МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА
РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____ Ніна РЖЕВСЬКА
«____»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ
КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «КІБЕРТЕРОРИЗМ ЯК ІНСТРУМЕНТ ПРОТИСТОЯННЯ ДЕРЖАВ НА МІЖНАРОДНІЙ АРЕНІ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 групи, Силаєва Ганна Олександрівна
Керівник: к.політ.н., доцент кафедри міжнародних відносин, інформації та регіональних студій Алієв Максим Михайлович

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ 2022

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРТЕРОРИЗМУ 6

1.1 Поняття та сутність кібертероризму 6

1.2 Класифікація та види кіберзагроз 12

1.3 Сучасні підходи до розуміння поняття «кібертероризм» 18

РОЗДІЛ 2. ПРАКТИКА ФУНКЦІОНУВАННЯ КІБЕРТЕРОРИЗМУ НА МІЖНАРОДНІЙ АРЕНІ 21

2.1. Особливості застосування кібератак у сучасному світі 21

2.2. Інформаційні війни як складова кібертероризму 31

2.3. Прояви кібертероризму як реальної загрози 37

РОЗДІЛ 3. КІБЕРТЕРОРИЗМ ЯК МЕТОД ПРОТИСТОЯННЯ ДЕРЖАВ НА МІЖНАРОДНІ АРЕНІ 44

3.1. Прояви кібертероризму та його використання як інструменту протистояння держав на міжнародній арені 44

3.2. Вплив кібертероризму на міжнародні відносини на прикладі США. 53

ВИСНОВКИ 66

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ 70

ДОДАТКИ 78

ВСТУП

Актуальність дослідження. Стрімкий розвиток інформаційних технологій сприяло виникненню нового виду злочинності - комп'ютерної, а перехід на методи електронного управління технологічними процесами появи нового виду тероризму - кібертероризм. На жаль, разом із цією тенденцією з’явилися нові загрози, у тому числі кібертерористичного характеру, які вимагають негайних дій для обмеження їх впливу на інформаційну безпеку. Це призвело до радикальних змін майже в кожному середовищі, включаючи середовище безпеки. Сучасне суспільство справді є інформаційним суспільством, в якому майже повністю домінували телекомунікаційні системи, що використовуються для надсилання, отримання та обробки інформації. Зараз інформація є невід'ємною частиною соціального та економічного життя і присутня в усіх сферах людського функціонування.

Тим часом кіберсфера з’явилася не так давно, але вона досягла величезних темпів зростання, що змусило окремі держави визнати необхідність реформувати свої оборонні системи. Кіберсфера перемістила фокус безпеки з фізичної війни на реагування та розробку ресурсів для протидії кібератакам, а також превентивних дій у кіберпросторі. Журналісти, політики та експерти в різних галузях популяризували сценарій, за яким досконалі кібертерористи електронним шляхом проникають в комп’ютери, які контролюють дамби або системи управління повітряним рухом, завдаючи хаосу та загрожуючи не лише мільйонам життів, а й самій національній безпеці. На думку фахівців, тероризм із використанням останніх досягнень у сфері високих технологій не менш небезпечний, ніж ядерний чи бактеріологічни й тероризм.

Важливість і актуальність протистояння в кіберпросторі підтверджується тим, що дослідження в цій галузі активно проводяться не

лише окремими вченими, а й дослідницькими групами низки аналітичних центрів провідних світових держав, насамперед США. Видаються досить цікавими висновки RAND , які лягли в основу положень нової геополітичної стратегії США по боротьбі із кібертероризмом :

– глобальна інформатизація всіх сфер життя суспільства не підвищує, а знижує рівень його безпеки;

– прискорення науково-технічного прогресу збільшує ймовірність застосування терористами як засобів ураження суто мирних технологій, причому можливість «подвійного» їх використання часто не тільки не передбачається, а й не усвідомлюється творцями технології;

– тероризм все більше стає інформаційною технологією особливого типу, оскільки, по-перше, терористи все ширше використовують можливості сучасних інформаційно-телекомунікаційних систем для зв'язку та збору інформації, по-друге, реалією наших днів стає так званий «кібертероризм», по-третє, більшість терористичних актів зараз розраховані не тільки на завдання матеріальних збитків і загрозу життю і здоров'ю людей, але і на інформаційно-психологічний шок, вплив якого на великі маси людей створює сприятливе середовище для досягнення терористами своїх цілей;

Таким чином, в умовах нарощування у світі процесів глобалізації та формування інформаційного суспільства тероризм став виступати як самостійний фактор, здатний загрожувати державній цілісності країн та дестабілізувати міжнародну обстановку. Зростає рівень впливу сучасного тероризму як на складові внутрішньої політики окремих держав, а й у міжнародну безпеку. При цьому особливо гостро питання забезпечення інформаційної безпеки як однієї з важливих складових національної безпеки постає у контексті появи транснаціональної (транскордонної) комп'ютерної злочинності та кібертероризму. Загроза кібератак цілком реальна, і пов'язані з нею ризики оцінюються фахівцями як високі.

Мета дослідження полягає у вивченні пріоритетних напрямків державної політики протидії цьому виду тероризму, виробленню

рекомендацій щодо попередження актів кібертероризму, аналізу стратегії боротьби з цим негативним явищем з урахуванням досвіду передових країн світу.

Мета дослідження визначила необхідність вирішення наступних **завдань:**

1. Систематизувати основні наукові підходи до вивчення феномену кібертероризму.

2. Виявити причини виникнення та активізації кібертероризму на сучасному етапі, його особливості та тенденції функціонування.

3. Виявити протиріччя, що впливають процес розробки та реалізації політики протидії кібертероризму.

4. Виявити значення міжнародного досвіду протидії кібертероризму.

5. Розглянути кібербезпеку у сучасному інформаційному світі – її ключові тенденції та загрози .

Об'єктом дослідження є кібертероризм як соціально-політичний феномен і методи його протидії.

Предметом дослідження є напрями державної політики передових країн світу протидії кібертероризму, а також суперечливі переконання , що впливають на процес розробки та реалізації політики протидії кібертероризму.

Методи дослідження. При виконанні кваліфікаційної роботи використовувалися методи політологічного, історичного, порівняльного, статистичного аналізу, класифікації, систематизації, узагальнення, описи.

Практична значущість роботи полягає у формуванні висновків щодо досвіду політики кібербезпеки передових країн світу та визначення стратегій національної безпеки та оборони держав-членів через різні стратегічні культури безпеки та підходи до зв’язку кібертероризму та політки безпеки країн.

Структура робота. Робота складається з вступу, трьох розділів, висновків, списку використаних джерел, а також додатки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРТЕРОРИЗМУ

1.1 Поняття та сутність кібертероризму

Технічний прогрес розвивається настільки стрімко, що деякі його наслідки усвідомлюються суспільством занадто пізно, коли для виправлення ситуації потрібні значні зусилля. Кібертерозм – є доволі широким поняттям та характеризує новий вид тероризму у світі. Власне саме поняття «кібертероризм» утворено злиттям двох термінів: «кібер» і «тероризм».

Термін «кібер», яким ми його знаємо сьогодні, походить від «кебернетес», що було давньогрецькою фразою, що перекладається як «мистецтво керувати» [1, с. 14].

Лише після того, як математик Норберт Вінер використав слово кібернетика в 1940 роках, цей термін став відомий як дослідження систем живих істот і штучних машин [2, с. 23].

Цей термін зазнав подальшого впливу поп-культури у 1980-х роках під час руху кіберпанку, який був натхненний романом Вільяма Гібсона «Нейромант» [3, с. 27], який додатково пов’язував термін «кібер» з антиутопічними та футуристичними концепціями.

Британський вчений Флаттер стверджує, що «кібер» – префікс – це не що інше, як звичайна фраза, яка призвела до появи терміну, який був занадто погано визначений через різноманітний спектр факторів, які він намагається пояснити [4, с.172].

Таким чином можна зауважити, що кібер-префікс став синонімом, який розрізняє традиційні злочини та більш сучасні злочини, які вчиняються завдяки технологічним можливостям.

У світлі цього такий термін, як «операції комп’ютерної мережі» або «інформаційна війна», може бути непридатним для подальшого вивчення та

визначення кібертероризму, оскільки ці терміни не враховують інші види терористичної діяльності.

У свою чергу, це відкидає нерозривні зв'язки між технологіями, тероризмом та їх впливом на спільноти, а не лише на комп'ютерні мережі. Тому використання кіберпрефікса є доречним для чіткої та синонімічної категоризації між традиційним тероризмом та кібертероризмом.

Однак, щоб розкрити сутність такого поняття як «кібертероризм» – необхідно визначитися з тим, що розуміється також під тероризмом у сучасному світі. В історичному аспекті термін «тероризм» вперше з'явився в 1798 році, коли філософ Еммануїл Кант використовував його для опису песимістичного погляду на долю людства.

У той же рік цей термін можна було знайти в додатку до великого словнику Французької академії, це було викликано ексцесами революційного терору і тому термін не мав такого значення, яке ми сьогодні в нього вкладаємо [5, с. 39].

У даний час під цим терміном в більшості випадків розуміються дії певних рухів, які впливають на уряд держави з метою радикальної зміни його політичного управління.

Визначення «тероризму» – є предметом багатьох дискусій [6 – 9]. Цю боротьбу у визначенні «тероризму» можна пояснити складністю відображення ідеологічних, філософських, політичних та релігійних нормативних відмінностей під одним терміном.

Тероризм зображений як соціальний конструкт, оскільки його значення формується поглядами людини, яка класифікує, що для неї означає тероризм [10]. На думку Хьюера і Тейлора, термін тероризм є лише маркером, який використовується урядами країн для легітимізації або делегітимізації політично мотивованого насильства, що відбувається в їхній країні [11, с. 53].

Хорошим прикладом цього є парадоксальний характер між Близьким Сходом і Заходом у їх характеристиках тероризму. На Близькому Сході існує змішування між релігійною ідентичністю та політикою, що безпосередньо

впливає на соціальні та культурні концепції [12, с. 72], тоді як на Заході існує сильна різниця між релігією та політикою, що призводить до демократичного суспільства, яке забезпечує низку суспільних і культурні ідеали до співжиття [13, 14].

Вірування та ідеології Заходу та Близького Сходу розглядають одна одну як загрозу їхнім відповідним основним нормам та цінностям, що потенційно є причиною виникнення поняття тероризму [15, 16]. Загалом, ця інформація підкреслює віру в те, що різні країни можуть мати різне значення того, що кваліфікується як терористичний акт, чи ні, залежно від їх політичної та релігійної приналежності.

У вітчизняному законодавстві закріплено визначення тероризму – як суспільно небезпечної діяльності, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей (ст. 1 Закону України «Про боротьбу з тероризмом»).

Найбільш загальне розуміння суті кібертероризму полягає у використанні інформаційного насильства з метою залякування. Суб’єктом якого є – певні особи, урядові організації, тощо. Об’єктом може виступати як суспільство в цілому (з метою створення панічних настроїв у суспільстві) або певні керівники держави, державних органів (з метою їх шантажування, залякування, отримання конфеденційної певної інформації), системи збереження даних громадян.

Таким чином можна вивести таке визначення: кібертероризм (Гриник Р.О., Пилипенко В.М. Львівський державний університет безпеки життєдіяльності) – це комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютерними системами, що створює небезпеку для людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської

безпеки, залякування населення, провокації військового конфлікту, отримання даних про певних осіб.

Кібертероризм часто визначають як будь-яку навмисну політично мотивовану атаку на інформаційні системи, програми та дані, що загрожує насильством або призводить до насильства. Акти навмисного, широкомасштабного порушення роботи комп'ютерних мереж, особливо персональних комп'ютерів, під'єднаних до Інтернету, за допомогою таких інструментів, як комп'ютерні віруси, комп'ютерні хробаки, фішинг, шкідливе програмне забезпечення, апаратні методи, скрипти програмування – усе це може бути формами інтернет-тероризму.

Кібертероризм (також відомий як цифровий тероризм) визначається як руйнівні атаки визнаних терористичних організацій на комп'ютерні системи з метою викликати тривогу, паніку або фізичне порушення роботи інформаційної системи.

Варто зазначити, що по-перше, «інтерес до питань кіберпространства почався лише в дев'яностих, тому терміни все ще зароджуються». По-друге, різні державні структури фрагментували визначення, оскільки значення залежить від їхніх різних інтересів [17, с.87].

ФБР опублікувало три чіткі визначення кібертероризму: «Тероризм, який ініціює… атаки на інформацію» у 1999 році, до «використання кібер-інструментів» у 2000 році та «кримінальне діяння, вчинене з використанням комп'ютерів» у 2004 році. Інші державні установи, відповідальні за реагування на кібератаки, такі як Міністерство оборони, Федеральне агентство з надзвичайних ситуацій, Національний центр захисту інфраструктури, Агентство з боротьби з наркотиками, Національне агентство внутрішньої безпеки та Міністерство юстиції, створили свої власні визначення.

Існують дискусії щодо основного визначення сфери кібертероризму. Ці визначення можуть бути вузькими, наприклад використання Інтернету для

атаки на інші системи в Інтернеті, що призводить до насильства проти людей або власності.

Вони також можуть бути широкими, які включають будь-яку форму використання Інтернету терористами до звичайних атак на інфраструктури інформаційних технологій.

Існують відмінності в кваліфікації за мотивацією, цілями, методами та центральним місцем використання комп'ютера в діянні. Урядові установи США також використовують різні визначення, і жоден з них досі не намагався запровадити стандарт, який є обов'язковим за межами їхньої сфери впливу. Таким чином, залежно від контексту, кібертероризм може значно перетинатися з кіберзлочинністю, кібервійною або звичайним тероризмом [18, с. 115-116].

На шляху створення чіткого та послідовного визначення терміну «кібертероризм» було декілька факторів, що визначали процес його формування.

По-перше, як щойно зазначалося, велика частина обговорень кібертероризму велася в популярних ЗМІ, де журналісти, як правило, прагнуть драматизму та сенсації, а не хороших оперативних визначень нових термінів.

По-друге, під час роботи з комп'ютерами було особливо поширено придумувати нові слова, просто розміщуючи слово «кібер», «комп'ютер» або «інформація» перед іншим словом.

Таким чином, цілий арсенал слів: кіберзлочинність, інформаційна війна, мережева війна, кібертероризм, кіберпереслідування, віртуальна війна, цифровий тероризм, кібертактика, комп'ютерна війна, кібератака та кіберзлом використовуються для опису того, що деякі військові та політичні стратеги описують як «новий тероризм» нашого часу.

На щастя, були зроблені деякі зусилля, щоб ввести більшу семантичну точність. Зокрема, Дороті Деннінг, професор комп'ютерних наук, у численних статтях і у своїх свідченнях на цю тему перед комітетом з питань

збройних сил у травні 2000 року висунула чудове однозначне визначення: кібертероризм – це конвергенція кіберпростору та тероризму. Це стосується незаконних атак і погроз атак на комп'ютери, мережі та інформацію, що зберігається в них, коли вони здійснюються з метою залякування чи примусу уряду чи його людей до досягнення політичних чи соціальних цілей.

ФБР розглядає кібертерористичну атаку як щось відмінне від звичайного вірусу або атаки типу «відмова в обслуговуванні» (DoS). За даними ФБР, кібертерористична атака – це тип кіберзлочину, спеціально призначеного для заподіяння фізичної шкоди. Проте серед урядів та спеціалістів з інформаційної безпеки немає єдиної думки про те, що вважати актом кібертероризму.

Інші організації та експерти заявили, що менш небезпечні атаки можна вважати актами кібертероризму. На думку інших груп, атаки, спрямовані на підрив або просування політичних планів зловмисників, можуть кваліфікуватися як кібертероризм.

У деяких випадках різниця між кібертерористичною атакою і звичайними кіберзлочинами полягає в намірі: основна мотивація кібертерористичних атак полягає в порушенні роботи або заподіянні шкоди жертвам, навіть якщо атаки не призводять до фізичних збитків або серйозних фінансових збитків.

Важливо розрізняти «кібертероризм» і «хактивізм». Хактивізм – термін, який вчені винайшли для опису поєднання хакерства з політичною активністю. («Злам» тут розуміється як діяльність, що здійснюється в режимі таємно в Інтернеті, спрямована на виявлення, маніпулювання чи інше використання вразливостей комп'ютерних операційних систем та іншого програмного забезпечення. На відміну від хактивістів, хакери, як правило, не мають політичних планів. Хактивісти мають чотири основні види зброї. в їх розпорядженні: віртуальні блокади; атаки на електронну пошту; злому та комп'ютерних зломів; а також комп'ютерні віруси та хробаки.

Віртуальна блокада – це віртуальна версія фізичної, сидячій або блокади: політичні активісти відвідують веб-сайт і намагаються створити таку кількість трафіку на сайт, що інші користувачі не можуть отримати доступ до нього, тим самим порушуючи нормальну роботу, завойовуючи публічність через повідомлення ЗМІ за справу протестувальників.

В інших випадках диференціація пов'язана з результатом кібератаки. Багато експертів з кібербезпеки вважають, що інцидент слід розглядати як кібертероризм, якщо він призводить до фізичних збитків або загибелі людей. Це може бути як пряма, так і непряма шкода у вигляді пошкодження або порушення роботи критичної інфраструктури.

Отже, можна дійти до висновку що поняття «кібертероризм» є широким за своєю суттю та може включати в себе різного роду атаки на комп’ютерне забезпечення інших країн, що полягає як прямій, так і непрямій шкоді у вигляді пошкодження або порушення роботи критичної інфраструктури (виведення з роботи веб-сайтів державних органів, атаки на електронні державні реєстри та бази доступу до даних громадян певної країни, тощо.

1.2 Класифікація та види кіберзагроз

Зброя кібертерориста не призначена для вбивства людей чи розбиття фізичних об’єктів. Швидше, вони існують виключно для знищення або зміни комп’ютерних даних. Зброя та цілі – це електрони, які рухаються у кіберпросторі. Хоча можна атакувати ці дані без будь-яких людських інтерфейсів, людина зазвичай є найслабшою ланкою в комп’ютерній системі.

Джозеф Сінор з CIBIR Corporation, групи розслідування комп’ютерних злочинів, нещодавно обговорив «Методи дій» кібертерористів. Його визначення є корисною відправною точкою для вивчення того, як кібертерористи можуть атакувати свої цілі. Важливим елементом кібертероризму та інформаційної війни загалом є знання.

Хоча «інструменти» кібертерориста (комп'ютерні модеми, телефонні з'єднання) майже повсюдно доступні, знання про комп'ютерні системи та їх слабкі сторони стають все більш поширеними.

Особи, які мають необхідний рівень знань, щоб стати кібертерористами поділяються на три основні категорії.

Перша – це «хакер», який визначається як «особа, яка вламується в комп'ютери, щоб довести, що це можна зробити. Деякі з них руйнівні за своєю природою, інші є суто райдерами».

Друга категорія – кіберпанк, «більш жорсткий комп'ютерний хакер, той, хто користується технологіями і використовує цю технологію, щоб заробляти гроші або виступати як анархіст.».

Третя категорія – це шифропанк, «особа, яка зацікавлена у використанні шифрування для захисту конфіденційності та використання методи розшифрування для доступу до інших захищених файлів.»

Американський дослідник Пол Страссман зазначає, що завдяки навичкам, які проживають у цих групах, існує кілька ризиків для комп'ютерних систем:

Програми-шкідники:

− Атаки троянських коней − імплантація шкідливого коду, розсилка листівних бомб;

− Логічні бомби − бомби часу або події;

− Зловмисні хробаки − забороняють доступ до розподілених ресурсів;

− Вірусні атаки − додавання коду до програм і його тиражування.

Обходи:

− Backdoor атаки − використання наявних недоліків у програмному забезпеченні для експлуатації;

− Атаки авторизації − злом паролів, злом контрольних файлів.

Активне зловживання:

− Створення, зміна, відмова в послуги, введення неправдивих або оманливих даних;

− Поетапні атаки − з використанням тактики салямі;

− Відмови в обслуговуванні − запуск атак насичення.

