Інформаційне право

УДК 327:004.738:004.056:341.232.7:351.746(100):327.56-047.37

DOI https://doi.org/10.5281/zenodo.19924866

Інтеграція протоколів кібердипломатії у механізми стримування міждержавних конфліктів у цифровому просторі

Новоскольцева Людмила Олександрівна,
кандидат політичних наук, доцент, завідувач кафедри політології і міжнародних відносин, факультет соціальних і гуманітарних наук, Луганський національний університет імені Тараса Шевченка, м. Лубни, Україна, https://orcid.org/0000-0003-1082-7979

Демідов Денис Валерійович,
доктор філософії, доцент, доцент кафедри політології і міжнародних відносин, факультет соціальних і гуманітарних наук Луганський національний університет імені Тараса Шевченка, м. Лубни, Україна, https://orcid.org/0009-0006-9545-1307

Прийнято: 14.03.2026 | Опубліковано: 30.03.2026

Анотація. Мета. У статті здійснено теоретико-прикладне обґрунтування інтеграції протоколів кібердипломатії у механізми стримування міждержавних конфліктів у цифровому просторі з урахуванням зміни природи міжнародної конфронтації, переходу від епізодичних реакцій на кіберінциденти до постійного керування ризиками ескалації, а також посилення ролі коаліційних форматів реагування. **Методи.** Методологічну основу дослідження становить комплекс взаємодоповнювальних підходів, що

поєднує структурно-функціональний підхід і порівняльний аналіз із контент-аналізом наукових праць 2021–2026 років. Зазначений інструментарій доповнено кейс-орієнтованою інтерпретацією практик публічної атрибуції, інституційним моделюванням та напівкількісним оціночним шкалюванням, що забезпечує поєднання теоретичного узагальнення із прикладним виміром дослідження. Для емпіричного обґрунтування отриманих результатів сформовано авторську матрицю, яка дає змогу вимірювати рівень інтеграції кібердипломатичних протоколів за п'ятьма параметрами, а саме: раннє попередження, скоординована атрибуція, правове та санкційне узгодження, спільна кіберстійкість і канали деескалації. **Результати.** Доведено, що кібердипломатія виконує стримувальну функцію не тоді, коли зводиться до декларативного засудження інциденту, а тоді, коли поєднує політико-дипломатичні, комунікаційні, правові та технічні протоколи в єдиний цикл реагування. Установлено, що найбільш ефективними є ті моделі, у яких дипломатичний сигнал підкріплюється узгодженими процедурами обміну інформацією, заздалегідь визначеними правилами публічної атрибуції, багаторівневими каналами кризового зв'язку та програмами спільного підвищення стійкості. З огляду на це запропоновано індекс інтеграції протоколів кібердипломатії, апробація якого на п'яти порівнюваних моделях засвідчила вищу результативність коаліційно-мережевих форматів порівняно з ізольованими національними підходами. **Висновки.** Обґрунтовано, що дієве стримування у цифровому просторі формується через інституціоналізацію повторюваних, передбачуваних і взаємно визнаних протоколів, які зменшують невизначеність, підвищують політичну ціну агресивних дій і водночас залишають простір для контрольованої деескалації. Практична цінність дослідження полягає в розробленні інтеграційної моделі, придатної для адаптації у безпековій політиці держав, що поєднують потребу в жорсткому стримуванні з необхідністю збереження комунікаційних каналів у кризових умовах.

ISSN: 3041-2110

Ключові слова: атрибуція кібератак, кризова комунікація, коаліційне реагування, довірчі заходи, кіберстійкість, санкційна координація, міждержавна деескалація, цифрове урядування.

Integrating Cyber Diplomacy Protocols into Deterrence Mechanisms for Interstate Conflicts in Digital Space

Lyudmila Novoskoltseva,
Candidate of Political Sciences, Associate Professor, Head of the Department of Political Science and International Relations, Faculty of Social and Humanitarian Sciences, Taras Shevchenko Luhansk National University, Lubny, Ukraine, https://orcid.org/0000-0003-1082-7979

Denys Demidov,
Ph.D., Associate Professor, Associate Professor of the Department of Political Science and International Relations, Faculty of Social and Humanitarian Sciences, Taras Shevchenko Luhansk National University, Lubny, Ukraine, https://orcid.org/0009-0006-9545-1307

