DOI: **0.33099/2311-7249/2024-50-2-11-28**

УДК: [004.01/.08+004.49+004.62+004.78]:355.4

Горгуленко Владислав Андрійович

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

КІБЕРБОРОТЬБА У ВОЄННИХ КОНФЛІКТАХ СУЧАСНОСТІ: ПЕРЕДОВИЙ ДОСВІД, ТЕНДЕНЦІЇ ТА ЗАКОНОМІРНОСТІ РОЗВИТКУ

У статті проаналізовано, узагальнено та систематизовано передовий досвід ведення кіберборотьби у воєнних конфліктах сучасності. Досліджені наукові джерела містять актуальні праці суміжної тематики. Проте більшість із них зосереджена на вивченні кібератак, серій кібератак та кіберінцидентів, які відбувалися протягом певного короткого проміжку часу, дослідженні окремих зразків шкідливого програмного забезпечення або аналізі кібероперацій, проведених певною державою. Внаслідок цього, у галузі кібербезпеки за означеним напрямом проведено значну кількість змістовних теоретичних і практичних досліджень. Однак, більшість із них існують у своєрідному вакуумі один від одного. На відміну від попередніх наукових напрацювань, у цій статті висвітлено комплексний підхід до опрацювання хронології передового досвіду ведення кіберборотьби: від постання її феномену до сучасного стану. Метою статті є узагальнення передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності, розкриття існуючих тенденцій та визначення закономірностей її подальшого розвитку для розробки рекомендацій щодо розвитку термінологічного апарату у сфері кіберборотьби, а також обґрунтування системи показників і критеріїв оцінювання ефективності кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави. Під час проведення дослідження було застосовано методи аналізу, абстрагування та узагальнення. Методом аналізу було вивчено досвід ведення кіберборотьби як сукупність взаємопов'язаних та узгоджених за метою, завданнями, місцем у кіберпросторі, часом, а також формами та способами імплементації, фактів проведення державами заходів із кіберзахисту, кіберрозвідки й кібервпливу, та отримано особливості їх цілей, форм і способів реалізації, ступеня досягнення мети, масштабу наслідків, а також інших причинно-наслідкових зв'язків. За допомогою методу абстрагування було усунуто несуттєві властивості, що притаманні досвіду ведення кіберборотьби у воєнних конфліктах сучасності з метою зосередження на основних – тих, які дають змогу простежити і виокремити наявні тенденції та визначити закономірності подальшого розвитку. Відповідно, використання методу узагальнення дало змогу отримати такі тенденції та закономірності. У статті вперше систематизовано хронологію подій, що сформували досвід ведення кіберборотьби у воєнних конфліктах сучасності. Крім того, розроблено періодизацію воєнних дій у кіберпросторі, яка складається з трьох періодів, особливості кожного з яких, зумовлені геополітичною ситуацією у світі та рівнем розвитку інформаційно-комунікаційних технологій. Теоретичною значущістю результатів дослідження є розкриття тенденцій кіберборотьби у воєнних конфліктах сучасності й визначення закономірностей її подальшого розвитку. В умовах перенасичення джерел неструктурованою інформацією щодо досвіду ведення кіберборотьби, результати цього дослідження висвітлюють лише основні положення, відображають актуальний стан означеної теми і формують емпіричний базис, який може доповнюватися та актуалізуватися з часом. Практична значущість результатів цього дослідження полягає у розроблених, на основі розкритих у статті тенденцій та визначених закономірностей кіберборотьби у воєнних конфліктах сучасності, рекомендацій щодо необхідності розвитку термінологічного апарату у сфері кіберборотьби, а також обґрунтування системи показників і критеріїв оцінювання ефективності ведення кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави.

Ключові слова: *кіберборотьба, воєнні дії у кіберпросторі, кібердомен, аналіз та узагальнення досвіду, кібероперація, кіберпротиборство, кібервійська, кібербезпека, кіберзахист, кіберінфраструктура, кіберстійкість.*

Вступ

Постановка проблеми. Воєнні конфлікти сучасності реалізують принципи гібридної та мережецентричної війни, а притаманна їм кіберборотьба, стає дедалі більш поширеним явищем через побудову високотехнологічного суспільства, його інформатизації та цифровізації [1]. Як наслідок, спектр об'єктів, що піддаються кібервпливу постійно розширюється, а форми та способи його нанесення – удосконалюються та урізноманітнюються [2].

«Сьогодні буває складно визначити межу, за якою починається і закінчується власне війна» [3]. Таким війнам характерний тривалий підготовчий етап, під час якого забезпечується вразливість

держави-об'єкта до нападу на неї. Зокрема, поширеним явищем є комплексне ведення кіберборотьби або окремих її складових елементів (кіберрозвідки, кіберзахисту, кібервпливу) до початку активної фази конфлікту, лише у дещо прихованішій манері аніж безпосередньо під час неї. Інтенсивність нанесення кібератак суттєво зростає напередодні активних конвенційних воєнних (бойових) дій, та досягає свого максимуму з їх початком, в цей період здійснюється вплив на заздалегідь виявлені вразливості у кіберінфраструктурі. Подібний сценарій відбувся з Грузією у 2008 році та з Україною на початку широкомасштабного вторгнення російської федерації (рф) – у 2022 році, за даними Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі – ДЦКЗ ДССЗЗІ України) було ідентифіковано у 18,3 разів більше кіберінцидентів категорії «Шкідливий програмний код» порівняно з аналогічним часовим проміжком 2021 року [4]. А враховуючи те, що гібридні війни не оголошуються та, відповідно, не завершуються в класичний спосіб, кіберборотьба триває і після основного загострення подій, коли конфлікт стає тліючим. Така природа сучасних воєнних конфліктів зумовлює дослідження кіберборотьби як процесу постійного виконання заходів із кібероборони держави, а досвіду її ведення – як сукупності різнорідних за метою, завданнями, а також формами та способами імплементації, фактів проведення державами або підконтрольними їм організаціями заходів з кіберзахисту, кіберрозвідки та кібервпливу – основних складових кіберборотьби [5; 6].

На сучасному етапі процесам планування та ведення кіберборотьби все ще притаманна певна невизначеність. Проте, об'єктивна дійсність свідчить про постання кібердомену як сегменту кіберпростору і середовища ведення воєнних дій. У збройних силах провідних країн світу створюються військові формування безпосередньо призначені для ведення операцій (воєнних дій) у цьому середовищі [7]. Водночас, проведений науковий пошук хоч і показав наявність теоретично виведених часткових показників ефективності деяких складових кіберборотьби, наприклад, система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки та модель оцінювання рівня збитків від кібератак, втім системність їм не властива, а тому комплексне оцінювання ефективності воєнних дій у кіберпросторі наразі не є можливим. Термінологічний апарат у сфері кіберборотьби не має однозначності, що призводить до підміни понять як у наукових дослідженнях, так і у військових стандартах та доктринах. Зокрема, на сьогодні не існує чіткої дефініції терміну «кібердомен», а його межі у кіберпросторі не окреслені [8; 9; 10].

Отже, постає питання невідповідності теорії практиці, створити підґрунтя для вирішення якого можливо шляхом вивчення (аналізу, узагальнення, систематизації) передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності, розкриття існуючих тенденцій та визначення закономірностей її подальшого розвитку. Адже уроки, винесені з передового досвіду, потенційно можуть містити в собі ключі до розуміння як у подальшому вести воєнні дії у кіберпросторі (оперувати в кібердомені) та запобігати загрозам кібербезпеці держави.

Аналіз останніх досліджень і публікацій. Інтерес до вивчення кіберборотьби зростає прямо пропорційно з підвищенням інтенсивності її ведення у воєнних конфліктах сучасності. Більшою мірою, актуальні публікації за темою висвітлюють результати дослідження однієї або декількох окремих кібератак (кіберінцидентів), досвіду кіберборотьби під час певного воєнного конфлікту, кібероперацій та спроможностей у кібердомені однієї з держав, або ж технічних характеристик і можливостей деякого програмного (програмно-апаратного) засобу призначеного для ведення кіберборотьби. Наприклад, детальний аналіз причин, перебігу та наслідків серії кібератак на інформаційну інфраструктуру Естонії у 2007 році надано в [11]. Автор праці також узагальнив ключові фактори, завдяки яким було досягнуто такого значного на той час ефекту, основним серед яких був високий рівень дигіталізації суспільства без належної кіберзахищеності. Колектив науковців із Федеральної вищої технічної школи Цюриха продемонстрував результати дослідження характеристик, особливостей, способу «доставки», кількісних показників деструктивного впливу та часу, який пішов на відновлення інфраструктури іранського заводу ядерної промисловості від атаки комп'ютерного хробака Stuxnet у однойменній статті [12]. Результати дослідження [13], де розглянуто перебіг та особливості російсько-українського інформаційної і кіберборотьби, засвідчили, що Україна досить вдало проводить кіберзахист своєї інфраструктури, маючи суперником такі кіберзлочинні групи типу розвиненої сталої загрози (advanced persistent threat (APT)), як Sandworm та FancyBear. Більш ніж ймовірно, ці групи діють під егідою Головного розвідувального управління генерального штабу збройних сил російської федерації (далі – ГРУ ГШ ЗС рф). Корисними є дослідження прикладного спрямування державних установ та агентств призначених для кіберзахисту та реагування на загрози кібербезпеці, а також приватних кібербезпекових компаній. Так, наприклад, дослідження Агентства національної безпеки США [14] висвітлює технічні характеристики, архітектуру побудови та особливості процесу «зараження» комп'ютерних пристроїв шкідливим програмним забезпеченням (далі – ШПЗ) Drovorub, яке, за даними агентства, розроблено зазначеним вище APT FancyBear.

Отже, на сьогодні наукові джерела переповнені інформацією про окремі події у кіберпросторі (кіберінциденти), різноманітність подання якої прямо залежить від її обсягу. Тоді як питання дослідження передового досвіду ведення кіберборотьби, яке дало б змогу розкрити існуючі тенденції та визначити закономірності її подальшого розвитку, залишається невирішеним.

Мета статті. Узагальнити передовий досвід ведення кіберборотьби у воєнних конфліктах сучасності, розкрити існуючі тенденції та визначити закономірності її подальшого розвитку для розробки рекомендацій щодо необхідності розвитку термінологічного апарату у сфері кіберборотьби, а також обґрунтування системи показників і критеріїв оцінювання ефективності кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави.

