Лук'янченко Є. В.,
аспірантка 4 курсу,
Київського національного університету
імені Тараса Шевченка
Навчально-наукового інституту міжнародних відносин
ID-ORCID-0000-0002-3586-1228
(м. Київ, Україна)

МІЖНАРОДНЕ ГУМАНІТАРНЕ ПРАВО У ЦИФРОВУ ЕПОХУ: ВИКЛИКИ ДЕЗІНФОРМАЦІЇ ДЛЯ ГУМАНІТАРНОГО РЕАГУВАННЯ

Міжнародне гуманітарне право вже понад сто років відіграє ключову роль у захисті цивільних осіб та працівників гуманітарних організацій під час збройних конфліктів. Однак з кожним новим десятиліттям ми стикаємося з новими викликами, що вимагають від нас оновлення підходів та адаптації міжнародних правових та інституційних механізмів. У цифрову епоху, коли інформаційні технології стрімко змінюють реалії війни, дезінформація та кібератаки стають такою ж потужною зброєю, як і звичні фізичні атаки. Це особливо помітно на прикладі сучасних збройних конфліктів, зокрема збройної агресії РФ проти Україні, де дезінформаційні кампанії та гібридні прояви війни набули особливих масштабів. У зв'язку з цим існує нагальна потреба у переосмисленні ключових аспектів МГП та гуманітарного реагування.

Одним із ключових викликів сучасності є зростаюча роль *дезінформації* у веденні війни. У конфліктах сьогодення дезінформація є інструментом та частиною військової стратегії, яка використовується для деморалізації противника та маніпулювання громадською думкою. Маніпуляції у медіапросторі та інформаційні атаки не просто дестабілізують громадську думку – вони прямо підривають роботу гуманітарних організацій, що, серед іншого, перешкоджає ефективному наданню життєво необхідної допомоги населенню.

В рамках повномасштабного вторгнення РФ в Україну дезінформація та кібератаки набули загрозливих масштабів. За останні роки ми стали свідками безпрецедентного поширення фейкових новин, створення підроблених сторінок гуманітарних організацій, шахрайських схем та маніпуляцій з метою дискредитації гуманітарних зусиль.

Прикладом дезінформаційної кампанії є спрямовані зусилля РФ з дискредитації Національного Товариства Червоного Хреста України, що створюють перешкоди для надання допомоги постраждалим. Фейкові новини, що поширюються в соціальних мережах, викликають сумніви серед населення щодо легітимності роботи організацій, що має катастрофічні наслідки для гуманітарного реагування.

Дезінформація все частіше спрямована на *дискредитацію жінок-лідерок*, гуманітарних працівниць та активісток. У контексті порядку денного «Жінки, мир, безпека» ця проблема набуває глобального значення. В Україні такі кампанії часто спрямовані на зниження суспільної довіри до жіночого лідерства

у кризових умовах, в той час як в Україні жінки мають значну роль у забезпеченні гуманітарного реагування. Це порушує принципи міжнародного права та суперечить глобальним зобов'язанням, спрямованим на зміцнення ролі жінок у миротворчих процесах.

Отже, у сучасних конфліктах маніпуляції інформацією використовуються як форма психологічної війни, що має за мету підірвати мораль цивільного населення та гуманітарних працівників. Це є серйозним порушенням принципів захисту цивільного населення, закріплених у Женевських конвенціях.

Сучасні гібридні війни стали викликом для МГП, яке повинно розвиватись, аби мати змогу відповідати на виклики цифрової епохи, коли важливість інформації є вищою, ніж будь-коли. І саме зараз захист цивільних осіб та гуманітарних організацій від дезінформації стає критично важливим завданням.

В Україні важливим інструментом у боротьбі з дезінформацією є *Центр протидії дезінформації при Раді національної безпеки і оборони*. Його діяльність спрямована на моніторинг інформаційного простору, ідентифікацію та спростування фейків, а також підвищення обізнаності населення про дезінформаційні загрози. Важливо зазначити, що Центр відіграє критичну роль у захисті гуманітарних ініціатив в умовах російської агресії.

Але дезінформація - не єдина загроза. *Кібератаки* є ще однією складовою гібридних війн. Вони мають безпосередній вплив на гуманітарну діяльність, особливо коли йдеться про атаки на критичну інфраструктуру. В Україні, з початку російської агресії, ми стали свідками масштабних кібератак на державні установи, медичні заклади та гуманітарні організації. Уявімо собі ситуацію, коли кібернапад паралізує роботу лікарні, зупиняє постачання ліків чи позбавляє медичних працівників доступу до електронних медичних даних. Це може призвести до катастрофічних наслідків, ставлячи під загрозу життя сотень і тисяч осіб.

У цьому контексті варто нагадати про ключові положення МГП, зокрема статтю 18 Додаткового протоколу I до Женевських конвенцій, яка гарантує захист цивільного медичного персоналу та гуманітарних працівників під час збройних конфліктів. Далі, у статті 19, вказується, що захист, на який мають право цивільні лікарні, не може припинитись навіть якщо вони використовуються, крім виконання гуманітарних обов'язків, для вчинення дій, шкідливих для супротивника.

