DOI: https://doi.org/10.26565/1684-8489-2024-2-16
УДК 351.862.1:007

Хряпинський Антон Петрович,
кандидат юридичних наук,
директор ТОВ «Хряпинський і компанія»,
вулиця Ахсарова, 4/6 А, 61051, м. Харків, Україна

e-mail: polifil1@ukr.net *https://orcid.org/0000-0002-2492-051X*

МОДЕЛЬ ГІБРИДНОГО ВПЛИВУ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. Зроблено аналіз специфіки функціонування та сутності моделі гібридного впливу в інформаційній сфері, внаслідок чого констатовано, що із зростанням загрози кібератак з боку національних держав, хакерів і злочинних організацій це почало впливати на те, як світ бачить Інтернет. Неадекватне управління кіберзагрозами наражає користувачів на небезпеку, підриває довіру до Інтернет і ставить під загрозу його здатність бути рушієм економічних і соціальних інновацій. Але поряд з цим, дезінформована та непропорційна реакція органів влади може потенційно загрожувати свободі Інтернету та створити атмосферу страху, невпевненості та сумнівів. Тому майбутнє Інтернету та подальше зростання мережі визначатиметься тим, як органи влади та приватні організації колективно реагуватимуть на обсяг і масштаб кібератак.

Оскільки органи влади відчувають тиск, щоб пом'якшити наслідки кібератак, зростає ризик того, що свободи онлайн і глобальне підключення будуть серйозно обмежені на користь національної безпеки. Щоб цього уникнути терміново необхідні нові моделі стимулів, підзвітності та відповідальності для підвищення готовності до забезпечення кібербезпеки, зменшення вразливості та забезпечення безпеки кінцевих користувачів. Складність і масштаби кібератак вимагають реагування, керованого багатьма зацікавленими сторонами та експертами, щоб цифрова економіка продовжувала процвітати та щоб відновити довіру до безпеки Інтернету. Ані публічний, ані приватний сектор не в змозі впоратися з розмахом і масштабом кіберзагроз поодинці. Через взаємопов'язану природу Інтернету дії, здійснені поодинокими зацікавленими сторонами, мало допоможуть пом'якшити або усунути кіберзагрози. Зазвичай держава реагує на нові кіберзагрози, керуючись потребою «щось робити» перед лицем дедалі складніших кібератак. Однак такі реактивні реакції не будуть ефективно пом'якшувати загрозу, а призведуть до надмірного регулювання. Ефективні дії та стійкість мережі до кіберзагроз можуть виникнути лише завдяки обміну інформацією, стратегічному мисленню та спільним зусиллям всіх зацікавлених сторін.

Аргументовано показано, що те, як зацікавлені сторони адаптуються до майбутніх кібератак, може перетворити Інтернет з платформи відкритості та співпраці на фрагментоване, закрите та безпечне мережеве середовище. Фундаментальна зміна архітектури та базових принципів Інтернету може створити антиутопічне майбутнє захищеного саду, огородженого стіною, з фільтрацією доступу без шифрування, анонімності та конфіденційності. Національна безпека національних держав затьмарить свободи та права, які ми зараз сприймаємо як належне, викликаючи боротьбу між уявними інтересами національної безпеки та заходами безпеки кінцевих користувачів. Цього можна уникнути, якщо довго обговорювана потреба у глобальній культурі кібербезпеки набуде нової актуальності та терміновості, оскільки кібербезпека стане відповідальністю кожного. При цьому кіберуправління більше не може залишатися виключно

Як цитувати: Хряпинський А. П. Модель гібридного впливу в інформаційній сфері. *Актуальні проблеми державного управління.* 2024. № 2 (65). С. 302–315. DOI: https://doi.org/10.26565/1684-8489-2024-2-16

In cites: Khryapynskyi, A.P. (2024). The model of hybrid influence in the information sphere. *Pressing Problems of Public Administration, 2 (65), 302–315.* DOI: https://doi.org/10.26565/1684-8489-2024-2-16 [in Ukrainian].

в руках органів влади, оскільки ризик зазнати кібератак постійно зростає. Значна частина глобальної Інтернет-інфраструктури сьогодні розробляється, належить і обслуговується приватними суб'єктами, і через складність і масштаби кібератак уряди самі по собі не в змозі забезпечити інклюзивні та керовані експертами нормативні відповіді, і, отже, потрібно заохочувати приватних суб'єктів приєднатися до дискусій про майбутнє Інтернету.

Ключові слова: публічне управління, гібридні загрози, протидія та превенція, інформаційна політика, органи влади, мережеві структури, інформаційні технології.

Постановка проблеми. Інформаційне середовище та величезний потенціал для його використання у зловмисних діях вже певний час тому привернули значну увагу фахівців у сфері гібридних загроз та гібридної війни. З початку тисячоліття використання операцій впливу як державними, так і недержавними акторами стає все більш очевидним як для тих, хто приймає рішення, так і для пересічного населення. Цифрова революція, що впливає на розповсюдження інформації та соціальний обмін у наших суспільствах і спільнотах, а також посилення зв'язаності ключових суспільних систем та інфраструктури відкрила не лише нові можливості, а також і вразливі місця. Крім того, зміни на ринках праці та у демографічному складі багатьох суспільств розширили можливості та горизонти для частини суспільства, але залишили інших невпевненими у своєму місці чи представленості їхніх інтересів у традиційних ЗМІ чи політичній сфері. Це мало прямий вплив як на національну публічну політику, так і на міжнародні відносини, що набуває особливого значення на сучасному етапі українського державотворення.

Аналіз останніх досліджень і публікацій. Останнім часом спостерігається зростання досліджень гібридних загроз та впливу в інформаційній сфері. Монографія Магди Є. (2022) розкриває концептуальні засади гібридної війни. Зубченко С. (2021) аналізує моделі стратегічних комунікацій в умовах гібридних конфліктів. Маттіс Дж. і Гоффман Ф. (2019) узагальнюють досвід протидії гібридним загрозам у США та НАТО. Актуальними є звіти міжнародних організацій: дослідження Римського клубу (2022) про ризики постправди, звіт СБ ООН (2021) про нові виміри міжнародної безпеки, аналітика ВЕФ (2023) щодо технологічних трендів. Українські вчені Курбан О. (2020), Литвиненко О. (2021), Рижук О. (2022) розкривають кейси інформаційної агресії РФ та досвід протидії. Водночас бракує комплексного осмислення феномену гібридності та розробки інноваційних методик детекції загроз.