Виклад основного матеріалу дослідження

Кіберборотьба – феномен XXI століття. Від звичайних кібератак, які беруть свій початок зі становлення комп'ютингу і, здебільшого, спрямовані на досягнення приватних цілей, її відрізняє обов'язкова приналежність до держави та стратегічний (оперативно-стратегічний) характер наслідків. Кіберборотьба може вестися регулярними силами та засобами (кібервійськами), неурядовими організаціями за державного спонсорування під військовим керівництвом (state-sponsored cyberattack), або, як найчастіше відбувається в країнах, що займаються кібертероризмом – кібервійськами під виглядом неурядових організацій із повним запереченням причетності до подій держави-агресора, що надає конфлікту ще більшої гібридності та унеможливлює притягнення суб'єкта до відповідальності за міжнародним гуманітарним правом. Сьогодні ДЦКЗ ДССЗЗІ України, на основі рекомендацій Європейської агенції з кібербезпеки та Європейського центру боротьби з кіберзлочинністю Європейської поліції (далі – Європол), розроблено та введено в дію класифікацію категорій кіберінцидентів – результатів кіберборотьби, форми та способи ведення якої у воєнних конфліктах сучасності еволюціонували (розвивалися) у декілька періодів, що зумовлені геополітичною ситуацією у світі та рівнем розвитку інформаційно-комунікаційних технологій. Перший період є початковим для тієї кіберборотьби, якою її прийнято розглядати сьогодні, він асоціюється з такими воєнними діями у кіберпросторі, як [11; 15–16]:

Titan Rain – кіберрозвідка за державною інформаційною інфраструктурою США та Великої Британії, яку вважають спонсорованою або реалізованою Китаєм. У результаті операції зловмисники, скориставшись вразливістю нульового дня (zero-day exploit), отримали доступ до службової інформації зі сховищ даних таких відомств як: Міністерств оборони та закордонних справ США та Великої Британії, Міністерства енергетики США, NASA та ін. Ця діяльність була викрита у 2005 році. Є підстави вважати, що кібершпіонаж приховано здійснювався з 2003 року. Titan Rain є першою відомою, але далеко не останньою операцією такого типу, в якій підозрюють Китай та підрозділ його Народно-визвольної армії (People's Liberation Army (PLA)) PLA Unit 61398;

кібервплив на інформаційну інфраструктуру Естонії шляхом нанесення серії кібератак у квітні-травні 2007 року. Спричинена суперечностями між етнічними естонцями та російськомовною (проросійсько налаштованою) діаспорою соціальна нестабільність в той момент досягла свого максимуму. Тогочасна інформаційна інфраструктура Естонії, що швидко розвивалася у напрямі «безпаперового» урядування, ще не мала достатнього рівня кіберзахисту. Скориставшись цим, зловмисники нанесли низку розподілених кібератак на відмову в обслуговуванні (DDoS-атаки) у період з 27 квітня до 18 травня. Отримуючи по 2000 запитів на секунду замість звичайних тисячі в день, офіційні веб-ресурси більшості міністерств держави, двох найбільших банків (протягом декількох днів транзакції були неможливими), декількох політичних партій правого спрямування та урядовий поштовий сервер вийшли з ладу. Незважаючи на заяви офіційних осіб держави щодо причетності до кібератак рф, невдовзі уряд Естонії був змушений визнати, що доказів, які б це підтверджували у ході розслідування виявлено не було. Тому, за офіційною версією відповідальними за заподіяну шкоду є група кіберзлочинців, які використовували ботнети – взламані персональні комп'ютери. Фізично ботнети розташовувалися у таких країнах як Єгипет, рф та США. Відповідно діапазон їх мережевих IP-адрес не був логічно зв'язаним, що значною мірою вплинуло на успішність атаки. Причиною тому, чим естонський досвід є таким важливим та визначним для подальшого розвитку подій є те, що реакцією на зазначені DDoS-атаки стало створення Об'єднаного центру передових технологій з кібероборони НАТО (2008 р.) і написання у 2012 році, за його ініціативи, Таллінського посібника з кібервійни – першого офіційного документу щодо застосування норм міжнародного гуманітарного права до воєнних дій у кіберпросторі;

масований кібервплив напередодні та впродовж російсько-грузинської війни (2008 р.), який є першим в історії випадком ведення державою координованих воєнних дій в кіберпросторі у синхронізації з кінетичним протиборством на морі, у повітрі та на суходолі. Щонайменше за три тижні до початку активної фази конфлікту інформаційна інстраструктура Грузії почала піддаватися кібератакам, інтенсивність яких досягла максимуму з її початком. Веб-ресурси 54-ох організацій держави за напрямами урядування, фінансів та комунікацій були недоступними на момент початку війни завдяки атаці на відмову в обслуговуванні. Основна мета цих кібератак – не дати уряду висвітлювати події для цивілізованого світу та отримати його реакцію, у короткі терміни

провівши наземну операцію, а також підсилити настрої зневіри та паніки серед населення. Ще одним виміром впливу був інформаційно-психологічний, прикладом чому є атака на викривлення контенту (вмісту) веб-сайту президента Грузії та зображення Михайла Саакашвілі в образі Гітлера. Серед особливостей можна вказати те, що перед враженням веб-ресурсів офіційних установ DDoS-атака була також направлена на популярний кіберзлочинний форум, для недопущення протидії грузинських хакерів. Останнім все ж вдалося дещо контратакувати, наприклад, на деякий час вивести з ладу веб-сайт інформаційного агентства «РІА Новини», однак це не спричинило якогось ефекту на хід війни. У цій ситуації спонсорування кібератак рф сумнівів не викликало, а безпосереднє їх виконання, на основі аналізу інтернет-трафіку, приписують APT Russian Business Network;

Agent.btz – кіберрозвідка за допомогою ШПЗ (комп'ютерного хробака), що розповсюдився військовими мережами США зі скомпрометованого флеш-накопичувача після його фізичного під'єднання до одного з комп'ютерів Центрального командування Збройних сил США. Виявивши у 2008 році, що за допомогою Agent.btz було отримано доступ як до не таємної, так і до інформації з обмеженим доступом, Пентагон витратив 14 місяців на повне очищення від нього своїх мереж та систем у межах оборонної кібероперації «Operation Buckshot Yankee». Базовою реакцією на витік конфіденційних даних стала заборона на використання сторонніх накопичувачів усіх типів на американських військових об'єктах, а стратегічною та визначною – утворення 21 травня 2010 року Кіберкомандування США, а згодом і кіберкомандування видів збройних сил. Agent.btz пов'язують із APT, відомим як Turla/Uroborus/Snake/Venomous Bear/Krypton, а його, відповідно, з Федеральною службою безпеки рф (далі – ФСБ рф);

кібервплив на інформаційну інфраструктуру США та Південної Кореї шляхом проведення циклу DDoS-атак. Кібератаки відбувалися у 3 хвилі, перша з яких розпочалася 04 липня 2009 року. Серед об'єктів, які піддалися атакам на відмову в обслуговуванні можна відмітити офіційні веб-ресурси Білого Дому, Пентагону, президента Південної Кореї та її оборонного і безпекового відомств, газети «The Washington Post», однієї з американських бірж та ін. Ці атаки одразу ж почали асоціювати із Північною Кореєю через їхній початок саме в день випробувань нею балістичних ракет малої дальності. Пізніше, у результаті аналізу декількох інших кібератак, дослідники дійшли висновку, що зазначені події 2009 року дійсно є результатом діяльності спонсорованого урядом КНДР APT Lazarus Group;

кібератаки на М'янму, що розпочалися 25 жовтня 2010 року з метою скомпрометувати проведення виборів до парламенту держави, які до цього не здійснювалися з 1990 року через режим військової диктатури. Кібератаки оцінюються як «значно потужніші» за ті, що відбулися в Естонії та Грузії у попередніх роках. Їхніми цілями стали сервери головного інтернет-провайдера країни, а також веб-ресурси міністерства зв'язку та телекомунікацій. Тодішня мережева організація М'янми дозволяла приймати та передавати інтернет-трафік обсягом до 45 МБіт/с, в той час як DDoS-атака забезпечила надсилання запитів зі швидкістю 10 – 15 ГБіт/с, триваючи більше восьми годин кожного дня. Атаку пов'язують із військовою диктатурою, яка не бажала передавати владу в країні демократам.

Підсумовуючи досвід ведення кіберборотьби першого періоду можна зробити такі висновки:

1. Основним типом об'єктів кібервпливу були об'єкти інформаційної інфраструктури (веб-ресурси, файлові та поштові сервери, сховища конфіденційних даних та ін.).

2. Для нанесення кібервпливу найчастіше застосовувалися DDoS-атаки, а також атаки на викривлення (зміну) контенту веб-ресурсів (defacement attack), ШПЗ було призначеним переважно для кіберрозвідки.

3. Кількісного значення кібервпливу тогочасних кібератак напряму залежало від кількості хостів (ботнетів), задіяних у DDoS-атаці та їх розподіленості у глобальній мережі Інтернет.

4. Під час цього періоду стали явними основні суб'єкти геополітичної арени кіберборотьби: Китай, США та рф.

5. Виникла потреба в обґрунтуванні застосування норм міжнародного гуманітарного права до кіберборотьби та категоріювання кіберінцидентів, які виникають внаслідок її ведення.

6. Необхідність кібервійськ (сил) стала очевидною для провідних держав світу.

Авторська візуалізація узагальнення основних типів кібератак та об'єктів кібервпливу першого періоду воєнних дій в кіберпросторі запропонована у вигляді діаграми Венна (рис. 1) [11; 15–16].

Рисунок 1 – Основні типи та об'єкти кібератак першого періоду воєнних дій у кіберпросторі (2005–2010 рр.)

З часом, а також з розвитком інформаційних технологій та всеосяжної дигіталізації, програмні (програмно-апаратні) засоби кіберзахисту, кіберрозвідки та кібервпливу видозмінювалися у якісному співвідношенні. Відповідно, форми та способи ведення кіберборотьби також еволюціонували. Найвагомішим досвідом ведення воєнних дій у кіберпросторі другого періоду є [12; 16]:

операція «Олімпійські ігри» – кібервплив із застосуванням ШПЗ (комп'ютерного хробака) Stuxnet (2010 р.) на завод ядерної промисловості у Натанзі, Іран. Stuxnet є особливим випадком деструктивного ШПЗ, спрямованим на Системи диспетчерського керування та збору даних (Supervisory Control And Data Acquisition (SCADA)) у промислових контролерах. Розповсюдившись з приєднаного в комп'ютерній мережі заводу скомпрометованого USB-накопичувача, Stuxnet використав чотири раніше невідомі вразливості (exploit) програмного забезпечення мікроконтролерів, та, змінюючи швидкість обертання центрифуг, призвів до масованого (більше тисячі) виведення їх з ладу. Відновити штатну роботу заводу до обсягів, які були перед початком кібератаки вдалося тільки через рік. Основним суб'єктом цієї кібератаки вважають США, які діяли в інтересах недопущення спроби кінетичного впливу Ізраїля на Іран та для зниження ядерного потенціалу останнього в цілому. Хоча хронологічно, ці події відбулися дещо раніше за розглянуті вище DDoS-атаки на М'янму, можна констатувати, що Stuxnet був технологічно та ідеологічно революційним для свого часу, вивів кіберборотьбу на принципово новий рівень, а також продемонстрував, що воєнні дії у кіберпросторі здатні безпосередньо впливати на обороноздатність держави та її наступальний потенціал;

