УДК 342.9(477)
DOI https://doi.org/10.32782/klj/2025.4.20

Ричка Д. О.,
кандидат юридичних наук,
доцент кафедри публічного управління та права
ННІ Придніпровська державна академія будівництва та архітектури
Українського державного університету науки та технології
ORCID: 0009-0001-0207-907X

КІБЕРСИЛИ ЗБРОЙНИХ СИЛ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ АНАЛІЗ ПРОЕКТУ ЗАКОНУ УКРАЇНИ «ПРО КІБЕРСИЛИ ЗБРОЙНИХ СИЛ УКРАЇНИ» У ПОРІВНЯННІ З МОДЕЛЯМИ НАТО

Анотація. Стаття присвячена комплексному аналізу проекту Закону України «Про Кіберсили Збройних Сил України», яким передбачається формування окремого військового компонента для ведення операцій у кіберпросторі та електромагнітному спектрі. Мета дослідження – оцінити правові засади, інституційний дизайн і передбачувані повноваження Кіберсил, а також вплив запропонованих норм на права людини та відповідність підходам НАТО. Методологія поєднує нормативно-правовий аналіз, інституційне порівняння з моделями NATO Cyberspace Operations Centre (CyOC) при SHAPE, NATO Integrated Cyber Defence Centre (NICC), доктриною AJP-3.20, а також огляд спроможнісних рамок NCI Agency/NCSC і навчально-дослідницького контуру CCDCOE. Результати свідчать, що законопроект відповідає тенденції інституціоналізації кібероборони та створює передумови для оперативної сумісності з НАТО, зокрема через централізоване командування, акцент на кіберстримуванні та можливість контрактного залучення цивільних фахівців (кіберрезерв). Водночас ідентифіковано ризики дублювання мандатів із вже існуючими у ЗСУ Військами зв'язку та кібербезпеки, недостатню деталізацію міжвідомчої взаємодії (Держспецзв'язку/CERT-UA, СБУ, НПУ, НКЦК при РНБО) та прогалини у процесуальних запобіжниках захисту прав людини (приватність і дані, пропорційність технічних заходів, судовий і парламентський контроль). Запропоновано внесення змін до базових оборонних актів для чіткого «розведення» компетенцій; затвердження SOP/порядків обміну даними й спільних операцій; імплементацію risk-based підходів і внутрішніх аудитів відповідності; інституційне «прошивання» інтерфейсів із CyOC/NICC, програмами NCI Agency та участю у вправах Locked Shields. Практична значущість полягає у формуванні дорожньої карти до другого читання, що поєднує вимоги нацбезпеки з гарантіями прав людини та підвищує стійкість і керованість кібероборони, тоді як наукова новизна – у синтезі правового, інституційного й спроможнісного вимірів порівняльного аналізу України та НАТО.

Ключові слова: *кібероборона, Кіберсили, ЗСУ, НАТО, CyOC, NICC, AJP-3.20, права людини, кіберрезерв, NCI Agency, CCDCOE.*

Rychka D. O. Cyberforces of the armed forces of Ukraine: scientific and practical analysis of the draft law of Ukraine "On cyberforces of the armed forces of Ukraine" in comparison with NATO models

Abstract. The article offers a comprehensive analysis of the Draft Law of Ukraine "On the Cyber Forces of the Armed Forces of Ukraine," which envisages the establishment of a distinct military component tasked with conducting operations in cyberspace and across the electromagnetic spectrum. The study aims to assess the legal foundations, institutional design, and anticipated powers of the Cyber Forces, as well as the implications of the proposed norms for human rights and their alignment with NATO approaches. Methodologically, it combines doctrinal legal analysis with an institutional comparison against the NATO Cyberspace Operations Centre (CyOC) at SHAPE, the NATO Integrated Cyber Defence Centre (NICC), the AJP-3.20 doctrine, and a review of the capability frameworks of the NCI Agency/NCSC alongside the training-and-research ecosystem of the CCDCOE.