Крім того, стаття 48 Додаткового протоколу I зобов'язує сторони конфлікту завжди розрізняти цивільне населення й комбатантів, а також цивільні й воєнні об'єкти та відповідно спрямовувати свої дії тільки проти воєнних об'єктів. Стаття 57 передбачає обов'язок зводити до мінімуму ризик для цивільного населення під час атак.

У цифрову епоху ми повинні розуміти, що кібератаки можуть бути такими ж руйнівними, як і фізичні атаки, а отже - повинні розглядатись як серйозні порушення норм МГП. Кібероперації, які націлені на цивільну інфраструктуру, такі як лікарні, водо- або електропостачання, повинні бути прирівняні до традиційних фізичних атак, які порушують норми МГП.

Отже, виникає питання: що ми можемо зробити для подолання цих викликів? Перш за все, *МГП повинно адаптуватись* до цих нових реалій ведення збройних конфліктів. Необхідно розробити нові правові та інституційні механізми, спрямовані на реагування на загрози кібератак, дезінформації та використання штучного інтелекту для цих цілей. Важливо, щоб технологічні компанії, держави та громадянське суспільство працювали разом, щоб розробити механізми захисту та реагування на ці загрози. Женевські конвенції, безумовно, залишаються важливим фундаментом для захисту цивільних осіб, але вони повинні бути доповнені положеннями, що забезпечують їх дієвість у цифрову епоху.

Право ЄС пропонує цінні приклади регулювання дезінформації та кібератак. *Кодекс належної практики щодо дезінформації* забезпечує механізми контролю за поширенням фейкових новин на цифрових платформах, тоді як *Акт про кіберстійкість* посилює захист критичної інфраструктури. Для України досвід ЄС є особливо корисним у контексті адаптації національного законодавства до вимог цифрової епохи та забезпечення захисту національної безпеки. Українське законодавство має бути змінене для врахування нових викликів, включно з механізмами кіберзахисту та протидії інформаційним атакам.

Також важливо наголосити на необхідності *міжнародного співробітництва* у боротьбі з дезінформацією та кібератаками. Жодна організація чи країна не зможе самостійно впоратися з цими викликами. Нам необхідно спільно працювати над створенням нових міжнародних стандартів, що будуть враховувати реалії цифрової епохи. І тут надзвичайно важливо залучати технологічні компанії до цього процесу, адже саме на їхніх платформах часто поширюється дезінформація, а їхнє оснащення може полегшити чи, навпаки, унеможливити кібератаки. Лише об’єднавши зусилля, ми зможемо забезпечити захист гуманітарної діяльності та прав цивільних осіб під час конфліктів. Для забезпечення безпеки в Україні це надзвичайно важливо.

Окрім цього, ми повинні приділяти особливу увагу освіті та просвітницькій роботі серед населення, щоб підвищити обізнаність про небезпеку дезінформації та шахрайства у цифровому просторі. Цивільні особи повинні мати доступ до правдивої та надійної інформації, особливо в умовах конфлікту.

Насамкінець, хочу зазначити, що хоча технології змінюють спосіб ведення війн, основна мета МГП залишається незмінною: захист цивільних осіб і забезпечення гуманітарної допомоги під час збройних конфліктів. Ми повинні адаптувати МГП до нових умов, щоб захистити гуманітарні місії від загроз, які несе цифрова епоха. Тільки разом ми можемо забезпечити, що МГП залишатиметься дієвим інструментом захисту цивільного населення у цьому новому світі.

Список використаних джерел:

1. Про Центр. ЦЕНТР ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ. URL: https://cpd.gov.ua/documents (дата звернення: 06.02.2025).

2. Katz E. Liar's war: Protecting civilians from disinformation during armed conflict. International Review of the Red Cross. 01.12.2021. URL: https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914 (дата звернення: 06.02.2025).

3. Cyber and information operations. International Committee of Red Cross. URL: https://www.icrc.org/en/law-and-policy/cyber-and-information-operations (дата звернення: 06.02.2025).

4. A strengthened EU Code of Practice on Disinformation. European Commission. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en (дата звернення: 06.02.2025).

5. EU adopts cyber resilience act – and other cybersecurity news to know this month. World Economic Forum. 14.10.2024. URL: https://www.weforum.org/stories/2024/10/eu-cyber-resilience-act-cybersecurity-news-october-2024/ (дата звернення: 06.02.2025).

6. Towards common understandings: the application of established IHL principles to cyber operations. Humanitarian Law and Policy. 07.03.2023. URL: https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/?utm_source=chatgpt.com (дата звернення: 06.02.2025).

7. Rodenhäuser T., D'Cunha S. IHL and Information Operations during Armed Conflict. Lieber Institute. 18.10.2023. URL: https://lieber.westpoint.edu/ihl-and-information-operations-during-armed-conflict/?utm_source=chatgpt.com (дата звернення: 06.02.2025).