кіберрозвідка за канадськими інституціями, що відносяться до критичної інфраструктури (виявлена у січні 2011 року). ШПЗ призначене для сканування та фільтрування ключової інформації (наприклад, логіни та паролі) та її відправлення суб'єкту кіберрозвідки доставлялося на службові комп'ютери за допомогою організованої фішингової схеми. У результаті відбулося заволодіння інформацією з обмеженим доступом Ради фінансів та Міністерства фінансів, а також профільної науково-технічної агенції Міністерства оборони Канади. Суб'єктом кіберрозвідки підозрюють Китай, проте доказів цьому знайдено не було;

«операція» Ababil – серія DDoS-атак, розпочатих 18 вересня 2012 року підпорядкованим керівництву ісламістської терористичної організації ХАМАС кіберзлочинним угрупованням «кібервоїни Ізз ад-Дін аль-Кассама», на американські фінансові інституції. Серед об'єктів кібератак можна виділити Нью-Йоркську фондову біржу, банки JPMorgan Chase, Bank of America, Sun Trust Bank та ін. Максимальна потужність кібервпливу досягла 65 ГБіт/с, призвівши до тимчасової відмови в обслуговуванні веб-ресурсів зазначених установ. Угруповання анонсувало свої дії, критикуючи США та Ізраїль і аргументуючи свої дії як відповідь на дискредитаційний відеозапис відомий як Innocence of Muslims. А отже, кіберборотьба може набувати і релігійного підтексту зокрема;

Flame – ШПЗ схожої до Stuxnet архітектурної побудови, вважається частиною описаної вище кібероперації «Олімпійські ігри», кібервплив під час проведення якої, був направлений на зменшення ядерного та, загалом воєнного, потенціалу Ірану. Не дивлячись на те, що експерти в області розробки ПЗ вважають Flame технологічно більш розвинутим за Stuxnet, за словами іранських військових, атакуючи персональні комп'ютери та сервери нафтового сектору держави у 2012 році, його активність була виявленою підрозділом кіберзахисту, а вжиті заходи не допустили подальшого розповсюдження комп'ютерного хробака мережею;

кібератаки на низку південнокорейських медіа та фінансових компаній 20 травня 2013 року, у період напружених відносин із КНДР через випробування Пхеньяном ядерної зброї 12 лютого того ж року. У подіях підозрюють APT Lazarus Group, яке скомпонувало DDo*S*-атаки із застосуванням призначеного для викрадення інформації ШПЗ DarkSeoul. Кібервпливу було піддано 32 тисячі персональних комп'ютерів та серверів, а загальні збитки оцінюються у більше ніж 750 млн доларів США. Розслідування інциденту привело до IP-адреси китайського сегменту мережі Інтернет, що збільшило підозри щодо безпосередньої реалізації атаки Північною Кореєю, так як використання її кібервійськами (кіберзлочинними угрупованнями) мережевих адрес Китаю є звичайною практикою і здійснюється з метою «зачищення слідів».

Узагальнюючи досвід ведення кіберборотьби під час другого періоду воєнних дій у кіберпросторі (відображено автором у табл. 1 [12; 16]) слід зазначити, що він пов'язаний із утворенням у складі збройних сил провідних держав військових формувань уповноважених та призначених для кіберзахисту, кіберрозвідки та кібервпливу. Так, у 2010 році було створено Кіберкомандування США, а згодом – підпорядковані йому кіберкомандування видів збройних сил, інші держави також почали формувати військові підрозділи еквівалентного призначення (Китай, рф, Іран, держави-члени НАТО, Південна Корея, КНДР тощо).

Таблиця 1

Узагальнення досвіду ведення кіберборотьби другого періоду воєнних дій у кіберпросторі (2010–2014 рр.)

Умовне найменування воєнних дій в кіберпросторі	Рік	Об'єкт кіберборотьби (держава, її інституції)	Ймовірний суб'єкт кіберборотьби (підрозділ, організація, група та / або держава)	Заходи кіберборотьби	Категорія кібер-інциденту
Операція «Олімпійські ігри» (Stuxnet)	2010	Іран, системи SCADA об'єкту ядерної промисловості	Підрозділи кіберборотьби США	Кібервплив	ШПЗ, exploit
Кіберрозвідка проти Канади	2011	Канада, фінансові установи та науково-технічний військовий об'єкт Канади	Китай	Кіберрозвідка	ШПЗ, сканування
«Операція» Ababil	2012	США, фінансові установи	«Кібервоїни Ізз ад-Дін аль-Кассама», ХАМАС	Кібервплив	DDoS
Flame	2012	Іран, нафтовий сектор	Підрозділи кіберборотьби США	Кібервплив	ШПЗ
DarkSeoul	2013	Південна Корея, медіа та фінансові установи	Lazarus Group, КНДР	Кібервплив	*DDoS*, ШПЗ

Основними положеннями винесеними з досвіду воєнних дій у кіберпросторі другого періоду вважаємо такі:

1. Прослідковується чітка тенденція до перенесення основних зусиль кіберборотьби із об'єктів інформаційної на об'єкти критичної інфраструктури (фінанси, медіа, військові об'єкти, нафтовий сектор, ядерна та інша промисловість тощо), за рахунок комп'ютеризації усіх сфер діяльності.

2. На рівні з вже класичними DDoS-атаками почали проводитися більш складні операції, ядром яких було розповсюдження комп'ютерними системами та мережами об'єктів впливу ШПЗ, функціонал якого безпосередньо реалізовував мету.

3. Спектр призначення ШПЗ розширився, нові його зразки почали розроблялися з метою нанесення деструктивного впливу.

4. Північна Корея – була і залишається «темним гравцем» на міжнародній арені воєнних дій у кіберпросторі, удосконалюючи форми та способи своїх дій.

5. Закономірність: якщо до кібератаки вважається причетним Китай, то її мета, як правило, полягає у кіберрозвідці.

Другий період був ключовим у становленні сучасних форм та способів ведення кіберборотьби, він довів, що воєнні дії в кіберпросторі можуть бути ефективним засобом впливу на держави та способом отримання розвідувальної інформації, у цей період планувалися і проводилися перші кібероперації. В подальшому результати воєнних дій у кіберпросторі визначалися спроможностям з кіберрозвідки і кібервпливу суб'єкта та спроможностями з кіберзахиту об'єкта кіберборотьби.

Наступний (третій) період воєнних дій у кіберпросторі триває донині, він логічно поділяється на два етапи, перший з яких тривав з 2014 по 2022 рік та ознаменований таким досвідом ведення кіберборотьби [17–19]:

розвідувальна кібероперація на основі зараження інформаційних систем державних установ та приватних підприємств критичної та інформаційної України ШПЗ Uroborus (комп'ютерний хробак з руткітом), активна фаза якої відбулась наприкінці 2013 – на початку 2014 років. Дослідники вважають Uroborus пов'язаним і створеним на основі розглянутого вище Agent.btz. За його допомогою здійснювалася кіберрозвідка за військовими інформаційними системами США (перший період воєнних дій у кіберпросторі). ШПЗ Uroborus розроблений кіберзлочинним угрупованням Turla, що діє в інтересах ФСБ рф. Основною метою застосування цього ШПЗ було викрадення «чутливої» інформації із заражених комп'ютерів, більшість яких відносилися до силових структур України, ЗМІ, промислового сектору та фінансових інституцій, а другорядною – формування бот-мережі із заражених комп'ютерів та віддалене керування ними у цілях подальшого використання їх потужностей при нанесенні *DDoS*-атак. Пік кібератак Uroborus відбувався одночасно із загостренням протестів у ході Революції гідності, що додатково засвідчує потенційну причетність російської сторони. Таким чином, цей досвід є повноцінним прикладом ведення кіберборотьби на етапі підготовки до воєнного конфлікту (російсько-української війни);

кібероперація із виведення з ладу енергосистеми західного регіону України. Вона відбулася 23 серпня 2015 року і здійснювалася з використанням ШПЗ BlackEnergy3. Ця операція призвела до втрати контролю над тридцятьма електропідстанціями та відсутності електроенергії для 230 тисяч споживачів у зоні відповідальності АТ «Прикарпаттяобленерго». Відновити електропостачання вдалося через 6 годин. Для досягнення мети, суб'єкту довелося спланувати та провести кібероперацію широкого спектру, яка включала такі етапи: компрометація корпоративної мережі за допомогою фішингу; зараження комп'ютерів та серверів ШПЗ BlackEnergy3; взяття під контроль систем SCADA електростанцій; виведення з ладу мережевих пристроїв (маршрутизаторів, комутаторів, джерел безперебійного живлення тощо); знищення файлової структури серверів з метою ускладнення відновлення системи; DDoS-атака на кол-центр. Кібератака є продовженням кіберборотьби під час російсько-української війни, яка почалася у 2014 році, вважається реалізованою APT Sandworm (ГРУ ГШ ЗС рф). Вважається першим в історії досвідом вдалого нанесення кібервпливу на об'єкт енергетичної інфраструктури. Кібератака має спільну мету з тією, що відбулася роком пізніше (2016) та тимчасово (до однієї години) вивела з ладу електропідстанцію, що обслуговує частину м. Київ, тому їх можна розглядати спільно;

кібероперація «Glowing Symphony» (2016 р.). Впродовж декількох років Кіберкомандування США готувало операцію для нанесення кібервпливу та знищення пропагандистського медіаресурсу Ісламської держави. Проведення операції стало можливим завдяки виявленню під час підготовчого етапу того, що для розповсюдження контенту використовується 10 базових акаунтів. Потім, через перехід за посиланням з фішингового email-листа одним із операторів медіаресурсу американська сторона отримала доступ до серверної частини платформи. Кібероперація була ретельно спланованою та включала в себе кіберрозвідку, соціальну інженерію, фішинг тощо. Конкретні її деталі залишаються таємними, проте своєї мети вона досягла – більшість серверів піддалися деструктивному впливу та не підлягали відновленню. Прослідковується чітка тенденція, як США після того як на початку 2000 років були частим об'єктом кібервпливу, у відносно короткі терміни сформували підрозділи кіберборотьби, які, принісши перші вагомі результати у 2010 році, розвинулися та провели у 2016 році таку складну багатоетапну кібероперацію, як «Glowing Symphony»;

