коли мільйони людей об'єднані спільною метою, вони створюють ефект, який жоден штаб не може прорахувати.

Цей феномен уже називають "українською моделлю опору". [https://warontherocks.com/2024/02/why-ukraine-is-not-a-universal-resistance-model/?utm_source=chatgpt.com]. Її сутність — у поєднанні традиційної військової стратегії з елементами громадянського спротиву, цифрової мобілізації (через соцмережі, донати, інформаційні кампанії) та психологічної стійкості. Тобто, сміливість перестала бути лише моральною категорією — вона стала стратегічною зброєю, яка компенсує нерівність у силах.

Сучасні аналітики НАТО, RAND Corporation, CSIS і британського IISS розглядають українську війну як лабораторію воєнних інновацій. Саме тут тестуються концепції, які раніше існували лише в теорії: масове використання безпілотників як автономних підрозділів розвідки та ураження; цифрове управління бойовими операціями через захищені комунікаційні платформи; "краудсорсинг війни" — коли цивільні структури беруть участь у забезпеченні, зборі інформації, інформаційній протидії.

Також формується нова культура взаємодії між військовими й суспільством. Якщо у XX столітті армія була окремим "корпусом", то сьогодні вона інтегрована у суспільну систему. Це змінює саму логіку державного управління: без довіри між владою, армією та громадянами перемога неможлива.

Україна фактично створює новий прецедент: коли малоресурсна країна, опинившись у війні з ядерною наддержавою, не тільки зберігає стійкість, а й примушує противника переглядати свої доктрини.

Окремо слід відзначити інформаційний фронт, який став невід'ємною частиною нової генерації воєн. У перші тижні вторгнення росія намагалася сформувати глобальний образ "сильної держави, що визволяє братній народ". Проте Україна застосувала протилежну стратегію — операцію правди, засновану на відкритості, документуванні злочинів, щоденному прямому спілкуванні з громадянами та світом.

Ця стратегія спрацювала. Україна виграла битву за наратив, чого не вдалося зробити жодній країні, проти якої діяла російська пропагандистська машина. Світ побачив не "конфлікт на Донбасі", а війну за незалежність і право існування держави. З того моменту інформаційна складова війни стала не лише оборонною,

а й наступальною. Українські журналісти, дипломати, волонтери, айті-спільнота створили мережу, яка формує глобальний контекст — від судових позовів проти російських злочинів до міжнародних кампаній підтримки.

Якщо у XX столітті війни точилися за території, то війни XXI століття точаться за смисли. Українська війна довела, що стійкість нації визначається не чисельністю армії, а наявністю ціннісного ядра — розумінням, за що саме борешся. російська ідеологія базується на страху, імперській ностальгії та міфах про "велич". Українська — на ідеї свободи, самоповаги й гідності. Саме тому ця війна сприймається у світі як етичний конфлікт, у якому агресор і захисник мають принципово різну мотивацію.

Україна стала символом того, що навіть у цифрову добу, коли межі між правдою й маніпуляцією розмиті, суспільство може залишатися вірним своїм цінностям. Це — головна відмінність нової генерації воєн: боротьба не лише за ресурси, а за моральну легітимність.

Війна за незалежність України зруйнувала постгельсінкську систему безпеки, засновану на ідеї непорушності кордонів. Світ побачив, що міжнародні гарантії безпеки не спрацьовують без готовності їх захищати силою. Тому відбувається перехід від "права" до "волі" як основи міжнародних відносин.

Те, що Трамп у своєму дописі назвав "property lines being defined by War and Guts", — не лише політична метафора, а діагноз сучасній системі. Кордони визначають не документи, а готовність їх утримувати. Україна доводить, що навіть за відсутності абсолютної переваги можна відстояти незалежність, якщо нація здатна чинити спротив у всіх доменах одночасно — від окопу до кіберпростору.