Abstract. Objective. The article provides a theoretical and applied substantiation of the integration of cyberdiplomacy protocols into mechanisms for deterring interstate conflicts in the digital space, taking into account the changing nature of international confrontation, the transition from episodic responses to cyber incidents toward the continuous management of escalation risks, and the growing role of coalition-based response formats. **Methods.** The methodological foundation of the study comprises a set of complementary approaches that combines a structural-functional approach and comparative analysis with the content analysis of scholarly works published between 2021 and 2026. This toolkit is supplemented by case-oriented interpretation of public attribution practices, institutional modeling,

and semi-quantitative evaluative scaling, thereby ensuring the integration of theoretical generalization with the applied dimension of the research. To provide empirical grounding for the results obtained, an author-developed matrix was constructed that enables the measurement of the level of integration of cyberdiplomacy protocols across five parameters, namely: early warning, coordinated attribution, legal and sanctions alignment, joint cyber resilience, and de-escalation channels. **Results.** It is demonstrated that cyberdiplomacy performs a deterrent function not when it is reduced to a declarative condemnation of an incident, but when it integrates political-diplomatic, communicational, legal, and technical protocols into a unified response cycle. The most effective models are those in which the diplomatic signal is reinforced by coordinated information-sharing procedures, predefined rules of public attribution, multilevel crisis communication channels, and joint resilience-enhancement programs. Accordingly, an index of cyberdiplomacy protocol integration is proposed, the testing of which across five comparable models confirmed the higher effectiveness of coalition-network formats relative to isolated national approaches. **Conclusions**. It is substantiated that effective deterrence in the digital space is formed through the institutionalization of recurrent, predictable, and mutually recognized protocols that reduce uncertainty, raise the political cost of aggressive actions, and simultaneously preserve space for controlled de-escalation. The *practical value of the study* lies in the development of an integration model suitable for adaptation within the security policies of states that combine the need for robust deterrence with the imperative of maintaining communication channels under crisis conditions.

Keywords: cyberattack attribution, crisis communication, coalition response, confidence-building measures, cyber resilience, sanctions coordination, interstate de-escalation, digital governance.

Постановка проблеми. Міждержавні конфлікти у цифровому просторі дедалі рідше розгортаються як одиничні технічні інциденти, натомість набувають форми багаторівневого тиску, у межах якого кібератаки,

інформаційні операції, публічна атрибуція, санкційні сигнали, спроби нав'язати власне тлумачення міжнародних норм та демонстративне нарощування технологічних спроможностей функціонують як елементи єдиного конфліктного процесу. За таких умов стримування перестає бути виключно військовою або суто технічною категорією і дедалі більшою мірою залежить від здатності держав розбудовувати передбачувані дипломатичні протоколи кризової взаємодії.

Проблемність наявної ситуації полягає у фрагментованості міжнародної практики реагування на кіберагресивні дії. Зокрема, частина держав тяжіє до жорсткої логіки публічного засудження та санкційної відповіді; друга – до мінімізації публічності й переходу до технічного врегулювання; решта – до формування гібридних моделей, у яких кібердипломатія поєднується з інструментами стратегічних комунікацій, правового сигналювання та коаліційного підвищення стійкості. Відсутність стандартизованих протоколів посилює невизначеність, ускладнює оцінку намірів сторін та збільшує ризик хибної ескалації. З огляду на це особливої ваги набуває питання не лише про те, якими мають бути дипломатичні дії у відповідь на кіберінцидент, а й про те, яким чином вони інтегруються в ширший механізм стримування. Отже, науково-практичне завдання полягає у виробленні такої моделі кібердипломатії, за якої дипломатичні протоколи не супроводжують конфлікт постфактум, а вбудовуються у його попередження, локалізацію, деескалацію та післякризове врегулювання.

Аналіз останніх досліджень і публікацій. Наукове розуміння кібердипломатії формується на перетині безпекових, комунікаційних і нормативних підходів. Зокрема, у дослідженні А. Лупини (A. Lupyna) продемонстровано продуктивність сценарного моделювання стійкості в умовах гібридних інформаційних загроз та наголошено на значенні цифрового середовища, стратегічних комунікацій і соціальної резильєнтності для протидії деструктивним впливам [1]. Наведене положення є показовим для

обраної теми з огляду на те, що міждержавний цифровий конфлікт дедалі частіше поєднує технічну дестабілізацію з інформаційно-психологічним тиском. У суголосному ключі А. Барріна (A. Barrinha) інтерпретував кібердипломатію як транзитне, проте вже достатньо оформлене поле дипломатичної практики, у якому взаємодіють державні інтереси, норми відповідальної поведінки та нові режими глобального врядування [2, p. 439].

Регіональний вимір досліджуваної проблеми переконливо представлений у працях, присвячених Азійсько-Тихоокеанському регіону та євроатлантичному простору. Так, М. Мананган (M. Manantan) довів, що посилення кіберзагроз і стратегічної конкуренції зумовило зростання ролі стримування всередині кібердипломатичних практик Японії та Австралії, де дипломатичні зусилля дедалі виразніше поєднуються з логікою довірчих заходів, інституційної координації та спільної безпекової підготовки [3, p. 432]. Крім того, К.-Е. Кирну та співавтори (C.-E. Cîrnu et al.) на матеріалі Європейського Союзу (ЄС) і Сполучених Штатів Америки (США) показали, що кібердипломатію доцільно розглядати не лише як зовнішньополітичний інструмент, а й як системний набір превентивних, кооперативних, стабілізаційних, обмежувальних і підтримувальних заходів [4, p. 77].