В останні 3-4 роки серед провідних вчених [2; 8; 4; 17] і, головне, великих аналітичних центрів і міжнародних організацій особлива увага приділяється таким перспективним напрямам досліджень, як операціоналізація концепту гібридності для емпіричного аналізу (Raitasalo, 2022), вивчення синергетичних ефектів поєднання різних інструментів впливу (звіт RAND, 2021), розробка проактивних моделей стратегічних комунікацій (RUSI, 2022), впровадження підходів на основі великих даних та штучного інтелекту для виявлення загроз (CCDCOE, 2023). В Україні актуальні дослідження еволюції російських наративів (НІСД, 2022), вразливостей національного інфопростору (НАНУ, 2023), взаємодії держави та громадянського суспільства у протидії дезінформації (НІСД, 2022). Потребують уваги проблеми адаптації кращих світових практик до українських реалій, розробки методик оцінювання ефективності контрзаходів в умовах «сірої зони» між миром і війною.

Мета статті – критичне узагальнення теоретичних моделей гібридного впливу в інформаційній сфері.

Застосована методологія і методи. Комплексне поєднання сучасних загальнофілософських і філософсько-правових підходів, загальнонаукових та спеціально-наукових методів, прийомів і принципів наукового пізнання, обумовлених унікальністю предмету дозволили забезпечити належний та комплексний доктринальний рівень методологічного забезпечення. В найбільш загальному світоглядному розумінні проблематика дослідження була розкрита за допомогою діалектичного підходу, що надало можливість досліджувати проблеми в єдності їх соціального змісту і форми, здійснити спектральний аналіз сутності та особливостей формування окремих аспектів гібридного впливу. Методологічний плюралізм став основою для характеристики стану й тенденцій розвитку моделей гібридного впливу в інформаційній сфері.

Виклад основного матеріалу. Розглядаючи безпеку інформаційної сфери у контексті гібридних загроз, не можна оминути питання кібербезпеки. Створення Інтернету дозволило світу стати більш глобалізованим і взаємопов'язаним, створивши середовище, в якому організації залежать від потоків даних для ведення своєї повсякденної діяльності, що впливає на все, від працездатності до моделей ефективності. У статті «The Economist» у 2017 р. стверджувалося, що дані стають такими ж важливими для суспільства, як нафта оскільки зростаюча залежність від взаємопов'язаної інформації робить неможливим від'єднання від неї [18]. Це з'єднання, у свою чергу, зробило інформацію надзвичайно цінною та відкрило нові вектори атак, створивши ринок для злому та крадіжки даних.

Якщо «дані – це нова нафта», то зростаючий ринок кіберзлочинів потенційно може поставити під загрозу майбутнє цифрове суспільство. Щоб відкритий Інтернет продовжував існувати як платформа для соціального та економічного зростання, користувачі повинні бути в змозі вірити в те, що органи влади можуть захистити системи, які керують суспільством, і мати можливість захистити особисту інформацію. Проте кілька випадків за останні роки довели, що ані уряди, ані підприємства не мають можливості пом'якшити неминучі кіберзагрози.

Через характер кібератак важко визначити, хто є актором і які їхні наміри. Кібератаки за своєю природою мають асиметричний характер, оскільки суб'єкт, який має невеликі засоби, може завдати значної шкоди окремій людині, організації, громаді чи суспільству. Завдяки триваючій тенденції підключення різноманітних організацій до Інтернету злочинні актори тепер можуть легко використовувати наявні помилки та вразливості в підключених пристроях і мережах для досягнення своїх цілей.

Кіберхаос, якого дуже бояться, або «цифровий Перл-Харбор» стає можливим, оскільки критична інфраструктура пристосовується до потреб все більш цифрового суспільства [5]. Щоб створити цифровий Перл-Харбор, зловмисники атакуватимуть промислові системи управління, відповідальні за критичну інфраструктуру. Системи є відповідними цілями, враховуючи, що системи, не розроблені для цифрового світу, часто застаріли, неналежним чином обслуговуються та їх важко виправити. Ситуація стає ще жахливішою, оскільки зловмисники використовують цифрові інструменти, такі як цільова реклама та глибокі фейки, щоб здійснювати невидимі маніпуляції громадською думкою та результатами виборів.

Поєднання погано розроблених систем у поєднанні з новими технологіями розширює масштаби та серйозність глобальних кіберзагроз, і те, як боротися з цими загрозами, матиме далекосяжні наслідки для майбутнього інформаційного суспільства, відтак, для державної інформаційної політики. Як відомо, Інтернет складається з багаторівневої та розподіленої архітектури, починаючи з фізичного рівня і закінчуючи користувачами та програмами. На найфундаментальнішому рівні інфраструктура включає апаратне забезпечення, фізичну інфраструктуру, взаємозв'язок, програмне забезпечення, протоколи, інформаційні служби та людські ресурси. Мережі або автономні системи підключаються до компонентів на фізичних рівнях, переносячи дані через набір протоколів до потрібного пункту призначення через схеми логічної адресації. Це дає змогу операторам виявляти несправності та негайно вживати заходів у разі виникнення проблем, оскільки затримка відповіді може спричинити збої та суттєво вплинути на роботу Інтернету. Між цими рівнями Інтернет складається з різних компонентів, необхідних для забезпечення надійності, стійкості та міцності. На кожному рівні стають очевидними різні ризики та вразливі місця, які різні учасники можуть використати на свою користь. До них належать, серед іншого, загрози маршрутизації або атаки на систему доменних імен (DNS). DNS-система є одним із наріжних каменів Інтернету, оскільки система дозволяє перетворювати URL-адреси в IP-адреси, створюючи каталог для кожного підключеного вузла, пристрою, комп'ютера або ресурсів, доступних в Інтернеті.

