КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1116
УДК 004.056:355.4

Мужанова Тетяна Михайлівна
к.держ.упр., доцент, доцент кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Легомінова Світлана Володимирівна
д.е.н., професор, завідувач кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Капелюшна Тетяна Вікторівна
д.е.н, доцент, професор кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0001-7490-6751
e-skr@ukr.net

Щавінський Юрій Віталійович
к.т.н., доцент, доцент кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002- 2319-8983
yushchavinsky@ukr.net

Запорожченко Михайло Михайлович
доктор філософії з кібербезпеки, доцент кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

ОСОБЛИВОСТІ СУЧАСНИХ КІБЕРОПЕРАЦІЙ ЗА ПІДТРИМКИ ДЕРЖАВ ЯК НОВІТНЬОЇ ФОРМИ МІЖДЕРЖАВНОГО ПРОТИБОРСТВА

Анотація. Встановлено, що впродовж 2020-2025 років масштаби кібератак, реалізованих державами або прихильними до них кібергрупами, значно зросли, а методи і підходи до їх проведення суттєво еволюціонували, поклавши початок новому етапу міждержавних конфліктів у глобальному цифровому просторі. У ході дослідження встановлено основні риси кібероперацій за підтримки держав. Як і кіберінцидентам, організованих іншими суб’єктами, кібератакам національних держав притаманні асиметричність, латентність і гібридність. Крім традиційних, держави використовують нові, раніше не притаманні їм методи: кібервимагання, незаконні операції з криптовалютою, впровадження віддалених працівників у країнах-конкурентах. Встановлено, що у четвірку держав-лідерів з протиправної кібердіяльності ввійшли Китай, РФ, Іран та Північна Корея, кібероперації яких мають переважно геополітичний підтекст і спрямовані на посилення впливу над територіально близькими країнами, за винятком США. Основними цілями кібероперацій за підтримки держав були ІТ, освіта й дослідження, урядові системи, аналітичні установи й НУО, об’єкти критичної інфраструктури (ОКІ) й ланцюги постачання ІТ-продуктів і послуг. Національно орієнтовані кіберсуб'єкти продовжують удосконалювати методи кібернападу, застосовуючи засоби автоматизації, хмарну інфраструктуру й технології віддаленого

доступу, швидко експлуатуючи невиправлені вразливості й активно впроваджуючи ШІ, щоб зробити кібератаки масштабнішими, ефективнішими, складнішими для відстеження, а також дешевшими. Важливою рисою сучасної злочинної діяльності держав у кіберпросторі є конвергенція зусиль національних суб'єктів і кіберзлочинних груп. Завдяки придбанню послуг зі здійснення кібератак, розробки шпигунського ПЗ і хакерських інструментів держави не тільки посилюють і здешевлюють свої кіберзусилля, але й ускладнюють можливості їх виявлення і встановлення відповідальності. Останнім часом зросли обсяги і значення державних кібероперацій ІПВ, які шляхом застосування засобів ШІ, зокрема створення синтетичних аналогів провідних новинних онлайн-ЗМІ і використання діпфейків, забезпечують ефективне маніпулювання громадською думкою і поширення бажаних пропагандистських наративів у країнах-конкурентах і на міжнародному рівні. З'ясовано, що національні суб'єкти почали активніше впроваджувати віддалених інсайдерів у компанії «ворожих» країн насамперед для отримання доступу до розвідувальних даних і шпигунства, а також впровадження шкідливого ПЗ, вимагання і саботажу за місцем праці. Дослідження показало, що лише в половині випадків кібератак, в тому числі за підтримки держав, були встановлені їхні справжні організатори, що є наслідком складнощів кібератрибуції – процесу відстеження й ідентифікації винуватця кібератаки, а також недосконалості й недотримання державами норм міжнародного права щодо кіберпростору. Наголошено, що глибоке розуміння передумов та специфіки кібероперацій, що підтримуються державою, сприятиме вирішенню проблем їхнього виявлення та протидії мирним шляхом та в рамках міжнародного права.

Ключові слова: міждержавне протиборство у кіберпросторі; кібероперації за підтримки держав; продержавні кіберзлочинні угруповання; кібернайманство; кіберздирництво; кібератрибуція.

ВСТУП

Упродовж останніх років відзначається значне зростання масштабів і складності кібератак, які спонсоруються державами. Згідно зі звітом Центру стратегічних і міжнародних досліджень (Center for Strategic and International Studies, CSIS) за 2024 рік, кількість кіберінцидентів, пов'язаних з державними суб'єктами, за останні три роки зросла на 42% [1]. У Звіті про ландшафт загроз від компанії Cognite 2025 року стверджується, що в 2024 році 36% кібератак було організовано або здійснено державними суб'єктами [2]. Хоча ця цифра може бути й більшою, з огляду на те, що держави нерідко використовують для проведення атак треті сторони: злочинні кібергрупи або хактивістів, які, за цими ж даними, реалізували 49% і 11% кібератак відповідно.

Постановка проблеми. Методи і підходи до реалізації кібероперацій національними державами продовжують стрімко еволюціонувати. На думку науковців і практиків ІТ-безпеки [3-4], розгортання й широке використання кіберзброї в гібридній війні в Україні стало початком нової ери конфліктів у глобальному цифровому просторі.

Водночас виявлення і протидія зловмисній діяльності держав у кіберпросторі стикається з низкою проблем і викликів, подолати які чи, принаймні, спрямувати зусилля на їх вирішення мирним шляхом і в рамках міжнародного права можливо на основі глибокого розуміння передумов і особливостей кібероперацій за підтримки держав.

Аналіз останніх досліджень і публікацій. Слід відзначити, що основою дослідження стали аналітичні матеріали провідних ІТ-компаній і дослідницьких установ, зокрема звіти про кіберзагрози від Cognite, CSIS, Microsoft, Verizon [1, 2, 4-7], а також результати моніторингу кіберподій, в тому числі організованих державами або

прихильними до них злочинними групами [8, 9], оскільки саме приватні суб'єкти мають більше можливостей постійного відстеження й оперативного аналізу кіберінцидентів.

У роботі розглянуто праці закордонних дослідників з питань злочинної діяльності держав у кіберпросторі, зокрема Gary D Brown [3], Seth G Jones [10], Michael McGuire [11]. Щодо доробку вітчизняних науковців з теми дослідження, то більшість публікацій присвячена юридичним аспектам кіберзлочинів, зокрема кібернайманства [12] і кібератрибуції [13]. Однак, бракує публікацій, які б комплексно висвітлювали риси й особливості сучасних кібероперацій за підтримки держав у контексті міждержавного протиборства.

Мета статті - дослідити особливості сучасних кібероперацій за підтримки держав (з початку 2020-х років і до сьогодні) як новітньої форми міждержавного протиборства.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Як відзначено вище, масштаби і складність державних кібератак продовжують зростати, несучи значні економічні збитки, загострюючи існуючі міждержавні протиріччя і посилюючи тенденції до їх вирішення у силовий та руйнівний спосіб, і зрештою сприяючи дестабілізації геополітичної ситуації на регіональних і глобальному рівнях. Для формування комплексного бачення щодо сутності й особливостей реалізації кібероперацій, реалізованих національними державами та прихильними до них кіберзлочинними групами, на сучасному етапі розглянемо їхні основні характеристики (Рис. 1).

Рис. 1. Риси зловмисної кібердіяльності держав і афілійових із ними суб'єктів Асиметричність, латентність, гібридність.

Сучасні кібероперації за підтримки держав часто називають атаками APT (Advanced Persistent Threat) через їхню безперервність, прихованість впливу і стійкість до виявлення. Завдяки асиметричності дій у кіберпросторі, навіть невеликі, але технологічно розвинуті держави можуть успішно протистояти потужних державам. Латентність кібервпливу перешкоджає виявленню кіберагресорів, внаслідок чого сьогодні неможливо зі 100-відсотковою впевненістю назвати суб'єкта, який реалізував кібератаку, і жодна держава не зізналася в кібератаках навіть за наявності чітких доказів. Гібридний характер кібероперацій за підтримки держав проявляється в тому, що кіберпорушення все частіше виходять за межі віртуальних ІКС і систем кіберзахисту,

проникаючи у фізичну сферу і маючи на меті руйнування інфраструктури й пошкодження матеріальних активів [11].