The findings indicate that the draft law accords with the broader trend toward the institutionalisation of cyber defence and creates preconditions for operational interoperability with NATO–inter alia through centralised command, an emphasis on cyber deterrence, and the possibility of contracting civilian experts (a cyber reserve). At the same time, the analysis identifies risks of mandate duplication with the Armed Forces' existing Signal and Cyber Security Troops, insufficient specification of inter-agency coordination (involving the State

Service of Special Communications and Information Protection of Ukraine – SSSCIP/CERT-UA, the Security Service of Ukraine – SBU, the National Police of Ukraine – NPU, and the National Cybersecurity Coordination Center – NCCC at the NSDC), and gaps in procedural safeguards for human rights (privacy and data protection, proportionality of technical measures, and judicial as well as parliamentary oversight).

The article proposes amendments to core defence statutes to delineate competences clearly; the adoption of standard operating procedures (SOPs) and protocols for data-sharing and joint operations; the implementation of risk-based approaches and internal compliance audits; and the institutional embedding of interfaces with CyOC/NICC, NCI Agency programmes, and participation in “Locked Shields” exercises. The practical significance lies in outlining a roadmap for the second reading that reconciles national-security requirements with human-rights guarantees while enhancing the resilience and governance of cyber defence. The scholarly contribution consists in synthesising legal, institutional, and capability dimensions within a comparative Ukraine–NATO perspective.

Key words: *cyber defence, Cyber Forces, Armed Forces of Ukraine (AFU), NATO, CyOC, NICC, AJP-3.20, human rights, cyber reserve, NCI Agency, CCDCOE.*

Вступ. 9 жовтня 2025 р. Верховна Рада України ухвалила у першому читанні проект Закону України «Про Кіберсили Збройних Сил України». За це рішення проголосували 255 народних депутатів. Вказаний документ отримав статус «прийнято за основу з доопрацюванням». Це відповідає стратегічній потребі Україні у ведені оборони в кіберпросторі та інтеграції і гармонізації зі стандартами НАТО.

Водночас у чинній структурі Збройних сил України вже існує окремий рід військ – Війська зв’язку та кібербезпеки, що породжує питання про необхідність розмежування повноважень та дублювання функцій і необхідність коригування базових законів.

1. Методологія та джерельна база. Дослідження спирається на: (1) офіційні матеріали Верховної Ради України (картка законопроєкту, оперативна інформація засідання, пресповідомлення), (2) публікації провідних національних ЗМІ про перебіг голосування, (3) доктринальні та інституційні документи НАТО (офіційні сторінки з кібероборони, CyOC при SHAPE, рішення щодо NICC, доктрина AJP-3.20), (4) чинне українське кіберзаконодавство (Закон України «Про основні засади забезпечення кібербезпеки України).

2. Нормативний та інституційний контекст в Україні. Українська національна система кібербезпеки визначена Законом «Про основні засади забезпечення кібербезпеки України», який фіксує ролі Держспецзв’язку (включно з CERT-UA), Служби безпеки України, Національної поліції України, Міністерства оборони України та Національного координаційного центру кібербезпеки при РНБО.

Законопроект № 12349 «Про Кіберсили Збройних Сил України» розвиває саме військову складову цієї системи через створення спеціалізованої структури – Кіберсил.

Паралельно вже існуючі в складі Збройних сил України Війська зв’язку та кібербезпеки, мають закріплені завдання із забезпечення зв’язку, функціонування інформаційних систем, систем бойового управління та участі в національній системі кібербезпеки (включно з кібероборoною). Це потребує точного «розведення» повноважень із новими Кіберсилами.

3. Короткий зміст законопроекту № 12349 «Про Кіберсили Збройних Сил України» визначає правовий статус і засади діяльності Кіберсил, як органу військового управління у складі Збройних сил України, відповідального за кібероборону України, захист суверенітету та територіальної цілісності в кіберпросторі. Кіберсили підпорядковуються Головнокомандувачу Збройних сил України, загальне політичне спрямування здійснює Президент, як Верховний Головнокомандувач.