Зловмисник може використати систему через так званий DNS-спуфінг, за допомогою якого зловмисник перехоплює DNS-запит користувача та перенаправляє його на скомпрометований DNS-сервер або заражає пристрій користувача шкідливим кодом через фішингове повідомлення, заражене посилання чи здійснюючи іншу шкідливу діяльність. Потім шкідлива програма змінює налаштування жертви та перенаправляє DNS-запити на DNS-сервер зловмисника. Одним із таких відомих випадків був Roaming Mantis, який заразив планшети та смартфони на базі Android у всьому світі у 2018 році [7]. З агрози маршрутизації реалізуються через серйозні DNS-атаки, оскільки маршрутизатори забезпечують основу для надійності Інтернету. Зловмисник може захопити, змінити конфігурацію або перехопити призначені номери, адреси чи простори імен, щоб вплинути або підірвати роботу однієї чи кількох взаємопов'язаних мереж.

Крім того, суб'єкти загрози можуть виконувати атаки відмови в обслуговуванні (DoS), про які ми вже згадували раніше. DoS-атаки характеризуються явною спробою зловмисників перешкодити законному використанню служби. Існує дві загальні форми DoS-атак: ті, що приводять до збою служб, і ті, що переповнюють служби. Найбільш серйозні атаки є розподіленими (DDoS-атаки). Щоб здійснити DDoS-атаку, потрібен контроль над великою кількістю підключених пристроїв, якими можна керувати з єдиного командно-контрольного центру. Метою DDoS-атаки є зробити пристрій або мережу недоступними для призначених користувачів. Зловмисники зазвичай атакують сайти або служби, розміщені на високопрофільних веб-серверах, таких як банки, шлюзи кредитних карток, сервери імен DNS або кореневі сервери імен. Цілі деяких нещодавніх DDoS-атак включають постачальників DNS Cloudflare та Akamai, що призвело до порушення працездатності постачальників та всіх їхніх клієнтів. Найбільша DDoS-атака на сьогодні сталася в лютому 2018 року,

коли зловмисники націлилися на GitHub, платформу, популярну для онлайн-керування кодом, якою користуються мільйони розробників. На піку трафіку платформа досягала 1,35 терабайта на секунду що вказує на те, якою величезною потужністю можуть володіти деякі зловмисні особи в будь-який момент часу [19].

У звіті, опублікованому компанією Synopsys, дослідники виявили, що приблизно 77% кодової бази в пристроях IoT походять від компонентів з відкритим кодом із середнім показником 677 уразливостей на додаток [16]. Оскільки зараз більшість програмного забезпечення є сумішшю коду з різних бібліотек і постійно оновлюється розробниками за допомогою моделей доставки, його стає важко перевірити, що дозволяє суб'єктам загрози вставляти шкідливий код у програмне середовище. Проте позитивним ефектом програмного забезпечення з відкритим вихідним кодом є застосування принципів «багатьох очей», що зменшує ризик небезпеки через невідомість у порівнянні з пропрієтарним кодом, тобто програмним забезпеченням із закритим кодом.

Загроза бекдорів продовжує розширюватися і тепер становить реальну небезпеку для публічних і приватних організацій, у тому числі для органів влади. Так, протягом першої половини 2018 року 3,1% всіх атак, спрямованих на системи промислової автоматизації, походили від бекдорів, що на 50% більше, ніж у попередньому році, а компанії спостерігали зростання виявлення бекдорів на 173% порівняно з минулим роком [20]. Тривожні приклади вразливостей бекдорів стали особливо очевидними з 2017 року, коли з'явилися WannaCry та NotPetya, які спричинили хаос у всьому світі. Хакерська група під назвою Shadow Brokers атакувала невиправлені системи по всьому світу за допомогою атаки WannaCry, яка використовувала експлойт, відомий як EternalBlue, поширений у 150 країнах. Зловмисники використовували вразливості в серверному протоколі Microsoft SMBv1, що вплинуло не лише на операційні системи Microsoft, такі як Windows XP і Windows 10, але й на інші системи, що працюють на серверному протоколі Microsoft SMBv1 [14]. Уразливість дозволяла зловмисникам віддалено виконувати довільний код у цільовій системі, надсилаючи створені повідомлення на сервер SMBv1. Microsoft виправила низку вразливостей у 2017 році, але виправлення не було виконано так швидко, як потрібно. А потім світ вразив NotPetya [6]. На даний момент більшість урядів світу не приділили достатньо часу оцінці безпеки та ризиків інтернет-інфраструктури, що призвело до різних підходів і рівнів безпеки. Багато урядів наразі продають або передають на аутсорсинг значні частини своєї критичної інфраструктури без ретельного аналізу ризиків третіх сторін і приватних суб'єктів, роблячи їх уразливими до атак, які можуть порушити критичні публічні послуги. Це потенційно може створити ситуацію невизначеності під час оцінки третіх сторін і приватних суб'єктів, оскільки їхні цілі та інтереси можуть не збігатися зі суспільно важливими.

Відомі приклади зловмисного використання кіберпростору є частиною кібервійни. Слід зазначити, що трактування сутності і змісту кібервійни викликає серйозні суперечки в міжнародному науковому дискурсі, через що не існує єдиного широко прийнятого визначення даного поняття. Протягом років дослідження кібервійни було запропоновано кілька її визначень, наприклад, «дії національної держави з метою проникнення в комп'ютери або мережі іншої країни з метою заподіяння шкоди або збою», запропоноване Річард А. Кларком, колишнім урядовцем США та національним координа-

тором з безпеки, захисту інфраструктури та боротьби з тероризмом [12]. Мартін Ч. Лібіцкі пропонує інше трактування та визначає кібервійну як два типи, стратегічний та оперативний, де стратегічний тип – це «кампанія кібератак, яку одна організація здійснює проти іншої», тоді як оперативний тип «передбачає використання кібератак військовими іншої сторони в контексті фізичної війни». Кібервійну також можна пояснити як атакуючі дії суб'єкта або спроби пошкодити комп'ютер або інформаційну мережу супротивника за допомогою шкідливого коду, націленого на системи онлайн-контролю, що керують логічними та фізичними мережами [3].