Держави-лідери зловмисної кібердіяльності. Глобальна платформа даних і бізнес-аналітики Statista провела дослідження даних Європейського репозиторію кіберінцидентів (European Repository of Cyber Incidents, EuRepoC) за 2002-2023 роки і встановила, що майже 12% політично мотивованих кібератак, виявлених з початку ведення бази, були здійснені з Китаю, за ним іде Росія з майже аналогічною часткою (11,6%). Іран є відповідальним за 5,3% кібератак за досліджуваний період, а Північна Корея (КНДР) – за 4,7%. Важливо зазначити, що в майже половині зловмисних кіберподій (45%) впевнено ідентифікувати країну походження було не можливо [14] (Рис. 2).

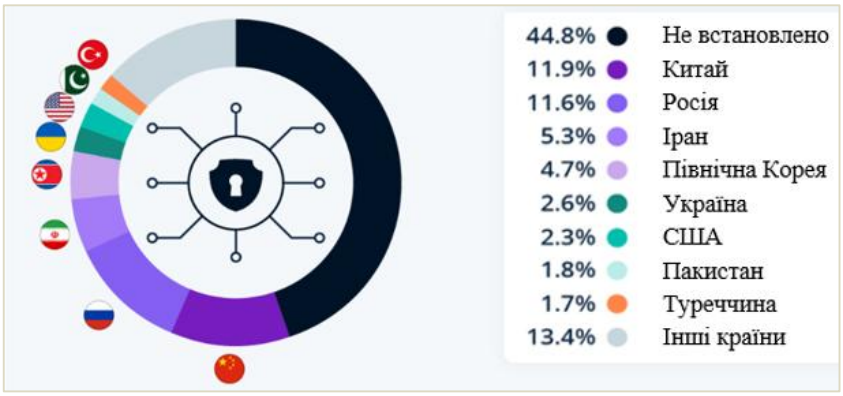

Рис. 2. Рейтинг держав, які реалізують кібератаки

Аналогічні висновки дозволяють зробити дані трекера [8], який веде Рада іноземних зв'язків США (Council on Foreign Relation, CFR) з 2005 року (Рис. 3). Варто також відзначити, що згідно з даними компанії Forescout [15], 43% нападів хакерських груп були реалізовані в інтересах зазначених держав.

Рис. 3. Держави з найбільшими показниками організованих кібератак
Види кібероперацій, реалізованих державами.

Дослідження показало, що кіберінциденти з вини вище згаданих держав охоплюють весь спектр кіберпорушень, зокрема такі категорії в порядку зростання наслідків [10] (рис. 4).

Розвідка / спроба проникнення	Ескалація привілеїв	Постійна присутність і шпигунство	Витік даних	Маніпулювання / знищення даних	Віртуальне пошкодження систем	Фізичне пошкодження об'єктів

Рис. 4. Види кіберінцидентів, організованих державами

Слід відзначити, що послідовність категорій інцидентів певною мірою відображає й еволюцію методів, які використовувалися в кібератаках з ініціативи держав.

Так, розвідка кіберсистеми передбачає зазвичай сканування портів або будь-яку подібну діяльність, а проникнення є першим етапом отримання несанкціонованого доступу до системи. Ескалація привілеїв користувача забезпечує розширення його можливостей щодо маніпулювання операційною системою та конфігурацією мережі, приховування слідів злому і, в кінцевому рахунку, здійснення наступних дій.

Отримавши доступ, зловмисник прагне встановити тривалу присутність в системі, зокрема шляхом завантаження шкідливих програм або створення додаткових облікових записів користувачів для атак «через чорний хід». Шпигунство передбачає спостереження за налаштуваннями й роботою системи, а також інформацією, що там зберігається і обробляється. Результатом шпигунської діяльності є надсилання копій даних за межі системи, тобто організація витоку даних. Саме володіння інформацією або знаннями є кінцевим результатом такого виду зловмисної кібердіяльності. Маніпулювання даними охоплюють будь-які їх зміни або видалення.

Віртуальне пошкодження системи або негативний вплив на її функціональність внаслідок навмисних шкідливих дій має наслідком тимчасове неналежне функціонування системи (збій у роботі) без завдання їй постійної шкоди. Фізичне пошкодження системи є найбільш серйозною ситуацією, коли систему необхідно фізично відремонтувати або замінити.

Відповідно до даних трекера CFR [8] найвищі показники в кожної з четвірки держав мають кібероперації з метою шпигунства. Кібератаки РФ часто спрямовані на компрометацію і розкриття даних, спуфінг і саботаж, а КНДР традиційно утримує лідерство у викраденні фінансових ресурсів (Рис. 5).

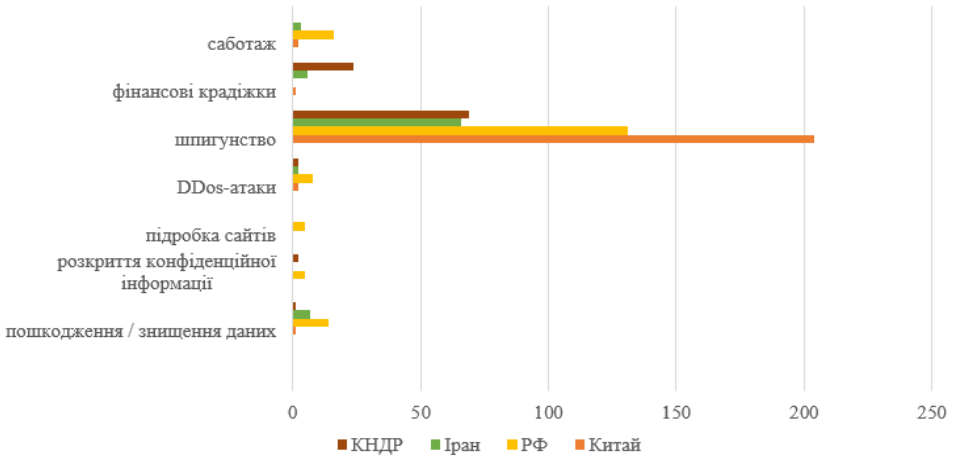

Рис. 5. Види кібероперацій національних держав

Побіжно слід відзначити, що трекер CFR не відносить до категорії кібероперацій операції ІПВ, в той час як інші джерела [5, 9] враховують їх як один із видів кіберзлочинної діяльності, зокрема через розширення масштабів їх застосування.

Геополітичний контекст зловмисної кібердіяльності держав. Незважаючи на те, що кібератаки, що спонсоруються державами, виникають з різноманітних мотивів, серед яких шпигунство, саботаж, пропаганда, отримання економічної вигоди, вони зазвичай слугують ключовими компонентами ширших геополітичних стратегій з метою забезпечення довгострокової переваги як у кіберпросторі, так і у фізичному вимірі, і досягнення конкретних національних цілей. А багатогранний характер кіберагресії з ініціативи держав свідчить про накладання політичної, економічної і технологічної сфер, формуючи сучасний ландшафт міжнародних відносин.

Внаслідок погіршення геополітичної ситуації в світі, зокрема з початком повномасштабного вторгнення РФ в Україну, а також посилення контролю з боку воєнізованих суб’єктів в інших країнах, національні суб'єкти стали більш зухвалими й агресивними, підвищили видатки на кібероперації, розширили масштаби і методи своєї зловмисної діяльності у цифровому просторі.