Пасивне зловживання:

− Перегляд – читання та копіювання з очевидною авторизацією;

− Втручання, агрегація − пошуки в базі даних, аналіз трафіку.

Непряме зловживання − підготовка до подальших зловживань, попереднє шифрування в автономному режимі, факторинг чисел для отримання криптоключів, автоматичний набір номерів і сканування голосової пошти.

Намір кібертерористичних груп полягає в тому, щоб спричинити масовий хаос, порушити критичну інфраструктуру, підтримати політичну активність або хактивізм, або завдати фізичної шкоди.

Таким чином, основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюються угрупованнями або окремими особами. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати кошти мережевого інформаційного обміну, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності

Суб'єкти кібертероризму використовують різні методи. До них відносяться наступні типи атак:

Розширені атаки постійної загрози (APT) використовують складні та концентровані методи проникнення для отримання доступу до мережі. Потрапляючи в мережу, зловмисники деякий час залишаються непоміченими з наміром вкрасти дані. Організації з високоцінною інформацією, такими як національна оборона, виробництво та фінансова промисловість, є типовою мішенню для атак APT.

Комп’ютерні віруси, хробаки та шкідливі програми націлені на системи контролю ІТ. Вони використовуються для нападу на комунальні

підприємства, транспортні системи, електромережі, критично важливу інфраструктуру та військові системи.

Атаки DoS намагаються перешкодити легальним користувачам отримати доступ до цільових комп'ютерних систем, пристроїв чи іншої комп'ютерної мережі. Ці зловмисники часто переслідують критичну інфраструктуру та уряди.

Злом або отримання несанкціонованого доступу намагається викрасти критично важливі дані з установ, урядів і компаній.

Програми-вимагачі, різновид зловмисного програмного забезпечення, утримують дані або інформаційні системи в заручниках, поки жертва не заплатить викуп. Деякі атаки програм-вимагачів також викрадають дані.

Фішингові атаки намагаються зібрати інформацію через електронну пошту цілі, використовуючи цю інформацію для доступу до систем або викрасти особистість жертви.

Шкідливе програмне забезпечення – це абревіатура від «зловмисного програмного забезпечення», яке включає віруси, хробаки, трояни, шпигунські програми та програми-вимагачі, і є найпоширенішим типом кібератак. Зловмисне програмне забезпечення проникає в систему, як правило, через посилання на ненадійний веб-сайт або електронну пошту або завантажуючи небажане програмне забезпечення. Він розгортається в цільовій системі, збирає конфіденційні дані, маніпулює та блокує доступ до мережевих компонентів, а також може знищити дані або повністю вимкнути систему.

Ось кілька поширених джерел кіберзагроз проти організацій:

Національні держави – ворожі країни можуть здійснювати кібератаки на місцеві компанії та установи з метою перешкодити комунікації, викликати безлад і завдати шкоди.

Терористичні організації – терористи здійснюють кібератаки, спрямовані на знищення або зловживання критичною інфраструктурою,

загрозу національній безпеці, руйнування економіки та заподіяння тілесних ушкоджень громадянам.

Злочинні групи – організовані групи хакерів, які прагнуть проникнути в комп'ютерні системи для отримання економічної вигоди. Ці групи використовують фішинг, спам, шпигунське та шкідливе програмне забезпечення для вимагання, крадіжки приватної інформації та онлайн-шахрайства.

Хакери – окремі хакери націлені на організації, використовуючи різноманітні методи атаки. Зазвичай їх мотивують особиста вигода, помста, фінансова вигода або політична діяльність. Хакери часто створюють нові загрози, щоб розвинути свої злочинні здібності та покращити особисте становище в хакерській спільноті.

Шкідливі інсайдери–працівники, які мають законний доступ до активів компанії та зловживає своїми привілеями, щоб викрасти інформацію або пошкодити комп'ютерні системи для економічної чи особистої вигоди. Інсайдерами можуть бути співробітники, підрядники, постачальники або партнери цільової організації. Вони також можуть бути сторонніми особами, які зламали привілейований обліковий запис і видають себе за його власника.

Ось деякі з основних типів атак зловмисного програмного забезпечення:

Віруси – фрагмент коду впроваджується в програму. Коли програма запускається, зловмисний код виконується.

Хробаки – шкідливе програмне забезпечення, яке використовує вразливості програмного забезпечення та бекдори, щоб отримати доступ до операційної системи. Після встановлення в мережі хробак може здійснювати такі атаки, як розподілена відмова в обслуговуванні (DDoS).

Трояни – шкідливий код або програмне забезпечення, яке видає себе за невинну програму, що ховається в програмах, іграх або вкладеннях електронної пошти. Нічого не підозрюючи користувач завантажує троян, дозволяючи йому отримати контроль над своїм пристроєм.

«Cryptojacking» – зловмисники розгортають програмне забезпечення на пристрої жертви і починають використовувати свої обчислювальні ресурси для створення криптовалюти без їхнього відома. Уражені системи можуть працювати повільно, а комплекти криптоджекінгу можуть вплинути на стабільність системи.

Шпигунське програмне забезпечення – зловмисник отримує доступ до даних нічого не підозрюючих користувачів, включаючи конфіденційну інформацію, наприклад паролі та платіжні дані. Шпигунське програмне забезпечення може впливати на настільні браузери, мобільні телефони та настільні програми.

Рекламне програмне забезпечення – активність перегляду користувача відстежується для визначення моделей поведінки та інтересів, що дозволяє рекламодавцям надсилати користувачам цільову рекламу. Рекламне програмне забезпечення пов’язане зі шпигунським програмним забезпеченням, але воно не передбачає встановлення програмного забезпечення на пристрої користувача і не обов’язково використовується зі зловмисними цілями, але воно може використовуватися без згоди користувача та ставить під загрозу його конфіденційність.

Безфайлове зловмисне програмне забезпечення – в операційній системі не встановлено програмне забезпечення. Вбудовані файли, такі як WMI та PowerShell, редагуються, щоб увімкнути шкідливі функції. Цю приховану форму атаки важко виявити (антивірус не може її ідентифікувати), оскільки скомпрометовані файли розпізнаються як легітимні.

Руткіти – програмне забезпечення впроваджується в програми, мікропрограми, ядра операційної системи або гіпервізори, забезпечуючи віддалений адміністративний доступ до комп'ютера. Зловмисник може запустити операційну систему в скомпрометованому середовищі, отримати повний контроль над комп’ютером і доставити додаткове шкідливе програмне забезпечення.

Таким чином, на сьогоднішній день у світі існує безліч шкідливих кодів або програмне забезпечення, яке зловмисники можуть використати як зброю у кібртероризмі. Тому з метою протидії кібер атакам необхідно володіти знаннями про комп'ютерні системи та їх слабкі сторони, щоб мати змогу вчасно передбачити та попередити певні види таких атак.

1.3. Сучасні підходи до розуміння поняття «кібертероризм»

Як зазначає І. Васильковський, кіберзлочинність (або «злочин з використанням комп'ютерних технологій») — це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет [19, с. 56].

Хоча кіберзлочини, значним чином, дійсно були здебільше економічними злочинами, але із впливом часу вони вийшли на новий рівень, а саме як соціально небезпечне явище, яке загрожує навіть інформаційній безпеці держави, тому для більш повного дослідження питання кіберзлочину ми маємо звернутися до думки В. Бутузова.

Визначення кібертероризму здебільшого базуються на традиційних визначеннях тероризму, таких як вищезгадані. Оскільки було припущення, що атаки можуть кваліфікуватися як кібертероризм, якщо є намір перешкодити політичному, соціальному чи економічному функціонуванню групи, організації чи країни, або спровокувати/вчинити акти фізичного насильства [20].

Британський вчений Холт також підтримує це визначення, припускаючи, що термін кібертероризм повинен охоплювати поведінку, яка призводить до акту, не обов'язково призводячи до фізичного порушення або пошкодження [21].

Обидва ці визначення акцентують увагу на намірах та мотивах кібертерористичної діяльності замість вузького фокусування на фізичному впливі. Навпаки, інші науковці зайняли іншу позицію з цього приводу і

стверджували, що для кваліфікації атаки за кібертероризмом має статися фізичне пошкодження та/або порушення роботи комп'ютера чи мережі [22, 23].

Незважаючи на зусилля науковців щодо визначення кібертероризму, дехто також стверджує, що кібер-префікс до тероризму пояснює лише метод, який використовується для вчинення тероризму, і, отже, «кібертероризм» не потребує власної категорії [24].

Британські вчені вважають, що «кібертероризм» як термін містить широкий спектр протиправної поведінки, включаючи хакерство та фішинг, поширення онлайн-пропаганди, радикалізацію та вербування людей. Тому спроба визначити все під терміном «кібертероризм» може стати складною проблемою через юридичний контекст, цілі протиправної поведінки та наміри [25, с. 37].

Засновник і виконавчий директор Центру передових досліджень у сфері науки та технологій Стілвелла, вважає, що «кібертероризм, яким би він не був, є марним терміном». Тайпал вважає, що «терористи використовуватимуть будь-який стратегічний інструмент, який можуть», тому «кібер-тероризм» не є більш важливим, ніж інші форми.

Проблема скоріше в тому, що немає «єдиного правового режиму», що створює «прірву між законодавцями та владою», – зазначив він. «Чи повинні реагувати військові чи поліція, національна чи іноземна – не повністю визначено», – сказав Тайпале. Ці окремі організації «несумісні та непослідовні, що робить нас більш вразливими до тероризму».

Тайпал пояснив, що така фрагментована юридична структура означає, що ми «не підготовлені для вирішення цілого ряду нових проблем», які виникають у сфері кібернетики. І це справді клопітно, тому що межа між «безпечним суспільством і хаосом тонка, – сказав Тайпале, — ми стоїмо в черзі за серйозних кібер-Катрін, з якими ми не готові мати справу».

Однак, як і Бейлі, Тайпал вважає, що «застаріла інфраструктура безпеки» існує тому, що різні організації мають різні проблеми. Наприклад,

після кіберзагроз банківським рахункам Слободана Мілошевича під час кризи в Косово 1999 року в ООН підняли дискусію про кібертероризм, і хоча Росія виявила зацікавленість у цій проблемі, США зупинили дискусію. «Що є, а що не дозволено, ніколи не вирішувалося через інтерес США до власної міжнародної відповідальності», – сказав Тайпале.

Побоювання Тайпале, що межа між безпечним суспільством і хаосом є крихкою, посилюється проблемою довіри, на яку наголосив доктор Ендрю Коларик, консультант із інформаційної безпеки. Коларик підкреслив етимологію терміну, сказавши, що «не буває кібертероризму без тероризму».

По суті, мета тероризму полягає в тому, щоб спричинити серйозні порушення через поширений страх у суспільстві, тобто проблема, сказав він, – це «наша залежність від цифрових матеріалів». «Більшість нашої валюти – це не паперова, це цифрова. І як гроші, якщо ми втратимо довіру до базової системи, у нас буде неплатоспроможність».

Ці визначення кібертероризму дають різне уявлення про те, що можна, а що ні, кваліфікувати як кібертероризм, але важливо визнати дати, коли ці визначення були задумані. Натомість технології значно еволюціонували з моменту концепції цих визначень, виникла необхідність узгодити сучасне визначення кібертероризму, яке охоплює всі аспекти сучасних технологій.

Нещодавнє дослідження було проведено з визначенням ключових характеристик, присутніх у низці визначень кібертероризму, щоб створити нове визначення, засноване на цих компонентах, і дослідження дійшло висновку, що : «Кібертероризм є навмисною атакою або її загрозою з боку не- державні суб’єкти, які мають намір використовувати кіберпростір, щоб спричинити реальні наслідки, щоб вплинути на страх чи примусити цивільних, урядових чи неурядових цілей для досягнення соціальних чи ідеологічних цілей. Реальні наслідки включають фізичні, психологічні, політичні, економічні, екологічні чи інші наслідки, які відбуваються за

межами кіберпростору». Це визначення акцентує увагу на акторі, мотивації, намірах, засобах, наслідках та цілях кібертероризму[26, с. 34].

Насправді кібертероризм є дуже широким поняттям, і визначення, яке може намагатися охопити всі характеристики, що підпадають під цей термін, здаються, складними.

РОЗДІЛ 2. ПРАКТИКА ФУНКЦІОНУВАННЯ КІБЕРТЕРОРИЗМУ НА МІЖНАРОДНІЙ АРЕНІ

2.1. Особливості застосування кібератак у сучасному світі

Звичайне визначення кібератак – це процес спроби викрадення даних або отримання несанкціонованого доступу до комп'ютерів і мереж за допомогою одного або кількох комп'ютерів. Кібератака часто є першим кроком, який робить зловмисник, щоб отримати несанкціонований доступ до індивідуальних чи корпоративних комп'ютерів чи мереж, перш ніж здійснити злом даних.

Мета кібератаки полягає в тому, щоб вимкнути цільовий комп'ютер і вивести його в автономний режим, або отримати доступ до даних комп'ютера та проникнути в підключені мережі та системи. Кібератаки також сильно відрізняються за своєю складністю: кіберзлочинці здійснюють як випадкові, так і цілеспрямовані атаки на підприємства.

Відповідно до здійсненого аналізу кібератак у країнах Близького Сходу, Європи та Африки найбільше від кібератак страждають урядові сайти, сайти фінансових організацій та сайти операторів зв'язку (рис. 1) [15].

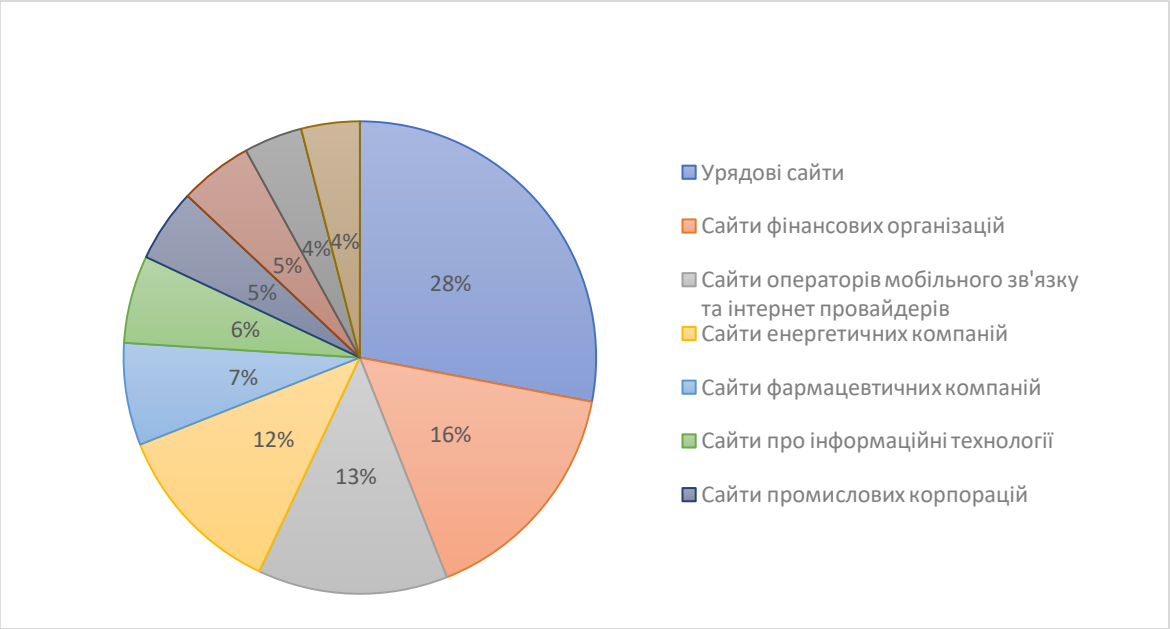

Рис. 1. Процентне значення кількості кібератак на різні джерела.

Зловмисники використовують широкий спектр методів для початку кібератаки, таких як відмова в обслуговуванні, зловмисне програмне забезпечення, фішинг і програмне забезпечення-вимагання.

Домен кіберпростору складається з трьох шарів. Перший – це фізичний рівень, включаючи обладнання, кабелі, супутники та інше обладнання. Без цього фізичного рівня інші рівні не можуть функціонувати. Другий – синтаксичний рівень, який включає програмне забезпечення, що надає інструкції з експлуатації фізичного обладнання. Третій – це семантичний шар, який включає взаємодію людини з інформацією, що генерується комп'ютером, і тим, як ця інформація сприймається та інтерпретується її користувачем. Усі три шари вразливі для атак.

Кібервійна може бути здійснена проти фізичної інфраструктури кіберпростору за допомогою традиційної зброї та методів бою. Наприклад, комп'ютери можуть бути фізично знищені, їхні мережі можуть бути зруйновані або зруйновані, а люди-користувачі цієї фізичної інфраструктури

можуть бути підпорядковані, обдурені або вбиті, щоб отримати фізичний доступ до мережі чи комп'ютера.

Фізичні атаки зазвичай відбуваються під час звичайних конфліктів, наприклад, під час операції Об'єднаних сил Організації Північноатлантичного договору (НАТО) проти Югославії в 1999 році та під час операції США проти Іраку в 2003 році, коли комунікаційні мережі, комп'ютерні засоби та телекомунікації були пошкоджені або знищено.

Атаки на синтаксичному рівні можна здійснювати за допомогою кіберзброї, яка знищує, заважає, пошкоджує, відстежує або іншим чином пошкоджує програмне забезпечення, яке керує комп'ютерними системами.

Така зброя включає зловмисне програмне забезпечення, зловмисне програмне забезпечення, таке як віруси, трояни, шпигунські програми та хробаки, які можуть вводити пошкоджений код в існуюче програмне забезпечення, змушуючи комп'ютер виконувати дії або процеси, ненавмисні його оператором.

Інша кіберзброя включає атаки розподіленої відмови в обслуговуванні або DDoS, під час яких зловмисники, використовуючи зловмисне програмне забезпечення, захоплюють велику кількість комп'ютерів, щоб створити так звані ботнети, групи комп'ютерів-«зомбі», які потім атакують інші цільові комп'ютери, запобігаючи їх належна функція.

Цей метод використовувався під час кібератак проти Естонії у квітні та травні 2007 року та проти Грузії в серпні 2008 року. В обох випадках стверджується, що російські хакери, переважно цивільні, здійснили атаки з метою відмови у наданні послуг проти ключових державних, фінансових, медіа та комерційних веб-сайти в обох країнах. Ці атаки тимчасово заборонили урядам і громадянам цих країн доступ до ключових джерел інформації та внутрішніх і зовнішніх комунікацій.

Терористи використовують кіберпростір для низки видів діяльності, включаючи мову ворожнечі, пропаганду, вербування та спілкування [27]. Теорія рутинної діяльності [28] і теорія космічного переходу [29] можуть

бути застосовані до кібертероризму, щоб підтримати більш чітке розуміння мотивів кібертерористів, у свою чергу, вказуючи на особливості застосування кібератак в сучасному світі [30, с. 111-115].

Теорія рутинної діяльності була розроблена Коеном і Фелсоном у 1979 році і запропонувала, що для того, щоб виникла віктимізація, необхідні три взаємодіючі фактори: по-перше, мотивований злочинець; по-друге, відповідна мішень; по-третє, відсутність дієздатного опікуна. Коли ця теорія застосовується до кіберзлочинності, поняття фізичного простору змінюється на кіберпростір [31–33].

Було проведено дослідження стосунків між студентами університету та їхніми комп'ютерами, і було виявлено, що студенти, які мали більшу тенденцію нехтувати своїм комп'ютерним способом життя та/або нехтувати програмним забезпеченням безпеки на своїх комп'ютерах, частіше ставали жертвами злочинів [33, с. 72].

Це дослідження підкреслює поміркованість до оригінальної теорії рутинної діяльності, згідно з якою відсутність опікуна може бути не тільки фізичною особою, але також може бути відсутність програмного забезпечення безпеки на технологічному пристрої жертви.

Хоча в цьому дослідженні йшлося саме про хакерство, теорія кіберрутинної активності все ж була застосована до інших форм кіберзлочинів [34], і ці висновки можна застосувати до кібертероризму.

