Це видання присвячене воїнам Збройних Сил України, які виконують священну місію – героїчно боронять Вітчизну від рашистських загарбників. Під час російсько-української війни відважні військові захищають європейську цивілізацію від хвилі варварства і жорстокості, демонструючи світові непохитну стійкість та самопожертву в обороні, неймовірну доблесть і відвагу під час наступу, вражаючі своєю професійністю та умінням в користуванні сучасною зброєю і технікою.

Складний і звитяжний історичний шлях, яким пройшли українці, гідний великого європейського народу. Війна не повинна залишитись у спадок прийдешнім поколінням. Подвиги героїв, які є взірцем виконання військового та громадянського обов'язку, вписані кров'ю в літопис боротьби українського народу за незалежність, завжди будуть нагадувати нащадкам, якою ціною дістається свобода, як здобувається право бути вільною, самодостатньою нацією.

Слава Україні! Героям слава!

Авторський колектив

ЗМІСТ

ПЕРЕДМОВА
ІНФОРМАЦІЙНА ВІЙНА
ЯК ЗАСІБ ПОЛІТИЧНОГО НАСИЛЛЯ

Інформаційна війна є засобом політичного насилля на теоретичному, змістовому та практичному рівнях. Для ефективної протидії слід розуміти не лише понятійно-категоріальний каркас цього явища, а й інструментальне забезпечення тареалізацію у прикладному вимірі. Комплексний аналіз даної проблематики уможливив осягнення предмету і як поняття, і як явища, що особливо актуально у сучасному цифровому світі.

Інформаційна війна пов'язана з контролем над інформаційною сферою, що передбачає формування та спрямування інформаційних потоків на тактичному, оперативному та стратегічному рівнях, це контроль над джерелами та розповсюдженням інформації. Вона може відбуватися у різних формах (війна у сфері командування та контролю; розвідувальна війна; радіоелектронна війна; психологічна війна; хакерська війна; економічно-інформаційна війна; кібервійна). Ведення інформаційної війни передбачає збір тактичної інформації; перевірку точності інформації; поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом та громадськістю; підривання якості інформації про опонента; позбавлення опонента можливості збирати інформацію тощо. Для досягнення політичних цілей переважно використовується психологічна форма інформаційної війни.

Політичний інтерес, спричинений соціально-політичними потребами, оформлюється у конкретну політичну мету, є мотивацією до політичної дії, вирізняється мультисуб'єктністю (переважно групи інтересів) і в разі труднощів в процесі реалізації (протистояння різних політичних інтересів) може призвести до політичного конфлікту. Останній, у свою чергу, має два основні способи реалізації: мирний та агресивний. Мирний спосіб роз-

гортання передбачає толерантне поводження суб'єктів по відношенню один до одного, ведення перемовин і пошук компромісного варіанту розв'язання конфлікту. Агресивний спосіб означає жорстку позицію кожного із суб'єктів протиборства, відмову від конструктивного діалогу, боротьбу за кінцеву мету будь-якою ціною. Власне, в межах останнього способу найчастіше і знаходить простір застосування політичне насилля. Його можна визначити як фізичний та/або психологічний тиск одного політичного актора (акторів) на іншого (інших) з метою реалізації власної політичної волі у вигляді досягнення конкретної політичної цілі, що може мати як ідеалістичний, так і матеріалістичний характер.

Політичне насилля поряд з іншими різновидами (економічне, соціальне, фінансове тощо) може відбуватися в інформаційній площині і бути одним із виявів інформаційного насильства. Не все насильство в інформаційному полі можна вважати політичним. До останнього можна віднести лише заходи, коли політичні цілі досягаються інформаційним інструментарієм. Окрім інформаційної війни до його арсеналу можуть бути зараховані: інформаційна атака, інформаційна операція, інформаційна експансія.

Розвиток інформаційно-комунікаційних технологій суттєво вплинув на посилення інформаційної складової військових активностей, створивши новий вид війни – інформаційної, яка з 1990-х років стала чи не одним із найбільш уживаних засобів політичної боротьби. Враховуючи той факт, що політика – це сфера управління усіма суспільними процесами, а держава є єдиним джерелом легітимного насилля, явище інформаційної війни важко помислити за межами політичного. Будь-яка війна, зокрема інформаційна, переважно носить політичний характер, адже має за мету або ж завоювання, утримання, зміцнення політичної влади, або ж нав'язування політичної волі суб'єктами об'єктам публічного управління.