Як показало дослідження, кібероперації національних суб'єктів поступово набувають все більш глобального масштабу, розширюючись зокрема до більшої частини Латинської Америки й Африки. Тим не менше, упродовж останніх років найчастіше мішенями кібероперацій були США, Україна та Ізраїль, а також країни Європи.

Загалом чітко прослідковується геополітична зацікавленість ключових держав-кіберактрів у посиленні впливу над територіально близькими країнами (Китай - Тайвань, РФ - Україна, Іран - Ізраїль, КНДР – Південна Корея).

Так, стратегічна зацікавленість Китаю у контролі над Тайванем має наслідком стабільно високий рівень атак китайських кіберзлочинців на тайванські компанії, а також проникнення в кіберпростір країн басейну Південно-китайського моря. Іранська держава спрямовує свою зловмисну кібердіяльність переважно на Ізраїль (64% кібератак) і держави Середнього Сходу (ОАЕ, Саудівська Аравія, Ірак, Туреччина тощо). РФ традиційно атакує кіберінфраструктуру України та держав, які надають їй оборонну підтримку. Кібероперації суб’єктів, пов’язаних із КНДР, націлені на країни Азійсько-Тихоокеанського регіону, насамперед Південну Корею.

Водночас, слід відзначити, що левова доля кібератак з ініціативи Північної Кореї (50%) та Китаю (35%) були націлені на об’єкти США, що є наслідком ідеологічного протистояння демократичного та авторитарного способів управління, геополітичних розбіжностей та економічної конкуренції. У табл. 1 показана кількість кібероперацій, спрямованих на країни світу у розрізі регіонів за період з липня 2024 по червень 2025 року [5].

Таблиця 1.

Зловмисна кіберактивність держав у розрізі регіонів у 2024-2025 роках

Америка		Азія і Тихий океан		Європа		Середній Схід	
США	623	Тайвань	143	Україна	277	Ізраїль	603
Канада	51	Південна Корея	126	Велика Британія	144	ОАЕ	166
Бразилія	24	Індія	100	Польща	97	Саудівська Аравія	70
Перу	16	Гонконг	95	Німеччина	74	Туреччина	70
Аргентина	11	Китай	49	Франція	72	Ірак	67
Колумбія	10	Австралія	47	Іспанія	61	Йорданія	44
Мексика	9	Тайланд	39	Росія	60	Ліван	39

У таблиці не відображені дані про кількість кібероперацій у країнах Африки, оскільки показники жодної з них не перевищували 10 випадків.

Галузі, які є цілями кібероперацій за підтримки держав. Дослідження показало, що основними мішенями кібератак з боку держав у період з липня 2024 по червень 2025 року були галузі, які є традиційними джерелами для збору розвідувальної інформації, в тому числі в геополітичному контексті: IT, освіта й дослідження, урядові системи, аналітичні й неурядові організації (рис. 6). Аналогічною була ситуація впродовж попередніх трьох років.

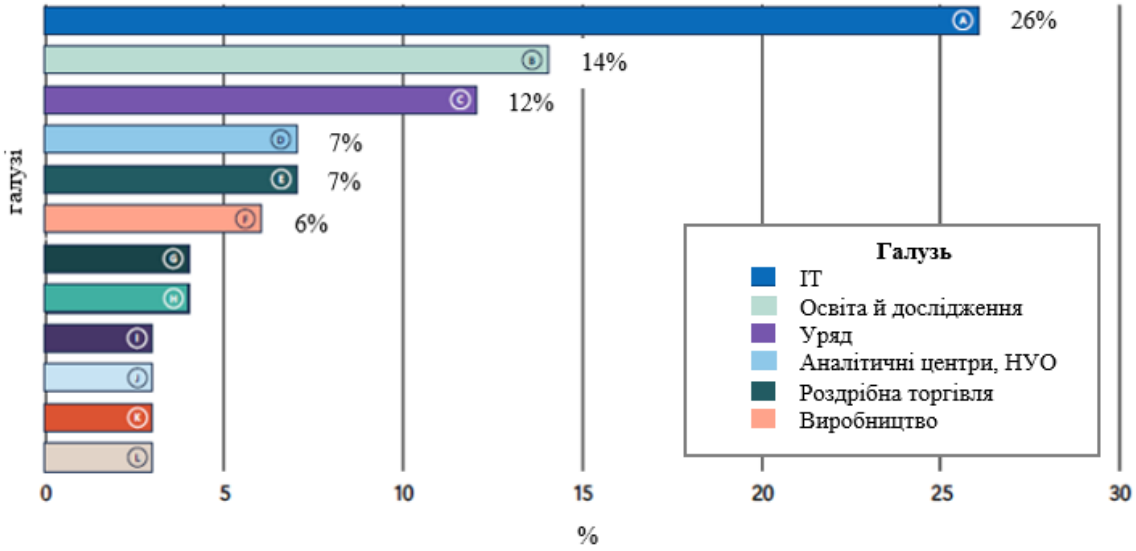

Рис. 6. Сектори, які найчастіше піддавалися кібератакам з боку держав у 2024-2025 роках

Показники менше 5% мають такі галузі як транспорт, комунікації, фінанси, охорона здоров'я, оборона, енергетика, які відносяться до критичної інфраструктури, об'єкти якої теж є однією з пріоритетних цілей держав-кіберзловмисників. Слід відзначити, що кібероперації проти критичної інфраструктури нерідко поєднуються з деструктивним фізичним впливом. Типовим прикладом поєднання методів кіберагресії з фізичним руйнуванням критичної інфраструктури (зв'язок, транспорт, енергетика, оборона) є діяльність РФ з початку повномасштабного вторгнення в Україну.

Інші держави четвірки також системно завдають кіберударів по критичній інфраструктурі країн-суперників. Так, китайські зловмисники атакують військові та IT-структури в США і державах басейну Південно-Китайського моря, Іран теж проявляє злочинну кіберактивність, націлену на критично важливі галузі США, а Північна Корея спрямовує кібератаки проти оборонних та аерокосмічних компаній по всьому світу [5].

Лідируюча позиція галузі IT в рейтингу основних цілей кібератак з боку держав і пов'язаних з ними кіберугруповань є логічним наслідком стійкого інтересу зловмисників до корпоративних ланцюгів постачання IT-послуг, як шлюзу для отримання доступу до кінцевих цілей кібератак. Згідно зі статистикою 2025 року, кількість порушень за участю третіх сторін подвоюється з року в рік, причому приблизно 30% усіх порушень даних пов'язані з проблемами третьої сторони або ланцюга постачання [16].

Упродовж останніх років зафіксовано перехід держав-кіберагресорів від використання ланцюгів постачання програмного забезпечення до ланцюгів постачання

ІТ-послуг, орієнтованих на хмарні рішення і постачальників керованих послуг. Таким чином за допомогою однієї атаки можна скомпрометувати велику кількість клієнтів кінцевого рівня, що робить атаки на ланцюги постачання одними з найнебезпечніших кіберзагроз. Наприклад, сумнозвісна проросійська кібершпигунська група Midnight Blizzard використовує ланцюги постачання програмного забезпечення та ІТ-послуг для атак на нижчих клієнтах в урядових та приватних організаціях Європи та Північної Америки, які беруть участь в політичній, військовій та гуманітарній підтримці України [6].

Злиття зусиль національних суб'єктів і кіберзлочинних угруповань. За період з початку 2020-х років зафіксовано стійку тенденцію неконтрольованого розширення ринку кібернайманців, що загрожує дестабілізацією всього цифрового середовища. Кібернайманство – це новий вид злочинного бізнесу, який полягає у наданні професійних кіберпослуг для вчинення кримінально протиправних посягань у кіберпросторі, зокрема здійснення кібератак, розробці і продажі шпигунського програмного забезпечення і хакерських інструментів на спеціалізованих ринках.