Передбачено можливість залучення цивільного компонента (кіберрезервістів) на договірній основі для виконання завдань кіберстримування та операцій у кіберпросторі.

4. Порівняння з моделями НАТО. Архітектура управління та планування NATO Cyberspace Operations Centre (CyOC) при SHAPE (м. Монс, Бельгія) забезпечує ситуаційну обізнаність, планування і координацію кібероперацій у системі об’єднаного командування, включно з інтеграцією суверенних

кіберефектів держав-членів. Це «вузол», який зводить цифровий простір до рівня спільного оперативного планування поруч із суходолом, морем та повітрям.

NATO Integrated Cyber Defence Centre (NICC), погоджений у липні 2024 р., розміщено при SHAPE, покликаний посилити захист власних мереж НАТО, об'єднати цивільний і військовий персонал та підвищити стійкість за рахунок сучасних технологій.

AJP-3.20 Allied Joint Doctrine for Cyberspace Operations – базова доктрина НАТО з планування, виконання та оцінки кібероперацій у складі спільних операцій; підтверджує вимогу щодо дотримання міжнародного права.

Висновок для України. Модель Кіберсил доцільно будувати, як оперативно-командний центр у військовій вертикалі з чітким інтерфейсом до національних кіберсуб'єктів (Державна служба спеціального зв'язку та захисту інформації України та функціонуючу у її складі CERT-UA, Служба безпеки України, тощо), за аналогією із CyOC/NICC як «вузлів» інтегрованого планування.

5. Сили, спроможності та підтримка. NCI Agency / NATO Cyber Security Centre (NCSC) забезпечують цілодобовий захист мереж НАТО, розвиток кіберспроможностей, оборонні кібероперації та сервісну підтримку C4ISR – інституційний аналог «тилового» компонента для стійкої кібероборони.

CCDCOE (м. Таллінн Естонія) – багатонаціональний центр передового досвіду, що надає навчання, дослідження і вправи (включно з «Locked Shields» – це щорічні навчання з кіберзахисту, які організовується Центром передового досвіду спільного кіберзахисту НАТО в Таллінні з 2010 року. Формат зазвичай такий, що червона команда імітує ворожу атаку, а сині команди із країн-учасниць імітують свою координацію та захист від цього), розвиває спільні підходи та правові позиції. Україні як учаснику та партнеру доцільно синхронізувати підготовку кадрів Кіберсил із програмами CCDCOE.

6. Політико-правові рамки. НАТО з 2016 р. визнає кіберпростір окремим простором для операцій; істотний кібернапад може досягти порогу впровадження статті 5 Північноатлантичного договору (встановлює принцип колективної оборони, згідно з яким збройний напад на одну державу-члена НАТО розглядається як напад на усіх. Це означає, що у разі нападу всі інші члени зобов'язані надати допомогу, включно із застосуванням збройної сили, для відновлення безпеки в регіоні. Рішення про конкретні заходи приймаються спільно, хоча кожна країна самостійно визначає свій внесок).

Це задає стандарт стримування або/та відповіді, релевантний для планування Кіберсил.

7. Аналітичний розділ: переваги та недоліки сторони законопроекту.

7.1. Перевагами є інституціоналізація кібероборони та сумісність із НАТО. Окремий військовий орган для кібероперацій і кіберстримування є вкрай необхідна відповідь на сучасну війну й шлях до оперативної сумісності з CyOC/NICC. Пряма підпорядкованість Головнокомандувачу Збройних сил України підвищує керованість і швидкість прийняття рішень при виникненні кризових ситуацій. Також слід визначити за позитивне рішення той факт, що планується контрактне залучення висококваліфікованих спеціалістів, що розширює кадрову базу, знижує час та матеріальні витрати, пов'язані із навчанням.