Інформація завжди була дієвим елементом політичної боротьби (агітація, пропаганда, дезінформація тощо). Але на сьогодні інформаційні операції вийшли на новий рівень і можуть нести системну загрозу, приміром, електронним системам державної інфраструктури, збройних сил, енергетичної царини, національній безпеці загалом і т.д. Інформаційна війна – це сукупність

спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій, або служб інформаційної інфраструктури загалом, або окремих її елементів. При дослідженні інформаційної війни стрижневим є поняття інформації. Адже інформаційна природа такого роду протистояння проявляється у тому, що інформація є або ціллю, або джерелом, або середовищем для досягнення поставленої мети.

Інструментальний арсенал інформаційної війни забезпечує інформаційна зброя. Під останньою розуміється сукупність засобів та методів, що дозволяють викрадати, спотворювати чи знищувати інформацію; обмежувати чи припиняти доступ до неї законних користувачів; порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави. А також інформаційна зброя здатна змінювати свідомість людей, змушує їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки. До ключових категорій інформаційної зброї належать: збір, передача, захист, маніпулювання, порушення, деградація та заперечення.

Перераховані вище методи можуть завдати серйозної шкоди воєнно-політичним операціям, що залежать від інформації. Сучасний контекст інформаційного суспільства робить держави та інших політичних акторів особливо у країнах з високорозвиненою інформаційно-комунікаційної інфраструктурою, з одного боку, найбільш дієвими, а з іншого, – найбільш уразливими. Тому аспект контрзасобів має не менш важливе значення.

Для атаки або захисту інформації слід використовувати такі операції: психологічні (використання інформації для впливу на міркування противника); електронна боротьба (заперечує ворогу точну інформацію); військовий обман (вводить противника в оману щодо його можливостей або намірів); фізичне знищення (перетворює накопичену енергію в руйнівну силу); заходи безпеки (заперечує інформацію про військові можливості та наміри); інформаційна атака (прямо пошкоджує інформацію, не змінюючи помітно фізичної одиниці, в якій вона знаходиться).

Інформаційна війна має спиратися на продуману стратегію як загальний план організаційних заходів. При цьому стратегія інформаційної війни має перманентно піддаватися моніторингу, оцінці та рафінуванню, адже її контексту властиві швидкі зміни та модернізація. Стратегія – це загальний план, що охоплює довготривалий проміжок часу, спосіб досягнення важливої мети. Завданням стратегії є ефективне використання наявних ресурсів для досягнення основної мети (стратегія набуває особливого значення, коли наявних ресурсів недостатньо для досягнення визначеної мети). Основні стратегії інформаційної війни: відмова в інформації; обман і мімікрія; порушення та знищення; підривна діяльність.

Основними «будівельними» блоками комплексного розуміння теми кібервійни є кіберпростір, кіберсила, кіберстратегія та кібервійна. На сьогодні кіберпростір офіційно занесений до переліку областей, в яких може вестись війна. Він займає п'яте місце після суходолу, моря, повітря та космосу, тому що здатність контролювати, порушувати чи маніпулювати інформаційною інфраструктурою супротивника стала настільки ж визначальною, як перевага кінетичної зброї у визначенні результату фізичних конфліктів. Кіберпростір – це всі комп'ютерні мережі у світі (не лише Інтернет) та все, що вони об'єднують та контролюють за допомогою кабелю, волоконно-оптичного або бездротового зв'язку. Влада, заснована на інформаційних ресурсах, – це кіберсила. У той час як кіберпростір – це сфера, в якій відбуваються кібероперації, кіберсила – це сума стратегічних ефектів, які генеруються кіберопераціями в кіберпросторі та з нього. Кіберстратегія полягає в розвитку та застосуванні можливостей для роботи у кіберпросторі, інтегрованих та координованих з іншими оперативними сферами, для досягнення або підтримки досягнення цілей за допомогою елементів державної влади. Кіберстратегія ґрунтується на систематичному і структурованому поєднанні цілей (цілей і завдань), засобів (ресурсів і можливостей) і способів (як засоби використовуються для досягнення цілей) з дотриманням належного аналізу та врахуванням ризиків і витрат. Кібервійна – це конфлікт, який використовує ворожі, незаконні транзакції або атаки на комп'ютери та мережі з метою порушити комунікації та інші частини інфраструктури як меха-

нізм для нанесення економічної шкоди чи порушення захисту. Серед актуальних тенденцій кібернетичної війни можна виділити: посилення залежності від розвитку апаратного та програмного забезпечення; зниження ресурсної витратності; домінування нападу над захистом; схильність до тиражування; зменшення вартості входу в кіберпростір тощо.