Оскільки Інтернет переплітається з національною безпекою держав, наступальні та оборонні кіберстратегії формуватимуть майбутнє Інтернету як для користувачів, так і для промисловості. Зараз кіберпростір вважається п'ятою сферою ведення бойових дій, поряд з землею, морем, повітрям та космосом, але на відміну від інших сфер, конфлікти в кіберпросторі не схожі на традиційну війну. Натомість національні держави, кримінальні організації, хактивісти і терористичні групи використовують і будуть використовувати існуючі слабкі місця в комп'ютерних і мережевих системах, що керують цивільним населенням і суспільством в цілому. Атакуючі актори будуть націлені на всі аспекти Інтернет-інфраструктури, включаючи фізичну та логічну інфраструктуру, Інтернет-провайдерів, на різні платформи, середовища передачі даних та мережеве обладнання. Через ці небезпеки національні держави в усьому світі розвивають кіберпотенціал і беруть участь у кіберконфліктах, включаючи Сполучені Штати, Китай, Росію, Ізраїль, Велику Британію, Іран і Північну Корею, роблячи кібервійну невід'ємною частиною загальної військової стратегії.

Оскільки суспільства стають більш цифровими, кібервійна як засіб досягнення стратегічних цілей ніколи раніше не була такою простою. Як національні держави, так і злочинні організації можуть потенційно використовувати таємні засоби в кіберпросторі для отримання секретної інформації, як це продемонстрували, наприклад, дії Агентства національної безпеки Сполучених Штатів (АНБ), яке відстежувало розмови по мобільному телефону на Багамах без дозволу уряду Багамських островів, або витік даних Управління персоналу США, який нібито був скоєний Китаєм.

Кіберпростір також є чудовим місцем для саботажу, економічного підриву та проведення кампаній впливу. Асиметричний характер Інтернет-атак ускладнює визначення мотиваційних факторів і приписування атаки конкретному суб'єкту, створюючи середовище невизначеності щодо того, чи можна конкретну дію вважати актом війни.

У середині липня 2010 року експерти з безпеки виявили шкідливу програму під назвою Stuxnet, яка проникла в комп'ютери на іранському ядерному об'єкті, затримуючи здатність Ірану розвивати ядерний потенціал. The New York Times назвала атаку «першою атакою на критичну інфраструктуру, яка лежить в основі сучасної економіки» [1]. У 2017 році світ зіткнувся, як вже згадувалось, з WannaCry і NotPetya, двома випадками шкідливого коду, виданого за програми-вимагачі, які серйозно вплинули на Національну службу охорони здоров'я Великобританії та транспортну компанію Maersk [15].

Цивільне населення також ризикує піддатися кібератакам, при цьому зловмисники вийшли за рамки крадіжки номерів кредитних карток і також здійснюють атаки на публічні послуги або фондовий ринок [9].

Кібервійна представляє безліч загроз, оскільки кібератаки можуть відігравати допоміжну роль у традиційній війні, як ми бачимо це у контексті російсько-української війни. Враховуючи «жорсткі» та «м'які» загрози, добре здійснена кібератака може сприяти втручанню в систему протиповітряної оборони країни з метою сприяння атаці з неба, відключати всю країну від електроенергії або сприяти кібершпигунству та кампаніям впливу.

Таким чином, із зростанням загрози кібератак з боку національних держав, хакерів і злочинних організацій це почало впливати на те, як світ бачить Інтернет. Неадекватне управління кіберзагрозами наражає користувачів на небезпеку, підриває довіру до Інтернет і ставить під загрозу його здатність бути рушієм економічних і соціальних інновацій. Але поряд з цим, дезінформована та непропорційна реакція органів влади може потенційно загрожувати свободі Інтернету та створити атмосферу страху, невпевненості та сумнівів. Тому майбутнє Інтернету та подальше зростання мережі визначатиметься тим, як органи влади та приватні організації колективно реагуватимуть на обсяг і масштаб кібератак.

Оскільки органи влади відчувають тиск, щоб пом'якшити наслідки кібератак, зростає ризик того, що свободи онлайн і глобальне підключення будуть серйозно обмежені на користь національної безпеки. Щоб цього уникнути терміново необхідні нові моделі стимулів, підзвітності та відповідальності для підвищення готовності до забезпечення кібербезпеки, зменшення вразливості та забезпечення безпеки кінцевих користувачів. Складність і масштаби кібератак вимагають реагування, керованого багатьма зацікавленими сторонами та експертами, щоб цифрова економіка продовжувала процвітати та щоб відновити довіру до безпеки Інтернету.

Ані публічний, ані приватний сектор не в змозі впоратися з розмахом і масштабом кіберзагроз поодинці. Через взаємопов'язану природу Інтернету дії, здійснені поодинокими зацікавленими сторонами, мало допоможуть пом'якшити або усунути кіберзагрози. Зазвичай держава реагує на нові кіберзагрози, керуючись потребою «щось робити» перед лицем дедалі складніших кібератак. Однак такі реактивні реакції не будуть ефективно пом'якшувати загрозу, а призведуть до надмірного регулювання. Ефективні дії та стійкість мережі до кіберзагроз можуть виникнути лише завдяки обміну інформацією, стратегічному мисленню та спільним зусиллям всіх зацікавлених сторін. Також важливо підкреслити, що те, як зацікавлені сторони адаптуються до майбутніх кібератак, може перетворити Інтернет з платформи відкритості та співпраці на фрагментоване, закрите та безпечне мережеве середовище. Фундаментальна зміна архітектури та базових принципів Інтернету може створити антиутопічне майбутнє захищеного саду, огородженого стіною, з фільтрацією доступу без шифрування, анонімності та конфіденційності. Національна безпека національних держав затьмарить свободи та права, які ми зараз сприймаємо як належне, викликаючи боротьбу між уявними інтересами національної безпеки та заходами безпеки кінцевих користувачів. Цього можна уникнути, якщо довго обговорювана потреба у глобальній культурі кібербезпеки набуде нової актуальності та терміновості, оскільки кібербезпека стане відповідальністю кожного.