Питання взаємозв'язку кібердипломатії зі стабілізацією міжнародного середовища неможливо з'ясувати без звернення до праць, присвячених нарощуванню спроможностей (capacity building) та довірчим заходам. Зокрема, Р. Коллетт (R. Collett) обґрунтував, що кібербезпекове нарощування спроможностей доцільно трактувати не як допоміжний напрям міжнародної взаємодії, а як окремий різновид практики, що одночасно підтримує норми, формує передбачуваність і створює основу для заходів зміцнення довіри [5, p. 298]. З наведеного випливає методологічно важлива теза: стримування у цифровому просторі є значно стійкішим там, де дипломатичні протоколи поєднані з інвестиціями у спільну стійкість, навчання, взаємосумісність і кризову комунікацію.

Суттєве значення для теоретичного осмислення цифрових конфліктів мають праці, у яких кіберпростір розглядається не як окремий театр дій, а як чинник трансформації міжнародних відносин у цілому. Так, М. Фулон і Г. Майбауер (M. Foulon, G. Meibauer) запропонували трактувати кіберпростір як «структурний модифікатор», що змінює природу взаємозалежності, сигналювання, асиметрії та вразливості держав [6, p. 426]. Цю теоретичну лінію продовжують Е. Ґарцке та Дж. Ліндсі (E. Gartzke, J. Lindsay), які в межах теорії стримування показали, що стримування залежить не лише від покарання чи заперечення, а й від управління складністю, достовірності сигналів та організаційної спроможності підтримувати тиск без втрати контролю над динамікою ескалації [7, p. 15]. Зважаючи на наведене, окреслені підходи у сукупності підводять до висновку про необхідність протокольного оформлення дипломатичних сигналів у кіберсфері.

Окремий блок наукової літератури пов’язаний із технологічним ускладненням кібердипломатії. Так, у працях А. Ґеорґеску (A. Georgescu) показано, що управління новими технологіями, зокрема штучним інтелектом, дедалі більше стає підсферою кібердипломатії, у якій класичні переговорні формати змушені адаптуватися до швидкості технологічної еволюції та трансатлантичних розбіжностей щодо регуляторних моделей [8, p. 13]. Наведений підхід розширює П. Раданліев (P. Radanliev), який довів, що штучний інтелект, Інтернет речей, блокчейн і квантові обчислення водночас створюють нові ресурси для міжнародної координації та нові типи ризиків, які неможливо ефективно врегулювати поза рамками посиленої кібердипломатії [9, p. 28].

Роботи з методології аналізу кібердипломатії демонструють зсув від описових оглядів до формалізованих моделей. Зокрема, у дослідженні Р. Коллетта (R. Collett) запропоновано мережеве моделювання як інструмент для аналізу кібердипломатичних коаліцій, голосувань, кластерів близькості та латентних ліній розмежування між державами [10, p. 377]. Такий підхід має

принципове значення, оскільки дає змогу побачити не лише офіційно проголошені позиції, а й реальну геометрію підтримки, координації та відстані між акторами, що прямо впливає на стримувальний потенціал будь-яких протоколів.

Для вивчення механізмів сигналювання особливо важливою є концепція офіційної публічної атрибуції. Так, Ґ. Барам (G. Baram) довів, що систематичне публічне приписування відповідальності за кібератаки не є лише комунікаційним жестом, а поступово формує практику, яка позначає межі допустимої поведінки в кіберпросторі й накопичувально працює на вироблення глобальних норм [11, p. 391]. З наведеного випливає, що атрибуція виступає не допоміжним, а центральним вузлом кібердипломатичного стримування за умови її поєднання з доказовістю, коаліційністю та прогнозованими наслідками.

Нормативний і геополітичний вимір кібердипломатії розкривається у працях, присвячених конкуренції моделей цифрового врядування. Зокрема, Х. Чень і Х. Гао (X. Chen, X. Gao) показали, що Китай дедалі активніше діє як норм-підприємець у сфері кіберврядування, просуваючи власний пакет уявлень про цифровий суверенітет, порядок і контроль [12, p. 2419].