Наприклад, якщо немає комп'ютерної безпеки або заблоковані веб-сайти, це може дати змогу мотивованому правопорушнику здійснити загрозу або акт терористичного насильства проти відповідної цілі.

Теорія космічного переходу, створена Джайшанкаром [35], була розроблена, щоб краще пояснити перехід кіберзлочинної поведінки з фізичного простору в кіберпростір і навпаки.

Ця теорія досліджує сім основних принципів:

− схильність до кіберзлочинності внаслідок придушення офлайнових злочинних тенденцій;

- гнучка ідентичність у кіберсередовищі;
- свобода переходу між фізичним та кіберпростором;
- кримінальна можливість з невеликим регулюванням і шансом бути спійманим;
- соціальні зв’язки правопорушників;
- зменшення загрози для правопорушників;
- розмиті межі між нормами та цінностями в кіберсередовищі.

Принципи теорії Джайшанкара [35] забезпечують краще розуміння парадоксальних характеристик між традиційними та кіберзлочинами, і три з них можуть сприяти кращому розумінню кібертероризму.

По-перше, через анонімну природу кіберпростору для кібертерористів є пряма можливість замаскувати свою ідентичність, яку раніше називали дисоціативною анонімністю [36]. Ця анонімність дозволяє терористам приховувати свою особистість, щоб обійти існуючі правила в кіберсередовищі.

По-друге, через анонімність кіберсередовища це не тільки впливає на те, як можна регулювати дії, але й дозволяє правопорушникам продовжувати свою злочинну поведінку без будь-яких наслідків.

Це також підтверджується ефектом когнітивного гальмування, при якому через відсутність стримування дисоціація між дією та кінцевим результатом спонукає до тривалої терористичної поведінки [37].

По-третє, здатність обмінюватися між фізичним та кіберпростором натякає на те, що терористична діяльність потенційно може проявлятися у кіберпросторі, де існують обмежені обмеження для поширення пропаганди та вербування, до переміщення у фізичний простір, де можна побачити офлайнові наслідки [38, с. 17].

Ця доступна взаємозамінність є фінансово вигідною для терористичних груп, оскільки вони можуть досягти своїх цілей і завдань для розвитку своєї терористичної ідеології за менших грошових витрат.

Нарешті, якщо терористична поведінка придушується у фізичному середовищі, це може спонукати терористів змінити свої підходи до кіберпростору, де діяльність може бути прихована від регулюючих органів та зацікавлених сторін, залучених до боротьби з тероризмом [39].

Хоча це вже було вигідним аспектом для терористів, це стало ще більш значущим через глобальну пандемію COVID та обмеження на карантин [2, с. 45-47].

У зв'язку з більшим збільшенням використання кіберпростору терористами та його динамічних просторово-часових характеристик, існує менший ризик бути спійманим через величезність кіберсередовища [39].

Загалом, принципи, висвітлені в теорії космічного переходу [40], спрощують переваги, які дозволяють терористичній діяльності продовжуватися переважно безперервно.

Деякі приклади серйозних терористичних злочинів включають підготовку терористичних атак; збір інформації про тероризм; розповсюдження терористичних публікацій з метою заохочення тероризму; допомога в приховуванні терористичної діяльності в Інтернеті; підтримка забороненої організації; відвідування місця підготовки терористів; і фінансова допомога терористичній діяльності.

Таким чином можна узагальнити, що кібертерористична діяльність поділяється на чотири основні категорії:

- вербування;
- попередня організація та планування;
- підготовче проведення;
- терористичний акт.

Ця структура може бути корисною для більш чіткого розуміння того, які загальні види терористичної діяльності мають місце, і, крім того, як один акт може призвести до іншого.

Кібератаки використовують уразливі місця в комп'ютерних системах і мережах комп'ютерних даних або обманом обманюють користувачів, щоб

отримати незаконний доступ з наміром або вкрасти, знищити або маніпулювати даними та системами.

Кібератаки зазвичай мають одну з трьох форм:

– атаки на конфіденційність, спрямовані на отримання доступу до інформації з обмеженим доступом;

– атаки на цілісність, які змінюють, маніпулюють або компрометують дані та комп’ютерні системи;

– атаки на доступність, які забороняють або обмежують доступ законних власників до їхніх даних.

Розглядаючи застосування кібератак в сучасному світі – важко не згадати про масштабну кібератаку на сайти центральних і регіональних органів влади України, котру зафіксували вночі 14.01.2022 р. Це відбулося на тлі великого скупчення російських військ вздовж українських кордонів і стало першою «інформаційною» агресією Росії проти України, перед початком перетину її військами нашого кордону.

Співголова Європейської ради з міжнародних відносин, експрем'єр-міністр Швеції Карл Більдт, тоді зазначив, що «…вона [кібератака] мала на меті встановити шкідливе програмне забезпечення, яке в певний момент за командою знищило би більшою чи меншою мірою всі системи», – написав він у Twitter.

Українські урядові сайти в ніч на 14 січня зазнали кібератаки. На деяких ресурсах хакери залишили повідомлення трьома мовами – українською, російською та польською – у якому йдеться, що всі особисті дані користувачів викладені у відкритий доступ, і закликали «готуватися до гіршого». Наразі невідомо, хто стоїть за цією масштабною кібератакою, але лише кілька тижнів тому західні ЗМІ попереджали, що до таких дій може вдатися Росія.

Хакерська атака зачепила десятки сайтів державних органів України – за оцінкою Держспецзв'язку, близько 70. Зокрема, не працюють сайти:

– Урядовий портал;

- Міністерства освіти та науки;
- Міністерства закордонних справ України;
- Міністерства у справах ветеранів;
- Міністерства енергетики;
- Державної служби з надзвичайних ситуацій;
- Міністерства молоді та спорту;
- Державного казначейства України;
- Міністерства розвитку громад та територій;
- Міністерства екології;
- Міністерства аграрної політики та продовольства;
- Державної інспекції ядерного регулювання.

У Європейському Союзі вже відреагували на кібератаку на українські держструктури. Верховний представник ЄС із закордонних справ та політики безпеки Жозеп Боррель засудив їх і повідомив, що комітет із політики безпеки та кіберпідрозділи зустрінуться, щоб обговорити допомогу Україні[27].

У такому разі можна стверджувати, що в сучасному інформаційному суспільстві – кібератака стає інструментом агресії проти інших держав, з метою створення сприятливих умов та отримання необхідних даних для введення бойових дій.

У разі повномасштабного вторгнення противника відключення ним за допомогою кіберзброї наших електромереж призведе до неспроможності української армії оперативно відреагувати, неспроможності для координації цивільного населення. Зв'язок, телекомунікації є надважливою складовою обороноздатності держави.

Кібератаки є найбільш небезпечними, коли вони загрожують критичній національній інфраструктурі, від енерго- та водопостачання до транспортних мереж та надання медичної допомоги.

Кібервійна зазвичай визначається як кібератака або серія атак, спрямованих на країну. Вона може завдати шкоди урядовій та цивільній

інфраструктурі та порушити критичні системи, що призведе до шкоди державі та навіть до загибелі людей.

Однак серед експертів з кібербезпеки точаться дискусії щодо того, який вид діяльності є кібервійною. Міністерство оборони США визнає загрозу національній безпеці через зловмисне використання Інтернету, але не дає більш чіткого визначення кібервійни. Деякі вважають кібервійну кібератакою, яка може призвести до негативних наслідків.

Кібервійна, як правило, включає в себе національну державу, яка здійснює кібератаки на іншу, але в деяких випадках атаки здійснюються терористичними організаціями або недержавними акторами, які прагнуть досягти мети ворожої нації.

У новітній історії є кілька прикладів нібито кібервійни, але не існує універсального формального визначення того, як кібератака може бути актом війни.

Більша частина їх загроз існує через зростаючу оцифровку цих послуг, зміну природи технологій, складність ланцюгів поставок і погану обізнаність у сфері кібербезпеки.

Критичні системи можуть містити вразливості «нульового дня» – слабкі місця, про які розробники та користувачі не знають, і які використовуються хакерами (а іноді й державними акторами) для вбудовування шляхів обходу коду в системи, що надає їм привілейований незаконний доступ.

Одним із найскладніших аспектів захисту від кібератак є стирання кордонів між корпораціями та національними урядами. Глобальні технологічні компанії, такі як Microsoft, виробляють програмне забезпечення, яке керує критичними елементами національної інфраструктури в багатьох країнах, тому одна точка слабкості операційної системи може мати далекосяжні наслідки.

За останні кілька років держави почали атакувати програмне забезпечення, що належить корпораціям, чия продукція, як правило,

вбудована в ланцюги поставок критичної інфраструктури – як легко заперечлива форма помсти, щоб посіяти зрив і надіслати повідомлення про їхню здатність захищатися [47, с. 118].

Кіберзлочинність є величезною загрозою для фінансів і особистих даних людей, а також для їх приватності та громадянських свобод. Це також має величезний вплив на світову економіку.

Одним із найбільш тривожних аспектів є те, як уряди, хакери-наймані компанії та корпорації перетинаються в розробці та використанні технологій проти окремих осіб.

Pegasus, дуже складне шпигунське програмне забезпечення, спочатку було розроблено ізраїльською фірмою, яка створює технології для «запобігання та розслідування» тероризму та злочинності.

Однак розслідування, проведене газетами Washington Post, Le Monde і Guardian, а також Amnesty International, показало, що Pegasus також використовувався урядами для спостереження за внутрішніми опонентами, які не мають жодного зв'язку з тероризмом або злочинністю, включаючи політиків, журналістів і активістів.

Країни все більше усвідомлюють загрозу, яку представляють постачальники технологій, які глибоко вбудовані в їхні складні ланцюги поставок.

Такі занепокоєння стали причиною рішення Великобританії у 2020 році видалити обладнання, встановлене Huawei (китайською телекомунікаційною фірмою), зі своєї мережі 5G.

Частково проблема полягає в тому, що багато політиків не завжди повністю розуміють природу загрози. Протягом кількох років основним занепокоєнням була одна великомасштабна подія, схожа на війну, яка завдала матеріальної та фізичної шкоди, хоча насправді найбільша загроза походить від величезного обсягу одночасних і часто не пов'язаних незначних атак [43, с. 101].

Правовий статус цієї нової сфери досі неясний, оскільки не існує міжнародного права, що регулює використання кіберзброї. Однак це не означає, що кібервійна не регулюється законом.

Отже, кібератаки надають державам інструмент у своєму арсеналі, який є надзвичайно гнучким, але може завдати шкоди противнику за порівняно невелику вартість. На відміну від атак із застосуванням звичайної зброї, кібератаки часто можна заперечувати, хоча це змінюється, оскільки інструменти атрибуції стають все більш досконалими.

Вони є частиною нового типу конфлікту, що відбувається у своєрідній «сірій зоні». Такі атаки чинять величезний тиск на їхні цілі, змушуючи їх перейти до оборони від загрози, що постійно розвивається.

2.2. Інформаційні війни як складова кібертероризму

Американські науковці джон Аркілла та Девід Ронфельдт фіксують широкий характер інформаційної війни у своїй праці Cyberwar is Coming! У цій роботі вони розглядають військову та цивільну, а також наступальну та оборонну складові інформаційної війни. Спектр конфліктів поділяється на «мережеву» та «кібервійну».

«Мережева війна» відноситься до інформаційних конфліктів на великому рівні між націями або суспільствами. Це означає спробу порушити, пошкодити або змінити те, що цільова група знає або думає, що знає про себе та навколишній світ.

Мережа може бути зосереджена на громадській чи елітній думці, або на обох. Вона може включати заходи публічної дипломатії, пропагандистські та психологічні кампанії, політичну та культурну підривну діяльність, обман або втручання в роботу місцевих засобів масової інформації, проникнення в комп’ютерні мережі та бази даних, а також зусилля з просування дисидентів. або рухи опозиції через комп’ютерні мережі.

Кібервійна означає проведення та підготовку до проведення військових операцій відповідно до інформаційних принципів. Це означає руйнування, якщо не руйнування, інформаційно-комунікаційної системи, широко визначеної, включаючи навіть військову культуру, на яку покладається противник, щоб знати себе: хто він, де він знаходиться, що він може зробити, коли, чому воює, яким загрози протистояти першим тощо. Це означає намагатися знати все про супротивника, не даючи йому знати багато про себе [13, с. 275].

Кібертероризм, використовуючи деякі тактики кібервійни, лежить у сфері мережевої війни. Досліджуючи кібер і мережеву війну, Аркілла і Ронфельдт підкреслюють зростаючу важливість контролю інформації для військової перемоги в інформаційну епоху.

У майбутньому контроль інформації також може мати вирішальне значення для успішного тероризму чи боротьби з тероризмом.

Національний університет оборони (NDU) висунув робоче визначення інформаційно-орієнтованої війни, яке окреслює наступальні та оборонні компоненти інформаційної війни. Він підкреслює застосовність інформації як цілі, так і зброї у всьому спектрі конфлікту:

Інформаційна війна – це підхід до збройного конфлікту, зосереджений на управлінні та використанні інформації в усіх її формах і на всіх рівнях для досягнення вирішальної військової переваги, особливо в спільному та комбінованому середовищі. Інформаційна війна носить як наступальний, так і оборонний характер, починаючи від заходів, які забороняють противнику використовувати інформацію, до відповідних заходів для забезпечення цілісності, доступності та сумісності дружніх інформаційних ресурсів.

Інформаційна війна, зрештою, має військовий характер, також ведеться на політичній, економічній та соціальній аренах і застосовна до всього континууму національної безпеки від миру до війни і від «зуба до хвоста». Нарешті, інформаційно-орієнтована війна зосереджується на потребах командування та контролю командира, використовуючи

найсучасніші інформаційні технології, такі як синтетичні середовища, щоб домінувати на полі бою.

Лібіцкі з NDU також розглянув концепцію інформаційної війни та її наслідки для майбутнього. У його статті Advanced Concepts and Technology «Що таке інформаційна війна?»

Лібіцкі виділяє сім конкретних форм інформаційної війни:

- війна командування та управління;
- інформаційна війна;
- електронна війна;
- психологічна війна;
- хакерська війна;
- економічна інформаційна війна;
- кібервійна.

Хоча більшість із цих форм конфліктів належать до військової сфери, кожен з них застосовний до тероризму в епоху інформації, що розвивається.

Форма, описана як хакерська війна (боротьба з комп'ютерними мережами), Лібіцкі розділяє на три області:

- фізичну;
- синтаксичну;
- семантичну.

За такою типологією фізична атака комп'ютерних мереж класифікується як технотероризм. Атака комп'ютерних систем на синтаксичному рівні (атака на потік електронів у мережі) і на семантичному рівні (атаки на правдивість інформації мережі – обман комп'ютера, щоб отримати неправильний результат) визначаються як кібертероризму, оскільки вони існують виключно у сфері кіберпростору.

Інформаційна війна складається з двох компонентів [11, с. 9].

По-перше, ваша власна інформація має бути захищена та довірена на всіх рівнях. Під час збору необхідно перевірити достовірність отриманої

інформації. Під час обробки інформація має бути захищена від крадіжки, знищення та модифікації. Нарешті, під час розповсюдження інформації іншим елементам засоби передачі повинні бути безпечними, щоб гарантувати, що інформація надходить до місця призначення в незміненому форматі. Захисна частина інформаційної війни спрямована на забезпечення конфіденційності, цілісності та доступності інформації.

По-друге, необхідно намагатися порушити функції збору, обробки та розповсюдження інформації противника. Зусилля маніпулювати інформацією ворога, захищаючи свою власну, відбувається на кількох рівнях. Інформаційна війна – це не лише комп'ютери, які посилають електрони з точки А в точку Б. Не тільки апаратне та програмне забезпечення, а й «мокре програмне забезпечення» (комп'ютерний сленг для людського мозку) є критичним для інформаційної війни.

Основна мета війни – змінити думку ворога і переконати його виконати вашу волю. Метою інформаційної війни є досягнення цього за допомогою маніпуляції здатністю противника контролювати інформацію. Це розміщує інформаційну війну в таборі Сунь Цзи. Міхаель Гендель фіксує суть інформаційної війни, цитуючи Клаузевіца і Сунь Цзи, які стверджують: «Бо здобути сто перемог у ста битвах – це не вершина майстерності. Підкорити ворога без бою — це вершина майстерності» [46, с. 195].

У інформаційну епоху необхідно створити абсолютно нову концепцію операцій. Інформація – це «палиця з двома кінцями». В епоху інформації інформація є не лише зброєю бою, а й об'єктом, якого шукають ворогуючі сторони. Кількість, якість і швидкість передачі інформаційних ресурсів є ключовими елементами інформаційної переваги. Тому інформація – це не просто новина, а інформаційна зброя не стосується лише такої інформаційної зброї, як високоточна зброя та зброя радіоелектронної боротьби. Найефективніша зброя – сама інформація. Інформація може використовуватися для атаки на ворожу систему розпізнавання та інформаційну систему як проактивно, так і реактивно, може залишатися

ефективною протягом короткого або тривалого періоду, і може використовуватися для нападу на ворога відразу або після періоду інкубації. Тому основними предметами підготовки до війни в інформаційну епоху стануть якісний інформаційний захист та здійснення контратаки інформаційною зброєю при атаці.

Інформація є інтеркомунікативною, тому її не можна класифікувати за секторами чи галузями. Дуже помилково вважати, що інформація лише у військовій сфері заслуговує на збереження таємниці, а інформація для цивільних цілей не відноситься до категорії секретності. Фактично, якщо не вжити заходів безпеки для захисту комп'ютерів і мереж, інформація може бути втрачена. Подібним чином, якщо ми думаємо, що отримувати інформацію ворога – це справа відділів розвідки та безпеки, і що вона не має нічого спільного ні з ким іншим, ми втратимо гарну нагоду виграти інформаційну війну.

Ця спроба перемогти без бою суперечить Клаузевіцу, який вважав, що бій і кровопролиття були невід'ємною частиною війни. «Люди з добрим серцем можуть, звичайно, подумати, що існує якийсь геніальний спосіб роззброїти чи перемогти ворога без зайвого кровопролиття, і можуть уявити, що це справжня мета мистецтва війни. бути розкритим».

Хоча обидві цитати суперечливі, вони стосуються тероризму в епоху інформації. Хоча фізичне знищення сприймається як «менш кривавий» і «насправді не бойовий», фізичне знищення може відігравати важливу роль в інформаційній війні.

Інформаційна війна повністю відрізняється від загальноприйнятої концепції націлювання на ціль і знищення її кулями, або командирів, які спираються на зображення та зображення, отримані за допомогою візуального виявлення та за допомогою обладнання дистанційного зондування, для проведення операцій з карти або піщаного столу. Багатовимірні взаємопов'язані мережі на землі, в повітрі (чи космічному просторі) і під водою, а також термінали, модеми та програмне забезпечення

є не лише інструментами, а й зброєю. Народна війна за таких умов була б складною, широкомасштабною та мінливою, з більшим ступенем невизначеності та ймовірності, що вимагає повної підготовки та обачної організації [46, с. 47].

Інформаційна війна коштує недорого, оскільки ворожа країна може отримати паралізуючий удар через Інтернет, а сторона, яка отримує, не зможе зрозуміти, дитяча це витівка чи напад її ворога. Ця характеристика інформаційної війни визначає, що кожен учасник війни має вищу незалежність і більшу ініціативу. Однак, якщо організація є неадекватною, вони можуть вести власні битви і не можуть формувати спільні сили. Крім того, Інтернет може генерувати велику кількість непотрібної інформації, яка займає обмежені канали та простір і блокує дію власної сторони. Тому лише ввімкнувши відповідні системи та поєднавши людський інтелект із штучним інтелектом за ефективної організації та координації, ми можемо втопити наших ворогів у океані інформаційного наступу.

