

retain control over Greenland. *Yevropeika pravda - European truth*, 14 sichnia 2025. URL: <https://www.eurointegration.com.ua/experts/2025/01/14/7202518/> [in Ukrainian]

3. Trump again demands to buy Greenland in 'horrendous' call with Danish PM. *The Guardian*. URL: <https://www.theguardian.com/world/2025/jan/25/trump-greenland-denmark> [in English]

УДК 340

Мазепа С.О.

*к.ю.н., доцент, доцент кафедри
кримінального права та процесу,
Західноукраїнський національний
університет, Оснабрюцький університет*

Яке значення має Tallinn Manual в російсько-українській війні в контексті прав людини?

Війна росії проти України характеризується багатьма вимірами, як наприклад: конвенційний, економічний, кібер, інформаційний, культурний [1]. Сьогодні справжнім викликом для міжнародних експертів є визначення кібервійни та закріплення її принципів та правил у міжнародному нормативно-правовому документі, і досвід України в цьому питанні є ключовим.

Поки ще існує тільки академічна спроба врегулювати це питання – це Tallinn Manual [2; 3]. У виданнях 2013 та 2017 років згадується як основний міжнародно-правовий документ, який допомагає тлумачити застосування норм міжнародного права до кібероперацій. Талліннські рекомендації допомагають аналізувати ці атаки як “застосування сили”: деякі масштабні кібератаки можуть кваліфікуватися як застосування сили, якщо мають наслідки, подібні до збройного нападу (наприклад, виведення з ладу енергосистем, що спричиняє жертви). Все ще складним є питання розмежування цивільних і військових об’єктів та як юридично довести, що атака була здійснена саме державою (РФ), а не хактивістами або приватними групами? Складність аналізу і кваліфікації також полягає у поєднанні кібератак з інформаційними кампаніями, фейками, маніпуляцією громадською думкою.

В академічних колах можна спостерігати дві протилежні ідейні групи: у першій – кібервійна існує, у другій – кібервійна це певна умовність. Так, у Таллінському мануалі (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017), робиться уточнення, що «кібервійна» вживається у чисто описовому, а не нормативному сенсі, і те, що Таллінський мануал є академічним, а не міжнародно-правовим актом.

На мою думку, небезпечна активність рф у кіберпросторі має достатній рівень небезпечної «мілітаризації», і російські кібератаки становлять серйозну проблему не лише для України. Росія застосує наступальні кіберможливості не лише проти України, але й проти Заходу і його критичної інфраструктури як покарання за санкції і підтримку України. РФ має великий досвід у здійсненні кібератак. Широко відомий каскад кібератак DDoS було застосовано в Естонії у

2007 році при кібернападі на сайти державних і приватних організацій, великих банків та парламент у зв'язку із загостренням відносин між Росією та Естонією у зв'язку із перенесенням пам'ятника радянським воїнам (неофіційна назва – «Бронзовий солдат») у Таллінні [4].

Талліннські експерти стверджують, що певні норми міжнародного гуманітарного права (Женевські конвенції та інші) застосовуються і до кібероперацій під час збройного конфлікту, проте з багатьох питань фахівці так і не знайшли спільної думки. Захист цивільного населення має поширюватися і на кіберпростір, як от кібератаки на критичну інфраструктуру, лікарні, медіа тощо [5]. Атаки, які завдають шкоди цивільним особам, можуть розглядатися як воєнні злочини, але інколи дуже складно розмежувати цивільні і воєнні об'єкти. І як бути, коли в результаті самооборони, українські кіберактивісти можуть завдати шкоди цивільним об'єктам?

Талліннський посібник допомагає інтерпретувати, як традиційні норми міжнародного права та прав людини діють у кібервійні. Він надає юридичну основу для захисту прав громадян від кіберзагроз і може бути інструментом для кваліфікації кібероперацій як порушень міжнародного гуманітарного права та права прав людини. Для України це важливий правовий ресурс у справі документування воєнних і кіберзлочинів росії.

ЛІТЕРАТУРА:

1. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації. URL: <https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi>
2. Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013. URL: <http://csef.ru/media/articles/3990/3990.pdf>;
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. URL: http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf
4. Таркін В. П. Особливості інформаційної війни РФ та український спротив //Актуальні проблеми політики. – 2023. – С. 204.
5. Tsybulenko, E., Kajander, A. (2021). The Hybrid Arsenal of Russia's War Against the Democratic World. In: Mölder, H., Sazonov, V., Chochia, A., Kerikmäe, T. (eds) The Russian Federation in Global Knowledge Warfare. Contributions to International Relations. Springer, Cham. https://doi.org/10.1007/978-3-030-73955-3_9