Жодна технологія не має сенсу без людини. Сучасна війна показала, що головною зброєю є психологічна стійкість. Українські військові, волонтери, медики, журналісти діють у середовищі постійного тиску, але саме їхня здатність адаптуватися й залишатися людяними визначає успіх. На відміну від класичних воєн, де солдат був лише частиною системи, сьогодні кожен учасник війни — суб'єкт, який приймає рішення, взаємодіє з технологіями, створює інформацію. Це змінює і моральну складову війни: вона стає персоналізованою, відповідальність — індивідуальною, а героїзм — не колективною міфологією, а конкретною дією.

Війна за незалежність України — це не лише оборона держави, а й випробування для цивілізаційної моделі, у якій ми живемо. Вона показала, що нова генерація воєн не має чіткої межі між фронтом і тилом, між солдатом і громадянином, між зброєю і словом. Україна не лише бореться — вона створює прецедент для майбутніх поколінь. Її досвід доводить: у світі, де війни стають гібридними, незалежність зберігається не стільки завдяки договорам, скільки завдяки сміливості людей, які відмовляються жити під диктатом страху.

Отже, українська війна за незалежність — це війна нового типу, де зброєю є технології, інформація, культура, віра у свободу. І якщо колись кордони визначалися картами, то сьогодні їх визначає людська воля.

3. Орієнтовна структура часу

Вступ (5 хв), коротке представлення лектора, мети лекції, контексту.

Основна частина (55 хв), виклад матеріалу з прикладами.

Обговорення (15 хв), відповіді на запитання, коротка дискусія про майбутнє воєн.

4. Рекомендації для лектора

Використовувати актуальні приклади з досвіду Сил оборони України (у межах відкритої інформації).

Підкреслювати роль суспільства та громадян у перемозі — від інформаційної гігієни до волонтерства.

Завершити лекцію меседжем про єдність держави, війська й громадянського суспільства у протидії агресору.

Рекомендований список джерел

Conflict in the 21st Century: The Rise of Hybrid Wars https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Доктрина інформаційної безпеки України. — Указ Президента України №47/2017. https://www.president.gov.ua/documents/472017-21374

NATO / Allied Command Transformation — матеріали про “Multi-Domain Operations” та гібридні загрози https://www.act.nato.int/activities/multi-domain-operations/?utm_source

CSIS — “Chronology of Possible Russian Gray Area and Hybrid Warfare Operations” (хронологія та кейси) https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf

Воєнна доктрина України. — Затверджена Указом Президента №555/2015.

Концепт “багатодоменної війни” оглядова стаття у науковому виданні — приклад для контексту https://www.tandfonline.com/doi/full/10.1080/01495933.2024.2445491?utm_source

Центр стратегічних комунікацій та інформаційної безпеки. Аналітичні огляди 2022–2025 рр. https://spravdi.gov.ua/dosldzhennya-ta-analtika/

Збірник матеріалів міжнародної науково-практичної конференції кафедри стратегії національної безпеки та оборони "Всеохоплююча оборона: досвід протидії збройній агресії рф проти України" https://nuou.org.ua/assets/documents/mnpk-vseob-2023.pdf

RAND, дослідження щодо імплікацій атак та прикладів кібероперацій в Україні https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf?utm_source

ISW — постійні аналітичні оцінки https://understandingwar.org/analysis/russia-ukraine/

Russia’s Shadow War Against the West https://www.csis.org/analysis/russias-shadow-war-against-west?utm_source

PISM (Polish Institute of International Affairs) — аналітика щодо української стратегії безпеки, нових підходів у воєнній політиці.
https://pism.pl/publications/Ukraines_New_Military_Security_Strategy?utm_source

Текст “Helsinki Final Act” (офіційний документ OSCE / U.S. Commission) — принцип “inviolability of frontiers”
https://www.csce.gov/wp-content/uploads/2016/10/Helsinki-Final-Act.pdf?utm_source