

УДК 355.45

DOI <https://doi.org/10.32782/chern.v4.2025.35>**Ю. О. Волошин**

доктор юридичних наук, професор  
професор кафедри міжнародного та європейського права  
Київського авіаційного інституту  
[orcid.org/0009-0004-4482-8317](https://orcid.org/0009-0004-4482-8317)

**А. О. Шаповал**

аспірант факультету права та міжнародних відносин  
Київського авіаційного інституту  
[orcid.org/0009-0007-9585-3725](https://orcid.org/0009-0007-9585-3725)

## ДЕРЖАВНИЙ СУВЕРЕНІТЕТ В УМОВАХ ЗБРОЙНИХ КОНФЛІКТІВ ТА ВІЙН: СУЧАСНІ ВИКЛИКИ ТА ДОКТРИНАЛЬНІ ПІДХОДИ

У статті здійснено комплексне дослідження трансформації поняття державного суверенітету в умовах гібридних і збройних конфліктів, які стали однією з визначальних характеристик сучасних міжнародних відносин. Класичне уявлення про суверенітет як про верховенство влади держави у межах своєї території та її незалежність від зовнішнього впливу сьогодні зазнає суттєвої еволюції. Сучасні форми конфліктів, що поєднують воєнні, інформаційні, економічні та кібернетичні засоби впливу, розмивають межі між війною та миром, між зовнішньою агресією та внутрішньою дестабілізацією. Це вимагає нового погляду на структуру та зміст суверенітету як ключової категорії міжнародного права.

Розкрито теоретико-доктринальні підходи до осмислення суверенітету у працях класиків, а також проаналізовано їхнє сучасне переосмислення у контексті міжнародно-правових викликів ХХІ століття. Показано, що розвиток міжнародного права та зростання впливу наднаціональних інституцій спричинили поступовий перехід від концепції абсолютного суверенітету до концепції взаємозалежного або функціонального суверенітету, який співіснує з принципами колективної безпеки, прав людини та глобальної відповідальності держав.

Окрему увагу приділено феномену гібридної війни як формі збройного протистояння, де поєднуються класичні воєнні дії з нетрадиційними методами – інформаційними кампаніями, кібератаками, санкційним тиском, втручанням у виборчі процеси, маніпуляцією суспільною думкою. На прикладі агресії російської федерації проти України розкрито, як саме гібридна війна стала каталізатором переосмислення державного суверенітету не лише як політико-правової, а й як технологічної та інституційної категорії. Український досвід продемонстрував, що забезпечення суверенітету у ХХІ столітті неможливе без інтеграції військової, дипломатичної, інформаційної, правової, культурної та цифрової політики.

У роботі аргументовано, що традиційні норми міжнародного права (зокрема принципи суверенної рівності та невтручання, закріплені у Статуті ООН) не завжди здатні забезпечити належну реакцію на новітні виклики. Це зумовлює потребу у правовій модернізації міжнародних механізмів, включно з уточненням дефініцій «збройної агресії», «гібридного нападу» та «кіберагресії». Розглянуто роль міжнародних організацій – ООН, ОБСЄ, НАТО, ЄС – у розробленні нових стандартів колективної безпеки, санкційної політики, кібероборони та правової відповідальності держав.

У статті також введено поняття «цифрового суверенітету» як нової наукової категорії, що формується на перетині міжнародного права, інформаційної безпеки та технологічного розвитку.

У підсумку обґрунтовано, що майбутня доктрина суверенітету має ґрунтуватися на триєдиній моделі – військовій, правовій та технологічній – із домінуванням правового регулювання як гаранта стабільності міжнародного порядку.

**Ключові слова:** державний суверенітет; цифровий суверенітет; гібридна війна; міжнародне право; міжнародні організації; доктрина міжнародного права; правова модернізація; трансформація.

### **Voloshyn Yu. O., Shapoval A. O. STATE SOVEREIGNTY IN THE CONTEXT OF ARMED CONFLICTS AND WARS: CURRENT CHALLENGES AND DOCTRINAL APPROACHES**

The article presents a comprehensive study of the transformation of the concept of state sovereignty in the context of hybrid and armed conflicts, which have become one of the defining characteristics of contemporary international relations. The classical understanding of sovereignty as the supreme authority of the state within its territory and its independence from external influence is undergoing significant evolution. Modern forms of conflict – combining military, informational, economic, cyber, and psychological instruments of influence – blur the boundaries between war and peace, as well as between external aggression and internal destabilization. This calls for a new perspective on the structure and content of sovereignty as a fundamental category of international law.

