УДК 341.3:623.61:004.7

В. В. Карпусь, А. В. Колесник

ПРАВОВЕ РЕГУЛЮВАННЯ ТА СТАТУС ВІЙСЬКОВИХ ЗАСОБІВ ЗВ'ЯЗКУ В УМОВАХ ВОЄННОГО СТАНУ: МІЖНАРОДНИЙ ТА НАЦІОНАЛЬНИЙ АСПЕКТИ

Анотація. *Проаналізовано міжнародно-правові критерії визначення військових комунікаційних об'єктів як воєнних цілей, обмеження щодо проведення радіоелектронних і кібероперацій та особливості національного регулювання зв'язку під час воєнного стану. Окреслено ризики для цивільної інфраструктури подвійного використання та запропоновано правові й організаційні напрями зменшення цих ризиків.*

Ключові слова: *міжнародне гуманітарне право, військовий зв'язок, воєнний стан, радіоелектронна боротьба, кібероперації, цивільна інфраструктура.*

Abstract. *The paper examines international legal criteria for identifying military communication facilities as military objectives, restrictions on electronic warfare and cyber operations, and national regulation of communications under martial law. It highlights risks to dual-use civilian infrastructure and proposes legal and organizational approaches to mitigating these risks.*

Keywords: *international humanitarian law, military communications, martial law, electronic warfare, cyber operations, civilian infrastructure.*

Вступ

Стійкість систем зв'язку визначає безперервність управління військами, обміну даними та координації дій під час збройного конфлікту. Водночас розвиток супутникових систем, цифрових платформ, програмно-керованих мереж і засобів радіоелектронної боротьби (РЕБ) посилює взаємозалежність військової та цивільної комунікаційної інфраструктури. Один і той самий канал або вузол може одночасно забезпечувати потреби оборони, медичних закладів, аварійних служб і населення. Саме тому питання правового статусу об'єктів зв'язку не може вирішуватися лише за ознакою їх технологічного призначення.

Мета дослідження — систематизувати міжнародні та національні правові підходи до використання й захисту засобів військового зв'язку під час воєнного стану, визначити межі допустимих дій щодо комунікаційної інфраструктури. Методами дослідження є нормативно-правовий аналіз, зіставлення положень міжнародного гуманітарного права (МГП) і законодавства України та узагальнення фахових підходів до кібероперацій.

Основна частина

1. Правовий статус комунікаційної інфраструктури у міжнародному гуманітарному праві.

Відповідно до статті 52 Додаткового протоколу I до Женевських конвенцій цивільні об'єкти не повинні бути об'єктами нападу. Військовими цілями є лише ті об'єкти, які за своїм характером, розташуванням, призначенням або використанням роблять ефективний внесок у воєнні дії та повне або часткове знищення, захоплення чи нейтралізація яких за наявних обставин дає конкретну військову перевагу [1].

Особливої уваги потребують об'єкти подвійного використання: базові станції мобільного зв'язку, волоконно-оптичні магістралі, центри обробки даних і супутникові термінали. Навіть коли окремий елемент відповідає критеріям воєнної цілі, напад залишається обмеженим правилами розрізнення, пропорційності та запобіжних заходів. Стаття 57 Протоколу I вимагає здійснювати практично можливу перевірку цілі, обирати засоби й методи з мінімізацією випадкової шкоди та відмовлятися від нападу, якщо очікувана супутня шкода буде надмірною порівняно з конкретною і безпосередньою військовою перевагою [1].

Правова оцінка має враховувати не тільки фізичне руйнування обладнання, а й передбачувані наслідки втрати зв'язку для швидкої медичної допомоги, цивільного оповіщення, енергопостачання та інших життєво необхідних послуг. Такий підхід особливо важливий для інтегрованих мереж, де порушення роботи одного вузла може вплинути на значну кількість користувачів.

2. Радіоелектронна боротьба, військові хитрощі та заборона віроломства.

Радіорозвідка, перехоплення сигналів, створення радіоперешкод і введення противника в оману не є самі собою універсально забороненими способами ведення війни. Однак законність конкретної операції залежить від її характеру, цілей, наслідків та застосовних норм МГП. Зокрема, широкомасштабне придушення зв'язку може створити неприйнятні гуманітарні наслідки, якщо одночасно порушується функціонування цивільних служб.

Стаття 37 Протоколу I розмежовує дозволені військові хитрощі та віроломство — дії, спрямовані на викликання довіри противника до захисту, який надається міжнародним правом, із наміром зрадити цю довіру [1]. Тому використання захищених гуманітарних імітація статусу осіб, що перебувають під спеціальним захистом,

3. Кібероперації та межі застосування

Цифрові системи військового зв'язку поєднують фізичне обладнання, програмне забезпечення, канали передавання інформації та дані. Кібероперації під час збройного конфлікту підпадають під застосовні норми МГП; технологічна форма впливу не усуває обов'язку захищати цивільних осіб та об'єкти [2; 3]. При цьому правова кваліфікація операції як «нападу», особливо якщо вона спричиняє втрату функціональності без фізичного руйнування, залишається предметом фахової дискусії.