Водночас паралельно розвивається пов'язаний з попереднім тренд, який полягає у зростанні популярності використання кібернайманців національними державами, основними причинами якого є:

- → відсутність у держав можливостей для здійснення зловмисної кібердіяльності або прагнення посилити наявний кіберпотенціал;
- → менша вартість оплати послуг проксі-компаній або утримання приватних кібергруп, ніж державних агенцій;
- → нестача потрібної кількості кваліфікованих кіберфахівців у державному секторі;
- → можливості заперечення участі й уникнення відповідальності держав за кібероперації.

На думку експертів, остання причина часто є найбільш вагомою, оскільки надає можливість державі-замовнику уникнути відкритого протистояння із країною-суперником [12].

Унаслідок сукупної дії перелічених чинників відбувається злиття зусиль національних кіберсуб'єктів і кіберзлочинних угруповань. Деструктивні дії кібернайманців від імені або під керівництвом національних держав незалежно від їхньої мети і методів призводять до розмивання меж між державами, що здійснюють кібератаки, та кіберзлочинцями і, відповідно, до ускладнення можливостей виявлення і встановлення справжнього винуватця кібероперацій.

Наприклад, за спостереженнями компанії Microsoft у 2023-2024 роках, РФ залучала для збору розвідувальних даних про українську оборону прихильні кіберзлочинні групи, які використовують широкий арсенал кримінальних засобів, зокрема програми для викрадення інформації, системи командування та управління (Command and Control, C2) тощо. Північнокорейські актори вже давно перетинають цю розмиту межу, проводячи фінансово мотивовані операції для забезпечення фінансування державної скарбниці та пріоритетних національних ініціатив. Іранські державні кіберактори прагнули отримати фінансову вигоду від деяких своїх наступальних кібероперацій, продаючи викрадені приватні дані за винагороду [6].

Для ілюстрації масштабів кіберзлочинності на службі у національних держав наведемо статистику, зібрану компанією Microsoft [24] (Табл. 2).

Таблиця 2.

Кількість кіберугруповань, які підтримуються державами

	Китай	РФ	Іран	КНДР
Кількість прихильних кібергруп	45	18	19	11
З них реалізують операції впливу	2	5	2	-

Варто зауважити, що згідно з даними Microsoft, кіберзлочинні групи, афілійовані з державами, становлять найбільшу категорію, яка охоплює трохи більше 100 суб'єктів, із них - 93 пов'язані з четвіркою лідерів, решта – іншими державами, такими як Ізраїль, Ліван, Туреччина, США, Пакистан тощо. Крім цього, виявлено 20 кібергруп з виключно фінансовою мотивацією, декілька кіберсуб'єктів приватного сектору, а також близько 20 груп, що розвиваються, і потенційно теж можуть зблизитися з державами-кіберагресорами.

Удосконалення технологій державних кібератак. Державні актори прагнуть реалізувати дедалі складніші кібератаки, щоб досягти своїх стратегічних пріоритетів і при цьому уникнути виявлення. Витонченість і гнучкість атак з боку національних суб'єктів продовжують зростати. Внаслідок використання засобів автоматизації, хмарної інфраструктури й технологій віддаленого доступу розширюється перелік потенційних цілей. Експерти відзначають, що іранські та північнокорейські державні кіберсуб'єкти демонструють щораз кращу продуманість і досконалість своїх кібероперацій, у деяких випадках скорочуючи розрив із більш потужними кіберсуб'єктами Росії та Китаю.

Використання вразливостей нульового дня. Національно орієнтовані кіберсуб'єкти швидко використовують невиправлені вразливості (інфраструктуру VPN/VPS, локальні сервери, програмне забезпечення третіх сторін), які є особливо ефективними для первинної експлуатації ІКС жертви. Крім цього, після того, як інформація про такі вразливості стає публічно доступною, вони можуть бути швидко використані повторно іншими державами та кіберзлочинцями.

Відповідно до даних проекту відстеження нових вразливостей Zero-Day [17] кількість нових вразливостей щороку незначно, але зростає (Рис. 7). Отже, можливості їх експлуатації державами-кіберагресорами й афілійованими з ними злочинними групами залишаються стабільно високими.

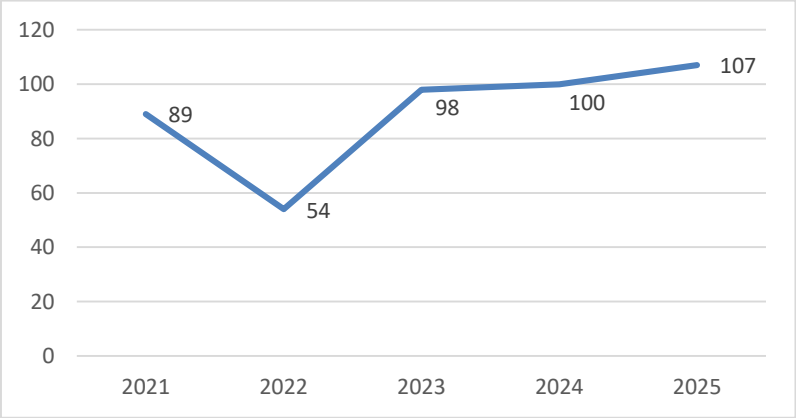

Рис. 7. Кількість вразливостей нульового дня у 2021-2025 роках

Оскільки кіберзлочинці стають більш вправними у використанні цих вразливостей, спостерігається скорочення часу між оголошенням про вразливість та її

комерціалізацією, що започатковує конкуренцію серед зловмисників, щоб вигідніше використати цю вразливість, перш ніж їхні потенційні жертви встановлять виправлення.

Розширення обсягів кіберздирництва в арсеналі держав. Національні кіберсуб'єкти суттєво збільшили обсяги використання у своїх атаках типового інструменту кіберзлочинців - програм-вимагачів. Загалом, така поведінка держав корелює зі стійкою тенденцією зростання масштабів кіберздирництва. Так, статистика показала, що програми-вимагачі фігурували у 44% порушень кібербезпеки за 2025 рік, порівняно з 32% у попередньому році [7]. За даними Microsoft кількість атак програм-вимагачів у 2024 році зросла на 252% у порівнянні з попереднім роком [18]. Це стрімке зростання підтверджує зростаючу роль програм-вимагачів як основного рушійного чинника кібератак, а також популярність цього методу через можливість легкої наживи.

Водночас, дослідники злочинної кібердіяльності держав [19] зробили висновок, що продержавні хакерські групи (КНР, РФ, КНДР) використовують програми-вимагачі не для збагачення, а для знищення доказів вторгнення, відволікання уваги розслідування, розширення можливостей правдоподібного заперечення шляхом приписування дій незалежним кіберзлочинцям, і як наслідок приховування своїх операцій.

Так, новий північнокорейський актор Moonstone Sleet розробив і застосував програму-вимагача FakePenny як для збору розвідувальних даних на об’єктах аерокосмічної та оборонної галузей, так і для монетизації доступу до них. А кібероперація впливу, реалізована групою Cotton Sandstorm, продавала викрадені дані ізраїльських сайтів знайомств через своїх кіберперсон, а також пропонувала видалити певні індивідуальні профілі зі свого сховища даних за певну плату.

Крім цього, встановлено факти використання програм-вимагачів суб'єктами Ірану та КНР для пошкодження цільових систем країн-регіональних конкурентів, включаючи критичну інфраструктуру. Іран також розширює атаки програм-вимагачів за межі регіону до критичних об’єктів США та ЄС з потенційною готовністю до руйнівних кібератак [5].

Щодо обсягів кібервимагання з боку держав, то всеохоплюючих даних немає. Однак, згідно з дослідженнями компанії Heimdal у 2024 році Росія, Китай та Північна Корея разом можуть отримувати приблизно 38% від загального обсягу виплат [20]. Віце-голова правління та президент Microsoft Б.Сміт на Мюнхенській конференції з безпеки 2025 року заявив, що понад половина коштів, отриманих вимагачами, йде Росії та Ірану [21]. Таким чином, на основі наведених даних можна зробити висновок, що програми-вимагачі досить активно використовуються четвіркою провідних держав світу, які реалізують кіберзлочинну діяльність.