The paper reveals theoretical and doctrinal approaches to the interpretation of sovereignty in the works of classical theorists and analyzes their modern reinterpretation in light of the international legal challenges of the twenty-first century. It demonstrates that the development of international law and the growing influence of supranational institutions have led to a gradual shift from the concept of absolute sovereignty to that of interdependent or functional sovereignty, which coexists with the principles of collective security, human rights, and the global responsibility of states.

Particular attention is devoted to the phenomenon of hybrid warfare as a form of armed confrontation that combines traditional military operations with non-traditional methods – information campaigns, cyberattacks, sanctions pressure, electoral interference, and manipulation of public opinion. Using the example of the Russian Federation's aggression against Ukraine, the study shows how hybrid warfare has become a catalyst for the rethinking of state sovereignty not only as a political and legal category but also as a technological and institutional one. The Ukrainian experience demonstrates that ensuring sovereignty in the twenty-first century is impossible without the integration of military, diplomatic, informational, legal, cultural, and digital policies.

The paper argues that traditional norms of international law – in particular, the principles of sovereign equality and non-interference enshrined in the UN Charter – are not always capable of providing an adequate response to new challenges. This necessitates the legal modernization of international mechanisms, including the clarification of definitions such as “armed aggression,” “hybrid attack,” and “cyber aggression.” The role of international organizations – including the United Nations, the OSCE, NATO, and the European Union – is examined in the development of new standards of collective security, sanctions policy, cyber defense, and state accountability.

The article also introduces the concept of “digital sovereignty” as a new scholarly category emerging at the intersection of international law, information security, and technological development.

In conclusion, it is substantiated that the future doctrine of sovereignty should be based on a threefold model – military, legal, and technological – with the predominance of legal regulation as a guarantor of stability and predictability in the international order.

*Key words:* state sovereignty; digital sovereignty; hybrid war; international law; international organizations; doctrine of international law; legal modernization; transformation.

У сучасному світі державний суверенітет, як основоположна категорія міжнародного права, зазнає суттєвої трансформації під впливом гібридних і збройних конфліктів, що поєднують воєнні, економічні, інформаційні, кібернетичні та політичні засоби впливу. Паралельно формується новий вимір – цифровий суверенітет, який розглядається як складова державного контролю над інформаційним і технологічним простором [1, с. 1]. Класичне розуміння суверенітету як виключної влади держави над територією та населенням еволюціонує у відповідь на багатовимірні виклики, де збройний, правовий і цифровий виміри взаємопов'язані.

Поняття державного суверенітету має глибоке історичне коріння. У класичному розумінні Жана Бодена суверенітет означає найвищу владу у межах держави, яка не підлягає зовнішньому впливу. У подальшому цю концепцію розвивали Томас Гоббс, Жан-Жак Руссо та інші мислителі [2]. У XX столітті традиційне уявлення про абсолютний суверенітет поступово змінюється на концепцію обмеженого суверенітету, який співіснує із міжнародними зобов'язаннями держав, правами людини та механізмами міжнародної відповідальності. Зокрема, у міжнародному праві принцип невтручання та поваги до територіальної цілісності є підґрунтям суверенітету держав, проте, у сучасних умовах він дедалі частіше порушується через неконвенційні форми втручання. У міжнародному праві поняття та сутність державного суверенітету закріплене у Статуті ООН (ст. 2), що проголошує принцип суверенної рівності держав та недопущення втручання у їхні внутрішні справи [3, ст. 2].

Як ми зазначили, державний суверенітет традиційно означає повну незалежність і верховенство влади на певній території, а також свободу від зовнішнього втручання. Водночас,

мусимо констатувати, що гібридні війни ставлять це визначення під сумнів. Зовнішній тиск може здійснюватися без перетину кордону, через медіа, соціальні мережі, економічні санкції, політичне лобювання чи, навіть, втручання у вибори. Все це створює ситуації, коли держави втрачають контроль над інформаційним простором, не маючи формального порушення територіальної цілісності [4, с. 145].