кібервплив із застосуванням ШПЗ (програми-вимагача) WannaCry, що розповсюдилась персональними комп'ютерами та серверами на базі операційної системи Windows та Windows Server, використавши викрадену у Агентства національної безпеки США вразливість (exploit) EternalBlue протоколу прикладного рівня Server Message Block (SMB) мережевої моделі OSI. Дізнавшись про викрадення 14 квітня 2017 року, агентство одразу ж повідомило про це Microsoft, яка в екстреному порядку розробила оновлення безпеки. А вже 12 травня, менше ніж через місяць, не оновлені операційні системи піддалися атаці – усі дані їх файлових систем було закодовано, доступ до системи – заблоковано. Для розблокування та розкодування файлів від користувача вимагалося перевести певну суму (300–600 доларів США) у криптовалюті на визначені електронні гаманці. Після спрацювання на одному комп'ютері ШПЗ сканувало мережу та розповсюджувалося нею, проте першоджерело зараження достеменно невідоме. Загалом кібератака нанесла кібервплив більш ніж на 300 тис. комп'ютерних пристроїв у 150 державах світу. Агентство національної безпеки США та Центр кібербезпеки Великої Британії вважають, що за кібератакою стоїть Північна Корея та їй підпорядковане APT Lazarus Group, дослідження Microsoft дійшли того ж висновку. WannaCry є прикладом розвитку форм та способів ведення кіберборотьби Північної Кореї, а також того, що сучасна кіберборотьба ведеться постійно. Зважаючи на особливості кібератаки, вважаємо, що у такий спосіб КНДР реалізувала одразу декілька цілей: відпрацювання навичок своїх військ (сил) кіберборотьби у реальних умовах; перехід державної концепції «проти всіх» і на воєнні дії у кіберпросторі; а також побічна – додаткове фінансування розробки нових видів ШПЗ на подальшу перспективу;

кібероперація з нанесення деструктивного кібервпливу із застосуванням ШПЗ NotPetya, що була реалізована у формі кібератаки на ланцюг постачання (supply-chain cyber attack). ШПЗ NotPetya, подібно до WannaCry, використовувало exploit EternalBlue операційних систем Windows. Особливістю цієї операції став вдало підібраний спосіб розповсюдження ШПЗ та «зараження» ним комп'ютерних пристроїв: спочатку компрометації піддалися сервери сервісу електронної звітності, документообігу та електронно-цифрового підпису M.E.Doc, який у 2017 році за призначенням використовувався багатьма українськими компаніями та державними органами. Після цього у пакет наступного оновлення M.E.Doc було приховано закладено ШПЗ NotPetya. 27 червня 2017 року пакет оновлення було розповсюджено сервером та автоматично встановлено на комп'ютери клієнтів (близько 400 тис. в Україні). Далі алгоритм дії був такий як у випадку з ШПЗ WannaCry (кодування усіх даних із файлової системи, розповсюдження мережею та блокування авторизації операційної системи, вимагання викупу за відновлення доступу до файлів). Ключовою відмінністю програмної реалізації ШПЗ NotPetya, порівняно з попередником, на думку

технічних експертів в галузі кібербезпеки, є те, що в окремих випадках, файлові системи об'єктів кібервпливу не підлягали відновленню навіть за допомогою декодування. Кібероперацію було проведено напередодні чергового дня Конституції України. Реальною її метою вважають нанесення максимальних збитків критичній та інформаційній інфраструктурі України (під маскою вимагання коштів). Основними об'єктами кібервпливу були веб-ресурси та об'єкти інформаційних систем міністерств, банків, ЗМІ та енергетичних компаній України. Послугами сервісу «M.E.Doc» користувалися: державне підприємство «Антонов», телекомунікаційні компанії «Київстар» та «Vodafone Україна», телеканали «ICTV» та «STB», Київський метрополітен, Кредобанк, Ощадбанк, та низка інших організації критичної та інформаційної інстраструктури держави. У лютому 2018 року Білий Дім визнав причетність збройних сил російської федерації до проведення кібероперації та назвав її «*найбільш руйнівною та дорогою кібератакою в історії*» [20]. Зважаючи на технологічну схожість ШПЗ NotPetya та WannaCry, можна дійти до висновку про гіпотетичну співпрацю рф та КНДР у розробленні програмних засобів кіберборотьби;

кібероперація у формі supply-chain cyber attack, реалізована з метою кіберрозвідки за допомогою компрометації ПЗ сервісу моніторингу стану корпоративних комп'ютерних систем та мереж Orion американської компанії SolarWinds. Для свого функціонування сервісу Orion потрібні привілейовані права на керування мережевим трафіком і продуктивністю систем. Станом на другу половину 2019 року цим ПЗ користувалося більше 30 тис. приватних установ та державних відомств, серед яких: Міністерство оборони США, Агентство національної безпеки США, Міністерство фінансів США, Міністерство торгівлі США та ін. Отже, Orion був більш ніж пріоритетною ціллю кіберборотьби, у черговий пакет оновлення якого, завдяки компрометації та несанкціонованому доступу до програмного коду, було додано ШПЗ Sunburst. ШПЗ розповсюдилося комп'ютерними мережами в березні 2020 року. Несанкціонований доступ було викрито лише у грудні цього ж року одним із клієнтів SolarWinds – кібербезпековою компанією FireEye. Ця компанія одразу сповістила про ситуацію із сервісом Orion Агентству кібербезпеки та безпеки інфраструктури США. Далі послідувала директива стосовно заборони використання ПЗ Orion для моніторингу федеральних комп'ютерних мереж, а також цілий комплекс заходів з кіберзахисту. Деякі дослідження свідчать, що кібератаку здійснило APT Nobelium служби зовнішньої розвідки рф. Інші ж, наприклад, компанія-розробник антивірусного ПЗ Kaspersky, дійшли висновку, що за атакою стоїть вище згадане APT Turla, пов'язана з ФСБ рф. Тим не менш, більшість джерел сходяться на причетності російської сторони до проведення кібероперації. Найвірогіднішою метою кібероперації була кіберрозвідка в інформаційних системах урядового, військового та фінансового сектору США, так як жодного факту деструктивного впливу виявлено не було;

серія виявлених у червні 2021 року розвідувальних кібероперацій проведених APT RedFoxtrot, безпосередньо пов'язаних, на думку експертів, із підрозділом кіберборотьби збройних сил Китаю PLA Unit 69010. Об'єктами кіберрозвідки були: військові та аерокосмічні об'єкти Індії; основні телекомунікаційні провайдери Афганістану, Пакистану, Індії та Казахстану; інформаційні системи урядових інституцій, приватних компаній та військових органів низки азіатських держав. Точних даних щодо обсягів отриманих конфіденційних даних немає, водночас описана серія кібероперацій доводить інтерес Китаю до розвідки через кіберпростір не тільки основних гравців геополітичної арени світу, але і держав свого регіону, які явно поступаються йому в розвитку;

09 липня 2021 року – російський кібервплив, як акт протидії військовим навчанням Сі Бриз-2021. Цей вплив складався з двох частин: перша – отримання несанкціонованого доступу до сайту Військово-морських Сил (далі – ВМС) Збройних Сил України для викривлення його контенту і публікації неправдивої інформації та документів щодо перебігу військових навчань; друга – DDoS-атаки на веб-портал Міністерства оборони України (далі – МО України). Якщо перша частина операції була вдалою завдяки успішному використанню вразливостей веб-фреймворку, на якому була побудована архітектура сайту українських ВМС, то призвести до відмови в обслуговуванні веб-порталу МО України не вдалося. Отже, основна мета кібероперації була досягнута, а її проведення засвідчило нетерпимість рф до будь-якої військової присутності у чорноморському регіоні. Також це можна розглядати як тренування перед початком активного ведення кіберборотьби, що безпосередньо передувала та збіглася у часі з широкомасштабним вторгненням в Україну 24 лютого 2022 року.

Першому етапові третього періоду воєнних дій у кіберпросторі притаманне максимальне розширення спектру об'єктів кіберрозвідки та кібервпливу, серед яких: об'єкти енерносистеми, силові відомства, ЗМІ, фінансові інституції, медіаресурси, об'єкти аерокосмічного сектору, телекомунікаційні провайдери та ін. Серед безлічі кіберінцидентів, які відбулися у межах цього етапу автором було відібрано ті, які за своєю метою, формою реалізації, суб'єктом та об'єктом впливу вважаються воєнними діями у кіберпросторі (табл. 2) [17–19].

Таблиця 2

Узагальнення досвіду ведення кіберборотьби першого етапу третього періоду воєнних дій у кіберпросторі (2014–2022 рр.)

Умовне найменування воєнних дій в кіберпросторі	Рік	Об'єкт кіберборотьби (держава, її інституції)	Ймовірний суб'єкт кіберборотьби (підрозділ, організація, група та / або держава)	Заходи кібер-боротьби	Категорія кібер-інциденту
Uroborus	2014	Україна, інформаційні системи органів державної влади	APT Turla, ФСБ рф	Кібер-розвідка	Фішинг, ШПЗ, сканування
BlackEnergy3	2015, 2016	Україна, національна енергосистема	APT Sandworm, ГРУ ГШ ЗС РФ	Кібервплив	Фішинг, ШПЗ, DDoS
Операція «Glowing Symphony»	2016	Ісламська держава, терористичний медіа-ресурс	Кіберкомандування США	Кібервплив	Фішинг, соціальна інженерія, компрометація системи
WannaCry	2017	США, держави-члени НАТО, ін. держави, комп'ютерні мережі та системи	APT Lazarus Group, КНДР	Кібервплив	ШПЗ, програма-вимагач, exploit (Eternal Blue)
NotPetya	2017	Україна, міністерства, банки, ЗМІ та енергетичні компанії	APT Sandworm, ГРУ ГШ ЗС РФ	Кібервплив	ШПЗ, експлуатація відомої вразливості (Eternal Blue)
SolarWinds	2020	США, об'єкти критичної державної інфраструктури	APT Nobelium, СЗР РФ	Кібервплив	ШПЗ, компрометація системи
RedFoxtrot	2021	Держави Центральної та Східної Азії, об'єкти критичної та інформаційної інфраструктури	PLA Unit 69010, Китай	Кібер-розвідка	ШПЗ, сканування
Сі Бриз-2021	2021	Україна, веб-ресурс Військово-морських сил ЗС України	APT Sandworm, ГРУ ГШ ЗС РФ	Кібервплив	Компрометація системи, DDoS

Узагальнення досвіду воєнних дій у кіберпросторі першого етапу третього періоду дозволило сформулювати такі положення:

1. Тенденція до ведення багатоетапних кібероперацій повного спектру, що зумовлено підвищенням загального рівня кіберзахищеності комп'ютерних інформаційних систем та мереж, а також зростанням вимог до результатів таких операцій.

2. Тенденція до здійснення DDo*S*-атак як одного з етапів кібероперації для посилення її ефекту або введення в оману противника, окреме ж застосування атак цього типу перестало бути таким ефективним як у попередніх періодах.

3. Для досягнення мети кібероперації, як правило, має спрацювати певний кіберсоціальний ланцюг (фішинг, соціальна інженерія тощо), сьогодні людина є найслабшою ланкою функціонування комп'ютерних систем та мереж, тоді як виявити раніше невідому вразливість у системах кіберзахисту стає дедалі складніше.

4. Кіберборотьба ведеться державами постійно як у мирний час, так і у воєнних конфліктах.

5. Закономірність: ШПЗ, застосування якого мало успіх, модернізується, видозмінюється та застосовується знову (Agent.btz став основою Uroborus, WannaCry – основою NotPetya).