Незаконна діяльність з криптовалютою. На відміну від кіберздирництва незаконні операції держав-кіберагресорів з криптовалютою однозначно є засобом акумулювання коштів для фінансування їхньої стратегічної діяльності. Основними видами протиправної криптодіяльності є викрадення й незаконні транзакції з криптовалютами, криптоджекінг (використання обчислювальної потужності чужих ПК, смартфонів чи серверів для незаконного майнінгу криптовалют), відмивання грошей у криптовалюті.

На фоні безпрецедентного розширення масштабів криптозлочинності у 2025 році, яке згідно з даними платформи Chainalysis, характеризувалося зростанням незаконних транзакцій з криптовалютою на 162% в порівнянні з попереднім роком, і досягло позначки в щонайменше 154 млрд доларів, держави четвірки кіберзловмисників також активізували свої незаконні дії з криптовалютою.

На Росію припадала найбільша частка незаконної (підсанкційної) он-чейн активності. Ця тенденція посилилася після того, як РФ у 2024 році запровадила свій

токен A7A5, прив'язаний до рубля. Загалом пов'язані з ним транзакції досягли обсягів у щонайменше 93 млрд доларів, що стало основним чинником майже семикратного збільшення криптоактивності серед підсанкційних організацій.

Іран також є одним із основних гравцем на ринку незаконної криптодіяльності, Так, Корпус вартових ісламської революції Ірану у 2025 році провів незаконні транзакції в криптовалюті на суму понад 2 млрд доларів, щоб обійти міжнародні санкції та фінансувати свої стратегічні плани, зокрема й кібероперації [21].

КНДР вже давно займає лідируючі позиції у викраденні криптовалют, як з точки зору викраденої вартості, так і з точки зору зростаючої досконалості їхніх методів атак та відмивання грошей. Північнокорейські хакери вкрали понад 3 млрд доларів США у криптовалюті з 2017 року. У 2025 році вони реалізували найбільше викрадення критовалюти з біржі Bybit в ОАЕ приблизно на 1,5 млрд доларів. Викрадені кошти спрямовуються на фінансування ядерних і ракетних програм, а також інших стратегічних ініціатив КНДР.

Неочікуваний внесок у загальний ландшафт незаконної криптоактивності зробив Китай, чиї мережі відмивання грошей (Chinese Money Laundering Networks, CMLN) стали домінуючою силою у 2025 році. Вони прискорили диверсифікацію та професіоналізацію злочинної діяльності в мережі, і зараз пропонують спеціалізовані послуги, включаючи відмивання грошей у криптовалюті як послугу та підтримку кримінальної кіберінфраструктури. CMLN підтримують шахрайство, афери, доходи від хакерських атак Північної Кореї, ухилення від санкцій та фінансування тероризму [22].

Використання штучного інтелекту в організації кібератак. Інтеграція інструментів ШІ з традиційними цифровими методами дозволяє зробити кібероперації легшими для масштабування, ефективнішими і складнішими для відстеження, а також зменшити їхню вартість. Національні держави, які активно реалізують зловмисну діяльність у кіберпросторі, прагнуть максимально вигідно для себе використати всі переваги ШІ для вирішення своїх стратегічних завдань і захисту національних інтересів.

Як показало дослідження, кібератакам на основі ШІ, організованим державами та афілійованими з ними кібергрупами, притаманні такі основні риси [23] (рис. 8).

Автоматизація атак	**Ефективний збір даних**	**Адаптація й налаштування атак**	**Удосконалення методів нападу**	**Таргетування цілей атак**

Рис. 8. Основні риси кібератак з боку держав і пов'язаних з ними груп

Автоматизація дозволяє значно пришвидшити й полегшити багато операцій у рамках підготовки й реалізації кібератак, звільнивши залучених кіберфахівців для вирішення більш важливих і складних завдань.

Використання ШІ сприяє підвищенню ефективності збору даних, виконуючи значну частину роботи з пошуку потенційних цілей, вразливостей і активів, які можуть бути скомпрометовані. Крім цього алгоритми ШІ дозволяють не тільки скоротити час, але й покращити точність і повноту аналізу.

Адаптація й налаштування атак охоплює зокрема скрапінг даних (data scraping), тобто збір і аналіз інформації з публічних джерел, таких як соціальні мережі й корпоративні веб-сайти. На основі цієї інформації створюють гіперперсоналізовані,

релевантні та своєчасні повідомлення для фішингових та інших соціоінженерних атак з метою отримання первинного доступу до цілі.

Завдяки здатності алгоритмів ШІ навчатися й адаптуватися в режимі реального часу зловмисники можуть безперервно вдосконалювати методи і засоби кібернападу й максимізувати можливості уникнути виявлення. Наприклад, у програмах-вимагачах ШІ використовують для адаптації та модифікації програмних файлів з часом, що ускладнює їх виявлення за допомогою інструментів кібербезпеки.

ШІ значно вдосконалив процеси таргетування цілей атак, полегшуючи ідентифікацію цінних осіб, які можуть мати доступ до конфіденційних даних або широкий доступ до системи, володіють слабшими технологічними навичками, або наближені до ключових цілей.

Кібероперації впливу. Деякі уряди поряд з кіберопераціями все частіше використовують кампанії ІПВ, які спрямовані на маніпулювання глобальною та національною громадською думкою і підрив демократичних інститутів у країнах, які вважаються ворожими.

В онлайн-середовищі кібероперації впливу часто використовують скоординовану обманну поведінку, таку як розгортання автоматизованих ботів і веб-ресурсів під контролем ферм тролів для створення, поширення та посилення контенту, часто з неправдивою або оманливою інформацією, поширення фейкових новин, використання згенерованих ШІ діпфейків і штучно створених кіберперсон, які поширюють інформацію в інтересах держав.

Примітною тенденцією є накладання, а в деяких випадках і синхронізація між традиційними операціями ІПВ та кіберкампаніями. Тому паралельно державні суб'єкти в реальному середовищі реалізують кампанії з метою пропаганди, дезінформування й дискредитації, інформаційні провокації з використанням традиційних державних ЗМІ або у прихований спосіб тощо.

Широко відомими є операції РФ «Doppelganger» («Двійник»), спрямовані проти України та країн, які її підтримують. У ході таких кампаній у соцмережах і месенджерах поширюються неправдиві повідомлення, новини, підробні документи, наприклад накази Міністерства оборони та головнокомандувача ЗС України з метою дискредитації військово-політичного керівництва держави і дестабілізації суспільно-політичної ситуації в Україні. Російська дезінформаційна мережа Doppelganger діє з 2022 року щонайменше в десяти країнах Європи. Вона використовує мережу підробних акаунтів-ботів для поширення посилань на фейкові версії справжніх новинних сайтів, таких, як французький Le Monde, німецький Der Spiegel, британський The Guardian та інші [25].

Китай також активно використовує методи ІПВ у кіберпросторі. У 2025 році в КНР розпочали реалізацію нової стратегії когнітивної війни (cognitive warfare), яка має на меті розширення можливостей контролю над свідомістю людей. В останні роки Китай робить ставку, зокрема, на TikTok і Telegram як засоби не тільки поширення розважального контенту, але й бажаного когнітивного впливу. І, як свідчать дослідження, ця тактика є дуже успішною. Наприклад, молодь Тайваню, яка обирає TikTok, має позитивне ставлення до Китаю, а 62% активних користувачів TikTok погодилися з тим, що США прагнуть втягнути Тайвань у війну з КНР [26].

У традиційному протиборстві зі США та ЄС Китай протягом 2022-2023 років провів найбільшу кампанію цифрового впливу у понад 50 соціальних медіа, серед яких Facebook, Instagram, X, YouTube, TikTok, Reddit, Pinterest. Там системно поширювалися позитивні коментарі щодо Китаю, а також критика США, зовнішньої політики Заходу та противників китайського уряду, включаючи журналістів і дослідників, звинувачення на

адресу Сполучених Штатів щодо створення пандемії COVID-19 та критика підтримки Вашингтоном Тайваню [27].