Народна війна в умовах інформаційної війни ведеться сотнями мільйонів людей за допомогою сучасних інформаційних систем відкритого типу. Оскільки традиційний спосіб промислового виробництва змінився від централізації до дисперсії, а комерційна діяльність поширилася з міських районів на сільську місцевість, робочий метод і спосіб взаємодії у первісному розумінні все більше базуються на інформації. Політична мобілізація на війну повинна покладатися на інформаційні технології, щоб стати ефективною, наприклад, шляхом створення та розповсюдження програмного забезпечення політичної мобілізації через Інтернет, розсилання патріотичних повідомлень електронною поштою та створення баз даних для традиційної освіти. Таким чином, сучасні технічні засоби масової інформації можуть бути повністю використані, а ефект відкритості та поширення Інтернету може бути розширений, щоб допомогти політичній мобілізації здійснювати свій тонкий вплив [48, с. 128].

Якщо коротко, то значення та наслідки народної війни глибоко змінилися в інформаційну епоху, і шанси того, що люди виявлять ініціативу та випадково беруть участь у війні, зросли. Етнічна ознака та географічна ознака на інформаційній війні більш яскраво виражені, а застосування стратегій є більш прихованим і непередбачуваним.

Інформаційні конфронтації будуть спрямовані на досягнення відчутного миру за допомогою нематеріальної війни, підтримання миру апаратного забезпечення за допомогою програмних конфронтацій, а також стримування та шантаж ворога за допомогою домінування у володінні інформацією [25, с. 71]. Кривавий тип війни все більше буде змінюватися боротьбою за інформацію та конфронтацією.

Одним із інструментів інформаційної війни є інфраструктурна війна, в якій на інфраструктуру противника націлені як «звичайні» технології (бомби, ракети, війська на землі), так і «інформаційні» технології, спроба використовувати шкідливе програмне забезпечення для руйнування. і змінювати телекомунікації ворога без фізичного знищення та викликати у ворога психологічний стан, який змусить його «виконувати вашу волю».

Інформаційна війна – це прагнення порушити, вимкнути, знищити або змінити інформаційні та інформаційні системи супротивника, одночасно захищаючи свою. Хоча електронні атаки мережі є «найчистішим» засобом інформаційної війни, фізичні атаки на інфраструктуру мережі також можливі, і їх завжди слід розглядати пряму загрозу.

2.3. Прояви кібертероризму як реальної загрози

Комп’ютери та мережі, які їх з’єднують, спільно відомі як домен кіберпростору. Західні держави залежать від кіберпростору для повсякденного функціонування майже всіх аспектів сучасного суспільства, а держави, що розвиваються, з кожним роком стають все більш залежними від кіберпростору.

Все, що необхідно для функціонування сучасного суспільства – від критичної інфраструктури та фінансових установ до способів торгівлі та інструментів національної безпеки – певною мірою залежить від кіберпростору.

Тому загроза кібервійни та її передбачувані наслідки є джерелом великої занепокоєння для урядів і військових по всьому світу, і відбулося кілька серйозних кібератак, які, хоча й не обов'язково відповідають суворому визначенню кібервійни, можуть слугувати ілюстрацією того, що можна очікувати в реальній кібервійні майбутнього.

Донедавна західні країни не визнавали, що володіють або використовують наступальний кіберспроможність, але останнім часом ситуація змінилася.

Наприклад, розвідувальні служби США вважаються відповідальними за Stuxnet, зловмисне програмне забезпечення, використане під час атаки на ядерні об'єкти Ірану в 2010 році.

І кіберкомандування США, і GCHQ Великобританії публічно визнали використання кібератак для припинення терористичної діяльності груп, включаючи ІДІЛ.

Російські угруповання, в тому числі ті, які мають зв'язки з російським урядом, нібито відповідальні за численні кібератаки на інфраструктуру інших країн протягом останніх 20 років.

У 2007 році серія кібератак була спрямована на парламент Естонії, банки та телевізійні станції в рамках суперечки про радянські військові могили в країні. Вона примітна тим, що є однією з перших великих кібератак, спонсорованих державою.

Російські спецслужби також були звинувачені у зламі системи електронної пошти Національного комітету Демократичної партії в США у 2015 та 2016 роках. Електронні листи витікали в рамках кампанії впливу на результати виборів у США 2016 року.

У 2015 році вважалося, що російське угруповання відповідало за атаку на українську енергосистему. У 2017 році зловмисне програмне забезпечення NotPetya, нібито розроблене російською розвідкою для нападу на Україну, поширилося на системи однієї з найбільших у світі контейнерних компаній «A.P. Moller — Maersk». В результаті Maersk повідомила про збитки до 300 мільйонів доларів.

Кібератака SolarWinds 2020 року була складною атакою зловмисного програмного забезпечення, спрямованою на програмний продукт Orion фірми SolarWinds, який використовується компаніями для управління IT-ресурсами.

Атака, яка місяцями залишалася непоміченою, дозволила хакерам шпигувати за клієнтами SolarWinds і встановлювати шкідливе програмне забезпечення в їхні системи [6, с. 9].

Цілі включали фірми з кібербезпеки, урядові установи США та Microsoft. У здійсненні нападу знову звинуватили російські спецслужби.

Вважається, що злом Microsoft Exchange, виявлений у січні 2021 року, був прямою атакою спонсорованих китайським урядом хакерів на локальні сервери обміну Microsoft, жертвами яких були уряд, промисловість та організації громадянського суспільства.

Атака була випадком хакерів, які використовували «вразливості нульового дня» на серверах. Вважається, що хакери мали доступ до адрес електронної пошти та паролів Microsoft деякий час до того, як злом був виявлений.

Це був приклад розширеної постійної загрози (APT), коли хакери проводять місяці в системі, збираючи інформацію, перш ніж атакувати. Це була дуже вмотивована і дуже витончена атака.

Деякий час США також звинувачували китайських хакерів у використанні кібератак як частини великомасштабної крадіжки інтелектуальної власності та промислового шпигунства.

Північна Корея найбільш відома своєю атакою на Sony Pictures Entertainment. Вважалося, що ця атака була відплатою за випуск компанією

фільму «Інтерв'ю», який критикує Північну Корею, у 2014 році. Хакери викрали конфіденційні документи, видалили оригінальні файли з комп'ютерів Sony та опублікували неопубліковані фільми та конфіденційну інформацію на загальнодоступних файлообмінних сайтах [60, с. 18].

Північнокорейська група Lazarus також стверджується, що була джерелом атаки програмного забезпечення-вимагача «WannaCry» у 2017 році, яка заразила сотні тисяч комп'ютерів, у тому числі деякі належали Національній службі охорони здоров'я Великобританії (NHS).

Національна служба охорони здоров'я не обов'язково була конкретною метою, але жертвою нецілеспрямованої, не особливо складної глобальної атаки зловмисного програмного забезпечення, яка використовувала наявні вразливості.

Широко стверджували, що за атакою стояла Північна Корея, використовуючи програмне забезпечення під назвою EternalBlue, яке спочатку було розроблено Агентством національної безпеки США (АНБ).

Обмежене розуміння політиками технології, пов'язаної з кібератаками, часто є проблемою при виробленні політики, яка відповідає цілям. Але все більше усвідомлюється необхідність розробки політики, яка допоможе країнам запобігати кіберзагрозам, готуватися до них і реагувати на них.

За останні кілька років багато країн розробили стратегії національного реагування на кіберзагрози.

Отже, у своїх зусиллях для цього уряди повинні спочатку зрозуміти, що вони намагаються захистити. Які сфери інфраструктури країни є найбільш важливими та чутливими, і де найімовірніше виникнуть загрози для них.

Наприклад, є певна тенденція до зростання кількості злочинів за ст. 362. КК України (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації,

вчинені особою, яка має право доступу до неї). Так, у 2015 році за нею було відкрито 75 справ, у 2016 — вже 311, у 2017 — 670, у 2018 та 2019 — біля 1070.

Графік 1. Кількість порушених справ за ст.361 КК України

Розвиток мережі Інтернет призвів до того, що однією з основних проблем користувачів став надлишок інформації. Це стосується передусім так званого «спаму», тобто масового розповсюдження попередньо не обумовлених електронних листів. Через масовий характер спамових повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм шкідливих програм і комп'ютерних вірусів, поширених із метою отримання доступу до комп'ютерних систем, виведення їх із ладу або отримання конфіденційної інформації.

Однією з характерних особливостей цього виду злочинів є їхня латентність, яка спричинена небажанням користувачів мережі інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів, а також небажанням публічно визнати слабкі місця у власних системах безпеки.

Тому існуюча ситуація з постійним підвищенням ролі комп'ютерної техніки у суспільному житті робить комп'ютерні віруси за характером їх дії подібними до певних видів зброї, незаконне виготовлення якої переслідується чинним законодавством .

Конвенції про кіберзлочинність

23 листопада 2001 року на конференції в Будапешті була підписана Конвенція Ради Європи про кіберзлочинність [10], яка стала юридичною основою для боротьби з кіберзлочинами із посяганнями на інформаційні системи включно. Особливістю цієї Конвенціє є те, що всі майбутні документи укладалися з огляду на її положення, а деякі з них – із прямим посиланням на Конвенцію. Наприклад, у Директиві ЄС 2013/40 про посягання на інформаційні системи [11]. У її преамбулі наголошено: «Нова стратегіяповинна бути розроблена державами-членами й Комісією, беручи до уваги зміст Конвенції Ради Європи про кіберзлочинність від 2001 року».

Отже, ця Конвенція стала фундаментом боротьби з кіберзлочинністю, заклавши основи співробітництва, стандарти криміналізації кіберзлочинів і вимоги до процесуального права не тільки для країн-членів Ради Європи, а й усієї світової спільноти.

Зазначається, що Другий додатковий протокол до Конвенції про кіберзлочинність («Будапештська конвенція» від 13.05.2022), спрямований на посилення співпраці та розкриття електронних доказів, сьогодні відкрито для підписання з нагоди міжнародної конференції, організованої під італійським головуванням у Комітеті міністрів Ради Європи.

Протокол у присутності кількох міністрів підписали такі держави-члени Ради Європи: Австрія, Бельгія, Болгарія, Іспанія, Естонія, Фінляндія, Італія, Ісландія, Литва, Люксембург, Північна Македонія, Чорногорія, Нідерланди, Португалія, Румунія, Сербія та Швеція, а також такі держави, що не є членами: Чилі, Колумбія, США, Японія та Марокко.

Генеральний секретар Ради Європи Марія Пейчинович Бурич зазначила, що кіберзлочинність продовжує рости та мутувати все швидше й

швидше. « Це заважає всьому – від бізнесу до лікарень і критичної інфраструктури, від якої ми всі залежимо. Відкриваючи для підписання Другий додатковий протокол до Будапештської конвенції про кіберзлочинність, ми сьогодні робимо великий внесок у глобальні зусилля по боротьбі зі злочинністю в Інтернеті», – наголосила генсек РЄ[17].

За її словами, протокол узгоджує Будапештську конвенцію з сучасними технологічними викликами, щоб вона залишалася найбільш актуальною та ефективною міжнародною базою для боротьби з кіберзлочинністю в найближчі роки.

Своєю чергою, міністр юстиції Італії Марта Картабія заявила: “Використання ІКТ (інформаційно-комунікаційних технологій) організованою злочинністю у всіх «секторах» (сексуальна експлуатація, обіг наркотиків, контрабанда, тероризм) є новим викликом для наших органів юстиції та для наших установ». За її словами, уряди повинні адекватно та ефективно реагувати на всі ці злочини відповідно до технологічного розвитку. «Таким чином, цей Другий додатковий протокол відповідає на потребу посилення та більш ефективного співробітництва між державами, а також між державами та приватним сектором, роз’яснюючи випадки, коли постачальники послуг можуть надавати дані, якими вони володіють, безпосередньо компетентним органам інших країн. Актуальність цього Протоколу – це надія для жертв кіберзлочинності», – зазначила міністр юстиції Картабія[15].

У повідомленні вказується, що протокол надає інструменти для посилення співпраці та розкриття електронних доказів, таких як пряма співпраця з постачальниками послуг і реєстраторами, ефективні способи отримання інформації про абонентів і даних про трафік, негайне співробітництво в надзвичайних ситуаціях або спільні розслідування, які підпадають під дію прав людини та верховенства права, включаючи гарантії захисту даних.

Протокол відкритий для підписання державами-учасницями Конвенції та набуде чинності, коли його ратифікують п’ять держав.

РОЗДІЛ 3. КІБЕРТЕРОРИЗМ ЯК МЕТОД ПРОТИСТОЯННЯ ДЕРЖАВ НА МІЖНАРОДНІ АРЕНІ

3.1. Прояви кібертероризму та його використання як інструменту протистояння держав на міжнародній арені

Історія говорить, що нації завжди знали про своїх ворогів. В епоху, коли світ рухається до цифровізації, ці відверті фізичні атаки також переходять до цифрових воєн. Іншими словами, нації ведуть війни з країнами третього світу; яка почала входити в сферу кібервійни. Згідно з опитуванням, одна третина населення планети має доступ до Інтернету, а до 2025 року ця цифра збільшиться до 1,7 мільярда. Це призвело до того, що хакерство стало одним із потужних засобів боротьби з політикою та економічні переваги перед ворогами. Зі збільшенням кількості користувачів Інтернету та інновацій Інтернету речей зростає загроза злому кіберзлочинців.

Як ж кібербезпека впливає на міжнародні відносини? Кіберзлочинці націлені на таких політичних діячів як Гілларі Клінтон і Дональд Трамп, а також серйозну занепокоєність викликала безпека націй та її даних. Таким чином, країни прагнули зробити кібербезпеку невід’ємною частиною національної оборони урядів. Крім того, кібербезпека створена як нова сфера ведення війни [29].

2016 рік призвів до того, що кібербезпека стала вершиною політики в усьому світі. Причиною цього був злом російським урядом конфіденційних електронних листів під час президентських виборів у США 2016 року. Експерти в галузі міжнародних відносин зосереджують увагу на наслідках технологій для національної та міжнародної безпеки. Окрім того, зростаючий рівень загроз передбачає необхідність відповідних політичних реакцій, які

уряд та зацікавлені сторони повинні прийняти. Досвід кіберзлочинності показує, що кібербезпека залишатиметься найважливішим порядком денним у міжнародних відносинах.

Ось як кібербезпека впливає на міжнародні відносини:

Урядові хакери

Багато людей не мають чіткого уявлення про хакерство. Такі люди звикли саботувати іноземні держави з боку уряду. Іншими словами, людей, які не мають уявлення про те, що хакерство є злочином, уряд навчає хакерським навичкам для вторгнення в зовнішню безпеку іншої країни[30].

Уряди по всьому світу використовують хакерство, щоб полегшити свою діяльність стеження. Але мало хто використовує цю можливість таємно, не знаючи кібер-законів.

Одним із найкращих прикладів урядових хакерів є наступний випадок:

У 2010 році уряд США саботував ядерну програму Ірану. Основною метою було не допустити отримання ними ядерної енергії. Але, на жаль, вірус був виявлений на ранній стадії, що призвело до гірких відносин між народами. Це створило більший потяг до загроз кібербезпеці.

Цифрова війна:

Страх перед ядерною зброєю проклав шлях до холодних війн у сучасну епоху. Цей цифровий перехід світу привів до вторгнення в конфіденційні дані, а не до фізичної війни. Це призвело до участі у виборах в одній країні іноземних держав. Через те, що Росія стала частиною цієї цифрової війни, та вона почала поширювати дезінформацію через Інтернет по всьому світу; Росія опанувала мистецтво злому політичних даних, що виявилося небезпечним для Укріни та усього світу .

Майбутнє близько, коли хакери атакуватимуть інфраструктуру безпеки противника за допомогою комп’ютерного коду. Кібер-війна все більше стає небезпечною зброєю для міжнародних конфліктів.

Атаки індивідуальності:

Основною причиною цих атак є взаємодія з іноземними громадянами через Інтернет. Нігерійці дуже популярні з точки зору кіберзлочинців, які націлені на людей за допомогою онлайн-схем[25].

Кіберпростір і кіберполітика

Традиційна теорія міжнародних відносин закріплена і стосується взаємодії у фізичних місцях. Усі форми простору в міжнародних відносинах надають можливості для розширення влади та впливу у світовій політиці. У цій книзі термін «простір» відноситься до областей взаємодії, які створюють потенційні джерела влади, забезпечують розширення впливу та важелів впливу, створюють нові послуги, ресурси, знання або ринки, і реалізувати подальший потенціал, якщо він посилений і підтримуваний технологічним прогресом. Коли діяльність одного суб'єкта загрожує суверенітету, стабільності чи безпеці інших акторів, простір стає важливою змінною в міжнародних відносинах.

З'єднуючи поняття кібернетики та космосу, Вільям Гібсон (1984) зазвичай розглядається як перше формальне позначення нової арени взаємодії, яку ми зараз знаємо як кіберпростір. Хоча позначення кіберпростору ознаменувало зміну розуміння, важливішими є особливості кіберпростору, які дозволяють взаємодіяти між людьми способами, які раніше були неможливими. Особливо важливими є способи використання кібер-майданчиків для формування ідей, обміну інформацією та розширення доступу до знань та альтернативних способів міркування. Оскільки доступ до віртуальних арен і участь у них збільшувався, концепція кібер набула багато нових відтінків. Зараз до терміну надається ряд метафоричних значень, а «кібер» асоціюється з безліччю занурювальних середовищ, можливістю взаємодії з синтетичними сутностями та різноманітним ігровим досвідом, багато, якщо не всі, відображають способи розширення кордонів. віртуального простору та людської уяви [26].

З часом термін кіберпростір набув багатьох різних значень, що випливають із його фундаментальних особливостей, ті, що стосуються

мережевої, комп'ютерної, комп'ютерної та створеної комп'ютером багатовимірної штучної або «віртуальної» реальності (Benedikt 1994b, 122). Цей термін зазвичай прив'язується до Інтернет-додатків. Але обидва вони не ідентичні: електронну зв'язок потрібно відрізняти від її схем, що дозволяють, з одного боку, і від арен взаємодії, що характеризуються акторами, діями та результатами, з іншого.

Загалом, глобальна інформаційна інфраструктура складається з комунікаційних мереж, інформаційного обладнання та програмного забезпечення, додатків і людей, які створюють контент або використовують контент або дозволяють створювати додану вартість і створювати нові види діяльності на основі комунікацій . Цей загальний опис вказує на складну структуру, яка включає широкий спектр ролей і функцій. Девід Кларк (2010) розширює цю характеристику, систематично організовує кібердомен і пропонує багатошарову модель кіберпростору. Такий погляд на кіберпростір прийнято в цій книзі. Відповідно до багатошарової моделі Кларка, ми розглядаємо кіберпростір як ієрархічну контингентну систему, що складається з фізичних основ та інфраструктур, які забезпечують кіберігрове поле, логічних будівельних блоків, які підтримують фізичну платформу та забезпечують надання послуг, інформаційний вміст, що зберігається, передається або трансформується, і учасники, організації та користувачі з різними інтересами, які беруть участь у цій арені в різних ролях [24].

Усі ці шари, функції та сутності мають відношення до кіберполітики в міжнародних відносинах, але в різному ступені й у різних модальностях. Як сплав взаємосумісних мереж, Інтернет став важливою частиною нової глобальної комунікаційної інфраструктури. Коли з'явилася всесвітня мережа, її описували як «вбивчу програму».

Рівень інформаційного вмісту розширюється з експоненційною швидкістю. Створюється та передається нова інформація, а також створюється більше механізмів для полегшення використання та повторного використання вмісту. Такі тенденції передбачають інноваційну організацію

та бізнес-практики, нові державні ініціативи, нові правила та норми, новий інституційний механізм управління та регулювання. Девід Д. Кларк (2010), знову ж таки, фіксує системи прийняття рішень у кіберпросторі, детально описуючи величезне коло акторів та організацій, які беруть участь у роботі кібер-майданчиків. На найзагальнішому рівні до них належать гравці Інтернету та комп'ютерної індустрії, ті, хто займається розробкою додатків та програмного забезпечення, постачальники контенту, уряди, міжнародні організації, менеджери кібер-майданчиків, неурядові організації та, що найважливіше, глобальна група користувачів. та групи.