У дослідженні Д.-Е. Попеску (D.-E. Popescu) на прикладі Індії продемонстровано, що у Глобальному Півдні кібердипломатія дедалі більше пов’язується з технологічним суверенітетом, цифровою автономією та переформатуванням позиції держав між блоковими центрами сили [13, p. 39]. Зважаючи на наведене, протоколи кібердипломатії не можуть бути універсальними у жорсткому сенсі: вони мають враховувати різні мотивації та різні уявлення про цифровий порядок.

Європейський напрям досліджень останніх років фокусується на кризовому навчанні та інституційній адаптації. Так, у праці П. Павляка (P. Pawlak) показано, що кібердипломатія ЄС визрівала через поступове накопичення уроків, реакцію на швидкі кризи та «рух уперед через неповноту»

у багатосторонніх процесах [14, p. 765]. Крім того, Н. Фазола та співавтори (N. Fasola et al.) на матеріалі російсько-української війни довели, що реакція ЄС у цифровому вимірі поєднала дипломатичні заяви, правове сигналювання, координацію обмежувальних заходів і підтримку стійкості партнера та функціонувала як комплексна відповідь, а не як сума ізольованих рішень [15, p. 749]. Цю картину доповнюють В. Воссе та М. Дізон (W. Vosse, M. Dizon), які показали, що кібердипломатичний вплив ЄС за межами власного регіону зростає там, де нормативна позиція підтримується інституційною присутністю, стабільними партнерствами та передбачуваними інструментами взаємодії [16, p. 707].

Виділення невирішених раніше частин загальної проблеми. Попри значний розвиток наукової літератури, у дослідницькому полі зберігається принаймні чотири принципові прогалини. По-перше, більшість праць або пояснює кібердипломатію як окрему сферу міжнародної практики, або аналізує окремі її інструменти, однак рідко демонструє, яким чином ці інструменти поєднуються у цілісний механізм стримування. По-друге, у дослідженнях часто розмежовують технічну кіберстійкість, дипломатичне сигналювання та правове реагування, хоча на практиці ефект стримування виникає саме на перетині зазначених вимірів. По-третє, у більшості праць недостатньо формалізовано питання про те, які саме протоколи доцільно вважати базовими для кібердипломатичного стримування та у який спосіб порівнювати їхню інтегрованість у різних моделях. По-четверте, наявні кейси засвідчують, що в цифровому просторі стримування має враховувати не лише загрозу кібератак на критичну інфраструктуру, а й конвергенцію кібероперацій з інформаційними впливами, кампаніями дискредитації, тиском на технологічні ланцюги та маніпуляціями навколо міжнародної легітимності відповіді. Отже, саме ця комплексність потребує додаткового наукового опрацювання.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування моделі інтеграції протоколів кібердипломатії у механізми стримування міждержавних конфліктів у цифровому просторі. Досягнення поставленої мети передбачає послідовне розв'язання таких дослідницьких завдань:

- з'ясувати функціональну роль кібердипломатії у наявних моделях цифрового стримування;
- систематизувати базові протоколи, без яких дипломатичне реагування не створює стабілізаційного ефекту;
- запропонувати індекс інтеграції протоколів кібердипломатії та здійснити на його основі порівняльний аналіз п'яти узагальнених моделей кібердипломатичної взаємодії;
- сформулювати прикладну інтеграційну схему для державної та коаліційної безпекової політики.

Виклад основного матеріалу дослідження. Ефективність кібердипломатії як інструменту стримування визначається не реакцією на вже розгорнуту кризу, а здатністю формувати передбачуване середовище взаємодії ще до її виникнення. Базова функція цього інструменту полягає у зменшенні невизначеності для всіх сторін конфлікту: потенційний порушник має заздалегідь розуміти, які дії будуть кваліфіковані як неприйнятні, яким чином здійснюватиметься атрибуція, у якому форматі формуватиметься міжнародна відповідь і де проходить межа між жорстким сигналом та неконтрольованою ескалацією. Відповідно, стримувальна цінність кібердипломатії визначається не публічністю заяв, а передбачуваністю протоколів. У межах цього дослідження під протоколами кібердипломатії розуміються повторювані, інституційно впізнавані процедури міжнародної взаємодії, що забезпечують перехід від інформації про цифрову загрозу до координованого політичного рішення. Такі протоколи відрізняються від разових дипломатичних кроків наявністю усталених умов активації, визначеного кола акторів, допустимих

інструментів та очікуваної послідовності дій. Саме протоколізація створює стримувальний ефект, оскільки знижує простір для помилкового трактування намірів і підвищує політичну ціну агресивної поведінки.