Сучасні міжнародні відносини дедалі більше характеризуються використанням нестандартних методів ведення війни. Одним із найнебезпечніших явищ ХХІ століття стала гібридна війна [5, с. 98]. Гібридна війна як явище передбачає комплексну, багатоформатну агресію, що поєднує як прямі військові дії, так і непрямі інструменти впливу: дезінформацію, втручання у вибори, кібератаки, блокаду економіки тощо. Унаслідок цього традиційна модель суверенітету виявляється недостатньою для повного захисту держави. Порушення кордонів сьогодні часто здійснюється не за допомогою важкої військової техніки, а у цифровій площині – комп'ютерними вірусами чи інформаційними операціями [6, с. 28–29]. Особливістю сучасних гібридних конфліктів є їхня складність і розмитість меж між війною та миром. Такі форми агресії дозволяють державам-агресорам уникати прямої відповідальності, водночас підриваючи основи суверенітету країни-жертви [5, с. 101].

Гібридна війна – це форма конфлікту, в якій застосовуються різні інструменти впливу, зокрема військові, економічні, інформаційні, дипломатичні та кібертехнології, з метою досягнення політичних цілей без офіційного оголошення війни. Основна мета – ослаблення чи підірив внутрішньої стабільності противника, послаблення довіри до державних інституцій та деморалізація населення. Така війна ведеться як

зовні, так і всередині держави, охоплюючи всі сфери суспільного життя [7].

Сьогодні Україна стала яскравим прикладом держави, чий суверенітет зазнає постійних гібридних атак з боку іншої держави. Починаючи з анексії Криму в 2014 році, через конфлікт на Донбасі та повномасштабне вторгнення у 2022 році, Україна змушена переосмислювати підходи до забезпечення свого суверенітету.

Умови гібридного протистояння вимагають перегляду як національних, так і міжнародно-правових концепцій суверенітету. Йдеться не лише про захист території, а й про утвердження інформаційного та цифрового вимірів державності через захист у тому числі цифрового суверенітету. Питання легітимності протидії гібридній агресії, відповідальності агресора, захисту інформаційного простору, забезпечення кібербезпеки кожної сучасної держави виходять на перший план. Крім того, міжнародні організації повинні адаптувати свої механізми до нових реалій, де агресія не завжди має ознаки відкритої війни. Зокрема, створення кібервійськ, впровадження системи стратегічних комунікацій, дипломатична мобілізація та посилення нормативно-правової бази мають стати елементами нового, комплексного бачення державного суверенітету [7].

Війна росії проти України після 2014 року стала класичним прикладом гібридної агресії – із залученням “зелених чоловічків”, інформаційних атак, економічного тиску, дестабілізації політичної системи та прямих воєнних дій.

На жаль, гібридна війна ускладнює застосування класичних норм міжнародного права, оскільки часто не має чітко визначеного акта агресії. Такі ситуації ставлять виклики перед ООН, ОБСЄ та іншими міжнародними організаціями, що зобов’язані реагувати на загрози суверенітету. Необхідність адаптації міжнародного права до нових форм конфліктів стає нагальною, зокрема і в частині визначення гібридної агресії як форми збройного нападу [8, с. 15].

В умовах гібридної загрози суверенітет більше не може розглядатися лише як фізичний контроль над територією. Державам необхідно інвестувати в інформаційну, кібернетичну та психологічну безпеку. Крім того, важливим є розвиток нормативної бази, яка дозволить оперативно фіксувати факти гібридної агресії та притягати агресора до відповідальності. Міжнародна спільнота повинна діяти скоординовано, щоб не допустити руйнування системи міжнародної колективної безпеки [5; 7].

Україна, маючи унікальний досвід боротьби з гібридною агресією, може виступати лідером у формуванні нової концепції захисту суве-

ренітету в умовах трансформації міжнародної безпеки.

Українська доктрина державного суверенітету за останнє десятиліття зазнала суттєвих змін, зумовлених безпрецедентним викликом з боку росії. Науковці акцентують увагу на необхідності активного захисту суверенітету не лише в межах територіальної оборони, але й у кіберпросторі, інформаційному та культурному середовищі. Міжнародна доктрина також визнає зміну парадигми – поняття “responsibility to protect”, інститути колективної безпеки та санкційна політика стають елементами нового підходу до забезпечення суверенітету. Водночас, спостерігається дискусія про допустимість втручання внутрішніх справ держав у випадках гібридної загрози, що породжує колізії між принципом невтручання та необхідністю захисту фундаментальних прав і безпеки [4, с. 125].