Протягом відносно короткого періоду часу на те, що спочатку було нейтральною сферою взаємодії, створеної технологічними інноваціями, що надходять переважно зі Сполучених Штатів, потрапили, якщо не домінували, політичні суперечки, як у Сполучених Штатах, так і в інших країнах. Зараз кіберсфера є місцем конкуренції між інтересами та групами інтересів, а також ареною конфліктів і суперечок навколо все більш помітної руки уряду. Ми більше не можемо ігнорувати політичну значимість кіберпростору: як зауважив один проникливий спостерігач, кіберпростір стає «сильно суперечливим, колонізованим і зміненим урядами, військовими, а також приватними корпоративними та громадянськими мережами [53].

Кіберполітика

Усі міжнародні відносини так чи інакше пов'язані з політикою, неявно чи явно. Закони політики, хоча й є предметом дебатів серед деяких політологів, загалом стосуються закономірностей людської поведінки в часі та просторі. Часто варіації пояснюють через область проблеми, емпіричний референт, конкретні модальності або винятковість, якщо відзначити деякі з найбільш поширених термінів. Оскільки досі немає вирішального викладу чи опису кіберполітики, мова та поняття, які ми використовуємо, є знайомими для політики в кінетичних сферах. Поєднання визначення політики Лассвелла (1958) як авторитетного розподілу цінностей у суспільстві з суворим твердженням Девіда Істона (1953) про те, хто що, коли і як отримує,

приводить нас до найбільш загального та відповідного погляду на політику, релевантного. в усіх контекстах, часах і місцях. Зі створенням кіберпростору формується нова арена для ведення політики, і ми цілком можемо бути свідками нової форми політики. Ці подвійні уявлення про природу політики, спочатку сформульовані для окремого державного устрою чи національної держави, мають потужне значення, яке можна легко перенести на міжнародну арену. Вони також вміло привертають нашу увагу до проблемних сфер, де домінує політика двозначності, сфер, де сфера нечітка, а ставки не чітко визначені [51].

Ми також повинні мати на увазі, що політика полягає в «більш-менш неповному контролі людської поведінки через добровільні звички підкорятися в поєднанні із загрозою ймовірного застосування» (Deutsch 1968, 17; курсив в оригіналі). Більше того, політика − це «взаємодія загроз примусу, які можна змінити відносно швидко, із існуючими звичками лояльності та дотримання вимог населення, які є потужнішими, але які найчастіше можна змінити лише повільніше». Будь-яка політика, як на кібернетичних, так і на реальних аренах, включає конфлікти, переговори та торг щодо механізмів, інституційних чи інших, для розв’язання суперечок щодо природи певних наборів основних цінностей авторитетним способом.

Від тероризму до кібертероризму

Визначення поняття «тероризм» добре вивчене, визначене та задокументовано. Існує також певний ступінь розуміння значень кібертероризму з популярних ЗМІ, інших вторинних джерел або особистого досвіду. У цій статті розглядається майбутнє кібертероризму – термін, який автор ввів десять років тому, оскільки ознаки технологічної залежності та слабкості формувались у нашому новосвітовому безладді. Справді, це майбутнє здійснилося сьогодні [18].

Обличчя тероризму змінюється. Хоча мотиви залишаються незмінними, зараз ми стикаємося з новою і незнайомою зброєю. Системи розвідки, тактика, процедури безпеки та обладнання, які колись

передбачалися для захисту людей, систем і націй, безсилі проти цієї нової і дуже руйнівної зброї. Більше того, методи боротьби з тероризмом, які вдосконалювали наші світові фахівці роками, неефективні проти цього ворога. Бо цей ворог не нападає на нас з вантажівками вибухівки, не з портфелями із зарином, ані з динамітом, прив'язаним до тіл фанатиків. Цей ворог атакує нас з одиницями і нулями, у місці, де ми є найбільш вразливими: точці, в якій сходяться фізичний і віртуальний світи. Давайте спочатку визначимо ці дві області.

Фізичний світ − це матерія й енергія − світло, темрява, гаряча й холодна, вся фізична матерія − те місце, де ми живемо й функціонуємо.

Віртуальний світ є символічним − істинним, хибним, двійковим, метафоричним уявленням інформації − це місце, в якому функціонують комп'ютерні програми і переміщуються дані.

Фізичний і віртуальний світи за своєю суттю є різнорідними світами. Тепер це перетин, зближення цих двох світів, що формує засіб кібертероризму, нової зброї, з якою ми стикаємося.

Залежність і залежність

Ця конвергенція фізичного і віртуального світів, ця решітка, стає все більшою і складнішою, оскільки ми все більше йдемо в технологічну залежність. Кожен день ми просуваємося вперед із сліпучою швидкістю в комп'ютеризації кожного завдання та процесу, з якими ми стикаємося. Ми стаємо все більш нерозривно залежними та залежними від зближення цих двох світів[39].

Точки зближення:

- Які найбільш очевидні точки зближення?
- Відкривач гаражних воріт.
- Кардіостимулятор.
- Комп'ютерний чіп в автомобілі новітньої моделі.
- Мікрохвильова піч.

Потенційні кібертерористичні акти

Розглянемо деякі приклади кібертерористичних актів. На основі визначень тероризму можна визначити, чи вони насправді є тероризмом:

− Кібертерорист матиме віддалений доступ до систем контролю обробки зернових виробників, змінюватиме рівень добавок заліза, хворіти та вбивати дітей нації, які насолоджуються їжею. Цей CyberTerrorist потім виконуватиме подібні віддалені зміни в процесорі дитячих сумішей. Ключ: кібертерористу не обов'язково бути на заводі, щоб здійснити ці дії.

− Кібертерорист зруйнує банки, міжнародні фінансові операції, фондові біржі. Ключ: люди країни втратять будь-яку довіру до економічної системи. Чи спробує кібертерорист проникнути в будівлю Федеральної резервної системи? Малоймовірно, оскільки арешт буде негайним. Крім того, велика вантажівка тягнеться вздовж будівлі. Однак у випадку з кібертерористом злочинець сидить на іншому континенті, поки економічні системи країни зупиняються. Дестабілізація буде досягнута.

− Кібертерорист атакуватиме наступне покоління систем управління повітряним рухом і зіткнеться з двома великими цивільними літаками. Це реалістичний сценарій, оскільки CyberTerrorist також зламатиме датчики в кабіні літака. Те ж саме можна зробити і з залізничними лініями.

− Кібертерорист дистанційно змінюватиме формули ліків у фармацевтичних виробників. Потенційна втрата життя неосяжна.

− Потім кібертерорист може вирішити дистанційно змінити тиск у газопроводах, що спричинить поломку клапана, а блок передмістя вибухне та згорить. Так само, електрична мережа стає все більш вразливою.

Фактично, кібертерорист переконається, що населення нації не зможе їсти, пити, рухатися чи жити. Крім того, люди, на яких покладено обов'язки захищати свою націю, не матимуть попередження і не зможуть закрити терориста, оскільки цей кібертерорист, швидше за все, знаходиться на іншому кінці світу.

Загалом, спільнота хакерів, що базується переважно в Сполучених Штатах, Європі, на Близькому Сході, в Азії та в країнах колишнього

Радянського Союзу, складається з людей, які бачать процес злому лише як виклик, головоломку. Вони вважають себе не тільки невинними в будь-якому злочині, але, можливо, навіть роблять щось праведне, протистояти темним монолітам корпоративного та урядового світів. Вони вважають, що їх переслідують. Ці люди вважають, що те, що вони роблять, не завдає справжньої шкоди. Щонайменше шкідливі, ці зломщики просто переглядають інформацію. Однак проблеми конфіденційності та військової таємниці можуть перетворити такі проникнення на терористичні акти.

На відміну від інших методів тероризму, кібертероризм є безпечним і прибутковим, і йому важко протистояти без належного досвіду та розуміння розуму кібертерористів. Поєднавши нашу зростаючу вразливість із вибуховим зростанням рівня насильства та збільшенням досвіду, доступного всередині терористичних організацій через нову кров і поза через посередників, ми бачимо, що в точці, де зближуються фізичний та віртуальний світи, старі моделі управління тероризмом застаріло [41].

Які ж методи захисту існують? При створенні програми боротьби з кібертероризмом варто враховувати наступні елементи:

Варто визнати, що, хоча теорії тероризму є правдивими, спосіб, у який ми підходимо до боротьби з тероризмом, у даному випадку, протидії кібертероризму, має змінитися.

− Варто співпрацювати та ділитися розвідданими так, як ніколи раніше.

− Варто заручитися підтримкою тих людей, які розуміють зброю, з якою ми стикаємося, і мають досвід ведення цих війн.

− Варто вивчати нові правила, нові технології та нових гравців.

На жаль, не можна навчитися боротися з цією дуже нетрадиційною війною від того, хто там не був, або від того, хто має досвід у старих способах і старих технологіях. Старі моделі обробки даних, аудиту та комп’ютерної безпеки, які використовуються сьогодні, застаріли. На цьому полі бою, проти цієї зброї, терорист уже далеко попереду. Побудова команди

по боротьбі з кібертерористами має відбуватися в режимі реального часу та динамічно, оскільки зброя буде постійно змінюватися, перетворюючись, намагаючись перемогти вас, ваші системи та ваших людей. Немає жодної повторної обробки, і на відміну від інших терористів, якщо кібертерорист програє сьогодні, він не вмирає — він дізнається те, що не спрацювало, і використає цю інформацію проти вас завтра.

Ex Post Facto

Ефективна система аудиту лише інформує цільового керівника про те, що він отримав удар; можливо, смертельний удар. До цього моменту вже пізно. Настав час діяти. На жаль, через такий відкритий характер цього документа конкретні заходи боротьби з кібертероризмом не можуть бути обговорені. Ці обговорення мають бути зарезервовані для захищених об'єктів.

Контртерористи різного походження зобов'язані рятувати власність і, що ще важливіше, рятувати життя. Проте ми не ізольовані. Ми всі стаємо все більш пов'язаними, залежними та вразливими. Основні речі, які ми сприймаємо як належне (наприклад, їжа, ліки, енергія, повітря, свобода пересування, комунікації, свобода від насильства), знаходяться під загрозою нової зброї кібертероризму.

Тож, зростання рівня проблем кібербезпеки вказує на те, що значні покращення в міжнародних відносинах не будуть помітні найближчим часом. Із зростанням технологічних інновацій кібербезпека стала життєво важливою темою, яка цікавить з точки зору міжнародних відносин. Зпитання кібербезпекистаючи з кожним днем все більш загрозливим для міжнародних відносин, він залишиться в центрі порядку денного лідера в усьому світі [18].

3.2. Вплив кібертероризму на міжнародні відносини на прикладі США

Сполучені Штати залишаються залученими в усьому світі, щоб зробити світ безпечнішим для американців і громадян світу. Але є ще один масштабний конфлікт, який продовжує наростати за розміром і значенням − кібервійна та міжнародна кіберзлочинність відіграють все більшу роль у тому, як ми ставимося до інших країн по всьому світу. Це питання, які стосуються урядів, військових і економіки, і, безсумнівно, залишаються в свідомості американських чиновників.

Кіберкомандування США: глобальна кібер-рука Америки

У червні 2009 року міністр оборони Роберт Гейтс керував створенням кіберкомандування США, в якому буде розміщена вся інфраструктура кібервійни для військових. Шість років потому Cyber Command є найважливішою кібер-засобом федерального уряду і починає відігравати велику роль у глобальному просторі.

Бюджет і зростання

У 2015 році Cyber Command отримало 509 мільйонів доларів і будує величезний сучасний спільний операційний центр за межами Форт-Мід в Меріленді. Звіт від «Новини оборони» описав нову кіберстратегію, оголошену на початку 2015 року, на якій буде спиратися цей зростаючий підрозділ. «Стратегія наголошує на стримуванні та спирається на сектор комерційних технологій, спираючись на поштовх до зміцнення зв'язків між Силіконовою долиною та Пентагоном», – йдеться в повідомленні Defense News [14].

Пошуки ефективного стримування

Основна проблема, з якою зараз стикається Cyber Command, полягає в тому, що вона намагається одночасно побудувати свою роботу та захистити від кібератак. Адмірал Майкл Роджерс, лідер кіберкомандування, заявив комітету Сенату з питань збройних сил у березні, що групі необхідно дістатися до «точки стримування». Це було підтвердженням того, що операція ще не була повністю обладнана для боротьби з перевантаженням кібератак на урядові цілі.

Атака на Управління персоналом у квітні викрила чотири мільйони нинішніх і колишніх федеральних службовців. Вторгнення було ідеальним прикладом атаки, від якої кібер-командування сподівається захиститися в міру її зростання. Безсумнівно, що подальша популярність угруповання матиме вплив на міжнародні відносини з кібер-агресорами, такими як Китай, Північна Корея та інші держави.

Міжнародна кіберзлочинність і зовнішня політика

Оскільки кібервійна стала більшою частиною міжнародних відносин, США довелося включити її в конкретні відносини з іншими країнами. Це стало особливо важливим для країн, чиї відносини зі США стали напруженими та суперечливими.

Китай

США отримують понад 5000 кібератак на годину, більшість з яких відбувається з Китаю. Цей потік атак з Далекого Сходу став серйозним предметом суперечки між Білим домом і Пекіном.

Реальність така, що масштаби китайських атак на американські об'єкти абсолютно масові. У 2010 році Google був одним із перших, хто повідомив, що китайські хакери націлені на атаки на її кіберінфраструктуру. Відтоді кілька компаній повідомили про атаки, включаючи Northrop Grumman, Symantec, Yahoo, Dow Chemical та Adobe Systems. Ці атаки зосереджені як на військових, так і на комерційних інтересах і, як правило, зосереджуються на секторах, у яких китайці відстають від США.

Злами, що тривають, були основною частиною вересневого саміту між двома сторонами, особливо після того, як американські чиновники приписували китайцям недавній злам Управління персоналом. Обама і Цзіньпін досягли консенсусу щодо кібербезпеки після двох днів переговорів. Проте ще невідомо, чи підкріплять китайці свої слова діями[37].

Росія

Хоча більша частина нинішньої напруженості між Росією та США зосереджена на війнах в Україні та Сирії, росіяни також причетні до багатьох

кібератак на кіберсистеми США. Про це повідомила компанія з кібербезпеки CrowdStrike у квітні всього за чотири місяці було зафіксовано понад 10 000 російських вторгнень у всьому світі. На сьогодні, Росія позиціонує себе не лише як країна-агресор та міжнародний терорист, а й як кібертерорист.

Здається, росіяни посилили свої атаки після того, як високорозвинені країни, у тому числі і США, ввели санкції через втручання в Україну. The Hill повідомляє, що ця нова хвиля кібератак вражає «найвищі рівні уряду США». Це збільшення порівняно з обмеженими масштабами атак, які Америка бачила з боку Кремля в минулому.

Кібертерористи

Багато з кібератак на США походять не від держави, а від терористичних груп. Довгий час говорять про загрози з боку різних терористичних груп, які використовують кібервійну, але останнім часом загрози здаються набагато більш присутніми.

Хакери, пов'язані з угрупованням «Ісламська держава», здійснили кілька публічних атак у соціальних мережах. На початку 2015 року ці хакери захопили профілі Newsweek, International Business Times та кількох інших ЗМІ. Вони навіть отримали контроль над Центральним командуванням Сполучених Штатів і обліковим записом Тейлор Свіфт. Вони використовували ці платформи, щоб демонструвати свої повідомлення про пропаганду угруповання «Ісламська держава» та ісламського екстремізму.

Хоча кібертерористи не мають таких можливостей та рівня організації, які мають державні кібератаки, вони є серйозною загрозою, за якою офіційні особи США постійно спостерігають. Оскільки такі групи, як Ісламська держава, продовжують набирати обертів, кібератаки можуть тривати.

Міжнародні ініціативи з кібербезпеки

Значна частина діяльності з кібербезпеки на міжнародному рівні відбувається між більш ніж двома країнами. Міжнародні групи розробили

ініціативи в галузі кібербезпеки, щоб тримати країни-члени на одній сторінці та допомогти покращити глобальну кібербезпеку.

Інтерпол

Міжнародна організація кримінальної поліції, або Інтерпол, є основною міжурядовою організацією, яка сприяє співпраці поліцейських груп через кордони. Інтерпол має швидкозростаючий офіс з кіберзлочинності зі штаб-квартирою в Сінгапурі. Там Інтерпол працює переважно як ресурс, який допомагає професіоналам по всьому світу розвивати складні заходи щодо кіберзлочинності. Три основні ініціативи Інтерполу – це гармонізація розслідувань, нарощування потенціалу та оперативна та криміналістична підтримка.

НАТО

Організація Північноатлантичного договору, або НАТО, також діє в просторі кіберзахисту. Як член-засновник, США прагне допомагати своїм членам брати участь у кіберзахисті. НАТО затвердила свою першу політику кіберзахисту в січні 2008 року і з тих пір розширила свої операції. НАТО працює над тим, щоб її комунікаційні мережі були сумісними з інфраструктурою інших держав-членів, і віддана захисту цих систем.

Майбутнє міжнародних відносин та кібербезпеки

Кібербезпека матиме неймовірний вплив на майбутнє міжнародних відносин. Це безсумнівно вплине на взаємодію США та інших країн на всіх рівнях дипломатії. Світу, безумовно, знадобляться висококваліфіковані професіонали, які знають сферу кібербезпеки, щоб допомогти проводити політику кіберзахисту США [44].

Заходи боротьби з кібертероризмом в США

Адміністрація Байдена-Харріса неодноразово попереджала про можливість участі Росії у зловмисній кіберактивності проти Сполучених Штатів у відповідь на безпрецедентні економічні санкції, які ми запровадили. Зараз з’являються дані розвідки, що Росія може вивчати варіанти потенційних кібератак.

Адміністрація з першого дня визначила пріоритети посилення захисту кібербезпеки, щоб підготувати нашу країну до загроз. Виконавчий указ президента Байдена модернізує оборону федерального уряду та покращує безпеку широко використовуваних технологій. Президент розпочав державно-приватні плани дій для підтримки кібербезпеки секторів електроенергетики, трубопроводів і водопостачання, а також наказав департаментам і агенціям використовувати всі існуючі урядові органи для встановлення нових заходів щодо кібербезпеки та захисту мережі. На міжнародному рівні адміністрація об'єднала понад 30 союзників і партнерів для співпраці з метою виявлення та знищення загроз-вимагачів, згуртувала країни G7, щоб притягнути до відповідальності країни, які приховують зловмисників, а також вжила заходів з партнерами та союзниками, щоб публічно приписувати зловмисну діяльність.

«Ми прискорили нашу роботу в листопаді минулого року, коли президент Росії Володимир Путін посилив свою агресію напередодні свого подальшого вторгнення в Україну, проводячи обширні брифінги та консультації американським компаніям щодо потенційних загроз і захисту кібербезпеки. Уряд США продовжить наші зусилля з надання ресурсів та інструментів приватному сектору, у тому числі через Кампанію CISA «Shields Up».і ми зробимо все, що в наших силах, щоб захистити націю та відповісти на кібератаки. Але реальність така, що більша частина критичної інфраструктури країни належить і керується приватним сектором, і приватний сектор повинен діяти, щоб захистити критичні послуги, на які покладаються всі американці.» − наголосив президент Байден[34].

Адміністрація президента США наголосила усі компанії терміново виконати наступні кроки:

− Обов'язково використовувати багатофакторну аутентифікацію у ваших системах, щоб зловмисникам було важче проникнути у вашу систему;

− Використовувати сучасні засоби безпеки на своїх комп'ютерах і пристроях, щоб постійно шукати та пом'якшувати загрози;

- Звернутися до фахівців із кібербезпеки, щоб переконатися, що системи виправлені та захищені від усіх відомих уразливостей, а також змініть паролі у ваших мережах, щоб раніше вкрадені облікові дані були марними для зловмисників;
- Створювати резервні копії даних і забезпечувати резервні копії в автономному режимі, недоступні для зловмисників;
- Виконувати вправи та розробляти свої плани надзвичайних ситуацій, щоб компанії були готові швидко реагувати, задля мінімізування впливу будь-якої атаки;
- Зашифровувати свої дані, щоб їх не можна було використати в разі їх крадіжки;
- Навчити своїх співробітників звичайним прийомам, які зловмисники використовуватимуть по електронній пошті або через веб-сайти, і заохочувати їх повідомляти, якщо їхні комп'ютери або телефони демонструють незвичайну поведінку, наприклад незвичайні збої або дуже повільну роботу;
- Активно співпрацювати з місцевим офісом ФБР або регіональним офісом CISA, щоб налагодити стосунки до будь-яких кіберінцидентів.