Аналіз наукових підходів і сучасних практик дає підстави виокремити п’ять опорних протоколів. Перший – протокол раннього попередження, що охоплює регулярний обмін сигналами, технічними індикаторами, попереджувальними повідомленнями та інформацією про зміну ризикового профілю. Другий – протокол скоординованої атрибуції, який включає критерії доказовості, порядок міждержавного узгодження позиції та правила публічного оголошення відповідальності. Третій – протокол санкційно-правового узгодження, завдяки якому атрибуція не залишається у комунікаційному просторі, а переходить у прогнозовані правові та політичні наслідки. Четвертий – протокол спільної кіберстійкості, що поєднує навчання, взаємну допомогу, технічну сумісність і захист критичних секторів. П’ятий – протокол деескалації, який забезпечує кризовий зв’язок, канали уточнення позицій і можливість припинення спіралі взаємних підозр. Відсутність будь-якого з цих компонентів робить цифрове стримування структурно неповним. Зокрема, атрибуція без попередньо сформованих каналів обміну інформацією ризикує бути сприйнята як політичне звинувачення, а не як обґрунтована правова позиція. Санкційний сигнал без деескалаційного контуру посилює конфліктність і звужує простір для врегулювання. Натомість технічна співпраця без механізмів політичної відповідальності формує корисну, проте недостатню для стримування стійкість. Відтак, визначальним є не потенціал окремого інструмента, а ступінь їхньої протокольної інтеграції у єдиний цикл реагування.

Для порівняльного аналізу різних моделей застосовано індекс інтеграції протоколів кібердипломатії (ІІПК). Його призначення полягає у вимірюванні не декларативної активності держав чи коаліцій, а ступеня зв’язності між структурними елементами дипломатичного стримування. Високе значення

 ISSN: 3041-2110

індексу свідчить про наявність не просто сукупності окремих практик, а інституційно інтегрованого циклу реагування. ІІПК розраховується за формулою:

$$ІІПК = (R + A + S + C + D) / 5,$$

де R – протокол раннього попередження, A – протокол скоординованої атрибуції, S – протокол санкційно-правового узгодження, C – протокол спільної кіберстійкості, D – протокол деескалації.

Розрахунок засвідчив, що найвищі значення індексу притаманні моделям, побудованим на коаліційній взаємодії та багаторівневому узгодженні. Умовна євроінституційна модель отримала значення ІІПК 4,6, оскільки поєднує розвинені механізми раннього попередження, координацію атрибуції, інструменти правового та санкційного реагування, а також сталу логіку підтримки й підвищення стійкості партнерів. Американська модель продемонструвала значення 4,2: її перевагою є атрибуційно-сигнальна спроможність, однак вища централізація та менша залежність від багатосторонніх процедур знижують гнучкість коаліційного деескалаційного виміру. Воєнно-адаптивна українська модель набрала 4,0, що відображає інтенсивне нарощування міжнародної координації, водночас засвідчуючи залежність від зовнішньої підтримки для доведення окремих протоколів до повної інституційної завершеності.

Партнерська індо-тихоокеанська модель, представлена передусім Японією та Австралією, продемонструвала значення 3,8. Її перевагою є поєднання безпекової, технологічної та дипломатичної співпраці, проте атрибуційний і санкційний контури залишаються залежними від ширших альянсних форматів і політичної кон’юнктури. Суверенітетно-орієнтована модель, характерна для частини держав Глобального Півдня, отримала значення 3,4: вона краще пристосована до захисту стратегічної автономії, ніж до формування оперативної коаліційної відповіді та спільної атрибуції. Узагальнені результати порівняльного аналізу наведено в таблиці 1.

ISSN: 3041-2110

Таблиця 1

Порівняльна оцінка інтеграції протоколів кібердипломатії в узагальнених моделях цифрового стримування

Модель	R	A	S	C	D	ІПК
Євроінституційна коаліційна	5	5	5	4	4	4,6
Американська атрибуційно-центрична	4	5	4	4	4	4,2
Українська воєнно-адаптивна	4	4	4	4	4	4,0
Японсько-австралійська партнерська	4	3	4	4	4	3,8
Індійська суверенітетно-орієнтована	3	3	3	4	4	3,4

Джерело: власна розробка авторів

Отримані дані засвідчують, що стримувальна спроможність перебуває у прямій залежності не від декларованої жорсткості позиції, а від рівня процедурної зрілості системи реагування. З наведеного випливає, що висока інтенсивність політичної риторики не продукує стримувального ефекту за відсутності верифікованих каналів обміну інформацією, доведеної атрибуції, узгодженого комплексу наслідків та інституційно закріпленого механізму виходу з кризової ситуації.

На підставі проведеного аналізу запропоновано інтеграційну модель кібердипломатичного стримування, що охоплює п’ять послідовно пов’язаних фаз. Перша фаза – превентивна – передбачає формування точок контакту, каналів раннього попередження, правил обміну технічною інформацією та меж допустимого ризику. Друга фаза – інцидентна – запускає верифікацію фактів, координацію оцінок та обмеження інформаційного хаосу. Третя фаза – атрибуційно-сигнальна – забезпечує узгодження політичної позиції, формули публічного оголошення та переліку наслідків. Четверта фаза – стабілізаційна – поєднує санкційне, правове, комунікаційне та технічне реагування. П’ята

фаза – післякризова – охоплює оновлення протоколів, переоцінку вразливостей і повернення до режиму стримування через стійкість.