6. Попередньо визначена закономірність щодо ведення Китаєм переважно кіберрозвідки підтверджується, нові факти свідчать про значну

скритність таких його дій, яка дозволяє роками непомітно мати доступ до конфіденційної інформації.

7. Існує гіпотетична співпраця (обмін досвідом) між Північною Кореєю та рф щодо розвитку форм та способів ведення кіберборотьби.

8. Кіберкомандування США – один із небагатьох підрозділів кіберборотьби держав світу, який визнає проведені ним кібероперації.

Наймасштабнішим воєнним конфліктом сучасності, який триває і сьогодні, є російсько-українська війна. Вона ведеться не тільки на суходолі, в повітрі та на морі, але і у кібердомені. Сьогодні складову російсько-українського протистояння, що відбувається у кібердомені визнано першою повноцінною кібервійною, а отже, вона є найактуальнішим джерелом досвіду ведення кіберборотьби. За канонами гібридних війн, всебічна «підготовка» держави до нападу на неї проводиться завчасно. Саме так події розгорталися і у кіберпросторі перед широкомасштабним вторгненням рф в Україну. У січні та лютому 2022 року основним вектором спрямування російської кіберборотьби був кібервплив на заздалегідь виявлені кіберрозвідкою вразливості, а саме [21]:

перша з них – кібератака раніше невідомого хакерського угруповання DEV-0586 із застосуванням ШПЗ (програми-вимагача), яку ідентифікував Центр аналізу загроз Microsoft-ту 13 січня 2022 року. Джерело та спосіб зараження залишаються невідомими. Водночас, об'єктами атаки стала низка урядових та неприбуткових організацій (Державна служба України з надзвичайних ситуацій, Моторне (транспортне) страхове бюро України та ін.), декілька українських ІТ-компаній. ШПЗ було спроєктовано так, щоб здавалося ніби його мета полягає в отриманні прибутку (викупу). Однак принцип дії застосованої програми-вимагача був атиповим. Зазвичай подібні зразки ШПЗ зашифровують файлову систему, у цьому ж випадку, під час вимкнення пристрою, відбувалося переписування головного завантажувального запису (master boot record) його жорсткого диску, без можливості відновлення. Враховуючи означене, основною метою кібератаки стало нанесення деструктивного впливу на комп'ютерні системи об'єктів критичної інфраструктури (кібервплив). Microsoft пізніше класифікував ШПЗ DEV-0586 як сімейство WhisperGate-подібних;

одразу після цього, 14 січня 2022 року, було здійснено кібератаку на викривлення контенту веб-ресурсів близько 70 державних інституцій України, серед яких сайти Кабінету Міністрів України, Міністерства закордонних справ України та Ради національної безпеки і оборони України. Скомпрометувавши адміністративні права розробника програмного забезпечення урядових веб-ресурсів, силами кіберборотьби противника було отримано доступ до керування ними. Після чого їх вміст було замінено на повідомлення «*Бійтеся і готуйтеся до гіршого*». Через декілька годин Україні вдалося повернути контроль за серверами, втім, противнику за допомогою засобів кібервпливу, на тлі наростаючої загрози збройного вторгнення, вдалося завдати необхідного морально-психологічного ефекту цільовій аудиторії (громадянам України);

15 лютого 2022 року – серія потужних DDoS-атак на веб-ресурси МО України, Міністерства закордонних справ України, Збройних Сил України, Приватбанку та Ощадбанку. Крім того, атаці піддалися сервери хостинг-провайдера Mirohost, на потужностях якого функціонують веб-ресурси деяких зі згаданих вище установ. На основі аналізу інтернет-трафіку, що показав передачу значних обсягів даних з кіберінфраструктури ГРУ ГШ ЗС рф на український сегмент мережі Інтернет саме у той період часу, Рада національної безпеки США заявила про причетність до кібератаки російської розвідки;

у переддень широкомасштабного вторгнення, близько 17:00 за київським часом – повторна кібератака з використанням HermeticWiper (видозміненого WhisperGate-подібного ШПЗ), яка, за даними ESET, вивела з ладу сотні комп'ютерних пристроїв належних низці оборонних, фінансових, та інших установ критичної інфраструктури, а також ІТ-компаній.

Отже, цикл описаних вище кібератак, що мали місце у січні – лютому 2022 року можна об'єднати в кібероперацію, цілями якої були дестабілізація інформаційного та кіберпростору України, відволікання зусиль основних суб'єктів забезпечення кібербезпеки держави на протидію кібератакам, компрометація онлайн-банкінгу та, в цілому, створення деякого переможного наративу ще до початку кінетичної фази конфлікту, на тлі зосередження вздовж державного кордону України стотисячного наступального угруповання військ (сил).

Кіберборотьба української сторони, у період наближення воєнного конфлікту, була зосереджена на кіберзахисті енергетичної сфери, державних порталів та сервісів. Так, за 3–4 місяці до початку широкомасштабного вторгнення активно велися пенетраційні тести Єдиного порталу державних послуг «Дія» із залученням фахівців на платній основі, що дало змогу усунути значну частку вразливостей застосунку. Слід зазначити, що саме портал «Дія», в критичні для України моменти активної фази війни, що спричинила масову втрату документів, що засвідчують особу, працював без суттєвих збоїв та запровадив «єДокумент» на період дії правового режиму воєнного стану.

В унісон з початком сухопутного вторгнення в Україну, рф зосередила основні зусилля сил і засобів кіберборотьби на подавленні системи зв'язку та управління військами (силами), зокрема, підсистеми супутникового військового зв'язку.

Супутниковий зв'язок ЗС України був організований шляхом отримання каналу від українського провайдера Datagroup через італійського Skylogic, який безпосередньо співпрацює із власником супутника Ka-Sat компанією Eutelsat (Франція). Шляхом кібервпливу (перевантаження трафіку) на мережеву інфраструктуру та обладнання Skylogic, який розпочався о 05:02 за київським часом та тривав близько 4-х годин [22], сили кіберборотьби рф призвели до втрати з'єднання терміналів Tooway, які використовуються для організації супутникового зв'язку між пунктами управління усіх ланок ЗС України та доведені до рівня батальйону, із супутником Ka-Sat. На основі досвіду ведення Антитерористичної операції та Операції об'єднаних сил, супутниковий зв'язок залишався єдиним засобом комунікації, що забезпечував управління військами (силами), особливо на початковому етапі зайняття ними районів, непідготовлених в плані зв'язку. Відтак значний сегмент системи військового зв'язку ЗС України був подавлений силами кіберборотьби рф на момент широкомасштабного вторгнення. На потенційний (імовірний) негативний вплив такої організації супутникового зв'язку для ЗС України, яка прямо залежить від цивільних нерезидентів, фахівці військового зв'язку наголошували задовго до широкомасштабного вторгнення рф. Усвідомивши це, влада України 26 лютого звернулася до компанії SpaceX з проханням надати термінали супутникового зв'язку Starlink, на що було отримано позитивну відповідь. Так з'явилася змога забезпечити супутниковий зв'язок на фронті, у тому числі, під час оборони Києва та Маріуполя.

Російське вторгнення у перші дні війни також підсилювалося масованою фішинговою атакою на електронні скриньки військовослужбовців ЗС України із закликом до здачі, а ті скриньки, які вдалося скомпрометувати, згідно з дослідженням компанії Google, в подальшому використовувалися для відправлення фішингу польським військовим. У цьому випадку кіберборотьба велася силами та засобами білоруського APT UNC1151.

Відповіддю України, зважаючи на несформованість кібервійськ із спроможностями до здійснення кібервпливу, було створення, так званої, ІТ-армії, яка складається переважно з волонтерів-фахівців в галузі кібербезпеки. Ці волонтери умовно розділилися на 2 групи (кіберзахист та кібервплив) та діяли за координацією Міністра цифрової трансформації України. Одразу ж в день створення ІТ-армія нанесла кібервплив у вигляді потужних DDoS-атак на веб-ресурси російської та білоруської інформаційної та критичної інфраструктури: було виведено з ладу сайти ФСБ рф, «Роскомнагляду», президента рф, уряду та парламенту рф, Московської біржі, Національного банку Білорусі та багатьох інших [23]. Крім цього, 24 лютого 2022 року було завдано атаки на групу компаній «Систематика». Зокрема, деструктивному кібервпливу піддалися її автоматизована система «Вибори» та системи електронного документообігу окупаційної влади на території АР Крим, а також так званих Донецької та Луганської народних республік . 25 лютого цього ж року було знищено систему керування даними Федерального казначейства рф.

Також українська ІТ-армія взаємодіяла із антиросійською білоруською хакерською командою «Кіберпартизани», яка ще в січні 2022 року скомпрометувала сервери автоматичного керування рухом поїздів Білоруської залізниці з метою сповільнення транспортування російських військ. З початком вторгнення російських військ до України, 27 лютого 2022 року, «Кіберпартизани» завдали деструктивного кібервпливу, який змусив поставляти припаси автомобільним транспортом та спричинив серйозні перебої з логістикою ударного угруповання російських військ на Півночі України, що вилилося у 40-кілометровий конвой на підступах до столиці України. Отже, досвід російсько-української кібервійни демонструє, що у кібердомені можливими є навіть партизанські дії.

Пізніше Кеннет Гірс, міжнародно визнаний фахівець з кібербезпеки, на конференції «DEF CON 30» 12 серпня 2022 року, висловив думку, що найвизначнішими кібератаками початку активної фази російсько-української війни стали російська атака на мережеве обладнання Skylogic, що призвела до подавлення супутникового військового зв'язку ЗС України та про-українська атака на систему управління білоруською залізницею. Також Кеннет Гірс вважає, що рф була націлена на швидку перемогу, її помилкою стало занадто потужне використання ресурсу кіберборотьби у січні – лютому 2022 року, розкриття відомих їй вразливостей інформаційної та кіберінфраструктури України, що за сукупністю призвело до сповільнення темпів нанесення кібервпливу та необхідності повернутися до кіберрозвідки [24].

Україна в цей час прискореними темпами вживала заходів щодо нарощування спроможностей із ведення кіберборотьби наявними суб'єктами забезпечення кібербезпеки держави. Надалі кіберборотьба, під час російсько-української кібервійни, може розглядатися як кіберпротиборство двох держав основні події якого наведені автором в таблиці 3 [25–29].