У міру розвитку технологій, терористичні угруповання почали використовувати їх. Сюди входять ракети та безпілотники, які розширюють дальність їх атак і зменшують їхні втрати. Доступні смартфони, соціальні мережі та шифрування – це інші технології, які також розширюють їхні мережі, полегшуючи поширення пропаганди та вербування.

Світ спостерігає за зростанням рівня внутрішнього досвіду та зростання випадків кібертероризму. На відміну від інших методів тероризму, кібертероризм є безпечним і прибутковим, і йому важко протистояти без належного досвіду та розуміння розуму кібертерористів. Поєднавши нашу зростаючу вразливість із вибуховим зростанням рівня насильства та збільшенням досвіду, доступного всередині терористичних організацій через

нову кров і поза через посередників, ми бачимо, що в точці, де зближуються фізичний та віртуальний світи, старі моделі управління тероризмом застаріло[15].

Додаток 1. Інциденти кібератак за останній рік.

Як можна побачити, за останній рік було вчинено велику кількість кібератак. Зміст та мета кожної кібератаки , принаймні на останній рік , наводить на думку, що дійсно, кожна кібератака – спланований акт отримання інформації задля дескридитації супротивника, що знову ж таки доказує те, що кібертероризм – це дійсно інструмент протистояння держав на міжнародній арені.

Розглянемо, як кібертероризм проникає в різні підрозділи країни. За останні декілька місяців, було задокументовано 71 випадків кібератак.

Уряд/держава	23 випадки
Критична інфраструктура/комп’ютерні мережі	19 випадків
Цивільні/фізичні особи	10 випадків
Організації/приватний сектор/корпорації/економіка	10 випадків
Суспільство	3 випадки
Будь-хто/кожний громадянин	3 випадки
Групи громадян	2 випадки
Політичні вибори	1 випадок

Таблиця 1. Референтні об'єкти загрози кібертероризму

Те, що респонденти розділилися на обидва аспекти цього питання – тупінь загрози та референтний об’єкт – було результатом чотирьох факторів.

Пее полягало в важливості конкретного розуміння «загрози». Особливо це стосується тих, хто визначає критичні інфраструктури та комп'ютерні мережі як центр потенційних атак. Таким чином, деякі респонденти посилалися на те, що цілі економіки, транспортні мережі чи енергетичні системи знаходяться під загрозою, здатність суспільства функціонувати буде скалічена, організації паралізовані, а повсякденне життя серйозно порушено. Деякі респонденти посилалися на можливе наслідування терористами останніх подій, таких як атака Stuxnet в Ірані. Інші, навпаки, сформулювали цю загрозу абстрактно, обговорюючи, наприклад, можливість насильства проти людей або власності.

По-третє, частина цього різноманіття було продуктом конкуруючих концепцій кібертероризму. Відтворюючи тенденцію, зазначену в розділі огляду літератури, ті, хто бажає підтримувати ширшу концепцію кібертероризму, визначили низку можливих сценаріїв загроз, що поширюються за межі атак на людей, майно, критичні інфраструктури та основні послуги. Четверо респондентів згадали про кібертерористів, які загрожують національній безпеці шляхом отримання конфіденційної розвідувальної та секретної інформації. Інші згадали терористів, які вчиняють кіберзлочини,

По-чеверте, відповіді респондентів на це запитання також викликали тимчасові проблеми. Таким чином, деякі негативні відповіді були кваліфіковані такими фразами, як «на даний момент» або «зараз». Інші, тим часом, були більш сумнівними, попереджаючи, що кібертероризм може стати значною загрозою, якщо наразі її не буде. Один респондент, наприклад, заявив: «Кібертероризм є потенційною загрозою і потенційно значною. ... [На даний момент кібертероризм — це не загроза, а ризик». Інші досі заявили, що кібертероризм наразі є значною загрозою через те, що терористи можуть робити в майбутньому.

Респонденти, які стверджували, що кібертероризм не становить суттєвої загрози, навели три причини на підтримку своєї позиції. По-перше, троє респондентів вказали на той факт, що кібертероризму (як вони концептуалізували це явище) ніколи не було. Один заявив, що у нас «немає прецеденту та мало показників» для оцінки кібертерористичної загрози. Інший сказав, що «емпіричних доказів майже не існує », додавши, що гіпотетичні сценарії часто є «мисленням блакитного неба». По-друге, шість респондентів заявили, що терористичним організаціям не вистачає здатності атакувати критично важливі інфраструктури та основні послуги. Двоє з них сумнівалися, чи терористи коли-небудь отримають такий рівень знань, у той час як троє інших припустили, що ситуація може змінитися в майбутньому.93 Як коментував один, «Здається, що недержавні суб'єкти (поки що) не мають ноу-хау».

Кібертероризму не вистачає героїчності, наприклад, теракту-смертника, тому він менш привабливий для потенційних терористів. Я думаю, що самоуявлення може бути дуже важливим фактором у процесі радикалізації, і в цьому сенсі кібертерористичні атаки не відповідають цій потребі в тій мірі, в якій це роблять інші форми тероризму.

Коли висновки щодо цього питання обмежуються тими респондентами, які раніше заявляли, що кібертероризм дійсно становить значну загрозу, лише 42 з цієї вибірки з 63 (67 відсотків) вважали, що атака все ще відбулася. Це вказує на важливість дедуктивних міркувань, а також індуктивних висновків у концепціях поточних і майбутніх ризиків. Як і слід було очікувати, враховуючи порівняльну новизну загроз кібербезпеці, минуле не обов'язково розглядається як надійний довідник для розуміння сьогодення чи майбутнього.

Респонденти, які заявили про те, що мали місце кібертерористичні атаки, запропонували низку прикладів, наведених у таблиці 2.

Напади на Естонію	11 респондентів

Stuxnet, Іран	6 респондентів
Напади на Грузію	3 респонденти
Індія-Пакистан	2 респонденти
Анонімний	2 респонденти
РПК Туреччини	1 респондент
Сапатистський спам	1 респондент
Wikileaks	1 респондент
Ізраїль-Газа	1 респондент
Індія (соціальні мережі)	1 респондент
Далай-лама	1 респондент
Бригади Таріка бін Зіяда	1 респондент
Аерокосмічний	1 респондент
Витік австралійських стічних вод	1 респондент
Киргизстан	1 респондент

Таблиця 2. Випадки кібератак на різні суб'єкти.

Випадки кібератак були різноманітні, серед них: крадіжка коштів для фінансування терористичних організацій; підготовка терористичних атак; заклики до домашнього тероризму; напади на осіб, яких уряди сприймають як дисидентів; і кібершпигунство.

Респонденти, які заявили про те, що кібертерористична атака ще не відбулася, прямо не заперечували, що будь-яка з подій у таблиці 2 сталася. Натомість вони зазвичай наводили підстави для сумнівів, що такі атаки можуть бути кібертероризмом. По-перше, вісім респондентів посилалися на конкретне визначення кібертероризму, стверджуючи, що деякі з найпопулярніших кібератак, які мали місце, такі як Stuxnet на Естонію, не були терористичними, оскільки їх не вчинили недержавні групи. Деякі з цих респондентів пояснили далі, припустивши, що атаки, які здійснюються державними акторами, краще розуміти як кібервійну.

По-друге, сім респондентів сказали, що гучні кібератаки не можна кваліфікувати як (кібер)терористичні, оскільки вони не призвели до насильства проти людей або власності. Як пояснив один респондент: «Жодна людина ніколи не загинула чи не була поранена в результаті атаки, здійсненої з використанням комп'ютерного коду з використанням зброї». По-третє, четверо респондентів стверджували, що існує відмінність між кібертероризмом і кіберзлочинністю. Один з них стверджував, що, хоча терористи можуть вчиняти кіберзлочинність з метою сприяння терористичній діяльності, це не робить злочинну діяльність терористичною. З цієї точки зору існує різниця між: (кібертероризмом і кіберзлочинами, вчиненими з терористичними цілями (наприклад, для збору коштів). Інший респондент стверджував, що хактивізм слід відрізняти від кібертероризму, хоча двоє інших респондентів припустили, що діяльність анонімних робить цю відмінність більш проблематичною. По-четверте, четверо респондентів заявили, що кібератаки, які відбулися, не викликали страх у ширшої аудиторії та/або були здійснені не з наміром викликати такий страх. За відсутності елемента залякування чи примусу ці респонденти сказали, що кібератаки не є кібертероризмом. Нарешті, троє респондентів сказали, що у тих, хто вчинив напади на сьогодні, не вистачало політичних чи ідеологічних мотивів, необхідних для того, щоб атака була кваліфікована як (кібер)терористична.

На додаток до вищезгаданого, також важливо відзначити два висновки за аналізом цих подій, які вказують на потенційну відмінність кібертероризму. По-перше, низка респондентів визначила потребу в певних видах експертизи для протидії кібертероризму порівняно з іншими тероризмами. У той час як деякі з них стосувалися довкілля , інші посилалися на необхідність нових типів партнерства між секторами та акторами з усього соціально-політичного спектру. Незважаючи на те, що боротьба з тероризмом завжди розвивалася з часом, і нові типи суб'єктів були залучені в цю сферу державної політики, ці висновки говорять про

дискусію щодо відмінності превентивної діяльності та реагування в цьому конкретному контексті.

Другим аспектом, у якому результати дослідження свідчать про відмінність кібертероризму, є рівень суперечливості цього терміну. Його первинна концепція, тероризм, безумовно, є предметом давніх, застарілих суперечок щодо визначення. Незалежно від того, чи виправдовують конкретні напади чи використання насильства, ця термінологія викликає гарячі дискусії: не в останню чергу стосовно «державного тероризму». Існують також дискусії щодо об'єктивного чи суб'єктивного статусу позначення акту як «терористичного» та щодо ймовірності майбутніх атак. Проте, незважаючи на це, було б важко знайти дослідника, який би стверджував, що це було ніколи не відбувалося. На відміну від цього, половина респондентів цього опитування вважала, що кібертероризм вже відбувся, а інша половина – ні.

ВИСНОВКИ

З огляду на широке занепокоєння з приводу кібертероризму та часте використання терміну «кібертероризм» в даний час, багато міжнародних організацій доклали зусиль для боротьби з цією загрозою. Оскільки кібертероризм є міжнародним злочином, самі місцеві правила не можуть захистити від таких атак; вони потребують транснаціональної реакції. Таким чином, країна, на яку здійснено напад, буде посилатися на міжнародне право, щоб домагатися справедливості за будь-яку заподіяну шкоду, використовуючи універсальну юрисдикцію. Без допомоги міжнародних організацій важко запобігти кібертероризм. При цьому міжнародні організації визначають, який державний або міжнародний суд, має повноваження вирішувати спір. Метою було дослідження ефективності та достатності поточних глобальних заходів реагування на кібертероризм через здійснення міжнародної юрисдикції. Також було розглянуто поняття кібертероризму як транснаціонального злочину та міжнародної загрози; таким чином, національні норми самі по собі не можуть цьому запобігти. Потреба в міжнародній організації для запобігання та захисту націй від кібертерористичних атак є нагальною. У цій роботі встановлено, що, оскільки кібертероризм є транснаціональним злочином, він повинен підлягати універсальній юрисдикції через багатонаціональне співробітництво, і це буде найбільш підходящим методом протидії майбутнім транснаціональним злочинам, таким як кібертероризм.

Не існує єдиного підходу до боротьби з кібертерористами та використанням Інтернету терористичними групами. Натомість було запропоновано кілька рішень. Як було доведено вище, оскільки справи кібертероризму носять транснаціональний характер, лише за кордоном міжнародний консенсус і глобальні спільні зусилля щодо криміналізації

терористичних дій у всіх їх формах, що реалізується шляхом здійснення універсальної юрисдикції міжнародних судів, здатні довести кібертерористів до правосуддя. Більше того, він може створити функціональну правову базу, яка охоплює всі пов'язані з цим питання, які були вирішені. Надзвичайно важливо, щоб країни мали спільне юридичне визначення терміну «кібертероризм», щоб реагувати на такі види транснаціональної злочинності. Визначення та визнання «кібертероризму» як проблеми, на основі його унікальних характеристик не тільки полегшує процес розслідування, але й сприяє співпраці між країнами. Разом із тим, необхідно знайти радикальний підхід, щоб відповісти на реальні проблеми, які стосуються глобальної природи кібертероризму. Стверджується, що справжня проблема полягає в тому, що потрібна глобальна та узгоджена відповідь, щоб оголосити кібертероризм міжнародним злочином проти людства.

Інформація, як сукупність знань про фактичні дані і залежності між ними, стала стратегічним ресурсом, основою для прийняття будь-якого рішення. В інформаційних системах, які створюються в органах державної влади і у комерційних структурах, циркулює інформація, що містить секретні відомості про досягнутий потенціал в області економіки, оборони, науки і техніки, конфіденційні відомості про управлінську, господарську, комерційну, фінансову й іншу діяльність. Відповідно захист інформації – складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв’язку, що набуває особливої гостроти.

Кібертероризм дійсно є засобом протистояння держав на міжнародній арені, адже анонімність та швидке розповсюдження інформації в мережі Інтернет дає змогу зловмисникам активно діяти онлайн та отримувати кошти на скоєння терору через дані джерела.

Останнім часом співтовариству з кібербезпеки стало відомо про численні спроби імітувати інформаційні програми, а також про те, що шкідливі дії можуть відбуватися під красивою картою зараження або

вигаданим «радаром зараження». Іншими словами, такі програми виконують роль троянів віддаленого доступу на пристроях користувачів. Коли троян встановлено на пристрої, актор загрози не тільки здатний фіксувати та маніпулювати конфіденційними даними, але також може виконувати цілий ряд шпигунських дій. Незважаючи на те, що такі кампанії спостерігалися у всьому світі, здається, що спроби розпочати подібні атаки зростають лише в певних регіонах і лише тоді, коли в цьому регіоні спостерігається черговий сплеск інфекцій COVID-19. Іншими словами, кампанії із загрозами безпосередньо корелюють із кількістю заражень та сприйняттям пандемії громадськістю – коли люди відчувають більше занепокоєння, актори загроз посилюють свою експлуатацію теми COVID-19.

Незважаючи на те, що існує багато договорів, жоден з них не передбачає обов'язкової нормативної юрисдикції. Більшість із них стосується обмежених територій і застосовуються на регіональному рівні. Організація Об'єднаних Націй та Інтерпол сприяють безпеці та намагаються запобігти та усунути кіберзлочинність на міжнародному рівні. Найважливішим договором у цій справі є Конвенція про кіберзлочинність . Хоча Конвенція про кіберзлочинність класифікується як регіональні зусилля у боротьбі з кібертероризмом, вона відіграє важливу роль у цьому випадку, оскільки ряд країн розташовані за межами її регіони ратифікували та стали членами Конвенції. Однак найвідоміший договір у сфері кіберзлочинності не охоплює кібертероризм.

Таким чином, оскільки він не пропонує персональну та територіальну юрисдикцію щодо кібертероризму, найкраще було б додати Протокол, що стосується кібертероризму. Нарешті, багатосторонні організації мають на меті покращити свою безпеку шляхом гармонізації законодавства, координації та співпраці в правоохоронних органах. і використання прямих і непрямих анти-кібертерористичних дій. Різні заходи, проілюстровані в цій статті, вказують на необхідність гармонізації законів, щоб не допустити

використання транснаціональних злочинців юрисдикційних і правових лазівок між країнами, забезпечуючи менше можливостей для них.

Розгортання заходів кібербезпеки в масштабах держави відбувається на кількох окремих рівнях. Це – рівень Уряду, який задає стратегію кібербезпеки в цілому, рівень об'єктів критичної інфраструктури та державних корпорацій, які передусім потребують захисту, а опісля – рівень приватних компаній та груп, що мають відчувати підтримку держави та водночас дотримуватись правил та норм інформаційної безпеки, наявних у законодавстві. Така схема організації розгалуженого захисту країни є достатньо ефективною та дозволяє: розподілити пріоритети захисту, виявити та нейтралізувати потенційні уразливості у інфраструктурі вищого рівня, розподілити повноваження: який орган і що має захищати, а також створити законодавство, здатне відповідати світом кібернетичним загрозам світу.

На мою думку, для ефективної боротьби з кіберзагрозами варто впровадити не лише закони, які дозволяють затримувати та переслідувати кіберзлочинців та кібертерористів. Варто роглянути можливість створення та впровадженння процедури, які дозволять поліції та іншим державним агентам точно аналізувати «звичайні» кіберзагрози (кіберзлочинність) і «нерутинні» кіберзагрози (кібертероризм і кібервійна). В сучасному світі існують дуже багато загроз для людства: ядерна зброя, війни, глобальне потепління, тому коли із розвитком суспільства з'являються нові загрози, ми повинні прилаштовуватись та знаходити шляхи протидії новим видам атак. Коли під час ведення війни злочинці отримують можливість отримувати, передавати інформацію, розповсюджувати ідеї тероризму – це веде до реальної глобальної загрози, саме тому розуміння та протидія кібертероризму на сьогодняшній день є актуальною темою.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Табанський Л. Основні поняття в кібервійні. Mil Strateg Aff. 2011;3(1):75–92. (дата звернення 15.04.2022)

2. Вайнер Н. Кібернетика або контроль і зв'язок у тварини і машини. Лондон: MIT Press; 1948 рік. (дата звернення 15.04.2022)

3. Гібсон В. Нейромант. Лондон: Orion Publishing Co.; 1948. (дата звернення 15.04.2022)

4. Флаттер А. «Кіберсемантика»: чому ми повинні відмовитися від останнього модного слова в дослідженнях безпеки. Кіберполітика. 2018; 3(2):201–16. вебсайт. URL: https://doi.org/10.1080/23738871.2018.1514417 (дата звернення 17.04.2022)

5. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави вебсайт. URL: http://pravolib.pp.ua/informatsionnyiy-terrorizm-15103.html (дата звернення 10.05.2022)

6. Enders W, Sandler T. The political economy of terrorism. 2nd ed. Cambridge: Cambridge University Press; 2012.

7. Hoffman B. Inside terrorism. 3rd ed. New York: Colombia University Press; 2017.

8. Sandler T. Terrorism and counterterrorism: an overview. Oxf Econ Pap. 2015;67(1):1–20. вебсайт. URL: https:// doi. org/ 10. 1093/ oep/ gpu039 (дата звернення 17.04.2022)

9. Anderson D. Shielding the compass: how to fight terrorism without defeating the law. SSRN Electron J. 2013. вебсайт. URL: https:// doi. org/ 10. 2139/ssrn.2292950. (дата звернення 17.04.2022)

10. Greene A. Defining terrorism: one size fits all? Int Comp Law Q. 2017;66(2):411–40. вебсайт. URL: https:// doi. org/ 10. 1017/ S0020 58931 70000 70 (дата звернення 10.05.2022)

11. Хевер С., Тейлор В. Деконструкція тероризму: політика, мова та соціальне представництво. В: Робертс Р, редактор. Просто війна: психологія і тероризм. Лондон: PCCS Books; 2007. с. 199–212 (дата звернення 18.05.2022)

12. Монро К.Р., Крейді Л.Г. Погляд ісламських фундаменталістів і межі теорії раціонального вибору. Політ психолог. 2002;18(1):19–43. вебсайт. URL: https://doi.org/10.1111/0162-895X.00043 (дата звернення 17.04.2022)

13. Лі Р.Д. Релігія та політика на Близькому Сході. 2-е вид. Нью-Йорк: Рутледж; 2013 рік.