7.2 Як недоліки, необхідно відмітити ті факти, що функції Військ зв'язку та кібербезпеки частково перетинаються із завданнями Кіберсил і без змін до базових актів і чіткого розмежування повноважень, можливі дублювання і втрати керованості. Крім того, виходячи з тексту вказаного проекту вбачається недостатня деталізація міжвідомчої координації. Потрібні формалізовані протоколи взаємодії з Державною службою спеціального зв'язку та захисту інформації, спецпідрозділів Служби безпеки України, Національної поліції України та Національним координаційним центром кібербезпеки при РНБО України (обмін даними, спільні операції, розмежування повноважень).

Відкриті матеріали першого читання не розкривають бюджет, чисельність, етапність розгортання, що ускладнює оцінку здійсненності. (Цей висновок зроблений на підставі публічних оглядів і картки законопроєкту.)

7.3 Вплив на права людини. Операції Кіберсил можуть у певних випадках стосуватися обробки персональних даних або тимчасового технічного впливу на мережі поза суто військовим контуром. Для мінімізації ризиків необґрунтованого втручання слід прямо відсилати до сфер дії Кримінально-процесуального законодавства України та спецзаконів (оперативно-розшукові, контррозвідувальні заходи), встановити судовий та парламентський контроль, вимоги до зберігання та знищення даних і внутрішній моніторинг, передбачити інші дії, для синхронізації з Законом України «Про основні засади забезпечення кібербезпеки України».

За умови контрдій інформаційно-технічним операціям ворога важливо уникати «надмірного впливу» на законну комунікацію цивільних осіб, рамки мандату Кіберсил мають бути чітко відмежовані від діяльності інших органів та демонструвати пропорційність (стандарти НАТО/AJP-3.20 вимагають дотримання міжнародного права).

7.3 До повноважень майбутніх Кіберсил входитиме підготовка й проведення військових кібероперацій, кіберстримування, захист військових інформаційно-телекомунікаційних технологій та автоматизованих систем управління, операції у спектрі, формування й використання кіберрезерву, взаємодія з партнерами та НАТО.

Головнокомандувач Збройних сил України та Президент України будуть здійснювати безпосереднє військове керівництво Кіберсилами; загальне політичне спрямування – у відповідності до чинних оборонних норм.

Інші суб'єкти нацсистеми кібербезпеки: Державна служба спеціального зв'язку та захисту інформації України та функціонуючу у її складі CERT-UA, Служба безпеки України, Національна поліція України, Національний координаційний центр кібербезпеки при РНБО України – зберігають власні повноваження. Необхідні письмово закріплені межі компетенцій (оперативні протоколи, обмін даними, чітко встановлені юрисдикції) для уникнення дублювань.

Ключовими ризиками реалізації, на наш погляд може стати кадровий дефіцит, який неодмінно виникне у зв'язку з конкуренцією з приватним сектором, ресурсні (фінансові та апаратні) обмеження воєнного часу, затримки з нормативним перерозподілом повноважень.

8. Рекомендації до другого читання. Необхідно внести зміни до законів, що визначають роди військ та органи військового управління, закріпивши місце Кіберсил, а також чітке розмежування повноважень із Військами зв'язку та кібербезпеки.

Слід затвердити порядок взаємодії Кіберсил Збройних сил України із Державної служби спеціального зв'язку та захисту інформації, Служби безпеки України, Національної поліції (обмін даними, спільні операції, реагування на інциденти, юрисдикції).

Необхідно передбачити судовий або парламентський контроль у разі виникнення питання, щодо додержання прав людини, затвердити правила обробки, збереження, знищення даних, внутрішні аудити відповідності (у т.ч. на кшталт risk-based підходів НАТО/AJP-3.20).

Крім того, більш чітко передбачити оперативну сумісність з НАТО: інституційно передбачити взаємодію із CyOC/NICC, програмами NCI Agency та навчальним контуром CCDCOE (сертифікації, SOP, участь у Locked Shields).