Міжнародний досвід протистояння політичному насиллю в інформаційному просторі підтверджує наявність спільного ворога демократичного світу в інформаційній боротьбі – Російської Федерації. Російський підхід до інформаційної війни – це глобальна стратегія, яка включає як кібер-удари, так і інформаційні операції проти більшості демократичних гравців світу (Республіка Болгарія, Грузія (Сакартвело), Республіка Молдова, США, Франція тощо). Російські кампанії інформаційної війни впливали і продовжують чинити вплив на демократії, пропагуючи екстремізм і невдоволення, підтримуючи антидемократичних лідерів, намагаючись похитнути вплив Заходу. Російські стратегії збігаються в багатьох країнах і можуть служити різним цілям. Однак, є три загальні: відновлення російського домінування в пострадянській/імперській сфері впливу; зменшення впливу західних демократичних цінностей, інститутів та систем з метою створення поліцентричної моделі світу; розширення політичної, економічної та військової гегемонії Росії в усьому світі, щоб зміцнити місце РФ як великої держави.

Для досягнення цих цілей Росія покладається на хакерів (групи APT 28, APT 29, Turla тощо), свою все більш потужну розвідувальну спільноту, використання державних ЗМІ (наприклад, Russia Today або RT і Sputnik), ферми тролів і ботів. Хоча Російська Федерація має все більш глобальні прагнення, інформаційна війна використовується, насамперед, для встановлення російського домінування в її колишній зоні впливу, яка включає колишні радянські та комуністичні республіки та території, які раніше входили до складу Російської імперії або перебували під її впливом.

Останніми роками кібер-дії Росії виявлені в 85 країнах, що охоплюють загалом 6 континентів і 16 регіонів світу: Центральна Америка, Центральна Азія, Східна Африка, Східна Азія, Східна Європа, Північна Америка, Північна Європа, Південна Америка,

Південно-Східна Азія, Південна Африка, Південна Азія, Південна Європа, Західна Азія та Західна Європа.

З 24 лютого 2022 року відбувається перманентне оновлення законодавства України з метою посилення інформаційної безпеки (Верховною Радою України прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції», Закон України «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора), Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам», Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» тощо.

Загалом аналіз законодавчих та нормативно-правових документів дозволяє вичленувати основні принципи державної політики щодо інформаційної безпеки (верховенство права; пріоритет захисту прав і свобод людини, що стосуються інформації; своєчасний і адекватний захист життєво важливих національних інтересів від реальних і потенційних загроз інформаційній безпеці; захист інформаційного суверенітету України; свобода думки, свобода слова і вільне вираження думок і переконань; свобода збору, зберігання, використання та поширення інформації тощо), її ключові напрямки (створення нормативної бази для організації розвитку інформаційного простору та його захисту від зовнішніх загроз та узгодження такої нормативної бази з нормами міжнародного права, вимогами міжнародного співробітництва та стандартами та правилами ЄС; розробка та реалізація ефективної національної інформаційної політики, спрямованої на розвиток національного інформаційного простору та гармонізацію

системи контролю та координації серед практиків національної інформаційної політики та експертів з інформаційної безпеки) та загрози (комунікативні та технологічні).

На сьогодні політико-правовий захист інформації в Україні відбувається з урахуванням зовнішніх і внутрішніх загроз, вирізняється оперативністю та дієвістю, зваженістю та системністю. Державна політика з інформаційної безпеки має стратегічну спрямованість і деталізована продуманими тактичними рішеннями. Лише так можна утримати інформаційну стабільність в середині країни, посилити підтримку України акторами в міжнародному інформаційному полі та захиститися від інформаційних провокацій ворога.

РОЗДІЛ І.

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ФІЛОСОФІЇ ІСТОРІЇ УКРАЇНИ

Залишимо в спадок – номи поколінням…
Залишимо те, що душею народу
Зовуть недаремно від роду до роду –
Як вищу красу і життєву основу,
Залишимо слово, ім'я своє, мову.

В. Григоренко

Протягом останніх десятиліть в європейській та вітчизняній історичній науці розвивається новий напрям дослідження, пов'язаний з вивченням такого суспільного феномену як національна пам'ять. І це не дивно, адже Україна, як і більшість країн пострадянського простору, переживає складний процес пошуку національної ідентичності, формування національної свідомості українського народу. А основним чинником формування національної свідомості та національної ідентичності є саме історична пам'ять. Завдяки спільному минулому, перемогам і поразкам попередників, спільним героям, місцям пам'яті тощо сучасні покоління відтворюють власний історичний досвід, і таким чином нація усвідомлює свою сутність, духовність.

Одним із важливих явищ духовного життя народів, які опиняються під впливом уніфікаційних проявів глобалізації, є національна пам'ять народів (націй) як складова їх національної та державницької свідомості.