Від використання засобів ІПВ не відмовляються й інші учасники кіберчетвірки. Інформаційні зусилля Ірану спрямовані на власне населення і міжнародну громадську думку, дискредитацію Ізраїлю й США, а КНДР - на пропаганду власного соціалістичного устрою та його лідерів, а також цькування «головних ворогів»: США та Південної Кореї. Офіційна позиція обох держав як союзників РФ є негативною по відношенню до України та підтримуючою щодо дій держави-агресора.

Втручання у вибори. Метою злочинних національних держав, є вплив на результати демократичних виборів та їх підрив. Так, Росія, Іран та Китай у 2024 році брали участь у протиправній кібердіяльності з метою впливу на вибори у США. Причому Росію звинувачували у кібератаках на державні установи і виборчі системи США ще у 2016 та 2020 роках. Також інтереси зазначених держав, насамперед КНР, збіглися в намірах зашкодити виборам на Тайвані у 2024 р. Іран прагнув впливати на вибори на Близькому Сході, зокрема муніципальні вибори в Ізраїлі в цьому ж році. Слід відзначити, що хакерські атаки на виборчі системи зазвичай поєднувалися з активними інформаційно-психологічними операціями у цифровому просторі, спрямованими на конкуруючі політичні сили та їх союзників [6].

ШІ в операціях інформаційно-психологічного впливу. Особливого розмаху в останні роки набуло використання ШІ в операціях ІПВ національних держав. У 2025 році Центр аналізу загроз Microsoft виявив кілька нових тенденцій, що формують ландшафт операцій на базі ШІ:

- → твінінг ШІ, тобто створення цифрових реплік надійних провідних новин, які транслюють офіційно схвалені державами наративи з маскою достовірності;
- → отруєння навчальних даних - впровадження упередженого, оманливого або маніпулятивного контенту в набори даних моделей ШІ з метою впливу на її результати;
- → клонування і маскування голосу й зображення передбачає використання генеративних аудіо- та візуальних інструментів ШІ для імітації певних осіб в обхід нормативно-правових вимог.

Як свідчить статистика, за 2023-2025 роки використання ШІ для створення й поширення підробного цифрового контенту з боку національних держав зросло у вражаючих обсягах [5] (Рис. 9).

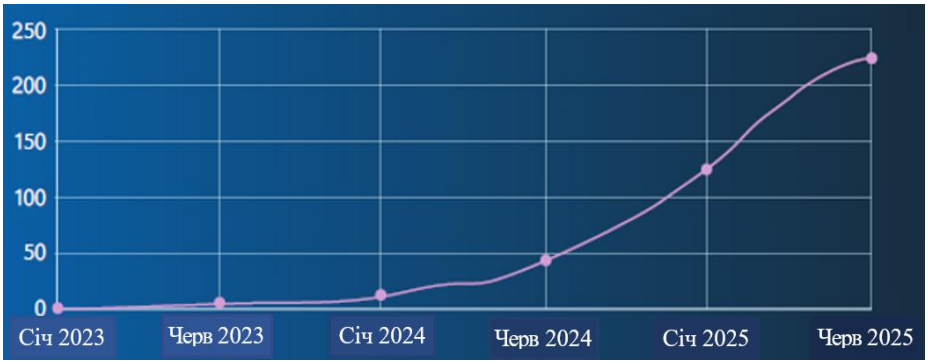

Рис. 9. Динаміка використання ШІ в операціях впливу за підтримки держав

Нові кіберактори впливу, які надають перевагу контенту й інструментам, створеним ШІ, перед традиційними методами та маніпуляціями, наповнюють

інформаційний простір синтетичними медіа й фейковими аудіо- та відеоматеріалами, щоб знизити чутливість аудиторії й виснажити системи виявлення.

Незважаючи на те, що ШІ-профілі вже давно є характерною рисою державних операцій ІПВ, використання складніших інструментів ШІ для швидкого й масового створення більш вражаючого і правдоподібного мультимедійного контенту є тенденцією, яка, ймовірно, збережеться з розширенням доступності таких технологій.

Як і в випадку кібератак, використання ШІ дозволяє проводити постійні, недорогі та масштабовані кампанії впливу з метою маніпулювання громадською свідомістю і просування вигідних ініціаторам наративів у конкуруючих державах і на світовому рівні.

Впровадження віддалених працівників. В останні роки державні суб'єкти почали активніше використовувати віддалених інсайдерів для отримання доступу до розвідувальних даних, усвідомлюючи, що внутрішнє шпигунство має результатом не тільки викрадення результатів інноваційних досліджень і розробок, але й нанесення негайних фінансових збитків і довгострокової втрати ринкових переваг для конкурентів.

Слід відзначити, що держави часто передають такі довгострокові й масштабовані операції для виконання кібернайманцям і підставним організаціям, прагнучи приховати свою зацікавленість.

Китай та Росія створили цілі екосистеми для проникнення в корпоративне середовище конкуруючих держав, часто використовуючи академічні або професійні зв'язки для виявлення й експлуатації вразливих інсайдерів. Найбільш ризикованими секторами у контексті експлуатації внутрішніх загроз є дослідження й впровадження ШІ, квантові технології, біотехнології та оборона, які мають як економічну, так і військову цінність для держав-зловмисників.

Великий резонанс викликало виявлення понад 10-річної кампанії Північної Кореї з таємного впровадження віддаленого персоналу в організації по всьому світу з метою розгортання за місцем праці шкідливого ПЗ, такого як програми-вимагачі, порушення санкцій, шпигунства, вимагання і саботажу. Північнокорейські працівники зосереджені переважно на ІТ-секторі, організаціях чи активах пов'язаних із банківською справою або технологією блокчейн, обороною та виробництвом. Крім того, пріоритетними цілями є будь-які організації, пов’язані зі східноазійською політикою. Водночас, найбільші показники віддаленої діяльності ІТ-працівників відзначено у США, оскільки саме в американських компаніях часто пропонують найвищі зарплати.

Ця зростаюча армія працівників щороку перераховує сотні мільйонів доларів до КНДР. У 2025 році північнокорейські державні актори застосували ще більш агресивний підхід до отримання доходів, подвоївши зусилля на традиційні засоби, такі як крадіжка криптовалюти та програми-вимагачі [5].

Складнощі кібератрибуції. Як відзначено вище, масштаби протиправної діяльності держав у кіберпросторі зростають вибуховими темпами, в той час, як винуватці майже половини кіберінцидентів, в тому числі й з ініціативи держав, так і не були встановлені [28].

Така ситуація викликана складнощами кібератрибуції – процесу відстеження та ідентифікації винуватця кібератаки, серед яких:

- → використання окремими державами посередників, насамперед кіберзлочинних угруповань, для здійснення протиправних дій в Інтернеті, внаслідок чого важко встановити справжніх організаторів кібернападів;
- → складність технічного виявлення держав-зловмисників через використання ними засобів, які дозволяють приховати докази протиправних дій (VPN, проксі-серверів, цибулевої маршрутизації тощо);

- → відсутність можливостей ефективного контролю за кіберінцидентами і скоординованого реагування на кіберінциденти в рамках правового поля;
- → обмеженість ресурсів держав у виявленні кіберзловмисників, навіть у співпраці з приватними компаніями Microsoft, CrowdStrike, Symantec тощо, які ведуть моніторинг і аналіз кібератак;
- → дотримання деякими державами стратегії обережності у звинуваченні потенційних кібернападників через неможливість з упевненістю встановити атрибуцію;
- → складнощі в застосуванні норм міжнародного права до кіберпростору, відсутність у ньому спеціальних правил щодо атрибуції кібератак;
- → слабкість механізмів забезпечення дотримання державами міжнародних норм відповідальної поведінки у кіберпросторі в існуючих міжнародних правових рамках [13].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження показало, що з початку 2020-х років масштаби кібератак, реалізованих державами або прихильними до них кібергрупами, значно зросли, а методи і підходи до їх проведення суттєво еволюціонували, поклавши початок новому етапу міждержавних конфліктів у глобальному цифровому просторі.