Зрозуміло, що у майбутньому жодна система не буде захищена від кібератак і кіберзлочинності, і ці загрози вплинуть на всі аспекти суспільства. Тому ідея про те, що «мережа настільки сильна, наскільки сильна її найслабша

ланка», набуде нового значення в гіперпов'язаному світі [4; 10; 11], оскільки підключені пристрої можуть підірвати безпеку цілого суспільства. Підвищення обізнаності про важливість безпеки на всіх рівнях має стати обов'язковим шляхом навчання грамотності з питань безпеки або розробки безпечних підключених пристроїв. Щоб задовольнити майбутні потреби, необхідно створити ринок безпеки, щоб забезпечити загальну безпеку мережі та пристроїв. Це можна зробити шляхом впровадження моделей відповідальності або вдосконалення практики державних закупівель. При цьому кіберуправління більше не може залишатися виключно в руках органів влади, оскільки ризик зазнати кібератак постійно зростає. Значна частина глобальної Інтернет-інфраструктури сьогодні розробляється, належить і обслуговується приватними суб'єктами, і через складність і масштаби кібератак уряди самі по собі не в змозі забезпечити інклюзивні та керовані експертами нормативні відповіді, і, отже, потрібно заохочувати приватних суб'єктів приєднатися до дискусій про майбутнє Інтернету.

Оскільки кібератаки стають все більш досконалими та стають інструментом для національних держав для отримання інформації, впливу на вибори в інших країнах та порушення критичної інфраструктури, загроза зросла до величезних масштабів. Зараз приватні суб'єкти все частіше закликають органи влади впроваджувати норми, які б захищали цивільних осіб у мирний час, і намагаються спонукати міжнародне співтовариство створити міжнародну організацію з мандатом на розслідування кібератак, спонсорованих державами. Є також заклики до приватних технологічних компаній взяти на себе зобов'язання захищати своїх користувачів від усіх кібератак, незалежно від походження, і ніколи не допомагати національній державі у проведенні наступальних операцій у кіберпросторі. Уряди в усьому світі повинні працювати разом, щоб усунути вразливості програмного забезпечення, а не накопичувати їх для використання один проти одного. Всі зазначені аспекти потрібно враховувати у формуванні та реалізації державної інформаційної політики.

Отже, можна констатувати, що наразі існує низка викликів, що виникають у сучасному нестабільному безпековому середовищі, яке характеризується, перш за все, дедалі більш розмитою відмінністю між війною та миром, що впливає на всі сфери державної політики, у тому числі й на державну інформаційну політику. У цьому природно складному та дедалі неоднозначному середовищі концепції гібридних загроз і гібридної війни (надалі ГЗ і ГВ) допомагають як у структуруванні розуміння природи загроз, з якими ми стикаємося, так і в стратегії та методах потенційних супротивників. Таким чином, слід використовувати комплексний погляд на загрози, а також на існуючі інструменти та засоби протидії їм. Такий комплексний погляд акцентує увагу на природі загроз і супротивників, а також викликах, які вони створюють для демократичних країн. При цьому стає все більш важливим питання спроможності демократій та демократичних державних інституцій безпеки протистояти ГЗ і ГВ, розуміючи конкретні вразливі місця в демократичних суспільствах і ліквідуючи їх, а також розробляючи відповіді на ворожі заходи з боку зовнішніх акторів. Особлива вразливість і обмеження, а також переваги демократій вимагають особливих підходів у цьому середовищі. Відкриті суспільства, побудовані на нормативних засадах верховенства права, прав людини та демократії, обов'язково захищаючи свободу слова, об'єднань і преси, повинні розробити рішення, які не тільки зберігають ці основні свободи,

але й спираються на їхні сильні сторони. Як показує досвід багатьох країн, ця робота йде повним ходом, для чого залучаються численні організації, яким доручено аналізувати та вирішувати проблему протидії гібридним загрозам, у тому числі (а часто і переважно) в інформаційній сфері.

Зокрема, це стосується ключових західних учасників колективної безпеки, представлених двома міжнародними організаціями, які несуть основну відповідальність за підтримку західного співтовариства безпеки, НАТО та ЄС, а також найбільшим і найвпливовішим гравцем у сфері безпеки, Сполученими Штатами. Маючи спільну точку відліку в анексії Криму Росією у 2014 році, усі три актори зіткнулися з необхідною переоцінкою своїх концептуалізацій супротивників, загроз і контрзаходів. Дійсно, ключовим викликом, спричиненим подіями 2014 року, була двозначність і незрозумілість подій, що відбувалися на місці, що викликало серйозні запитання щодо того, коли та як реагувати на подібні атаки проти членів НАТО чи ЄС, які перебувають нижче порогу фактичного збройного нападу. З тих пір і НАТО, і ЄС розробили низку механізмів виявлення та реагування, зосереджених на ранньому попередженні та виявленні агресивних дій, а також на стримуванні та відповіді. Цю реакцію можна охарактеризувати як спільне усвідомлення раніше невизначених слабких сторін західних суспільств і здійснення спільних зусиль для усунення відповідних прогалин [12].

Враховуючи складний характер наявних загроз, реагування має бути організованим відповідно спільних принципів, інтегруючи різні сектори суспільства, а також різні держави. Ще один важливий висновок, який випливає з розглянутого вище, це важливість знання свого противника. У той час як ідентифікація та приписування загроз створює реактивні відповіді, проактивне усунення наявних вразливостей для підвищення стійкості вимагає усвідомлення не лише того, що робить супротивник, але й чому. У зв'язку з цим актуальним стає погляд на світ очима супротивника, щоб визначити стратегічні цілі та шляхи їх досягнення, а також уразливі місця супротивника.

Проблема захисту від супротивників і ворожих дій, які, – дуже свідомо, – діють у сірій зоні, за порогом реальної війни, є постійною темою в дослідженнях багатьох науковців. І навіть якщо можливості стримування у сенсі військової сили можуть бути дуже сильними, як у випадку Сполучених Штатів, розподіл обов'язків між цивільними службами та військовими, заснований на, можливо, застарілому розумінні війни та миру, обмежує здатність до адекватної відповіді на гібридні загрози. Як яскравий приклад можна навести політику Китаю по відношенню до Тайваню, яка є узгодженою, витонченою та стратегічною комбінацією засобів, яка, однак, не включає (наразі) активне використання військової сили.

Той факт, що стратегії, пов'язані з ГЗ і ГВ, здійснюються через уявну необхідність кинути виклик військовій перевазі Заходу іншими засобами, підкреслюється і прикладом Ірану, який, через уявну загрозу існуванню з боку Сполучених Штатів, розробив стратегію партизанської війни, що значною мірою виконується проксі-силами та в районах за межами території Ірану. А в Іспанії узгоджена російська інформаційна кампанія, спрямована на підживлення та розширення національних розбіжностей щодо референдуму в Каталонії, є яскравим прикладом того, як суб'єкти, які використовують ГЗ і ГВ, шукають і атакують вразливі місця в цільових країнах, які там вже існують і не виникають як результат зовнішнього впливу або агресії [13].