Національна пам'ять виступає важливою складовою само-ідентифікації та консолідації народів, що населяють Україну, в єдину політичну націю – Український народ.

Відновлення й збереження колективної пам'яті про державотворчі традиції, цивілізаційні досягнення, бойову й трудову звитягу, історичні трагедії сприяє єднанню громадянства та мобілізації духовних сил й будівничого потенціалу Українського народу, його утвердженню як рівноправного суб'єкта системи міжнародних відносин, збереженню державного ладу та територіальної цілісності України, творенню позитивного суспільно-політичного та морально-культурного поля буття української політичної нації.

§ 1.1. Трансформація інформаційної війни в епоху штучного інтелекту

За останні роки спостерігається експоненціальний темп розвитку технологій штучного інтелекту (ШІ), які визначаються як здатність цифрового комп'ютера або керованої комп'ютером роботизованої системи виконувати завдання, притаманні живим біологічним організмам. Технологія ШІ описується як двигун Четвертої промислової революції, оскільки за останній час відбувся значний прогрес у здатності машин виконувати складні завдання, а також відповідати або перевищувати продуктивність людини. Одна з цілей розробки технологій ШІ є автономія, тобто здатність системи приймати рішення та діяти з мінімальним втручанням людини або взагалі без нього.

Можливості цієї технології не залишилися непоміченими країнами, які прагнуть отримати військову перевагу. Так, Міністерство оборони США намагається використати швидкий розвиток технологій ШІ в рамках стратегії «Third Offset», яка фокусується на отриманні переваги в асиметричних військових засобах на базі ШІ[1]. Керівництво РФ заявляє, що будь-яка країна, яка домінуватиме у сфері ШІ буде світовим гегемоном. КНР прийняла у 2017 році загальнонаціональну стратегію ШІ, яка спрямована на створення передової індустрії штучного інтелекту вартістю 150 мільярдів доларів, і планує використовувати цю галузь для отримання військової переваги в безпрецедентному прикладі застосування ідеї цивільно-військового співробітництва.

Разом з тим, ідея адаптації штучного інтелекту до військових потреб спричинила значну дискусію у громадських і наукових колах. Так компанія Google нещодавно припинила підтримку проекту Міністерства оборони США «Maven», в рамках якого штучний інтелект використовувався для сканування відео з безпілотних літальних апаратів та надання пропозицій щодо вибору

[1] Larry Lewis, Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations, CNA Research Memorandum DRM-2017-U-016281-Final. Sept. 2017.

цілей на основі класифікації об'єктів[1]. Сотні наукових організацій та окремих представників науки виступають за превентивну заборону автономних летальних військових платформ. В рамках ООН з 2019 року триває обговорення можливості внесення пункту про заборону застосування автономних (без участі оператора) військових систем летального характеру у Конвенцію про застосування звичайних озброєнь, а також у положення Міжнародного гуманітарного права. Таким чином визнається необхідність зменшення можливих ризиків застосування ШІ на полі бою та зменшення небезпеки для некомбатантів.

В цьому контексті необхідно згадати основний принцип управління ризиками, який полягає у необхідності правильного визначення головних ризиків, оскільки неправильна розстановка пріоритетів призводить до неефективного використання наявних ресурсів. Тому необхідно відповісти на питання – чи зосереджує світове співтовариство свою увагу на дійсно важливих ризиках ШІ і автономних військових систем, або обговорює другорядні негативні чинники та «не бачить а деревами лісу»? Спробуємо проаналізувати існуючі концепції, які найчастіше застосовується для обґрунтування необхідності обмеження застосування ШІ.

Концепція «Термінатора». Концепція базується на укорінених у масовій культурі та засобах масової інформації ідеї апокаліптичних наслідків застосування потенціалу штучного інтелекту. Одним з основних провідників зазначеної концепції є відомий американський бізнесмен Ілон Маск, який в ході своїх виступів неодноразово висловлював занепокоєння щодо майбутніх «армад роботів зі штучним інтелектом, які можуть знищити людство»[2]. Таку ж думку активно просували і ряд інших видатних науковців сучасності, зокрема Стівен Гокінг[3].

---

[1] Google Walks Away From America's Security. It bowed to pressure instead of standing up for our country. bloomberg.com/opinion/articles/2018-06-06/google-s-decision-to-ditch-project-maven-is-a-grave-error

[2] Maureen Dowd, «Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse,» Vanity Fair, March 26, 2017, https://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade- to-stop-ai-pace.

[3] Ana Santos Rutschman, «Stephen Hawking warned about the perils of artificial intelligence – yet AI gave him a voice». The Conversation, March 15, 2018,