З початку анексії Криму та збройного конфлікту на Донбасі, а згодом – повномасштабного вторгнення, Україна стала полем випробування міжнародно-правових механізмів забезпечення суверенітету. У відповідь на гібридну агресію держава розвинула систему стратегічних комунікацій, реформувала Збройні Сили, активізувала кіберзахист, посилила дипломатичний фронт та розширила міжнародні союзи. Значну роль у протидії агресії відіграє також внутрішня консолідація українського суспільства. Україна подає приклад модернізації концепції суверенітету як активного, захисного та багатовимірного процесу, що включає як військову, так і гуманітарну компоненти [6].

Тобто, сьогодні традиційне розуміння державного суверенітету, що базувалося на уявленні про монополію держави на легітимне застосування сили в межах її території, поступово трансформується в новітню доктрину, що включає розширення змісту цього поняття на інформаційний, кібернетичний, культурний та економічний виміри.

Українські науковці та експерти вказують на потребу перегляду статичної правового уявлення про суверенітет. Якщо раніше увага зосереджувалась переважно на проблематиці територіальної цілісності та охороні державних кордонів, то тепер ключовими аспектами стали захист цифрового простору, протидія інформаційним атакам, збереження ідентичності та культурного середовища. Наприклад, розширене тлумачення суверенітету включає право держави на контроль за власним інформаційним полем, цифровими платформами та засобами комунікації, що набули стратегічного значення в умовах гібридної агресії [9, с. 148–149].

Міжнародна доктрина державного суверенітету також еволюціонує, хоча не завжди однознач-

но. Зокрема, концепція “Responsibility to Protect” (R2P), що виникла як відповідь на масові порушення прав людини, запровадила прецедент, коли міжнародне співтовариство може (і має) втручатися у внутрішні справи держави задля захисту цивільного населення. Ця доктрина порушує класичний принцип невтручання, закладений у Статуті ООН, та демонструє конфлікт між двома фундаментальними засадами міжнародного права – повагою до суверенітету та необхідністю забезпечення міжнародної безпеки [5].

Паралельно з цим, інститути колективної безпеки, як-от НАТО чи ЄС, почали активніше застосовувати механізми стримування через санкції, кібервідповідь, контрпропаганду, інформаційне протиборство. Санкційна політика стала одним із базових елементів нової системи захисту державного суверенітету, зокрема, у випадках, коли класичні методи (збройне втручання або миротворчі місії) є юридично чи політично неможливими.

Водночас на міжнародному рівні триває жвава дискусія щодо меж втручання у внутрішні справи держав. Питання полягає у тому, наскільки гібридна загроза може бути підставою для перегляду класичних принципів, зокрема: невтручання, суверенної рівності та ненасильства. Ці колізії залишаються невирішеними, а міжнародне право часто виявляється неспроможним оперативно реагувати на складні, багатofакторні конфлікти, які не мають ознак класичної війни [8, с. 17].

Таким чином, у вітчизняній доктрині утверджується концепція активного суверенітету, що передбачає не тільки оборону, а й проактивну позицію держави в інформаційній, цифровій, економічній та гуманітарній сферах. Міжнародна доктрина, своєю чергою, демонструє поступовий перехід до адаптивного суверенітету, де державність розглядається як динамічний феномен, здатний до правового та інституційного оновлення відповідно до змін глобальної безпеки.

Не менш важливою є інформаційна та культурна складова спротиву. Україна посилила державну політику у сфері мовної, історичної та культурної безпеки. Відбулася системна боротьба з російською пропагандою, дезінформацією, використанням соціальних мереж та медіа для розпалювання внутрішніх конфліктів. Прийняття законів про медіа, інформаційну безпеку, а також санкцій щодо пропагандистських каналів стали важливими кроками у формуванні інформаційного суверенітету.

Окремо варто відзначити дипломатичну складову української стратегії. З 2014 року Україна активно працює над створенням міжнародних коаліцій, зокрема у межах ООН, Ради Європи, Міжнародного кримінального суду. Україна іні-

ціювала десятки резолюцій, звернень та позовів до міжнародних інституцій, спрямованих на визнання фактів агресії, порушень прав людини, а також на притягнення росії до міжнародної відповідальності.