Висновки. Законопроєкт № 12349 є своєчасним кроком з огляду на характер сучасної війни та стандарти НАТО. Його перевага – у створенні чіткої військової вертикалі для кібероборони і можливості залучення кіберрезерву; недоліки – потенційні колізії з уже існуючими інститутами та недостатня деталізація процедурних запобіжників. За умови доопрацювання до другого читання у напрямі узгодженості мандатів, міжвідомчої координації й гарантій прав людини, Кіберсили можуть стати центральним елементом української кібероборони, сумісним із архітектурою CyOC/NICC та доктриною AJP-3.20.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Проект Закону України «Про Кіберсили Збройних Сил України» : картка законопроєкту № 12349 від 19.12.2024 [Електронний ресурс]. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453 (дата звернення: 12.10.2025). itd.rada.gov.ua

2. Верховна Рада України. Кіберсили Збройних Сил України (пресповідомлення) [Електронний ресурс]. 09.10.2025. URL: https://www.rada.gov.ua/print/266780.html (дата звернення: 12.10.2025). Верховна Рада України

3. Оперативна інформація засідання ВРУ (щодо результатів голосування) [Електронний ресурс]. 09.10.2025. URL: https://www.rada.gov.ua/meeting/faxiv/show/8598.html (дата звернення: 12.10.2025). Верховна Рада України

4. Суспільне. Рада в першому читанні ухвалила законопроєкт № 12349 про створення Кіберсил ЗСУ [Електронний ресурс]. 09.10.2025. URL: https://suspilne.media/1134650-rada-pidtrimala-stvorenna-kibersil-zsu/ (дата звернення: 12.10.2025). Суспільне | Новини

5. LIGA.net. Rada adopts draft law on cyber forces of the Armed Forces as a basis [Електронний ресурс]. 09.10.2025. URL: https://news.liga.net/en/politics/news/rada-adopts-draft-law-on-cyber-forces-of-the-armed-forces-as-a-basis (дата звернення: 12.10.2025). LIGA.net

6. Укрінформ. Рада підтримала створення Кіберсил ЗСУ [Електронний ресурс]. 09.10.2025. URL: https://www.ukrinform.ua/rubric-polytics/4045455-rada-pidtrimala-stvorenna-kibersil-zsu.html (дата звернення: 12.10.2025). Укрінформ

7. Міноборони України. Війська зв’язку та кібербезпеки – окремий рід військ ЗСУ [Електронний ресурс]. URL: https://mod.gov.ua/pro-nas/vijska-zv-yazku-ta-kiberbezpeki (дата звернення: 12.10.2025). mod.gov.ua

8. Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-viii (дата звернення: 12.10.2025). Законодательство Украины

9. NATO. Cyber defence – офіційна сторінка теми [Електронний ресурс]. Оновл. 30.07.2024. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 12.10.2025). NATO

10. SHAPE (ACO). Cyber Defence / Cyberspace Operations Centre (CyOC) [Електронний ресурс]. URL: https://shape.nato.int/about/aco-capabilities2/cyber-defence (дата звернення: 12.10.2025). shape.nato.int

11. NATO. Allies agree new NATO Integrated Cyber Defence Centre (NICC) [Електронний ресурс]. 10.07.2024. URL: https://www.nato.int/cps/en/natohq/news_227647.htm (дата звернення: 12.10.2025). NATO

12. GOV.UK / UK MoD. Allied Joint Doctrine for Cyberspace Operations (AJP-3.20) [Електронний ресурс]. Оновл. 17.03.2023. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320 (дата звернення: 12.10.2025). GOV.UK

13. NCI Agency – офіційний сайт (місія, кіберспроможності) [Електронний ресурс]. URL: https://www.ncia.nato.int/ (дата звернення: 12.10.2025). ncia.nato.int

14. CCDCOE – About us (місія та напрями) [Електронний ресурс]. URL: https://ccdcoe.org/about-us/ (дата звернення: 12.10.2025). ccdcoe.org

Дата першого надходження рукопису до видання: 12.11.2025
Дата прийнятого до друку рукопису після рецензування: 10.12.2025
Дата публікації: 30.12.2025