Сучасні дослідження також включають (принаймні більшість з них) успішні приклади протидії гібридній війні. У країнах Балтії відносно низький рівень російської гібридної активності частково пояснюється низьким пріоритетом, який надається цим країнам в російській зовнішній політиці, а також значною мірою успішною стратегією стримування, яка поєднує різноманітні засоби, що спрямовані на забезпечення стримування нижче порогу збройного нападу. У свою чергу, Україна в розпал збройного нападу виявилася спроможною поєднати звичайну військову відповідь із тривалою інформаційною кампанією, яка, незважаючи на деякі проблеми, сприяла викриттю Росії як агресора та зміцненню внутрішньої єдності, а також міжнародній підтримці України.

Результатом багатьох досліджень стало комплексне уявлення про те, що можна назвати «гібридністю», яке замість статичної картини дій і реакцій забезпечує крос-секційне та міжчасове розуміння взаємодії між акторами, загрозами, відповідями та результатами. До цього гібридність була певним «ярликом», який використовувався в соціальних науках «для позначення процесів, у яких окремі соціальні практики або структури, що існували різними способами, поєднуються, створюючи нові структури, об'єкти та практики, у яких змішуються попередні елементи» [15, с. 40]. Запропонована нами нижче модель гібридного впливу в інформаційній сфері дає картину того, як поточні або потенційні ворожі гібридні заходи та відповіді на них динамічно впливають на довгострокову суспільну вразливість і стійкість.

Безумовно, повне розуміння та протидія ГЗ і ГВ є складним, але водночас дуже важливим завданням державної інформаційної політики. Далі ми наведемо схематичну модель того, як зрозуміти ГЗ і ГВ в інформаційній сфері. Дану модель можна представити в трьох версіях, перша з яких представляє спрощену картину динаміки ГЗ і ГВ та, а також відповіді на них і контрзаходів. Друга версія додає часовий вимір до цього зв'язку, демонструючи, як короткострокові дії та відповіді пов'язані з довгостроковою вразливістю та стійкістю. Третя версія, навпаки, спрямована на надання точнішої картини складної ситуації в реальному світі. Метою моделі є надання можливості не тільки краще зрозуміти саму динаміку, але й те, як ідентифікувати, зрозуміти та протидіяти ГЗ і ГВ.

Спрощена модель гібридного впливу в інформаційній сфері включає виміри часу та акторів. Обидва вони важливі, оскільки ГЗ і ГВ не є ані одноразовою подією, ані її неможливо тимчасово відокремити від певного контексту. У цій моделі включено два актори, захисник та нападника, разом із двома часовими вимірами, «короткий термін» і «тривалий термін». У короткостроковій перспективі битва складається з безперервного взаємного процесу між ГЗ і ГВ, який здійснює нападник, і різними відповідями та контрзаходами захисника. Це безперервний і постійний процес без заздалегідь визначеного початку чи кінця.

Однією з проблем спрощеної моделі є те, що, хоча вона надає схематичну картину гібридних конфліктів, вона не враховує аспекти хаосу, обману та заперечення ГЗ і ГВ у реальному світі, вона просто не повністю враховує безлад, що там існує. Щоб забезпечити додаткове та точніше уявлення про складне середовище безпеки, ми пропонуємо більш складну версію моделі гібридного впливу в інформаційній сфері. Дана модель особливо корисна для зображення ситуації, коли ціль ГЗ і ГВ постійно буде наосліп атакована з усіх можливих кутів незліченними невеликими атаками, які неможливо відокремити одна від одної чи локалізувати, що робить захисника нездатним адекватно відповісти та протидіяти.

Спостережувані дії чи події можуть бути невизначеними або невідомими, коли невідомо, чи спостерігається гібридний захід або щось інше. Наприклад, ви спостерігаєте за чиїмось проксі-сервером, чи «проксі» насправді є джерелом, а не частиною чиєїсь більшої стратегії/плану? Чи є проблеми з електромережею проявом гібридної війни чи просто «збоєм». Чи є загроза, яку ви бачите стосовно ланцюгів поставок медичних або продовольчих товарів, гібридною загрозою чи це просто проблема, але без гібридного походження? В цілому ж, гібридність зображується не як дві схематичні стрілки вперед і назад, а як основа хуртовини подій і дій, де «нормальна ситуація, частиною якої ви мали бути, тепер настільки зіпсована, що перевертає все сценарій у фарс» [5, с. 100]. І цей фарс – реальність, у якій ми живемо, і з якою треба вчитися поводитись, водночас підтримуючи демократичні цінності та норми.

Наразі безсумнівно, що ГЗ і ГВ в інформаційній сфері потрібно вирішувати за допомогою комплексного всеохоплюючого підходу. Немає жодної загрози, немає правильної відповіді на те, як протидіяти ГЗ і ГВ і реагувати на них, ані як створити стійкість. Також немає жодного актора чи структури, які можуть досягти успіху як сьогодні, так і завтра. Необхідно адаптуватися та адаптуватися заново, коли опонент і загроза постійно змінюються.

Висновки з даного дослідження і перспективи подальших досліджень.

1) Наявні теоретичні моделі гібридного впливу в інформаційній сфері демонструють комплексність і багатовимірність цього явища. Ефективна протидія вимагає врахування динаміки взаємодії між суб'єктами впливу, об'єктами, інструментами, часовими горизонтами. Ключова методологічна проблема - операціоналізація концептів «гібридності», «вразливості», «стійкості» для емпіричного аналізу інформаційних загроз. Україні варто розвивати крос-секторальні підходи до оцінювання інфопростору, поєднуючи кількісні метрики (big data) з якісними параметрами (наративний аналіз). Потрібні нові методики виявлення гібридних впливів на основі штучного інтелекту, сценарного моделювання, краудсорсингу даних.