Tallinn Manual 2.0, виданий у 2017 році за редакцією М. Шмітта, є не міжнародним договором, а не обов'язковим до виконання експертним дослідженням застосування міжнародного права до кібероперацій [4]. Його положення доцільно використовувати як аналітичний орієнтир, але не як самостійну юридичну підставу для твердження про наявність нової заборони чи дозволу. Міжнародний Комітет Червоного Хреста наголошує на небезпеці поширення шкідливого програмного забезпечення та непрямих наслідків кібероперацій для медичних, комунальних та інших цивільних систем [2; 3].

Відтак доцільно розглядати ризик непередбачуваного поширення шкідливого впливу, взаємозалежність мереж та можливість порушення критичних послуг як складники правової оцінки очікуваних наслідків операції. В умовах розподілених мереж це вимагає не лише технічного, а й міждисциплінарного аналізу.

4. Національне регулювання зв'язку та відповідальність за інформаційну безпеку.

В Україні особливості функціонування державних органів, військового командування та запровадження заходів правового режиму воєнного стану визначає Закон України «Про правовий режим воєнного стану» [5]. Закон України «Про електронні комунікації» встановлює загальні засади регулювання електронних комунікацій, зокрема положення щодо управління мережами в умовах надзвичайних ситуацій і воєнного стану [6]. Конкретні повноваження суб'єктів, порядок взаємодії та обмеження слід визначати за чинною редакцією законодавства й відповідними підзаконними актами, а не виводити із загального поняття «контролю над зв'язком».

Питання використання особистих засобів зв'язку військовослужбовцями має організаційний і правовий виміри. Стаття 143 Статуту внутрішньої служби Збройних Сил України передбачає, що порядок зберігання та користування мобільними телефонами й іншими засобами передавання інформації встановлюється командиром військової частини [7]. Це положення не слід трактувати як безумовну законодавчу заборону всіх особистих пристроїв у будь-яких умовах.

Інформаційна безпека передбачає запобігання розкриттю місцезнаходження підрозділів, маршрутів, службових повідомлень і персональних даних. У науково-правовому аспекті важливо поєднувати організаційні правила користування пристроями з принципами правової визначеності, пропорційності обмежень і належного розподілу відповідальності між командуванням, операторами мереж та користувачами.

5. Напрями вдосконалення правового забезпечення.

За результатами аналізу можна запропонувати три взаємопов'язані напрями. Перший — чітке документування критеріїв оцінювання комунікаційних об'єктів подвійного використання, зокрема характеру їх фактичного застосування та можливих наслідків припинення роботи для цивільних. Другий — удосконалення взаємодії між органами оборони, регуляторами та операторами електронних

комунікацій для забезпечення безперервності критичних послуг у межах законодавчо визначених повноважень. Третій — систематична правова підготовка персоналу з питань розрізнення військових і цивільних об’єктів, запобіжних заходів під час операцій та захисту інформації.

Ці напрями є авторськими узагальненими рекомендаціями за результатами нормативного аналізу, а не твердженням про вже запроваджені державні механізми. Їх реалізація потребує подальшого дослідження з урахуванням чинних нормативних актів, технічних стандартів і практики правозастосування.

Висновки

Правовий статус засобів військового зв’язку визначається не лише їх технічними характеристиками, а насамперед конкретним використанням, внеском у воєнні дії та очікуваною військовою перевагою від нейтралізації. Визнання об’єкта воєнною ціллю не скасовує вимог пропорційності та запобіжних заходів для захисту цивільного населення. Радіоелектронні та кібероперації потребують оцінки як безпосередніх, так і передбачуваних непрямих наслідків для інфраструктури подвійного використання. Національне регулювання має забезпечувати керованість військового зв’язку, правову визначеність повноважень та належну інформаційну дисципліну. Подальші дослідження доцільно спрямувати на критерії оцінювання ризиків для цивільних комунікаційних сервісів і узгодження технічних заходів стійкості мереж із вимогами МГП.

Список використаних джерел:

1. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), 8 червня 1977 р. Ст. 37, 52, 57. URL: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977

2. International Committee of the Red Cross. International humanitarian law and cyber operations during armed conflicts. 2019. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

3. International Committee of the Red Cross. IHL and cyber operations during armed conflicts: short papers. 2023. URL: https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts

4. Schmitt M. N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

5. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19

6. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20

7. Про Статут внутрішньої служби Збройних Сил України: Закон України від 24.03.1999 № 548-XIV. Ст. 143. URL: https://zakon.rada.gov.ua/laws/show/548-14

Карпусь Віталій Володимирович – помічник військового капелана ЗСУ, Вінниця; e-mail: karpus-v-v@ukr.net.

Колесник Андрій Вікторович – викладач військової кафедри, Вінницький національний технічний університет, Вінниця; e-mail: andrey.enginer@gmail.com.

Karpus Vitaliy – Assistant to a Military Chaplain of the Armed Forces of Ukraine. e-mail: karpus-v-v@ukr.net.

Kolesnyk Andrii Viktorovych – Lecturer at the Military Department, Vinnytsia National Technical University, Vinnytsia, Ukraine; e-mail: andrey.enginer@gmail.com.