Громадянське суспільство є фундаментом демократії і національної стійкості, тож воно потребує максимального залучення всіх громадян. Перспективи беззаперечно є у громадського суспільства. Але треба працювати задля цього – створювати ще більше організацій і задіювати людей. Адже саме народ є рушійною силою держави. Народ – це громадянське суспільство.

Література

1. Енциклопедія сучасної України. Громадянське суспільство. URL: https://esu.com.ua/article-31976 (дата звернення 12.05.2026 р.).
2. Цитати Леся Курбаса. URL: https://newsproteatr.blogspot.com/2019/02/blog-post_25.html?m=1 (дата звернення 12.05.2026 р.).

Михаць Роман Андрійович,
здобувач першого (бакалаврського) рівня вищої освіти факультету інформатики та обчислювальної техніки спеціальності 123 «Комп'ютерна інженерія» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Тарасюк Марина Юріївна,
Докторка філософії з історії та археології, викладачка кафедри історії Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

ЦИФРОВІЗАЦІЯ СУЧАСНОЇ ВІЙНИ: НОВІ ВИКЛИКИ ДЛЯ МІЖНАРОДНОЇ БЕЗПЕКИ

Сучасний стан глобальної безпекової архітектури характеризується фундаментальною трансформацією природи воєнних конфліктів. Інформаційно-комунікаційні технології більше не є лише допоміжним інструментом забезпечення зв'язку та перетворились на

самостійну і вирішальну складову ведення бойових дій. Цифровізація війни вимагає переосмислення класичних доктрин, оскільки бойовий простір розширився до «п'ятого виміру» – кібернетичного середовища, де програмний код та алгоритми стають рівнозначними за ефективністю з конвенційною зброєю [1, с. 22].

Одним із найгостріших викликів для міжнародної безпеки є вразливість об'єктів критичної інфраструктури. Тепер держави знаходяться в глибокій залежності від автоматизованих систем керування технологічними процесами (SCADA), які забезпечують роботу енергомереж, логістичних вузлів та систем водопостачання. Масштабні кібератаки на такі системи здатні спричинити гуманітарну катастрофу без фізичного перетину кордонів. Технічна складність проблеми посилюється «проблемою атрибуції»: у цифровому просторі ідентифікація справжнього агресора є вкрай ускладненою, що створює сіру зону відповідальності та дозволяє суб'єктам міжнародного права уникати санкцій за агресивні дії [3, с. 134].

Впровадження штучного інтелекту (Далі – ШІ) у воєнну сферу відкриває нові можливості, але водночас створює серйозні етичні та правові дилеми. Використання летальних автономних систем (LAWS), здатних самостійно обирати та вражати цілі на основі алгоритмів машинного зору, змінює динаміку бою в бік гіпершвидкостей. Проте делегування права на застосування сили неживому об'єкту ставить під сумнів дотримання принципів міжнародного гуманітарного права. Питання про те, хто несе відповідальність за «алгоритмічну помилку» – розробник, оператор чи командувач – залишається відкритим і потребує нагального нормативного врегулювання [4, с. 25].

На додачу, сучасна цифрова війна ведеться не лише за територію, а й за свідомість. Використання технологій Deepfake, бот-мереж та алгоритмічного маніпулювання соціальними медіа дозволяє агресору здійснювати ефективний інформаційно-психологічний тиск на населення та армію супротивника. Когнітивна війна стає стратегічним імперативом, оскільки дестабілізація внутрішньої ситуації в країні через цифрові канали може бути більш ефективною за пряму військову агресію [2, с. 142].

Війна в Україні наочно продемонструвала нову роль Big Tech у глобальній безпеці. Супутниковий інтернет, хмарні обчислення та системи супутникового моніторингу, які належать приватним корпораціям, стають критично важливими елементами державної оборони. Це змушує держави переглядати концепцію цифрового суверенітету та вибудовувати нові формати державно-приватного партнерства в оборонній сфері [5, с. 112].

Отже, цифровізація війни – це незворотний процес, який несе як технологічні переваги, так і екзистенційні ризики. Для забезпечення сталого миру варто ініціювати створення нових міжнародних конвенцій, що регламентували б використання кіберзброї та ШІ. З інженерної точки зору, пріоритетом має стати розвиток систем кіберзахисту, побудованих на принципах Zero Trust, та впровадження надійних механізмів верифікації цифрового контенту.

Література

1. Горбулін В. П. Світова гібридна війна: український фронт. Київ: НІСД, 2017. 280 с.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва. Київ: НІСД, 2014. 328 с.
3. Невара Л. Міжнародно-правова відповідальність за кібератаки під час збройного конфлікту. *Право України*. 2024. № 3. С. 132–145.
4. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони : аналітичний звіт. Київ: УГСПЛ, 2024. 44 с.
5. Міжнародне гуманітарне право та основи безпеки у період збройних конфліктів : матеріали міжнар. наук.-практ. конф. (м. Київ, 6 лют. 2025 р.). Київ, 2025. 248 с.