Таблиця 3

Російсько-українське кіберпротиборство

Російська кіберборотьба	Українська кіберборотьба
1	2
березень 2022 року: кіберрозвідка інформаційної та кіберінфраструктури державних органів України російським APT UAC-0035 (InvisiMole) шляхом фішингу з використанням ШПЗ LoadEdge; березень – квітень 2022 року: російське кіберзлочинне угруповання Sandworm здійснило кібервплив на комп'ютерні мережі української агропромисловості з метою перешкоджання стратегічно важливому експорту зернових культур та на системи контролю електропідстанцій за допомогою ШПЗ Industroyer2; липень 2022 року: кіберрозвідка кіберзлочинного угруповання Turla, що здійснювалася через розповсюдження Android-застосунку «Cyber Azov» для DDoS-атак на російські веб-сайти, який насправді використовувався для отримання доступу та збору даних із пристроїв; протягом періоду, який тривав із серпня 2022 року до липня 2023 року, основні зусилля сил та засобів кіберборотьби рф (Gamaredon, Sandworm, Turla) були переважно спрямовані на кіберрозвідку інформаційної інфраструктури державних інституцій України та телекомунікаційної інфраструктури, у тому числі проводилася дорозвідка вразливостей виявлених ще 2013 року. Окремо слід відмітити фішинг-атаки проти Сил оборони України, які несли за собою компрометацію службових комп'ютерних пристроїв, їх зараження ШПЗ CAPIBAR та KAZUAR та отримання доступу до конфіденційних даних; серпень 2023 року: кіберрозвідка шляхом зараження ШПЗ Android-планшетів українських військових з метою перехоплення даних їх комунікації з терміналами супутникового зв'язку Starlink та відслідковування пересування підрозділів ЗС України, здійснена під час контрнаступальної операції на Півдні України; листопад 2023 року: деструктивний кібервплив APT Sandworm, нанесений за допомогою нового варіанту ШПЗ CaddyWiper, на промислові системи керування українськими електростанціями, що призвів до відключення електроенергії та посилення наслідків ракетної атаки, яка відбулася того ж дня; 12 грудня 2023 року, у результаті ретельно спланованої та проведеної кібероперації кіберзлочинним угрупованням Sandworm було завдано кібервпливу спрямованого на виведення з ладу мережі стільникового зв'язку та доступу до	березень 2022 року: кібервплив IT-армії шляхом кібератаки на відмову в обслуговуванні веб-ресурсів корпорації «Ростех», що виконує близько 40% усього державного оборонного замовлення російської федерації, в тому числі, постачає її збройним силам танки Т-14 «Армата», Т-90М «Прорив», зенітні ракетно-гарматні комплекси «Панцир-С1» та ін. Кібератака призвела до тимчасового призупинення роботи серверів корпорації ; квітень 2022 року: розвідувальна кібероперація Головного управління розвідки МО України (далі – ГУР МО України) проти «Газпрому», у результаті якої вдалося отримати 1,5 терабайти службових даних російського газового монополіста. Ці дані включали адміністративні файли управління компанії, мапи газових трубопроводів, інформацію щодо замовлення на капітальний ремонт пристроїв релейного захисту та автоматики, а також масивний 3600-сторінковий файл з усіма вимогами для будівництва нового об'єкта трубопроводу. Окрім цього, фахівець з кібербезпеки Джеффрі Карр, заявив, що він особисто співпрацює з ГУР МО України та має перевірену інформацію щодо деструктивного кібервпливу на системи SCADA «Газпрому», який шляхом зміни тиску призвів до кінетичного ефекту – загоряння на ділянці газопроводу «Уренгой-Центр-2». 17 червня 2022 року: DDoS-атака IT-армії на сервери Петербурзького міжнародного економічного форуму, яка змусила відкласти на 1 годину виступ президента рф в. путіна; у період з 27 червня по 10 липня 2022 року українська IT-армія здійснила кібервплив на веб-ресурси більше ніж 800 об'єктів інформаційної та критичної інфраструктури рф. Було виведено з ладу сайт Роскосмосу у відповідь на публікацію ним супутникових знімків центрів НАТО, завдано DDoS-атаки на підприємства приватного сектору, а також знищено дані 500 тисяч користувачів «Роселторгу» – найбільшого тендерного майданчику рф, за рахунок чого досягнуто економічного ефекту; протягом усього періоду кібервійни, все більше проукраїнсько налаштованих приватних осіб надають свої обчислювальні потужності у використання українській IT-армії, яка постійно проводить кібервплив у вигляді DDoS-атак, по усьому спектру об'єктів інформаційної та кіберінфраструктури противника. Окремо слід відмітити успішні кібероперації ГУР МО України кінця 2023 – початку 2024 років:

Закінчення табл. 3

1	2
мережі Інтернет українського телекомунікаційного оператора «Київстар». Щонайменше чотири дні тривали роботи з відновлення голосового зв'язку та близько тижня – GSM-інтернету [60]. Слід зауважити, що в Україні користувачами зазначеного оператора є більше 24 млн осіб, з яких певний відсоток представників силового сектору. «Київстар» не є елементом військового чи урядового зв'язку України, проте нерідко на полі бою, коли система зв'язку не розгорнута або втрачена, стільниковий зв'язок залишається чи не єдиним варіантом виходу із ситуації. Згідно з розслідуванням Служби безпеки України, яке наразі ще не завершене, кіберрозвідка вразливостей інфраструктури оператора зв'язку почалася з березня 2023-го, а безпосередній несанкціонований доступ до його серверів та систем керування було отримано не пізніше травня того ж року. За результатами розслідування ключем до успіху кібероперації стало не ШПЗ противника, а компрометація персональних акаунтів співробітників. Не зважаючи на заяву «Київстару», що витоку персональних даних користувачів не відбулося, відкидати таку можливість, зважаючи на тривалість доступу Sandworm до його ресурсів, недоцільно; 02 січня 2024 року: завдяки попередній компрометації двох IP-камер у Києві, рф мала доступ до відслідковування в режимі реального часу результатів ракетної атаки.	листопад 2023 року: завдяки кіберрозвідувальній операції ГУР МО України, вдалося здобути значний обсяг закритих службових документів структурного підрозділу міністерства транспорту рф – Федерального агентства повітряного транспорту рф «Росавіація»); грудень 2023 року: у результаті двох паралельних кібероперацій ГУР МО України здійснено проникнення у центральний ключовий сервер Федеральної податкової служби російської федерації та у 2300 регіональних серверів, знищено конфігураційні файли функціонування податкової системи рф та вся база даних із резервними копіями. А також було отримано доступ до інтернет-трафіку податкових даних у масштабах усієї рф; січень 2024 року: кібервплив ГУР МО України на Міністерство оборони російської федерації, що призвів до виходу з ладу сервера спецзв'язку та отримання доступу до службових документів функціонування системи спеціального зв'язку в оборонному відомстві противника; березень 2024 року: кібероперація ГУР МО України, спрямована на кіберрозвідку електронної системи документообігу Міністерства оборони російської федерації «Бюрократ» дала змогу, на основі одержавної інформації, встановити повну будову системи російського міноборони та його ланок.

Інтенсивність та інноваційність російсько-українського кіберпротиборства дали підставу виділити воєнні дії в кіберпросторі, починаючи з 2022 року, в окремий етап їх періодизації, під час якого кібердомен дійсно постав як сегмент кіберпростору, який використовується у воєнних цілях, та в якому ведуться військові операції, а спектр об'єктів кіберборотьби охоплює усі сфери функціонування держави, її збройних сил та суспільства.

Отже, під час першого періоду воєнних дій у кіберпросторі (до 2010 р.) кіберборотьба фокусувалася, переважно, на об'єктах інформаційної інфраструктури. Пізніше, під час другого періоду (2010 – 2014 рр.) увага акцентувалася на ураження об'єктів критичної інфраструктури, ШПЗ почало проєктуватися та розроблятися не тільки для проведення кіберрозвідки, а й з метою нанесення деструктивного кібервпливу. Третій період, ознаменований максимальним розширенням спектру об'єктів кіберборотьби, логічно поділяється на 2 етапи: під час першого (2014 – 2022 рр.) з'явився феномен кібероперацій, кібервійська (сили) провідних держав світу досягли спроможностей з їх ведення; другому етапу (2022 р. – донині) притаманна перша повноцінна кібервійна, під час якої активно ведеться російсько-українське кіберпротиборство. Під час третього періоду воєнних дій у кіберпросторі кібердомен постав як сегмент кіберпростору, що використовується державами як середовище ведення кіберборотьби.

Також, на основі статистичних даних [30] зі звітів ДЦКЗ ДССЗЗІ України, одним з етапів дослідження стало екстраполяційне прогнозування (із поліноміальною апроксимуючою функцією) загроз кібербезпеці України за показником кількості кіберінцидентів, які потенційно можуть виникнути за поточних умов обстановки в кіберпросторі. Результати авторського прогнозування (рис. 2) свідчать про тенденцію до зростання кількості загроз кібербезпеці України на інтервалі часу, щонайменше, до кінця II кварталу 2024 року.

Рисунок 2 – Результати прогнозування загроз кібербезпеці України

Вище викладені результати аналізу та узагальнення досвіду ведення кіберборотьби у воєнних конфліктах сучасності створили підґрунтя для його систематизації у вигляді періодизації воєнних дій у кіберпросторі, яка схематично відображена автором на рис. 3.

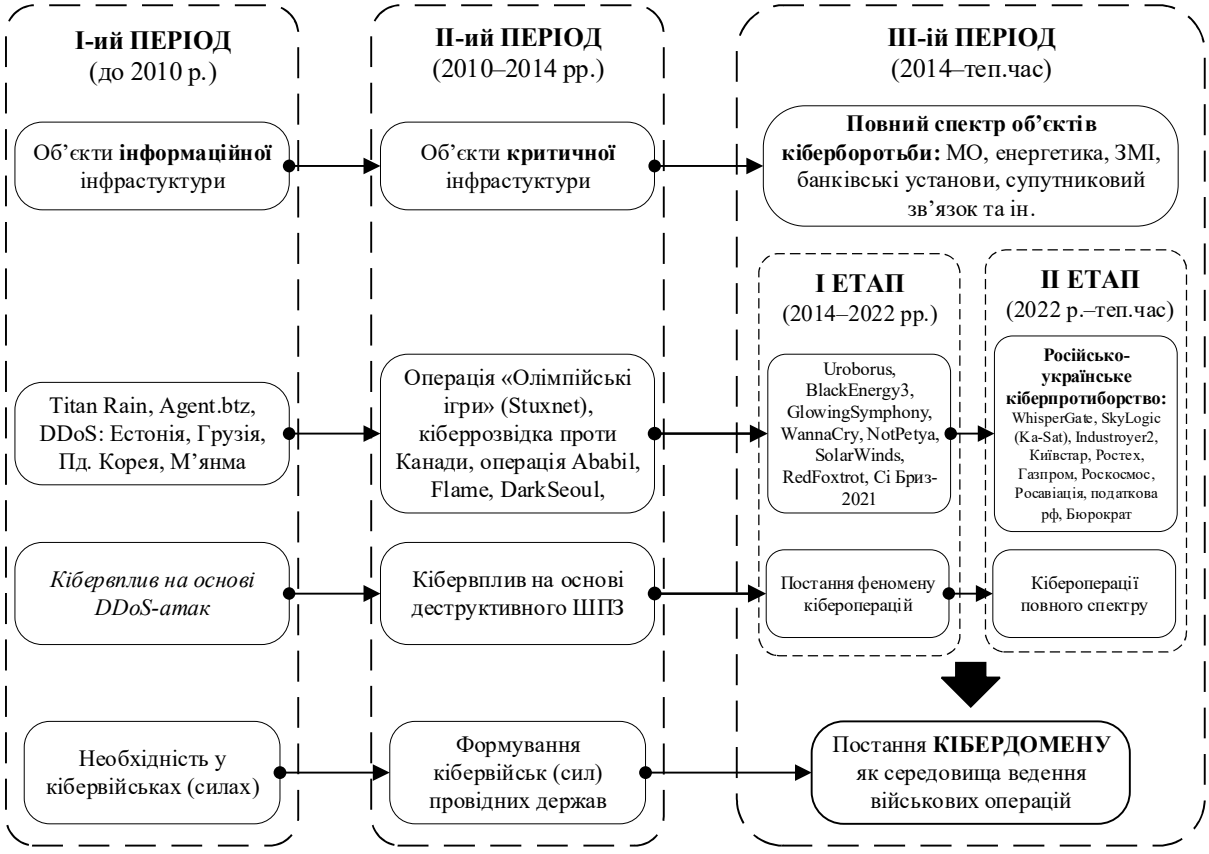

Рисунок 3 – Періодизація воєнних дій у кіберпросторі

Процес проведення дослідження та результати узагальнення передового досвіду ведення відкрили невідповідності теорії практиці, а саме:

1. Між повсюдним веденням кіберборотьби у воєнних конфліктах сучасності, постійним удосконаленням її форм та способів та відсутністю обґрунтованої системи показників та критеріїв оцінювання ефективності кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави.