2) Розглянуті моделі вказують на критичну важливість проактивності та гнучкості у протидії гібридним загрозам. В умовах швидкоплинності інформаційного ландшафту Україні потрібно розвивати спроможності завчасного виявлення вразливостей, прогнозування еволюції загроз, стратегічних комунікацій. Методологічно на часі перехід від реактивної «контрпропаганди» до проактивного формування порядку денного, культивування суспільного імунітету до дезінформації. Необхідні інституційні інновації для швидкого поширення кращих практик детекції та відповіді на гібридні атаки між різними суб'єктами. Ключовим методологічним викликом є оцінювання ефективності контрзаходів в умовах перманентного інформаційного протиборства.

3) Під час розробки заходів з протидії гібридним загрозам в інформаційній сфері також може бути корисним аналіз витрат і вигод. Хоча його застосування до цілей опонента може не поставити основні публічні організації та координаційні безпекові центри на перше місце в списку. Дійсно, вигода від їх зриву була б великою, але оскільки вони, швидше за все, також підготовлені та мають навички запобігання загрозам у зоні своєї відповідальності, позитивний результат стає невизначеним, а ризик швидкого викриття – великим. Натомість цей аналіз може принести користь сферам, які перебувають між відповідальністю публічних організацій, є «сліпими плямами», де загрози можуть виявлятися повільно, а реагування потребує певного часу.

4) Дуже важливо розробити систему виявлення, яка одночасно розпізнає хибнопозитивні та хибнонегативні результати. Існує потреба в прагматичності, гнучкості та інклюзивності акторів, секторів і рівнів – усередині та між країнами. Гібридний захід не прийде туди, де його очікують, принаймні не завжди. Коли контрзаходи будуть успішними, супротивник змінить схему атаки. Тому необхідно залучати всіх акторів і враховувати як короткострокові, так і довгострокові перспективи. Тобто важливо співпрацювати між секторами та рівнями та не допускати, щоб традиційні кордони перешкоджали співпраці. Це ніколи не є таким важливим, як під час протидії гібридних загроз і гібридної війни, оскільки вразливі місця, як правило, існують саме в прикордонних сферах між секторами та рівнями, і це те, на що опонент буде цілитися. Це вимагає співпраці насамперед в інформаційній сфері, яка повинна розвиватися в публічному та приватному секторах, а також від місцевого та регіонального рівнів до національного та міжнародного. Тоді як перспективами подальших досліджень мають стати напрацювання методик та постулатів оцінювання гібридних загроз на всі сфери суспільно-державного життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Armerding T. The Future of Open Source Software: More of Everything. Synopsys. 24 January 2019. URL: https://www.synopsys.com/blogs/software-security/future-of-open-source-predictions/

2. Balcaen P., Bois C. D., Buts C. A Game-theoretic Analysis of Hybrid Threats. *Defence and Peace Economics*. 2021. 33(1). С. 26–41. DOI: https://doi.org/10.1080/10242694.2021.1875289

3. Cadwalladr C., Graham-Harrison E. Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. The Guardian. 17 March 2018.

4. Caliskan M., Liégeois M. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies.* 2020. 32(2). С. 295–319. DOI: https://doi.org/10.1080/09592318.2020.1860374

5. Clarke R., Knake R. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins, 2020. 320 p.

6. Confessore N. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. 2018. URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

7. Ishimaru S. Roaming Mantis Uses DNS Hacking to Infect Android Smartphones. Securelist. 2018. URL: https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

8. Jung S. C., Tan E. W. Middle powers and minilateralism against hybrid threats in the Indo-Pacific: South Korea, Singapore, and Taiwan. *Australian Journal of International Affairs*. 2024. 78(6). С. 889–910. DOI: https://doi.org/10.1080/10357718.2024.2399339

9. Kulkarni P., Patil S., Kadam P. EternalBlue: A Prominent Threat Actor of 2017–2018. Virus Bulletin. 2018. URL: https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/

10. Libiseller C. 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies*. 2023. 46(4). С. 858–880. DOI: https://doi.org/10.1080/01402390.2023.2177987

11. McWilliams A., Legnér M. Threat assessments and heritage in the age of hybrid warfare. *International Journal of Heritage Studies*. 2024. 30(12). С. 1379–1392. DOI: https://doi.org/10.1080/13527258.2024.2393610

12. Newman L. Ha. GitHub Survived the Biggest DDOS Attack Ever Recorded. Wired. 1 March 2018. URL: https://www.wired.com/story/github-ddos-memcached/

13. O'Sullivan D., Griffin D., DiCarlo P. Cambridge Analytica's Facebook Data was Accessed from Russia, MP Says. CNN. 17 July 2018.

14. Parfitt T. Georgian Woman Cuts Off Web Access to Whole of Armenia. The Guardian. 6 April 2011. URL: https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access

15. Reign: Top-Tier Espionage Tool Enables Stealthy Surveillance. Symantec Security Response. Symantec Security. URL: https://docs.broadcom.com/doc/regin-top-tier-espionage-tool-15-en

16. Richmond R. Malware Hits Computerized Industrial Equipment. The New York Times. 24 September 2010. URL: https://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/

17. Sadowski A., Maj J. Interoperability and Complementarity of Civil Defense as Crucial Problems of Regional Security: The Case of the Suwalki Corridor. *The Journal of Slavic Military Studies*. 2022. №35 (2). С. 205–225. DOI: https://doi.org/10.1080/13518046.2022.2139576

18. The Economist. The World's Most Valuable Source Is No Longer Oil, but Data. The Economist. 6 May 2017. URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

19. Weinstein D. Stop Saying "Digital Pearl Harbor". DARK Reading. 2 October 2018. URL: https://www.darkreading.com/threat-intelligence/stop-saying-digital-pearl-harbor/a/d-id/1332932

20. White R. China and Russia vs. US Grid! Wired. 4 August 2009. URL: https://www.wired.com/2009/04/china-and-russi/

Стаття надійшла до редакції 25.09.2024 р.
Стаття рекомендована до друку 30.10.2024 р.