Важливим фактором стало також підвищення рівня внутрішньої консолідації. Українське суспільство, попри намагання агресора спровокувати розкол, продемонструвало високий рівень солідарності, самоорганізації та готовності до оборони держави. Це сприяло формуванню нового бачення суверенітету як не лише юридичного, а й соціального, національного та морального явища [6, с. 29–30].

Україна продемонструвала приклад ефективної адаптації до умов гібридної агресії, сформувавши комплексну модель захисту суверенітету. Ця модель передбачає поєднання класичних методів (збройна оборона, дипломатія) із новітніми (кібербезпека, інформаційна стійкість, культурна політика). Український досвід уже сьогодні розглядається як зразок для інших держав, що можуть зіткнутися з аналогічними викликами.

У сучасній науковій доктрині з’являється нова категорія – цифровий суверенітет, що формується на стику міжнародного права, інформаційної безпеки та технологічного розвитку. Під цим поняттям пропонується розуміти спроможність держави здійснювати повноваження та контроль у цифровому просторі, включаючи національні інформаційні ресурси, критичну інфраструктуру, потоки даних, алгоритми та цифрові платформи, що мають суспільно-значущий характер [11, с. 13–14]. Цифровий суверенітет є не самостійним різновидом державності, а функціональним виміром державного суверенітету, який доповнює класичні територіальний та політико-правовий аспекти. Відповідно, сучасна концепція державного суверенітету дедалі частіше трактується як триєдина система – військова, правова та технологічна.

Таким чином, Україна перетворила концепцію суверенітету на динамічний, багаторівневий процес, що охоплює не лише зовнішній, а й внутрішній захист державності, забезпечення ідентичності, стабільності та стійкості до сучасних загроз. Гібридні конфлікти і війни суттєво змінюють підходи до розуміння та реалізації державного суверенітету. Умовна незворушність кордонів, виключна юрисдикція і монополія на силу більше не є достатніми критеріями для визначення суверенітету. Нові реалії потребують гнучкого і динамічного тлумачення цього поняття, а також розробки дієвих механізмів міжнародного реагування на загрози. Український досвід може стати основою для формування нової парадигми державного суверенітету, адаптованої до умов гібридного світу.

### Література

1. Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. *Journal of Digital Technologies and Law*, 1(3), 673–690. <https://doi.org/10.21202/jdtl.2023.29>
2. Боден// *Юридична енциклопедія* : [у 6 т.] / ред. кол.: Ю. С. Шемшученко (відп. ред.) [та ін.]. К. : Українська енциклопедія ім. М. П. Бажана, 1998. Т. 1 : А–Г. С. 254. ISBN 966-7492-01-X.
3. Статут Організації Об'єднаних Націй від 26 червня 1945 р. *Офіційний вісник України*. 2006. № 17. С. 83–108.
4. Коваль І. П. *Державний суверенітет у контексті глобалізаційних викликів*: монографія. Львів: ЛНУ імені Івана Франка. 2018. 280 с.
5. Мартинюк Р. І. *Інформаційна безпека в умовах гібридної війни: правовий вимір*. Одеса: Фенікс. 2020. 200 с.
6. Гавриленко В. В. *Гібридна війна як виклик національній безпеці України: правовий аспект*. Вісник Національного університету оборони України. 2017. № 1(50). С. 28–34.
7. Задорожний О. В. *Актуальні проблеми міжнародного гуманітарного права*: монографія. Київ: Юридична думка. 2021. 312 с.
8. Лукашевич І. В. *Гібридні війни: правові механізми захисту суверенітету держав*. *Юридичний вісник України*. 2020. № 7(1419). С. 14–19.
9. Калайда Ю. П. *«Забезпечення цифрового суверенітету в умовах геополітичного протистояння: кращі практики зарубіжного досвіду»*. *Інформація і право*. 2021. № 2(37). С. 145–154.
10. Савченко В. А. *Кібербезпека держави в умовах гібридної агресії*. Харків: Право. 2021. 224 с.
11. Бесчастний В., Костицький М., Кушакова-Костицька Н. *Цифровий конституціоналізм: нова парадигма та перспективи розвитку в Україні*. *Філософія права і загальна теорія права*. 2023. № 2(25). С. 9–26.

Дата першого надходження рукопису до видання: 30.09.2025  
Дата прийнятого до друку рукопису після рецензування: 27.10.2025  
Дата публікації: 26.11.2025