Встановлено основні риси кібероперацій за підтримки держав, серед яких загальні ознаки: асиметричність, латентність і гібридність дій у кіберпросторі; використання всього набору традиційних кіберметодів: від розвідки, шпигунства, компрометації даних до фізичного знищення ІКС; постійне удосконалення методів кібернападу з використанням засобів автоматизації, хмарної інфраструктури, технологій віддаленого доступу, невиправлених вразливостей і ШІ; низький рівень відстеження й ідентифікації винуватців кібератак (кібератрибуції), а також недосконаліть і недотримання державами норм міжнародного права щодо кіберпростору.

Водночас кібероперацїям, організованим національними державами, характерна низка спеціальних рис: широкий спектр мотивів зловмисної кібердіяльності (розвідка і шпигунство, економічна конкуренція і боротьба за контроль над ресурсами, порушення функціонування інфраструктури, маніпулятивний ІПВ); використання нових форм кіберзлочинів: кібервимагання, незаконні операції з криптовалютою, створення штучних онлайн-ЗМІ, аудіо- та відеозображень, цифрових персон, впровадження віддалених працівників у компанії країн-конкурентів.

Встановлено, що у четвірку держав-лідерів протиправної кібердіяльності ввійшли Китай, РФ, Іран та Північна Корея, кібероперації яких переважно мають геополітичний підтекст і спрямовані на посилення впливу над територіально близькими країнами. Водночас, найчастіше мішенню кібероперацій вище згаданих держав були США. Основними цілями кібероперацій за підтримки держав були галузь ІТ, освіта й дослідження, урядові системи, аналітичні установи й НУО, об’єкти критичної інфраструктури й ланцюги постачань ІТ-продуктів і послуг.

Важливою рисою сучасної злочинної діяльності держав у кіберпросторі є конвергенція зусиль національних суб’єктів і кіберзлочинних груп. Завдяки придбанню послуг зі здійснення кібератак, розробки шпигунського ПЗ і хакерських інструментів держави не тільки посилюють і здешевлюють свої кіберзусилля, але й ускладнюють можливості їх виявлення і встановлення відповідальності.

Останнім часом зросли обсяги й вага державних кібероперацій ІПВ, які шляхом застосування засобів ШІ, зокрема створення синтетичних аналогів провідних новинних онлайн ЗМІ і використання діпфейків, забезпечують ефективне маніпулювання громадською думкою і поширення бажаних пропагандистських наративів у країнах-конкурентах і на міжнародному рівні.

З'ясовано, що національні суб'єкти почали активніше впроваджувати віддалених інсайдерів у компанії «ворожих» країн насамперед для отримання доступу до розвідувальних даних і шпигунства, а також впровадження шкідливого ПЗ, вимагання і саботажу за місцем праці.

Наголошено, що завдяки глибокому розумінню передумов і особливостей кібероперацій за підтримки держав можна спрямувати зусилля з їх виявлення і протидії у русло мирного вирішення й дотримання міжнародного права. У цьому контексті цікавими напрямами подальших досліджень можуть бути питання конвергенції протиправної кібердіяльності національних держав і кіберзлочинних угруповань та її вплив на формування нових обрисів відносин у кіберпросторі, а також формування комплексної моделі виявлення і протидії цифровим злочинам на як на рівні держав, так і на міжнародному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ERMA. (2024). *The rising threat of state-sponsored cyber warfare.* https://surl.li/iygmto
2. Cognyte. (2025). *2025 threat landscape report.* https://engage.cognyte.com/s/c8036aeb/?page=2
3. Jones, S. G. (2025). The new cyber wars. In *The American edge: The military tech nexus and the sources of great power dominance* (online ed.). Oxford Academic. https://academic.oup.com/book/60904/chapter-abstract/538760999
4. Microsoft. (2022). *Microsoft digital defense report 2022.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2022
5. Microsoft. (2024). *Microsoft digital defense report 2024.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
6. Microsoft. (2025). *Microsoft digital defense report 2025.* https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/
7. Verizon. (2025). *2025 data breach investigations report: Executive summary.* https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
8. Council on Foreign Relations. (n.d.). *Cyber operations tracker.* https://www.cfr.org/cyber-operations/#OurMethodology
9. Center for Strategic and International Studies. (2025). *Significant cyber incidents since 2006.* https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-11/251114_Significant_Cyber_Incidents.pdf
10. Brown, G. D. (2020). *State cyberspace operations: Proposing a cyber response framework.* Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/rusi_pub_184_op_strategic_military_operations_final_web_version.pdf
11. McGuire, M. (2021). *Nation states, cyberconflict and the web of profit.* HP Wolf Security. https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf
12. Yurtaeva, K. (2022). Cybermercenary: Phenomenological analysis and the problem of legal assessment. *Legal Scientific Electronic Journal*, *4*, 345–348. https://doi.org/10.32782/2524-0374/2022-4/82
13. Pavlyukh, O., & Sanzharova, G. (2024). Crime attribution as a critical cybersecurity problem. *Legal Scientific Electronic Journal*, *9*, 303–306. https://doi.org/10.32782/2524-0374/2024-9/72
14. Fleck, A. (2024). *Who's behind cyber attacks?* Statista. https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/
15. Ribeiro, A. (2025). Hacktivists, state-sponsored groups step up cyberattacks targeting manufacturing operations and OT systems. *Industrial Cyber.* https://industrialcyber.co/manufacturing/hacktivists-state-sponsored-groups-step-up-cyberattacks-targeting-manufacturing-operations-and-ot-systems/
16. SOCRadar. (2025). *Top 10 supply chain attacks of 2025.* https://socradar.io/blog/top-10-supply-chain-attacks-2025
17. Zero-Day Tracking Project. (n.d.). *Zero-day vulnerability database.* https://www.zero-day.cz/database/

18. GZERO Media. (2025). *The growing cyber threat: Ransomware, China, and state-sponsored attacks.* https://www.gzeromedia.com/global-stage/munich-security-conference/ransomware-china-and-state-sponsored-attacks
19. Vicens, A. J. (2024). Chinese hackers are increasingly deploying ransomware, researchers say. *CyberScoop.* https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/
20. Heimdal Security. (2025). *Nearly 40% of 2024 ransomware payouts may have gone to Russia, China & North Korea.* https://heimdalsecurity.com/blog/ransomware-payouts-russia-china-north-korea/
21. Grigera Naón, C. (2026). Iran used $2 billion in crypto to run its militant proxies in 2025. *Yahoo Finance.* https://surl.lu/jefeyu
22. Chainalysis. (n.d.). *Crime.* https://ww.chainalysis.com/blog/category/crime/
23. Stanham, L. (2025). *AI-powered cyberattacks.* CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/
24. Microsoft. (n.d.). *How Microsoft names threat actors.* https://learn.microsoft.com/en-us/unified-secops/microsoft-threat-actor-naming
25. Antoniuk, D. (2024). Russian disinformation network's infrastructure is spread across Europe, report says. *The Record.* https://therecord.media/doppelganger-disinformation-infrastructure-european-companies
26. Wu, D. (2025). Assessing China's cognitive warfare against Taiwan on TikTok. *SPF China Observer.* https://www.spf.org/spf-china-observer/en/document-detail064.html
27. Meta. (2023). *Q2 2023 adversarial threat report.* https://www.politico.eu/wp-content/uploads/2023/08/29/NEAR-FINAL-DRAFT-Meta-Quarterly-Adversarial-Threat-Report-Q2-2023.pdf
28. ISA Global Cybersecurity Alliance. (2025). *Defending against state-sponsored cyberattacks in 2025.* https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Tetiana Muzhanova
Ph.D. in Public Administration, Associate Professor, Associate Professor of Department
of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Svitlana Lehominova
Doctor of Economics, Professor, Head of Department
of Cybersecurity and Information Protection Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Tetiana Kapeliushna
Doctor of Economics, Associate Professor, Professor of Department
of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-7490-6751
e-skr@ukr.net