2. Між потребою в уніфікації законодавчої і доктринальної бази, розробленні відповідних військових стандартів та неоднозначністю термінологічного апарату у сфері кіберборотьби.

З огляду на вище вказане, рекомендуємо:

визначити єдину дефініцію для термінів «кіберборотьба», «кібервплив», «кіберзахист», «кіберрозвідка», «кіберпростір», яка буде використовуватися як у державній сфері, так і у військовій. Також, необхідним є запровадження терміну «кібердомен» у доктринальній базі ЗС України щодо планування кібероперацій, визначення якого повинно чітко відділити сегмент кіберпростору, який використовується у воєнних цілях;

розробити та обґрунтувати систему показників та критеріїв оцінювання ефективності ведення кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави, яка в подальшому може бути використаною під час проведення досліджень направлених на отримання раціонального складу сил та засобів кіберборотьби, їх оптимального розподілу за завданнями (кіберзахист, кіберрозвідка, кібервплив) для проведення кібероперацій.

Висновки й перспективи подальших досліджень

Сьогодні кіберборотьба є невід'ємною частиною воєнних конфліктів, а кібердомен постав як сегмент кіберпростору, який використовується у воєнних цілях. Під час проведення дослідження було з'ясовано, що еволюція (розвиток) форм та способів ведення кіберборотьби відбувалася у декілька, зумовлених геополітичною ситуацією у світі та рівнем розвитку інформаційно-комунікаційних технологій, періодів. Тому, запропонована періодизація воєнних дій у кіберпросторі виокремлена у три періоди, при чому третій додатково поділяється на два етапи.

Під час першого періоду (до 2010 р.) основним об'єктом кіберборотьби були об'єкти інформаційної інфраструктури противника, відповідно, через їх низьку кіберзахищеність переважаючою формою кібервпливу були DDoS-атаки, тоді ж постали основні гравці геополітичної арени кіберборотьби, для яких стала очевидною необхідність формування власних кібервійськ (сил).

Другому періоду воєнних дій у кіберпросторі (2010 – 2014 рр.) притаманне перенесення основних зусиль кіберборотьби на об'єкти критичної інфраструктури, розробка новітніх видів ШПЗ та їх застосування не тільки з метою кіберрозвідки, а й в цілях нанесення кібервпливу, а також формування штатних підрозділів призначених для ведення кіберборотьби у структурі оборонних відомств провідних держав світу.

Третій період ознаменований максимальним розширенням спектру об'єктів кіберборотьби, включно з об'єктами оборонних відомств, ЗМІ, банковими установами, об'єктами енергетики, системами військового зв'язку, організаціями нафто-газового сектору та ін. Перший етап цього періоду (2014–2022 рр.) пов'язаний з набуттям кібервійськами (силами) провідних держав світу спроможностей з планування та ведення кібероперацій. Поточний, станом на зараз, другий етап третього періоду, що триває з початку 2022 року охоплює воєнні дії в кіберпросторі на етапах підготовки та ведення російсько-української кібервійни, що спровокувала постання кібердомену та задає тенденції ведення кіберборотьби для інших держав.

Не зважаючи на те, що у кіберпросторі кожного дня стається (виникає) більше тисячі кіберінцидентів, під час проведення дослідження з усієї їх множини було відібрано для аналізу і узагальнення лише ті, що за ознаками можна вважати веденням державами кіберборотьби.

Основною науковою новизною вважаємо те, що під час дослідження було вперше проаналізовано та узагальнено досвід ведення кіберборотьби у воєнних конфліктах сучасності на всю хронологічну глибину (від виникнення феномену і до сьогодення), що дало змогу розкрити існуючі тенденції та визначити закономірності її подальшого розвитку.

Практичною цінністю результатів дослідження є розроблені на основі розкритих у статті тенденцій та визначених закономірностей рекомендації щодо необхідності розвитку термінологічного апарату у сфері кіберборотьби, а також обґрунтування системи показників та критеріїв оцінювання ефективності ведення кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави.

Вважаємо, що без внесення до законодавчої та доктринальної бази змін зазначеного характеру вкрай можливими є дублювання наукових досліджень за цим та спорідненими напрямами, а також перешкоди на шляху до уніфікації термінів та понять з нормативними документами держав-членів НАТО. Врегулювання питанням щодо термінологічного апарату є ключем до можливості адекватного оцінювання ефективності ведення кіберборотьби та кіберстійкості об'єктів критичної інформаційної інфраструктури держави.

Реалізація розроблених рекомендацій за сукупністю і є напрямом подальших досліджень.

Список бібліографічних посилань

1. Грищук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т 17. № 1. С. 80–86. **2. Грищук Р. В.** Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. С. 16–17. **3. Магда Є. В.** Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України*. 2014. № 5. С.138–142. **4. Статистичний звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022 рік.** 2022. URL: https://scpc.gov.ua/uk/articles/233 (дата звернення: 01.04.2024). **5. Грищук Р. В.** Дії в кіберпросторі як асиметрична відповідь на «гібридну» агресію росії. *Уроки збройної агресії росії проти України – воєнно-стратегічні аспекти* : зб. матеріалів міжн. наук-практ. конф., м. Київ, 29 квітня 2021 р. Київ : Національний університет оборони України імені Івана Черняховського, 2021. С. 204–209. **6. Грищук Р. В., Даник Ю. Г.** Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с. **7. Kassab H. S.** The Role of Cyber-attacks in 21st Century War. *Journal of Studies and Applied Research on Third Sector*. 2019. *Special issue of REPATS*. № 2. P. 90–110. DOI: 10.31501/repats.v2i2.10404. **8. Богданович В. Ю., Грищук Р. В., Левченко О. В.** Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України*. *Сер.: Військові та технічні науки*. 2017. № 4(74). С. 21–37. **9. Park J., Kim D., Shin D.** Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness). *Journal of the Korea Institute of Information Security & Cryptology*. 2019. Vol. 29. № 2. P. 465–472. DOI: 10.13089/JKIISC.2019.29.2.465. **10. Crowther G. A.** The Cyber Domain. *The Cyber Defense Review*. 2017. Vol. 2. No 3 (FALL 2017). P. 63–78. **11. Herzog S.** Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security 4*. 2011. Vol. 2. P. 49–60. DOI: 10.5038/1944-0472.4.2.3. **12. Baezner M., Robin P.** Hotspot Analysis: Stuxnet. Zürich: Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, 2017. 15 p. URL: https://www.researchgate.net/publication/323199431_Stuxnet (Accessed: 25 February 2024). **13. Bronk C., Collins G., Wallach D.** The Ukrainian Information and Cyber War. *The Cyber Defense Review*. 2023. Vol. 8. № 3. P. 33–50. **14. Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware.** 2020. URL: https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF (Accessed: 27 February 2024). **15. Hollis D.** Cyberwar Case Study: Georgia 2008. Small Wars Journal, 2011. 10 p. URL: https://smallwarsjournal.com/blog/ journal/docs-temp/639-hollis.pdf (Accessed: 01 March 2024). **16. Martin D.** Tracing the Lineage of DarkSeoul. SANS Institute, 2021. 20 p. URL: https://sansorg.egnyte.com/dl/nurZpNn8ee (Accessed: 03 March 2024). **17. Uroburos Highly complex espionage software with Russian roots.** 2014. https://web.archive.org/web/20201007053804/https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf (Accessed: 04 March 2024). **18. Kostyuk N., Zhukov Y.** Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*. 2019. Vol. 63. № 2. P. 317–347. DOI: 10.1177/0022002717737138. **19. How the U.S. Hacked ISIS.** 2019. URL: https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis (Accessed: 05 March 2024). **20. Statement from the Press Secretary.** 2018. URL: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25 (Accessed: 05 March 2024). **21. Destructive malware targeting Ukrainian organizations.** 2022. URL: https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (Accessed: 07 March 2024). **22. KA-SAT Network cyber attack overview.** 2022. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview (Accessed: 08 March 2024). **23. Ministry of Digiral Transformation: IT army blocks Russian sites in a few minutes - the main victories of Ukraine on the cyber front.** 2022. URL: https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti (Accessed: 09 March 2024). **24. Computer Hacks in the Russia-Ukraine War. Kenneth Geers. Very Good Security.** 2022. URL: https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf (Accessed: 09 March 2024). **25. An overview of Russia's cyberattack activity in Ukraine. Special Report: Ukraine.** 2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (Accessed: 09 March 2024). **26. Industroyer2: Industroyer reloaded. ESET Research.** 2022. URL: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Accessed: 09 March 2024). **27. CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network.** 2023. URL: https://cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar (Accessed: 10 March 2024). **28. Cyber Intelligence Report.** 2023. URL: https://cscis.org/2023/02/03/cyberwarfare-russia-vs-ukraine-russia-deploys-wipers/ (Accessed: 12 March 2024). **29. Софт, шифри, секретні документи – кіберфахівці ГУР зламали мінооборони росії.** 2024. URL: https://gur.gov.ua/content/soft-shyfry-sekretni-dokumenty-kiberfakhivtsi-hur-zlamaly-minoborony-rosii.html (Accessed: 15 March 2024). **30. Статистичні звіти про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022 та 2023 роки (квартальні).** 2022; 2023. URL: https://scpc.gov.ua/uk/articles/161; https://scpc.gov.ua/uk/articles/163; https://scpc.gov.ua/uk/articles/306; https://scpc.gov.ua/uk/articles/318; https://scpc.gov.ua/uk/articles/327; https://scpc.gov.ua/uk/articles/341 (дата звернення: 15.03.2024).