Суттєвою перевагою запропонованої моделі є її здатність інтегрувати два взаємодоповнювальні підходи до стримування: обмеження можливостей агресора щодо досягнення поставленої мети та формування чітких сигналів про неприйнятність ворожих дій. Спільна кіберстійкість зменшує ймовірність реалізації агресором запланованого ефекту, тоді як верифікована атрибуція, санкційна координація та дипломатична публічність підвищують сукупну політичну вартість ворожих дій. Принципово важливим при цьому є те, що обидва підходи функціонально пов'язуються протоколом деескалації: за його відсутності навіть результативне покарання може ініціювати цикл взаємного нарощування конфліктного потенціалу.

Практичне значення запропонованої інтеграційної моделі є особливо вагомим для держав, що функціонують в умовах підвищеного цифрового тиску. За таких обставин кібердипломатія не може зводитися до апеляції до норм міжнародного права чи декларативних закликів до солідарності. Вона має бути організаційно інтегрована в систему національної безпеки, передбачати чітко визначені тригери активації, розмежовані функції дипломатичних, безпекових і технічних інституцій, а також заздалегідь сформовані пакети міжнародного реагування. Крім того, ефективність такої моделі перебуває у прямій залежності від здатності держави трансформувати двосторонні домовленості у стійкі та інституційно закріплені мережі партнерства.

У міжнародному вимірі наведені результати свідчать про те, що перспективи цифрового стримування визначаються не стільки формуванням універсального глобального режиму, скільки досягненням сумісності протоколів між коаліціями, регіональними блоками та групами держав зі спільними безпековими інтересами. Підвищення рівня конвергенції стандартів атрибуції, правил кризової комунікації, порогів санкційного

ISSN: 3041-2110

реагування та форматів підтримки постраждалої сторони безпосередньо знижує ризик хаотичної ескалації. З огляду на це інтеграція протоколів кібердипломатії має розглядатися як самостійний і стратегічно значущий напрям безпекової політики, а не як похідний елемент зовнішньополітичної комунікації.

З огляду на результати проведеного аналізу запропонована модель дає змогу конкретизувати прикладні пріоритети для державної безпекової політики. Першим пріоритетом є інституціоналізація єдиного сценарію переходу від технічного виявлення інциденту до дипломатичного рішення. Другим – створення стандартизованого шаблону багатосторонньої атрибуції. Третім – прив'язка дипломатичних кроків до заздалегідь узгодженого комплексу правових, економічних і комунікаційних наслідків. Четвертим – закріплення у протоколах окремого блоку підтримки стійкості постраждалої сторони. П'ятим – підтримання кризових комунікаційних каналів навіть в умовах максимальної конфліктності. Відсутність хоча б одного з цих компонентів у протокольній логіці помітно знижує стримувальний ефект. Отже, авторська позиція полягає в тому, що кібердипломатія має бути переосмислена як інфраструктура керованої взаємодії в умовах цифрової конфронтації. Її стратегічна функція полягає не у запереченні конфлікту як такого, а у звуженні простору для непрогнозованих рішень, підвищенні політичної вартості деструктивної поведінки та підтриманні таких процедур, за яких навіть гостре протистояння не унеможливлює контрольованого виходу з кризи.

Важливим аспектом, що потребує окремого аналізу, є багатофазова природа цифрового конфлікту, який у переважній більшості випадків не вичерпується однією часовою стадією розгортання. Зокрема, у той час як одна сторона здійснює збирання технічних даних для атрибуції, інша вже розгортає активність у комунікаційному просторі, формуючи альтернативну версію подій, знижуючи довіру до доказової бази та конструюючи наратив

симетричної провини. Відтак протоколи кібердипломатії мають забезпечувати не лише юридичну та технічну доказовість, а й темпоральну синхронізацію дипломатичних і комунікаційних дій. За відсутності такої синхронізації навіть методологічно коректно проведена атрибуція виявляється запізнілою, що частково нівелює її стримувальний потенціал. Відтак протоколи кібердипломатії мають забезпечувати не лише юридичну та технічну доказовість, а й темпоральну синхронізацію дипломатичних і комунікаційних дій. За відсутності такої синхронізації навіть методологічно коректно проведена атрибуція виявляється запізнілою, що частково нівелює її стримувальний потенціал.