Khryapynskyi A. P.,
Ph.D. in Law,
Director of LLC "Khryapynskyi and Company", Kharkiv, Ukraine
4/6 A, Akhsarova St., Kharkiv, 61051, Ukraine
e-mail: polifil1@ukr.net https://orcid.org/0000-0002-2492-051X

THE MODEL OF HYBRID INFLUENCE IN THE INFORMATION SPHERE

Abstract. An analysis of the specifics of the functioning and essence of the model of hybrid influence in the information sphere was carried out, as a result of which it was established that with the growing threat of cyber-attacks by national states, hackers and criminal organizations, it began to affect the way the world sees the Internet. Inadequate management of cyber threats puts users at risk, undermines trust in the Internet, and jeopardizes its ability to drive economic and social innovation. But at the same time, a misinformed and disproportionate response by authorities can potentially threaten Internet freedom and create an atmosphere of fear, uncertainty and doubt. Therefore, the future of the Internet and its continued growth will be determined by how governments and private organizations collectively respond to the scope and scale of cyberattacks.

As governments feel pressure to mitigate the effects of cyberattacks, there is a growing risk that online freedoms and global connectivity will be severely curtailed in favor of national security. To avoid this, new models of incentives, accountability, and responsibility are urgently needed to increase cybersecurity readiness, reduce vulnerabilities, and ensure end-user security. The complexity and scale of cyber-attacks require a multi-stakeholder and expert-led response to keep the digital economy thriving and to restore confidence in internet security. Neither the public nor the private sector can handle the scope and scale of cyber threats alone. Because of the interconnected nature of the Internet, actions taken by individual stakeholders will do little to mitigate or eliminate cyber threats. Usually, the state reacts to new cyber threats, guided by the need to "do something" in the face of increasingly sophisticated cyber-attacks. However, such reactive responses will not effectively mitigate the threat and will lead to over-regulation. Effective action and network resilience to cyber threats can only come about through information sharing, strategic thinking and collaborative efforts by all stakeholders.

It is argued that how stakeholders adapt to future cyberattacks could transform the Internet from a platform of openness and collaboration to a fragmented, closed, and insecure network environment. A fundamental change in the architecture and basic principles of the Internet could create a dystopian future of a protected walled garden, filtering access without encryption, anonymity, or privacy. The national security of nation-states will eclipse the freedoms and rights we now take for granted, creating a battle between perceived national security interests and end-user security measures. This can be avoided if the long-discussed need for a global cyber security culture takes on new relevance and urgency as cyber security becomes everyone's responsibility. At the same time, cyber governance can no longer remain solely in the hands of the authorities, as the risk of being subjected to cyber-attacks is constantly increasing. Much of the global Internet infrastructure today is

developed, owned and maintained by private actors, and due to the complexity and scale of cyber-attacks, governments alone are unable to provide inclusive and expert-led regulatory responses, and therefore private actors need to be encouraged to join discussions about the future of the Internet.

Keywords: public administration, hybrid threats, countermeasures and prevention, information policy, authorities, network structures, information technologies.

REFERENCES

1. Armerding, T. (2019, January 24). The future of open source software: More of everything. Synopsys. URL: https://www.synopsys.com/blogs/software-security/future-of-open-source-predictions/

2. Balcaen, P., Bois, C. D., & Buts, C. (2021). A game-theoretic analysis of hybrid threats. *Defence and Peace Economics, 33(1), 26–41*. DOI: https://doi.org/10.1080/10242694.2021.1875289

3. Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.

4. Caliskan, M., & Liégeois, M. (2020). The concept of 'hybrid warfare' undermines NATO's strategic thinking: Insights from interviews with NATO officials. *Small Wars & Insurgencies, 32(2), 295–319*. DOI: https://doi.org/10.1080/09592318.2020.1860374

5. Clarke, R., & Knake, R. (2020). Cyber war: The next threat to national security and what to do about it. New York: HarperCollins.

6. Confessore, N. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. The New York Times. URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

7. Ishimaru, S. (2018). Roaming Mantis uses DNS hacking to infect Android smartphones. Securelist. URL: https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

8. Jung, S. C., & Tan, E. W. (2024). Middle powers and minilateralism against hybrid threats in the Indo-Pacific: South Korea, Singapore, and Taiwan. *Australian Journal of International Affairs, 78(6), 889–910*. DOI: https://doi.org/10.1080/10357718.2024.2399339

9. Kulkarni, P., Patil, S., & Kadam, P. (2018). EternalBlue: A prominent threat actor of 2017–2018. *Virus Bulletin*. URL: https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/

10. Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies, 46(4), 858–880.* DOI: https://doi.org/10.1080/01402390.2023.2177987

11. McWilliams, A., & Legnér, M. (2024). Threat assessments and heritage in the age of hybrid warfare. *International Journal of Heritage Studies, 30(12), 1379–1392*. DOI: https://doi.org/10.1080/13527258.2024.2393610

12. Newman, L. H. (2018, March 1). GitHub survived the biggest DDoS attack ever recorded. Wired. URL: https://www.wired.com/story/github-ddos-memcached/

13. O'Sullivan, D., Griffin, D., & DiCarlo, P. (2018, July 17). Cambridge Analytica's Facebook data was accessed from Russia, MP says. CNN.

14. Parfitt, T. (2011, April 6). Georgian woman cuts off web access to whole of Armenia. The Guardian. URL: https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access

15. Symantec Security Response. (n.d.). Reign: Top-tier espionage tool enables stealthy surveillance. Symantec Security. URL: https://docs.broadcom.com/doc/regin-top-tier-espionage-tool-15-en

16. Richmond, R. (2010, September 24). Malware hits computerized industrial equipment. The New York Times. URL: https://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/

17. Sadowski, A., & Maj, J. (2022). Interoperability and complementarity of civil defense as crucial problems of regional security: The case of the Suwalki corridor. *The Journal of Slavic Military Studies, 35(2), 205–225.* DOI: https://doi.org/10.1080/13518046.2022.2139576

18. The Economist. (2017, May 6). The world's most valuable source is no longer oil, but data. The Economist. URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

19. Weinstein, D. (2018, October 2). Stop saying "digital Pearl Harbor". DARK Reading. URL: https://www.darkreading.com/threat-intelligence/stop-saying-digital-pearl-harbor/a/d-id/1332932

20. White, R. (2009, April 4). China and Russia vs. US grid! Wired. URL: https://www.wired.com/2009/04/china-and-russi/

The article was received by the editors 25.09.2024.

The article is recommended for printing 30.10.2024.