14. Фокс Дж. Відділення релігії від держави та секуляризація в теорії та на практиці. Релігійна держава соц. 2011; 39(4): 384–401. вебсайт. URL: https:// doi.org/ 10.1080/ 09637494.2011.621675 (дата звернення 11.05.2022)

15. Нікфар Дж. Глобалізація та майбутнє відносин влади на арабському Близькому Сході: приклад Єгипту та Лівії. Humanit Soc Sci Commun. 2020;7:134. вебсайт. URL: https:// doi. org/ 10. 1057/ s41599-020-00631-7 (дата звернення 15.05.2022)

16. Стоккетті М. Політика страху: критичне дослідження ролі насильства в політиці 21 століття. В: Ходжес А, Нілеп С, редактори. Дискурс, війна і тероризм. Амстердам: видавнича компанія Джона Бенджаміна; 2007. с. 223–48 (дата звернення 12.05.2022)

17. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами вебсайт. URL: http://www.lj.kherson.ua/ 2015/pravo06/part_3/16.pdf (дата звернення 17.04.2022)

18. Aliiev M.M., Slashchova Y.I. Information support for the international conflict settlement process in Ukraine // The Eighth World Congress «AVIATION IN THE XXI-st CENTURY» Safety in Aviation And Space Technologies, National Aviation University, October 10-12, 2018. – K., 2018. – Режим доступу:

http://congress.nau.edu.ua/doc/congress-2018/Congress_program_2018.pdf. (дата звернення 11.05.2022)

19. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2018. Вип. 1-2 (10-11). С. 276–282 (дата звернення 11.05.2022)

20. Фольц до н.е. Кібертероризм, комп'ютерна злочинність і реальність. Inf Manag Comput Secur. 2004;12(2):154–66. вебсайт. URL: https:// doi.org/10.1108/09685220410530799. (дата звернення 11.05.2022)

21. Холт Т. Дослідження перетину технологій, злочинності та терору. Терор Політ Насильство. 2012;24(2):337–54. вебсайт. URL: https:// doi.org/10.1080/09546553.2011.648350 (дата звернення 11.05.2022)

22. Conway M. Reality check: assessing the (un)likelihood of cyberterrorism. In: Chen TM, Jarvis L, Macdonald S, editors. Cyberterrorism: understanding, assessment, and response. Berlin: Springer; 2014. p. 103–21 (дата звернення 11.05.2022)

23. Denning DE. A view of cyberterrorism 5 years later. In: Himma KE, editor. Internet security: hacking, counterhacking, and society. Burlington: Jones and Bartlett Publishers; 2006. p. 123–39 (дата звернення 12.05.2022)

24. Lehto M, Huhtinen A, Jantunen S. The open definition of cyber: technology or a social construction? Int J Cyber Warf Terror. 2011;1(2):1–9. вебсайт. URL: https://doi.org/10.4018/ijcwt.2011040101 (дата звернення 12.05.2022)

25. Luiifj E. Definitions of cyber terrorism. In: Staniforth A, Bosco F, editors. Cyber crime and cyber terrorism investigator's handbook. Amsterdam: Elsevier Science; 2014. p. 11–7 (дата звернення 12.05.2022)

26. Plotnek JJ, Slay J. Cyber terrorism: a homogenized taxonomy and definition. Comput Secur. 2021;102:1–9. вебсайт. URL: https://doi.org/10. 1016/j.cose.2020.102145 (дата звернення 12.05.2022)

27. Choi KS, Lee CS. The present and future of cybercrime, cyberterrorism, and cybersecurity. Int J Cybersecur Intell Cybercrime. 2018;1(1):1–4.

28. Cohen LE, Felson M. Social change and crime rate trends: a routine activity approach. Am Sociol Rev. 1979;44(4):588–608. вебсайт. URL: https://doi.org/10.2307/2094589 (дата звернення 12.05.2022)

29. Jaishankar K. Establishing a theory of cyber crimes. Int J Cyber Criminol. 2007;1(2):7–9. вебсайт. URL: https:// doi. org/ 10. 5281/ ZENODO. 18792 (дата звернення 15.05.2022)

30. Enders W, Sandler T. The political economy of terrorism. 2nd ed.Cambridge: Cambridge University Press; 2012 (дата звернення 17.05.2022)

31. Choi KS. Computer crime victimisation and integrated theory: an empirical assessment. Int J Cyber Criminol. 2008;2(1):308–33

32. Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. Int J Forensic Sci Pathol. 2016;4(7):253–8. вебсайт. URL: https:// doi.org/10.19070/2332-287X-1600061 (дата звернення 17.05.2022).

33. Suler J. The online disinhibition effect. Cyber Psychol Behav. 2004;7(3):321–6. вебсайт. URL: https://doi.org/10.1089/1094931041291295 (дата звернення 17.05.2022)

34. Jaishankar K. Establishing a theory of cyber crimes. Int J Cyber Criminol. 2007;1(2):7–9. вебсайт. URL: https:// doi. org/ 10. 5281/ ZENODO. 18792 (дата звернення 17.05.2022)

35. Agustina JR. Understanding cyber victimization: digital architectures and the disinhibition effect. Int J Cyber Criminol. 2015;9(1):35–54. вебсайт. URL: https://doi.org/10.5281/zenodo.22239 (дата звернення 17.05.2022)

36. Lee CS, Choi KS, Shandler R, Kayser C. Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. J Contemp Crim Justice. 2021;37(3):333–55. вебсайт. URL: https://doi.org/ 10.1177/10439862211001606. (дата звернення 11.05.2022)

37. Stalans LJ, Finn MA. Understanding how the internet facilitates crime and deviance. Vict Offenders. 2016;11(4):501–8. вебсайт. URL: https:// doi.org/10.1080/ 15564886.2016.1211404 (дата звернення 12.05.2022)

38. Crown Prosecution Service. Terrorism. 2021. вебсайт. URL: https:// www. cps. gov.uk/crime-info/terrorism (дата звернення 13.05.2022)

39. Helbing D, Brockmann D, Chadefaux T, Donnay K, Blanke U, Woolley-Meza O, Moussaid M, Johansson A, Krause J, Schutte S, Perc M. Saving human lives: what complexity science and information systems can contribute. J Stat Phys. 2014;158:73581. вебсайт. URL: https://doi.org/10.1007/s10955-014-1024-9 (дата звернення 13.05.2022)

40. Біда Д., Халаві Л. Кіберпростір: місце для тероризму. Проблеми Inf Syst. 2015;16(3):33–42 (дата звернення 05.05.2022)

41. Арора Б. Дослідження та аналіз злочинів в Інтернеті та їх поведінки. Perspect Sci. 2016;8:540–2. вебсайт. URL: https://doi.org/10.1016/j.pisc.2016.06.014 (дата звернення 14.05.2022)

42. Марсілі М. Війна з кібертероризмом. Democr Secur. 2018;15(2):172–99. вебсайт. URL: https://doi.org/10.1080/17419166.2018.1496826 (дата звернення 13.05.2022)

43. Луїф Е. Визначення кібертероризму. В: Станіфорт А, Боско Ф, редактори. Посібник для слідчого з питань кіберзлочинності та кібертероризму. Амстердам: Elsevier Science; 2014. с. 11–7 (дата звернення 20.05.2022)

44. For a more detailed analysis of these problems see U. Sieber, The Threat of Cybercrime, in : Council of Europe (ed.), Organized Crime in Europe, Strasbourg 2005, pp. 81–218 (212–218) (дата звернення 11.05.2022)

45. Council Framework Decision on Combating Terrorism (2002/475/ JHA of 13.6.2002), OJ L 164/3 of 22.6.2002 (дата звернення 17.05.2022)

46. Council of Europe Parliamentary Assembly, Recommendation 1706 (2005) of 20.6.2005 on “Media and Terrorism.” (дата звернення 17.05.2022)

47. Zanini, M. & Edwards, S. J. A. (2001). The Networking of terror in the information age. In J. Arquilla & D. Ronfelt (Eds), Networks and netwars, (pp.29-60). Santa Monica, CA: RAND Corporation (дата звернення 19.05.2022)

48. WordReference.com Dictionary. (2000). Definition of vulnerability. Retrieved from March 10, 2020. вебсайт. URL: http://www.wordreference.com (дата звернення 21.05.2022)

49. ИТАР-ТАСС. (2016). Крупные атаки хакеров в 2001-2016 годах. вебсайт. URL: http://tass.ru/info/1408961[Accessed: 16. 12. 17.] (дата звернення 01.05.2022)

50. Андрей, Н. (2012). Борьба Вокруг Проекта Конвенции ООН О Международной Информационной Безопасности. вебсайт. URL: https://www.fondsk.ru/news/2012/07/14/borba-vokrug-proekta-konvencii-oono-mezhdunarodnoj-informacionnoj-bezopasnosti-15499.html[Accessed: 14. 12. 17.] (дата звернення 01.05.2022)

51. Алієв М.М. Публічна дипломатія держав світу: порівняльний аналіз // Комунікативні проблеми сучасних міжнародних відносин: зб. матеріалів міжн. наук.-практ. конф., 11 квітня 2017 року, м. Київ. – К., 2017. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31517 (дата звернення 01.05.2022)

52. Алієв М.М., Куньо А.М. «Проблема кіберзлочинності та шляхи її подолання у сучасному інформаційному суспільстві» // XI Міжнародна науково-технічна конференція «АВІА-2013» 21-23 травня 2013 р. – К.: НАУ, 2013. – Т.6. – С. 36.5-36.8. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31516 (дата звернення 07.05.2022)

53. Ржевська Н.Ф. Роль глобалізації в транснаціоналізації політичної експертизи та прогнозування / Н. Ржевська. – «Політікус». Науковий журнал. – 2016. – № 1. – С.59-70. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31106

54. Ржевська Н.Ф. Американські аналітичні центри як суб'єкти прогнозування зовнішньої політики / Н. Ф. Ржевська // Проблеми міжнародних відносин: Збірник наукових праць. – Вип. 10-11 . – К.: КиМУ, 2015. – С. 316- 332. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31098

55. Троян С.С. Концептуалізація сучасних міжнародних відносин // Матеріали Міжнародної науково-практичної інтернет-конференції «Міжнародні відносини: історія, теорія та практика» (28 лютого 2019 року). - Суми.: ФОП Цьома С.П., 2019. - С. 140 – 143. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/43352

56. Міжнародні регіональні процеси та зовнішньополітичні пріоритети України : монографія / за заг. ред. професорів С. Шергіна і В. Космини. – Київ: Дипломатична академія України при МЗС України, 2017. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31672

57. Ричка М.А., Попова Ю.О. Стратегія розвитку України (економіка, соціологія, право). – 2015. – № 2. – С. 112-119. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/29906

58. Кияниця Л.Л. Міжнародна анархія та міжнародно-політична поведінка держав: до концептуалізації проблеми / Л.Л. Кияниця // Вісник Львівського університету. Серія «Філософсько-політологічні студії». – 2017. – Вип. 12. – С. 195-202. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31086 (дата звернення 22.05.2022)

59. Кияниця Л.Л. Регіональне співвідношення сил у контексті теорії регіональних комплексів безпеки (ТРКБ) / Л.Л. Кияниця // Гілея: науковий вісник: Зб-к наукових праць. – К., 2014. –Випуск 87 (№ 8). – С. 349-353. вебсайт. URL: http://er.nau.edu.ua/handle/NAU/31083 (дата звернення 22.05.2022)

60. Лобода С. М. , Кириленко А.Ю. Навчально-методичний комплекс з дисципліни "Методи наукових досліджень". вебсайт. URL: http://er.nau.edu.ua/handle/NAU/36349 (дата звернення 22.05.2022)

61. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016#n11 (дата звернення 22.05.2022)

62. Про національну безпеку України: Закон України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 22.05.2022)

ДОДАТКИ

Додаток 1. Інциденти кібератак за останній рік.

Березень 2022 року.	Хакери використали DDoS-атаку, щоб закрити Національне управління телекомунікацій Маршаллових островів. Атака порушила роботу Інтернету на островах понад тиждень.
Березень 2022 року.	Хакери, пов'язані з урядом Пакистану, атакували індійських державних службовців під час шпигунської операції. Група також створила підроблені урядові та військові веб-сайти для доставки шкідливого програмного забезпечення своїм цілям.
Березень 2022 року.	Атака на супутниковий широкосмуговий доступ, яким керує американська компанія Viasat, призвела до порушення інтернет-послуг по всій Європі, включаючи українські військові комунікації на початку російського вторгнення. Зловмисники зламали супутникові модеми, що належать тисячам європейців, щоб порушити роботу служби компанії.
Березень 2022 року.	Хакери проникли на веб-сайти кількох російських агентств, включаючи Міністерство енергетики, Федеральну службу державної статистики, Федеральну службу виконання покарань і Федеральну службу судових приставів. На веб-сайтах було розміщено кілька антиурядових зображень і повідомлень проти вторгнення, перш ніж агентства змогли вигнати зловмисників.
Березень	Міністерство юстиції США висунуло звинувачення

2022 року.	чотирьом російським державним службовцям, причетним до хакерських кампаній, які мали місце в період з 2012 по 2018 рік. Ці зловживання були спрямовані на компанії та організації критичної інфраструктури, переважно в енергетичному секторі. Хакери намагалися встановити бекдори та розгорнути шкідливе програмне забезпечення в операційній технології своїх цілей.
Березень 2022 року.	За даними російського міністерства цифрового розвитку та комунікацій, хакери зіпсували та зламали кілька російських урядових і державних медіа-сайтів. Сайт МНС зламали, і зловмисники писали повідомлення, в яких закликали російських солдатів до переходу. Також було проникнуто державне інформаційне агентство ТАСС, і хакери закликали людей «вийти на вулиці проти війни».
Березень 2022 року.	Національна дослідницька рада, найбільша дослідницька агенція Канади, яка фінансується державою, поділилася, що хакери проникли в її мережі. У повідомленні на веб-сайті Ради пояснювалося, що частина її онлайн-присутності була вимкнена в результаті цього інциденту.
Березень 2022 року.	Хакери, пов'язані з китайським урядом, в рамках шпигунської операції проникли в мережі, що належать державним установам щонайменше 6 різних штатів США. Хакери скористалися вразливістю Log4j для доступу до мереж, а також кількома іншими вразливими веб-програмами, що працюють в Інтернеті.
Березень 2022 року.	Хакери використали DDoS-атаку, щоб націлитися на великого ізраїльського провайдера телекомунікацій. У результаті кілька урядових веб-сайтів Ізраїлю були вимкнені.
Лютий 2022 року.	Дослідники виявили кампанії двох підтримуваних урядом Північної Кореї груп, націлених на співробітників численних

	медіа, фінтех- та програмних компаній. Хакери використовували фішингові електронні листи, рекламуючи фальшиві вакансії, і скористалися вразливістю в Google Chrome, щоб зламати веб-сайти компаній і поширювати шкідливе програмне забезпечення.
Лютий 2022 року.	Сайти Кабінету міністрів України та Міністерства закордонних справ, інфраструктури та освіти були порушені за кілька днів до вторгнення російських військ в Україну. Зловмисне програмне забезпечення Wiper також було використано для проникнення в мережі однієї української фінансової установи та двох державних підрядників.
Лютий 2022 року.	Пекінська компанія з кібербезпеки звинуватила Агентство національної безпеки США у створенні бекдора для моніторингу компаній і урядів у більш ніж 45 країнах світу. Речник міністерства закордонних справ заявив, що подібні операції можуть загрожувати безпеці критичної інфраструктури Китаю та порушити комерційну таємницю.
Лютий 2022 року.	15 лютого DDoS-атака вибила з мережі веб-сайти Міністерства оборони України та двох найбільших банків країни. США та Велика Британія приписують напад російському ГРУ. В Українській кіберполіції заявили, що атака була пов’язана з іншою «інформаційною атакою», коли громадяни України отримували спам-повідомлення про те, що банкомати не працюють.
Лютий 2022 року.	Пекінська компанія з кібербезпеки звинуватила Агентство національної безпеки США у створенні бэк-дора для моніторингу компаній і урядів у більш ніж 45 країнах світу. Речник міністерства закордонних справ заявив, що подібні операції можуть загрожувати безпеці критичної інфраструктури

	Китаю та порушити комерційну таємницю.
Лютий 2022 року.	Пакистанська група розгорнула троян віддаленого доступу для шпигунства проти індійських військових і дипломатичних цілей. Група зазвичай використовує соціальну інженерію та/або USB-хробаків для проникнення в мережу.
Лютий 2022 року.	Група, пов'язана з Іраном, здійснювала шпигунство та інші зловмисні кібероперації проти низки приватних компаній та місцевих і федеральних урядів.
Лютий 2022 року.	Загрози, пов'язані з Кремлем, зламали численні оборонні підрядники в період із січня 2020 року по лютий 2022 року. Хакери збирали та викрадали електронні листи та конфіденційні дані, що стосуються продуктів та інформації компаній, а також взаємодії з іноземними урядами.
Лютий 2022 року.	Кілька нафтових терміналів у деяких з найбільших портів Європи в Бельгії та Німеччині стали жертвами кібератаки, через що вони не могли обробляти баржі, що надходять. Вимагання, пов'язані з російськомовною хакерською групою, були використані, щоб порушити здатність енергетичних компаній обробляти платежі.
Лютий 2022 року.	З жовтня 2021 року хакерська група атакувала палестинських осіб та організації з використанням шкідливих програм. Дослідники припускають, що операція може бути пов'язана з більш широкою кампанією хакерської групи, яку зазвичай приписують кібер-підрозділу ХАМАС, яке почалося в 2017 році.
Лютий 2022 року.	У звіті ООН стверджується, що хакери Північної Кореї вкрали понад 50 мільйонів доларів у період з 2020 по середину 2021 року з трьох бірж криптовалют. У звіті також додається, що в 2021 році ця сума, ймовірно, збільшилася, оскільки КНДР

	здійснила 7 атак на криптовалютні платформи, щоб допомогти фінансувати свою ядерну програму в умовах значного режиму санкцій.
Лютий 2022 року.	Розслідування під керівництвом Mandiant виявило, що хакери, пов'язані з китайським урядом, зламали облікові записи електронної пошти, що належать журналістам Wall Street Journal. Хакери нібито спостерігали та вилучали дані з газети більше двох років, починаючи принаймні з лютого 2020 року.
Лютий 2022 року.	Мережі міністерства закордонних справ Великобританії були проникнуті хакерами. Усі деталі інциденту залишаються конфіденційними.
Січень 2022 року.	Група білоруських активістів увійшла в мережі державної Білоруської залізниці. Група зашифрувала більшість серверів Залізниці та знищила дані, що зберігалися на резервному сервері, можливо, щоб ускладнити переміщення російських військ по всій країні.
Січень 2022 року.	Китайська хакерська група зламала кілька німецьких фармацевтичних і технологічних фірм. За словами уряду Німеччини, злом мереж постачальників послуг і компаній був перш за все спробою вкрасти інтелектуальну власність.
Січень 2022 року.	Хакери двічі за два тижні закривали інтернет-трафік до та з Північної Кореї через, за словами дослідників, серію DDoS-атак. Другий напад стався відразу після 5 нападу Північної Кореїthракетне випробування місяця.
Січень 2022 року.	Хакери зламали міністерство закордонних справ Канади, перешкоджаючи роботі деяких служб міністерства, підключених до Інтернету. Злом стався на наступний день після того, як уряд оприлюднив попередження про посилення безпеки мережі в очікуванні кібератак на критично важливу інфраструктуру в