Не менш істотною є проблема розриву між національним суверенітетом і коаліційною ефективністю. Чим складніша система багатостороннього узгодження, тим повільнішою може виявитися колективна реакція; натомість чим вищий рівень односторонності, тим легше агресору представити відповідь як політично вмотивовану або недостатньо легітимну. Отже, протокольна інтеграція має забезпечувати баланс між оперативністю і легітимністю. У практичному вимірі це передбачає наявність заздалегідь підготовлених кризових шаблонів заяв, попередньо узгоджених критеріїв оприлюднення інформації, визначених пакетів допомоги та умов підключення партнерів до спільного реагування.

Додатковим ускладненням є відмінна культура сприйняття стримування в цивільних, дипломатичних і військово-безпекових інституціях. Дипломатичні структури тяжіють до поступового узгодження формулювань і збереження каналів діалогу; технічні органи орієнтуються на оперативність, точність і мінімізацію поширення ураження; безпековий сектор нерідко акцентує на рішучості сигналу та невідкладності наслідків. Якщо зазначені логіки не узгоджені процедурно, кібердипломатія втрачає зв’язність і дієвість. З огляду на це інтеграція протоколів має розпочинатися всередині держави –

 ISSN: 3041-2110

із формування єдиного міжвідомчого механізму, який надалі може бути масштабований на коаліційний рівень.

У стратегічній перспективі це означає, що кібердипломатія має розвиватися за логікою «протоколів з відкритою архітектурою». Такі протоколи формують інваріантне ядро – критерії активації, порядок атрибуції, принципи доказовості, процедури кризового зв'язку, – проте водночас допускають варіативність інструментів залежно від регіону, типу інциденту, ступеня коаліційної підтримки та політичної чутливості конкретного випадку. Саме ця комбінація нормативного стандарту й операційної гнучкості уможливлює їх застосування в системі стримування у цифровому просторі, де повна уніфікація є малоймовірною, а повна імпровізація – небезпечною.

Результати, відображені на рис. 1, підтверджують, що підвищення рівня інтеграції протоколів має кумулятивний ефект: кожен додатково інституціоналізований компонент не лише зміцнює відповідну складову реагування, а й підвищує надійність усього циклу стримування. Відповідно, розрив між значеннями 3,4 та 4,6 не є суто кількісним – він відображає перехід від частково сумісних інструментів до зрілої системи керованої коаліційної взаємодії.

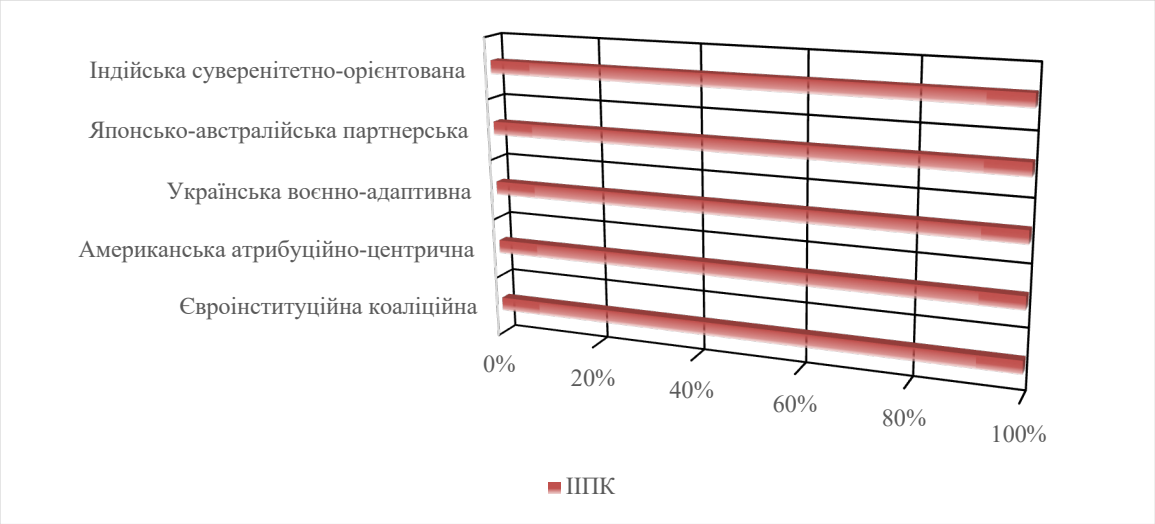

Рис. 1. Індекс інтеграції протоколів кібердипломатії в порівнюваних моделях

Джерело: власна розробка авторів

Висновки. Проведене дослідження дало підстави стверджувати, що протоколи кібердипломатії є не периферійним, а системоутворювальним елементом сучасних механізмів стримування міждержавних конфліктів у цифровому просторі. Їхня роль полягає у перетворенні розрізнених дипломатичних, технічних, правових і комунікаційних заходів на передбачувану послідовність дій, що зменшує невизначеність і підвищує вартість агресивної поведінки. Доведено, що максимального стримувального ефекту досягають не ті моделі, які демонструють найбільш жорстку риторику, а ті, що забезпечують найвищий рівень інтеграції раннього попередження, скоординованої атрибуції, санкційно-правового узгодження, спільної кіберстійкості та каналів деескалації. Запропонований індекс інтеграції протоколів кібердипломатії підтвердив перевагу коаліційно-мережевих конструкцій над ізольованими або переважно суверенітетно орієнтованими підходами.