CYBER WARFARE IN MODERN MILITARY CONFLICTS: EXPERIENCE, TRENDS AND REGULARITIES OF DEVELOPMENT

Horhulenko Vladyslav

Central Research Institute of the Armed Forces of Ukraine

Formulation of the problem in general. *Modern military conflicts implement the principles of hybrid and network-centric warfare, and cyber warfare inherent in them is becoming an increasingly widespread phenomenon due to the construction of a high-tech society, its informatization and digitization. As a result, the range of objects of cyber influence is constantly expanding, and the forms and methods of its application are being improved and diversified. At the same time, although conducted scientific research showed the presence of theoretically proven partial effectiveness indicators of some components of cyber warfare, they aren't characterized by systematicity, and therefore a comprehensive effectiveness assessment of the military operations in cyberspace is currently not possible. The terminological apparatus in the field of cyber warfare is quite ambiguous, which leads to the substitution of concepts both in scientific research and in military standards and doctrines. Thus, there is a problem of inconsistency between theory and practice, which can be solved by studying (analysis, generalization, systematization) the best experience of cyber warfaring in the modern military conflicts. The main aim of the article is to generalize the best experience of cyber warfare in modern military conflicts, reveal existing trends and determine the patterns of its further evolution in order to produce recommendations for the terminological apparatus in the field of cyber warfare development, as well as to substantiate the system of indicators and effectiveness evaluation criteria of cyber warfare and the state critical information infrastructure objects cyber resistance level.*

Research methods. *During the research, methods of analysis, abstraction and generalization have been applied to fulfill a goal of investigation. Using the method of analysis, the experience and best practice of cyber warfaring were studied as a set of interrelated and agreed upon goals, tasks, place in cyberspace, time, as well as forms and methods of implementation, the facts of states conducting cyber protection, cyber intelligence, and cyber influence measures, and thereafter the specifics of their goals, features of forms and methods of implementation, which were often hidden,, degree of goal achievement, scale of consequences, as well as other cause-and-effect relationships have been determined. By the method of abstraction, non-essential properties inherent in the experience of cyber warfaring in modern military conflicts were eliminated in order to focus on the main ones - those that make it possible to trace and formalize existing trends and determine the patterns of further development. Accordingly, the use of the generalization method made it possible to obtain the following trends and patterns.*

Analysis of the latest research findings. *The sources are full of relevant scientific works on related topics. However, the attention in such works, to a greater extent, is given to the study of cyber attacks, series of cyber attacks and cyber incidents that occurred during a certain short period of time, or to the study of individual samples of malicious software, or is directed to the study of cyber operations carried out by a certain state. As a result, a significant amount of meaningful theoretical and applied research has been conducted in the field of cyber security in this direction, but the results of most of them exist in a kind of "vacuum" from each other. In contrast to previous studies, this article is characterized by a comprehensive and chronological approach to research the experience and best practice of cyber warfaring: from the emergence of its phenomenon to the current state.*

Presenting the main results. *Based on the analysis and generalization, the experience of conducting cyber warfare in modern military conflicts was systematized, its existing trends were revealed and regularities of further development were determined. As a result, the periodization of military actions in cyberspace have been suggested, which consists of three periods, the peculiarities of each of which are determined by the geopolitical situation in the world and the current level of information and communication technologies development of that time.*

An element of scientific novelty. *In the article, for the first time, the experience and best practice of cyber warfaring in modern military conflicts were systematized in all its chronological depth and the periodization of military actions in cyberspace has been developed.*

Theoretical and practical significance of the article. *The theoretical significance of the research results is the disclosure of the existing trends of cyber warfare in modern military conflicts and the determination of its further development patterns. In the conditions of sources oversaturation with unstructured information on the cyber warfaring experience, the results of this study highlight only the main points, reflect the current state of the given topic and form an empirical basis that can be supplemented and updated over time. An applied significance. The applied significance of this study results lies in the developed on the basis of revealed trends and determined regularities of cyber warfare in modern military conflicts recommendations regarding the need of terminological apparatus in the field of cyber warfare development, as well as the system of indicators and effectiveness evaluation criteria of cyber warfare and the state critical information infrastructure objects cyber resistance level substantiation.*

Conclusion and the perspectives of future research. *Taking into account the contradictions and discrepancies in the terms and concepts presented in the scientific works of both domestic and foreign scientists discovered during the scientific search (analysis of sources), we consider it expedient to conduct further research in the direction of the terminological apparatus in the field of cyber warfare development.*

Keywords: *cyber warfare, military operations in cyberspace, cyber domain, analysis and generalization of experience, cyber operation, cyber opposition, cyber warfare troops, cybersecurity, cyber defence, cyberinfrastructure, cyber resilience.*

References

1. Hryschuk, R. V., Kankin, I. O., Okhrimchuk, V. V, (2015). Technological aspects of information warfare at the modern stage. *Zakhyst informatsii*. 17 (1), 80–86. **2. Hryschuk, R. V.,** (2016). Information and cyber security: role and place in hybrid warfare. In: *Kiberbezpeka v Ukraini: pravovi ta orhanizatsijni pytannia* : *materialy Vseukr. nauk.-prakt. konf. Odesa*, *Ukraina*, 21 zhovtnia 2016. Odesa: ODUVS. **3. Mahda, Ye. V.,** (2014). Challenges of hybrid warfare: the informational dimension. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy*. 5, 138–142. **4. Statistical report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks for 2022** [online], (2022). *DTsKZ DSSZZI Ukrainy*. Available at: https://scpc.gov.ua/uk/articles/233 [Accessed: 01 April 2024]. **5. Hryschuk, R. V.,** (2021). Actions in cyberspace as an asymmetric response to russia's «hybrid» aggression. In: *Uroky zbrojnoi ahresii rosii proty Ukrainy – voienno-stratehichni aspekty: zb. materialiv mizhv. nauk-prakt. konf. Kyiv*, *Ukraina*, 29 kvitnia 2021. Kyiv: Natsional'nyj universytet oborony Ukrainy imeni Ivana Cherniakhovs'koho. **6. Hryschuk, R. V., Danyk, Yu. H.,** (2016). *Fundamentals of cyber security: a monograph*. Zhytomyr: ZhNAEU. **7. Kassab, H. S.** (2019). The Role of Cyber-attacks in 21st Century War. *Journal of Studies and Applied Research on Third Sector*. 2, 90–110. DOI: 10.31501/repats.v2i2.10404. **8. Bohdanovych, V. Yu., Hryschuk, R. V., Levchenko, O. V,** (2017). A system of criteria and indicators for evaluating the effectiveness of the information security system. *Zbirnyk naukovykh prats' Natsional'noi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Ser.: Vijs'kovi ta tekhnichni nauky*. 4 (74), 21–37. **9. Park, J., Kim, D., Shin, D.** (2019). Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness). *Journal of the Korea Institute of Information Security & Cryptology*. 29 (2), 465–472. DOI: 10.13089/JKIISC.2019.29.2.465. **10. Crowther, G. A.,** (2017). The Cyber Domain. *The Cyber Defense Review*. 2 (3), 63–78. **11. Herzog, S.,** (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security 4*. 2, 49–60. DOI: 10.5038/1944-0472.4.2.3. **12. Baezner M., Robin P.**, (2017). *Hotspot Analysis: Stuxnet*. Zürich : Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, [online]. Available at: https://www.researchgate.net/publication/323199431_Stuxnet [Accessed : 25 February 2024]. **13. Bronk, C., Collins, G., Wallach, D.,** (2023). The Ukrainian Information and Cyber War. *The Cyber Defense Review*. 8 (3), 33–50. **14. Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware** [online], (2020)**.** *U.S. Department of Defense*. Available at: https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF [Accessed: 27 February 2024]. **15. Cyberwar Case Study: Georgia 2008** [online], (2008)**.** *Small Wars Journal*. Available at: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf [Accessed: 01 March 2024]. **16. Martin, D.**, (2021). *Tracing the Lineage of DarkSeoul*. SANS Institute, [online]. Available at: https://sansorg.egnyte.com/dl/nurZpNn8ee [Accessed : 03 March 2024]. **17. Uroburos Highly complex espionage software with Russian roots** [online], (2014). *GDataSoftware*. Available at: https://web.archive.org/web/20201007053804/https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf [Accessed: 04 March 2024]. **18. Kostyuk, N., Zhukov, Y.** (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*. 63 (2), 317–347. DOI: 10.1177/0022002717737138. **19. How the U.S. Hacked ISIS** [online], (2019). *NPR*. Available at: https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis [Accessed: 05 March 2024]. **20. Statement from the Press Secretary** [online], (2018). *Trump White House*. Available at: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25 [Accessed: 05 March 2024]. **21. Destructive malware targeting Ukrainian organizations** [online], (2022). *Microsoft*. Available at: https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ [Accessed: 07 March 2024]. **22. KA - SAT Network cyber attack overview** [online], (2022). *Viasat*. Available at: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview [Accessed: 08 March 2024]. **23. Ministry of Digiral Transformation: IT army blocks Russian sites in a few minutes - the main victories of Ukraine on the cyber front** [online], (2022). *Government Portal*. Available at: https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti [Accessed: 09 March 2024]. **24. Computer Hacks in the Russia-Ukraine War. Kenneth Geers. Very Good Security** [online], (2022). *DEF CON Media Server*. Available at: https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf [Accessed: 09 March 2024]. **25. An overview of Russia's cyberattack activity in Ukraine. Special Report: Ukraine** [online], (2022)**.** *Microsoft*. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/ binary/RE4Vwwd [Accessed: 09 March 2024]. **26. Industroyer2: Industroyer reloaded. ESET Research** [online], (2022). *We Live Security*. Available at: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ [Accessed: 09 March 2024]. **27. CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network** [online], (2023). *DSSZZI Ukrainy*. Available at: https://cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar [Accessed: 10 March 2024]. **28. Cyber Intelligence Report** [online], (2023)**.** *CSCIS*. Available at: https://cscis.org/2023/02/03/cyberwarfare-russia-vs-ukraine-russia-deploys-wipers/ [Accessed: 12 March 2024]. **29. Software, ciphers, secret documents – cyber specialists of HUR MOU hacked the Russian Ministry of Defense** [online], (2024). *Holovne upravlinnia rozvidky Ministrestva oborony Ukrainy*. Available at: https://gur.gov.ua/content/soft-shyfry-sekretni-dokumenty-kiberfakhivtsi-hur-zlamaly-minoborony-rosii.html [Accessed: 15 March 2024]. **30. Statistical report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks for the 2022 and 2023 (quarterly) first quarter of 2022** [online], (2022; 2023). *DTsKZ DSSZZI Ukrainy*. Available at: https://scpc.gov.ua/uk/articles/161; https://scpc.gov.ua/uk/articles/163; https://scpc.gov.ua/uk/articles/306; https://scpc.gov.ua/uk/articles/318; https://scpc.gov.ua/uk/articles/327; https://scpc.gov.ua/uk/articles/341 [Accessed: 15 March 2024].