Yurii Shchavinsky
Ph.D. in Technical Science, Associate Professor, Associate Professor of Department
of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Mykhailo Zaporozhchenko
Ph.D. in Cybersecurity, Associate Professor of Department
of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

ASSESSMENT FEATURES OF MODERN STATE-SUPPORTED CYBEROPERATIONS AS A NEW FORM OF INTERSTATE CONFRONTATION

Abstract. The study showed that during 2020-2025, the scale of cyberattacks carried out by states or cyber groups loyal to them increased significantly, and the methods and approaches to their implementation evolved significantly, marking the beginning of a new stage of interstate conflicts in the global digital space. The main features of cyberattacks in support of states were identified. Like cyberincidents organized by other entities, cyberattacks by nation states are characterized by asymmetry, latency, and hybridity. The motives for malicious cyber activity by states include intelligence and espionage, economic competition and the struggle for control over resources, disruption of infrastructure, and manipulative information and psychological influence (IPI). In addition to traditional methods, states use new methods that were not previously inherent to them: cyber extortion, illegal cryptocurrency transactions, and the introduction of remote workers into competing countries. It was found that the four leading states of illegal cyber activity include China, the Russian Federation, Iran and North Korea. Their cyberoperations have a predominantly geopolitical connotation and are aimed at increasing influence over territorially neighboring countries, with the exception of the United States. The main targets of cyber operations in support of states were IT, education and research, government systems, analytical institutions and NGOs, critical infrastructure facilities and supply chains of IT products and services. Nationally oriented cyber actors continue to improve cyberattack methods, using automation tools, cloud infrastructure and remote access technologies, quickly exploiting unpatched vulnerabilities and actively

implementing AI to make cyberattacks larger, more effective, more difficult to track, and also cheaper. An important feature of modern state criminal activity in cyberspace is the convergence of efforts of national actors and cybercriminal groups. By providing cyberattack services, developing spyware and hacking tools, states not only strengthen and reduce the cost of their cyber efforts, but also ensure the possibility of their identifying and establishing responsibility. Recently, the volume and importance of state cyber IPI operations have increased, which, through the use of AI tools, in particular the creation of synthetic analogues of leading online news media and the use of deepfakes, ensure the effective manipulation of public opinion and the dissemination of desired propaganda narratives in competing countries and at the international level. It was observed that national actors are increasingly introducing remote insiders into companies of "hostile" countries, primarily to gain access to intelligence data and espionage, as well as to introduce malicious software, extortion and sabotage in the workplace. The study showed that only in half of cases of cyberattacks, including those supported by states, their true organizers have been identified, which is a consequence of the difficulties of cyber attribution – the process of tracking the identification of the perpetrator of a cyberattack, as well as the imperfection and non-compliance by states with the norms of international cyberspace law. The authors emphasized that a deep understanding the prerequisites and specifics of state-sponsored cyber operations will contribute to solving the problems of their detection and counteraction peacefully and within the framework of international law.

Keywords: interstate confrontation in cyberspace; cyber operations in support of states; pro-state cybercriminal groups; cyber mercenary; cyber extortion; cyber attribution.

REFERENCES

1. ERMA. (2024). *The rising threat of state-sponsored cyber warfare.* https://surl.li/iygmto
2. Cognyte. (2025). *2025 threat landscape report.* https://engage.cognyte.com/s/c8036aeb/?page=2
3. Jones, S. G. (2025). The new cyber wars. In *The American edge: The military tech nexus and the sources of great power dominance* (online ed.). Oxford Academic. https://academic.oup.com/book/60904/chapter-abstract/538760999
4. Microsoft. (2022). *Microsoft digital defense report 2022.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2022
5. Microsoft. (2024). *Microsoft digital defense report 2024.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
6. Microsoft. (2025). *Microsoft digital defense report 2025.* https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/
7. Verizon. (2025). *2025 data breach investigations report: Executive summary.* https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
8. Council on Foreign Relations. (n.d.). *Cyber operations tracker.* https://www.cfr.org/cyber-operations/#OurMethodology
9. Center for Strategic and International Studies. (2025). *Significant cyber incidents since 2006.* https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-11/251114_Significant_Cyber_Incidents.pdf
10. Brown, G. D. (2020). *State cyberspace operations: Proposing a cyber response framework.* Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/rusi_pub_184_op_strategic_military_operations_final_web_version.pdf
11. McGuire, M. (2021). *Nation states, cyberconflict and the web of profit.* HP Wolf Security. https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf
12. Yurtaeva, K. (2022). Cybermercenary: Phenomenological analysis and the problem of legal assessment. *Legal Scientific Electronic Journal*, *4*, 345–348. https://doi.org/10.32782/2524-0374/2022-4/82
13. Pavlyukh, O., & Sanzharova, G. (2024). Crime attribution as a critical cybersecurity problem. *Legal Scientific Electronic Journal*, *9*, 303–306. https://doi.org/10.32782/2524-0374/2024-9/72
14. Fleck, A. (2024). *Who's behind cyber attacks?* Statista. https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/
15. Ribeiro, A. (2025). Hacktivists, state-sponsored groups step up cyberattacks targeting manufacturing operations and OT systems. *Industrial Cyber*. https://industrialcyber.co/manufacturing/hacktivists-state-sponsored-groups-step-up-cyberattacks-targeting-manufacturing-operations-and-ot-systems/

16. SOCRadar. (2025). *Top 10 supply chain attacks of 2025.* https://socradar.io/blog/top-10-supply-chain-attacks-2025
17. Zero-Day Tracking Project. (n.d.). *Zero-day vulnerability database.* https://www.zero-day.cz/database/
18. GZERO Media. (2025). *The growing cyber threat: Ransomware, China, and state-sponsored attacks.* https://www.gzeromedia.com/global-stage/munich-security-conference/ransomware-china-and-state-sponsored-attacks
19. Vicens, A. J. (2024). Chinese hackers are increasingly deploying ransomware, researchers say. *CyberScoop.* https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/
20. Heimdal Security. (2025). *Nearly 40% of 2024 ransomware payouts may have gone to Russia, China & North Korea.* https://heimdalsecurity.com/blog/ransomware-payouts-russia-china-north-korea/
21. Grigera Naón, C. (2026). Iran used $2 billion in crypto to run its militant proxies in 2025. *Yahoo Finance.* https://surl.lu/jefeyu
22. Chainalysis. (n.d.). *Crime.* https://ww.chainalysis.com/blog/category/crime/
23. Stanham, L. (2025). *AI-powered cyberattacks.* CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/
24. Microsoft. (n.d.). *How Microsoft names threat actors.* https://learn.microsoft.com/en-us/unified-secops/microsoft-threat-actor-naming
25. Antoniuk, D. (2024). Russian disinformation network's infrastructure is spread across Europe, report says. *The Record.* https://therecord.media/doppelganger-disinformation-infrastructure-european-companies
26. Wu, D. (2025). Assessing China's cognitive warfare against Taiwan on TikTok. *SPF China Observer.* https://www.spf.org/spf-china-observer/en/document-detail064.html
27. Meta. (2023). *Q2 2023 adversarial threat report.* https://www.politico.eu/wp-content/uploads/2023/08/29/NEAR-FINAL-DRAFT-Meta-Quarterly-Adversarial-Threat-Report-Q2-2023.pdf
28. ISA Global Cybersecurity Alliance. (2025). *Defending against state-sponsored cyberattacks in 2025.* https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025

Отримано редакцією журналу / Received: 05.01.26
Прорецензовано / Revised: 20.02.26
Схвалено до друку / Accepted: 26.03.26