У практичному вимірі наведені результати означають, що державам, які прагнуть посилити цифрове стримування, доцільно інвестувати не лише у захист інфраструктури та розвиток кіберпотенціалу, а й у формалізацію міжнародних процедур реагування. Центральним завданням постає створення механізмів, за яких дипломатичний сигнал є доказовим, узгодженим, своєчасним і підкріпленим реальними інструментами міжнародної взаємодії.

Перспективним напрямом подальших досліджень є деталізація критеріїв вимірювання протокольної інтеграції на матеріалі конкретних регіональних організацій, а також розроблення галузевих моделей застосування кібердипломатії для захисту критичної інфраструктури, виборчих процесів, цифрових платформ і транснаціональних технологічних ланцюгів.

Список використаних джерел

1. Lupyna A. Modeling Scenarios for Cultural Resilience Among Youth in Conditions of Hybrid Information Threats. *Вісник гуманітарних наук*. 2026. № 16. DOI: 10.5281/zenodo.18937107.

2. Barrinha A. Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*. 2024. Vol. 19, no. 3. P. 439–466. DOI: 10.1163/1871191X-bja10183

3. Manantan M. B. F. Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*. 2021. Vol. 75, № 4. P. 432–459. DOI: 10.1080/10357718.2021.1926423

4. Cîrnu C.-E., Rotuna C., Vasiloiu I.-C. Comparative Analysis on Cyber Diplomacy in EU and US. *Romanian Cyber Security Journal*. 2023. Vol. 5, no. 1. P. 77–86. DOI: https://doi.org/10.54851/v5i1y202307

5. Collett R. Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy*. 2021. Vol. 6, no. 3. P. 298–317. DOI: 10.1080/23738871.2021.1948582

6. Foulon M., Meibauer G. How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*. 2024. Vol. 45, no. 3. P. 426–458. DOI: 10.1080/13523260.2024.2365062

7. Gartzke E., Lindsay J. R. Elements of Deterrence: Strategy, Technology, and Complexity in Global Politics. New York : Oxford University Press, 2024. 466 p. DOI: 10.1093/oso/9780197754443.001.0001

8. Georgescu A. Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic Example. *International Journal of Cyber Diplomacy*. 2022. Vol. 3. P. 13–22. DOI: 10.54852/ijcd.v3y202202

9. Radanliev P. Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*. 2025. Vol. 9, no. 1. P. 28–78. DOI: 10.1080/23742917.2024.2312671

10. Collett R. Network modelling as a tool for cyber diplomacy. *Journal of Cyber Policy*. 2024. Vol. 9, № 3. P. 377–398. DOI: 10.1080/23738871.2024.2433773

11. Baram G. Cyber Diplomacy through Official Public Attribution: Paving the Way for Global Norms. *International Studies Perspectives*. 2025. Vol. 26, no. 4. P. 391–411. DOI: 10.1093/isp/ekae022

12. Chen X., Gao X. Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*. 2024. Vol. 100, no. 6. P. 2419–2440. DOI: 10.1093/ia/iiae237

13. Popescu D.-E. Cyberdiplomacy and the New Digital Non-Alignment in the Global South: India as a Case Study of Technological Sovereignty in the Age of AI. *International Journal of Cyber Diplomacy*. 2025. Vol. 6. P. 39–59. DOI: 10.54852/ijcd.v6y202503

14. Pawlak P. Forged in Crises: Learning and Adaptation in the European Union's Cyber Diplomacy. *The Hague Journal of Diplomacy*. 2025. Vol. 20, no. 4. P. 765–780. DOI: 10.1163/1871191X-bja10227

15. Fasola N., Lucarelli S., Moro F. N. Cyber Diplomacy and the Russia–Ukraine War: The European Union's Response. *The Hague Journal of Diplomacy*. 2025. Vol. 20, № 4. P. 749–764. DOI: 10.1163/1871191X-bja10224

16. Vosse W., Dizon M. EU Influence on Cyber Governance in the Indo-Pacific: A Normative Power in a Contested Space. *The Hague Journal of Diplomacy*. 2025. Vol. 20, no. 4. P. 707–742. DOI: 10.1163/1871191X-bja10229