	Росії.
Січень 2022 року.	Серія DDoS-атак була спрямована на турнір Minecraft з високими ставками і в кінцевому підсумку вплинула на Andorra Telecom, єдиного постачальника інтернет-послуг у країні. Атака порушила 4G та інтернет-послуги для клієнтів.
Січень 2022 року.	Інформаційне управління грецького парламенту виявило спробу злому 60 електронних поштових акаунтів парламенту. У відповідь влада тимчасово закрила систему розсилки в законодавчому органі.
Січень 2022 року.	Речник Австралії звинуватив WeChat у тому, що він заблокував обліковий запис прем'єр-міністра Скотта Моррісона та перенаправив користувачів на веб-сайт, який надає інформацію для китайських експатріантів. В Уряді стверджують, що вперше зіткнулися з проблемою розміщення на рахунку прем’єр-міністра в середині 2021 року.
Січень 2022 року.	Хакери зламали системи, що належать Міжнародному комітету Червоного Хреста, отримавши доступ до даних про понад 500 000 людей і порушивши роботу їхніх служб у всьому світі.
Січень 2022 року.	Кібератака була спрямована на український уряд, вразивши 90 веб-сайтів та розгорнувши зловмисне програмне забезпечення, яке маскується під програму-викуп, щоб пошкодити десятки комп’ютерів в державних установах.
Січень 2022 року.	Хакери атакували кілька ізраїльських ЗМІ, включаючи Maariv і Jerusalem Post, розміщуючи на своїх веб-сайтах повідомлення з погрозами. В одному з повідомлень було написано: «Ми поруч з вами, де ви про це не думаєте» англійською та івритом.
Січень	Група, пов’язана з ДРПК, націлила на кількох російських

2022 року.	дипломатів зловмисне програмне забезпечення. Дипломати отримали електронний лист, замаскований під заставку для новорічних привітань, але після відкриття встановив троян віддаленого доступу.
Грудень 2021 року.	Кібератака на міністерство оборони Бельгії змусила частину його комп'ютерної мережі, включаючи поштову систему міністерства, вимкнути на кілька днів. Хакери скористалися вразливістю Log4j, щоб зламати мережу.
Грудень 2021 року.	Протягом останніх 9 місяців хакери атакували кілька урядів Південно-Східної Азії, використовуючи спеціальні зловмисні програми, пов'язані з китайськими державними групами. Багато країн, на які потрапили цілі, зараз ведуть суперечки з Китаєм щодо територіальних претензій у Південно-Китайському морі.
Грудень 2021 року.	Порушення Twitter прем'єр-міністра Моді дозволило хакерам твітити з облікового запису про те, що Індія офіційно прийняла біткойн як законний платіжний засіб. Твіт також містив посилання на шахрайство, яке обіцяло роздачу біткойнів.
Грудень 2021 року.	Розслідування Bloomberg публічно пов'язало вторгнення в телекомунікаційні системи Австралії в 2012 році зі шкідливим кодом, вбудованим в оновлення програмного забезпечення від Huawei.
Грудень 2021 року.	Фірми з кібербезпеки виявили, що пов'язані з урядом хакери з Китаю, Ірану та Північної Кореї намагалися використати вразливість Log4j для отримання доступу до комп'ютерних мереж. Після оголошення Log4j дослідники вже знайшли понад 600 000 спроб використати вразливість.
Грудень 2021 року.	Китайські хакери зламали ще чотири американські оборонні та технологічні фірми в грудні, а також одну

	організацію в листопаді. Хакери отримали паролі для доступу до систем організацій і намагалися перехопити конфіденційні комунікації.
Грудень 2021 року.	Російське угруповання взяло на себе відповідальність за атаку програм-вимагачів на австралійську комунальну компанію CS Energy. Це оголошення з'явилося після того, як австралійські ЗМІ звинуватили в атаці хакерів китайського уряду.
Листопад 2021 року.	Російськомовна група атакувала особисту інформацію близько 3500 осіб, у тому числі урядовців, журналістів та правозахисників. Група отримала доступ до приватних облікових записів електронної пошти та фінансових даних, а також керувала шкідливими програмами на пристроях Android і Windows.
Листопад 2021 року.	Хакери отримали доступ до номерів соціального страхування та водійських прав співробітників після того, як зламали американського оборонного підрядника.
Листопад 2021 року.	Китайські чиновники стверджують, що агентство іноземної розвідки зламало кілька авіакомпаній у Китаї та вкрало інформацію про пасажирів. Чиновники заявили, що хаки пов’язані через використання спеціального трояна в усіх атаках.
Листопад 2021 року.	Після того, як CISA оприлюднила подробиці уразливості, китайські хакери з вересня по жовтень атакували дев’ять компаній і 370 серверів, використовуючи ту саму вразливість.
Листопад 2021 року.	Постачальник, який обробляє дані Лейбористської партії Великобританії, піддався кібератаці, що вплинуло на дані її членів і філій.
Листопад 2021 року.	Хакери отримали доступ до порталу правоохоронних органів ФБР — системи, яка використовується для зв’язку з державними та місцевими чиновниками — і надіслали

	попередження про кібератаку в електронному листі, який стверджував, що надійшов від Департаменту внутрішньої безпеки (DHS).
Листопад 2021 року.	Платформа для біржової торгівлі Robinhood розкрила кібератаку соціальної інженерії, яка дозволила хакеру отримати доступ до особистої інформації близько 7 мільйонів клієнтів. Дані включали імена, електронні адреси, а для деяких — дані про народження та поштові індекси. Після злому хакер запросив платіж, імовірно, щоб не розголошувати вкрадені дані.
Жовтень 2021 року.	Згідно з повідомленням CrowdStrike, пов'язана з Китаєм хакерська група отримала доступ до записів дзвінків і текстових повідомлень від операторів зв'язку по всьому світу. У звіті зазначено, що група почала свої кібератаки в 2016 році і проникла щонайменше в 13 телекомунікаційних мереж.
Листопад 2021 року.	Кібератака була спрямована на випущені урядом електронні картки, які іранці використовують для купівлі субсидованого палива, і змінила текст електронних білбордів, щоб відображати антирежимні повідомлення проти верховного лідера аятоли Алі Хаменеї.
Листопад 2021 року.	Група, пов'язана з Іраном, намагалася зламати понад 250 облікових записів Office 365. Усі цільові облікові записи були або американськими та ізраїльськими оборонними технологічними компаніями, зосередженими на портах входу в Перську затоку, або морськими транспортними компаніями, які присутні на Близькому Сході.
Листопад 2021 року.	Бразильські хакери здійснили кібератаку на веб-сайт Національного центру шкідливих програм, що належить Державному агентству з кібер і паролів Індонезії. Хакери відредагували вміст веб-сторінки та вказали, що кібератака була

	розплатою за індонезійський злам на державний веб-сайт Бразилії.
Листопад 2021 року.	Хакери злили дані та фотографії з Міністерства оборони Ізраїлю після того, як отримали доступ до 165 серверів і 254 веб-сайтів, загалом зібравши близько 11 терабайт даних.
Листопад 2021 року.	Американська компанія оголосила, що Служба зовнішньої розвідки Росії (СВР) запустила кампанію, націлену на торговельних посередників та інших постачальників технологічних послуг, які налаштовують, розгортають і керують хмарними сервісами.
Листопад 2021 року.	Китайські хакери, пов'язані з державою, націлилися на афганського провайдера телекомунікацій Roshan і вкрали гігабайти даних з їхнього корпоративного поштового сервера за останній рік.
Вересень 2021 року.	ЄС офіційно звинуватив Росію в її участі в кіберкампанії «Ghostwriter», яка була спрямована на вибори та політичні системи кількох країн-членів. З 2017 року російські оператори зламали акаунти урядовців у соцмережах та новинні веб-сайти з метою викликати недовіру до військ США та НАТО.
Вересень 2021 року.	Хакери отримали 15 ТБ даних від 8000 організацій, які співпрацюють з ізраїльською компанією Voicenter, і запропонували дані в Інтернеті за 1,5 мільйона доларів. Деякі експерти стверджують, що хакери мають зв'язки з Іраном, але жодного зв'язку не було підтверджено.
Вересень 2021 року.	Міністерство оборони Литви виявило приховані функції в популярних моделях смартфонів 5G, вироблених у Китаї, повідомляє його державний орган з кібербезпеки. Модуль, вбудований у телефони, виявляє та цензурує 449 ключових слів або груп ключових слів, які суперечать повідомленням

	китайського уряду.
Вересень 2021 року.	Через дві години після початку голосування на первинних виборах угорської опозиції виборчі системи у виборчих округах по всій країні стали жертвою кібератаки. Відповідальний актор поки невідомий, але кібератака призвела до того, що уряд продовжив голосування на два дні.
Вересень 2021 року.	Міністерство юстиції США засудило Галеба Алаумарі до понад 11 років в'язниці за допомогу північнокорейським кіберзлочинцям у відмиванні грошей. Його допомога включала операції з виведення готівки в банкоматах, крадіжки банків із підтримкою кібернетики та схеми компромісу ділової електронної пошти (BEC). Ці атаки були спрямовані на банки, професійні футбольні клуби та інші неназвані компанії в США та Великобританії
Вересень 2021 року.	У квітні 2021 року відбулася кібератака на Організацію Об’єднаних Націй, спрямована на користувачів мережі ООН для подальшого довгострокового збору розвідувальних даних. Хакер отримав доступ до їхніх мереж за допомогою вкрадених облікових даних користувачів, придбаних у темній мережі.
Вересень 2021 року.	Уряд Норвегії заявив, що низка кібератак на приватну та державну IT-інфраструктуру була здійснена від поганих акторів, спонсорованих та керованих Китаєм. У їхньому розслідуванні злому стверджується, що актори намагалися захопити секретну інформацію, що стосується розвідки національної оборони та безпеки Норвегії.
Вересень 2021 року.	Дослідники та експерти з кібербезпеки розкрили мобільну шпигунську кампанію проти курдської етнічної групи. Хакери націлювали на людей у Facebook, переконуючи їх завантажувати програми, які містять бекдори Android, які використовуються

	для шпигунства.
Вересень 2021 року.	У квітні 2020 року китайські боти обрушилися на мережі австралійського уряду через кілька днів після того, як Австралія закликала провести незалежне міжнародне розслідування походження коронавірусу. Ці боти шукали потенційні вразливості в мережі, щоб використати їх у майбутніх кібератаках.
Серпень 2021 року.	Кібератака на уряд Білорусі зламала десятки баз даних поліції та міністерства внутрішніх справ. Злом стверджується, що є частиною спроби повалення режиму президента Олександра Лукашенка.
Серпень 2021 року.	Хакерська група націлена на відому іранську в'язницю, виявивши документи, відео та зображення, які демонструють насильницьке поводження з її в'язнями. Група стверджує, що є хактивістами, які вимагають звільнення політв'язнів.
Серпень 2021 року.	З лютого по липень 2021 року група кібершпигунів, пов'язана з однією з російських розвідувальних сил, намагалася ловити слова на уряд Словаччини.
Серпень 2021 року.	Росія націлила та заблокувала вміст у додатку «розумне голосування», створеному критиком Кремля Олексієм Навальним та його союзниками, які мали намір організувати голосування проти Кремля на парламентських виборах наступного місяця.
Серпень 2021 року.	Виявилося, що хакерські дії, які спочатку приписували Ірану в 2019 та 2020 роках, були здійснені китайськими оперативниками. Кібератака вдерлася в комп'ютери уряду і технологічних компаній Ізраїлю.
Серпень 2021 року.	Кібератака на веб-сайт планування вакцинації від Covid-19 для італійського регіону Лаціо змусила веб-сайт тимчасово

	закритися. Протягом кількох днів після нападу не можна було призначити нові прийоми щеплень.
Серпень 2021 року.	Різні китайські кібершпигунські групи несуть відповідальність за злом принаймні п’яти основних постачальників телекомунікацій Південно-Східної Азії, починаючи з 2017 року. Атаки були здійснені трьома різними хакерськими групами, і вони, здавалося б, не пов’язані, незважаючи на те, що всі групи мають зв’язок із китайськими шпигунськими зусиллями.
Липень 2021 року.	Естонія заявила, що хакер із Таллінна завантажив 286 438 фотографій посвідчення особи з урядової бази даних, виявивши вразливість у платформі, керованої їх Управлінням інформаційної системи (RIA).
Липень 2021 року.	Кібератака отримала доступ до 1 терабайта даних від Saudi Arabian Oil Company шляхом використання нульового дня. Хакери пропонують видалити дані в обмін на 50 мільйонів доларів у криптовалюті.
Липень 2021 року.	Проти користувачів у Південно-Східній Азії було виявлено поширену операцію APT, яку, як вважають, очолювали китайські організації. Дослідники знайшли загалом 100 жертв у М’янмі та 1400 на Філіппінах, включаючи багато державних установ.
Липень 2021 року.	Сполучені Штати, Європейський Союз, НАТО та інші світові держави оприлюднили спільні заяви, в яких засуджують уряд Китаю за низку зловмисних кібер-діяльностей. Вони приписують відповідальність Китаю за злом Microsoft Exchange на початку 2021 року і компрометацію понад 100 000 серверів по всьому світу.
Липень	Transnet Port Terminals (TPT), державний портовий

2021 року.	оператор Південної Африки і монополіст на вантажні залізничні перевезення вантажів, перервав роботу залізниць після злому невідомими особами. Повідомляється, що Transnet оголосив це актом «форс-мажор».
Липень 2021 року.	Кілька країн використовували Pegasus, програмне забезпечення для спостереження, створене NSO Group, яке націлено на операційні системи iPhone та Android, на пристроях, що належать активістам, політикам та журналістам.
Липень 2021 року.	ФБР та Агентство кібербезпеки та безпеки інфраструктури США (CISA) оприлюднили заяву, в якій викривають кампанію підводного полювання, яку проводили китайські державні хакери в період з 2011 по 2013 рік. Ця кампанія була спрямована на нафто- та газопроводні компанії в Сполучених Штатах.
Липень 2021 року.	Іран використовував облікові записи Facebook, щоб видавати себе за вербувальників, журналістів і філій НУО, націлюючись на американських військових. Хакери надсилали файли, заражені шкідливим програмним забезпеченням, або обманом обманювали цілі, щоб вони надіслали конфіденційні облікові дані на фішингові сайти.
Липень 2021 року.	Міністерство оборони Росії стверджує, що воно було вражено DDoS-атакою, що спричинило закриття його веб-сайту, заявляючи, що атака була здійснена за межами Російської Федерації.
Липень 2021 року.	Норвегія приписувала Китаю кібератаку на систему електронної пошти парламенту в березні 2021 року.
Липень 2021 року.	Міністерство транспорту та урбанізації Ірану стало жертвою кібератаки, яка вплинула на рекламні табло на станціях по всій країні. Атака спричинила затримки та скасування сотень поїздів по всьому Ірану.

Липень 2021 року.	Російські хакери скористалися вразливістю в програмному забезпеченні адміністратора віртуальних систем/серверів Kaseya (VSA), що дозволило їм розгорнути атаку програм-вимагачів у мережі. Злом вплинув на близько 1500 малих і середніх підприємств, а зловмисники вимагали виплати 70 мільйонів доларів.
Липень 2021 року.	Міністерство оборони України стверджує, що веб-сайт Військово-морських сил України став мішенню російських хакерів, які опублікували фейкові повідомлення про міжнародні військові навчання Sea Breeze-2021.
Червень 2021 року.	Росія заявила, що щорічна телефонна сесія Володимира Путіна була мішенню DDoS-атак.
Червень 2021 року.	Китайомовна хакерська група очолювала триваючу шпигунську діяльність проти афганського уряду за допомогою фішингових листів. Хакери видавали себе за Офіс президента Афганістану та атакували Раду національної безпеки Афганістану.
Червень 2021 року.	Іранський уряд розпочав широкомасштабну кампанію дезінформації, спрямовану на групи WhatsApp, канали Telegram та додатки для обміну повідомленнями, якими користуються ізраїльські активісти. Кампанія була спрямована на розвиток політичних заворушень і недовіри в Ізраїлі.
Червень 2021 року.	Китайські актори націлені на організації, зокрема Verizon і столичний водний район Південної Каліфорнії, використовуючи платформу, яку використовують численні урядові установи та компанії для безпечного віддаленого доступу до своїх мереж.
Червень 2021 року.	Хакери, пов’язані зі Службою зовнішньої розвідки Росії, встановили шкідливе програмне забезпечення в систему Microsoft, що дозволило хакерам отримати доступ до облікових

	записів і контактної інформації. Більшість цільових клієнтів були в США, працюючи на IT-компанії або уряд.
Червень 2021 року.	Уряди США та Великобританії оголосили, що російське ГРУ з 2019 по 2021 рік здійснило серію грубого доступу до сотень державних та приватних об’єктів по всьому світу, націлюючись на організації, які використовують хмарні сервіси Microsoft Office 365®.
Червень 2021 року.	Військово-морський інститут США (USNI) заявив, що дані відстеження двох кораблів НАТО, HMS Defender Королівського флоту Великобританії та HNLMS Evertsen Королівського флоту Нідерландів, були сфальсифіковані біля берегів підконтрольної Росії військово-морської бази в Чорному морі. Підроблені дані визначили два військових кораблі біля входу до великої російської військово-морської бази.
Червень 2021 року.	Як повідомляється, кібератака з Росії зламала поштові скриньки понад 30 відомих польських чиновників, міністрів і депутатів політичних партій, а також деяких журналістів.
Червень 2021 року.	Sol Oriens, невеликий державний підрядник, який працює в Міністерстві енергетики з питань ядерної зброї, зазнав нападу з боку пов'язаної з Росією хакерської групи REvil.
Червень 2021 року.	У WhatsApp витік електронна таблиця, яка містить секретні особисті дані 1182 солдатів спецназу Великобританії.
Червень 2021 року.	Атака програмного забезпечення-вимагача була спрямована на iConstituent, службу інформаційних бюлетенів, яку американські законодавці використовують для зв’язку з виборцями.
Червень 2021 року.	Вважається, що хакери, які працюють від імені російських спецслужб, зламали внутрішню мережу поліції Нідерландів у 2017 році. Атака сталася під час розслідування в країні рейсу 17

	(MH17) Malaysia Airlines, який був збитий у 2014 році.
Травень 2021 року.	LineStar Integrity Services, бізнес, орієнтований на конвеєр, зазнав атаки програмного забезпечення-вимагача в той самий час, що й Colonial Pipeline, і було вкрадено 70 гігабайт його внутрішніх файлів.
Травень 2021 року.	Північнокорейська кібератака на державний Корейський науково-дослідний інститут атомної енергії (KAERI) сталася через вразливість у VPN постачальника.
Травень 2021 року.	Найбільша в світі компанія з переробки м'яса, бразильська JBS, стала жертвою атаки програм-вимагачів. Внаслідок нападу були закриті підприємства в США, Канаді та Австралії. Атаку приписують російськомовній кіберзлочинній групі REvil.
Травень 2021 року.	24 травня хакери отримали доступ до систем Fujitsu і викрали файли, що належать кільком державним установам Японії. Наразі постраждали чотири державні установи.
Травень 2021 року.	Дослідники кібербезпеки визначили північнокорейську хакерську групу, яка відповідальна за кампанію кібершпигуну, спрямовану на високопоставлених урядовців Південної Кореї, використовуючи методологію фішингу. Цілі групи базувалися в Південній Кореї та включали: Корейське агентство Інтернету та безпеки (KISA), Міністерство закордонних справ РК, Посол Посольства Шрі-Ланки в державі (у РК), Офіцер з ядерної безпеки Міжнародного агентства з атомної енергії, Заступник генерального консула в Генеральному консульстві Кореї в Гонконзі, Сеульському національному університеті та Daishin Securities.
Травень 2021 року.	14 травня національна служба охорони здоров'я Ірландії, виконавчий орган охорони здоров'я (HSE), стала жертвою атаки програмного забезпечення-вимагача. Виявивши атаку, державні

	органи закрили систему HSE. Зловмисники використовували програму-вимагач як послугу Conti (RaaS), як повідомляється, керує російська група кіберзлочинців.
Травень 2021 року.	ФБР і Австралійський центр кібербезпеки попередили про триваючу кампанію з викупу Avaddon, спрямовану на кілька секторів у різних країнах. Цільовими країнами є Австралія, Бельгія, Бразилія, Канада, Китай, Коста-Ріка, Чеська Республіка, Франція, Німеччина, Індія, Індонезія, Італія, Йорданія, Перу, Польща, Португалія, Іспанія, ОАЕ, Великобританія, США. Цільові галузі включають: наукові кола, авіакомпанії, будівництво, енергетика, обладнання, фінанси, вантажні перевезення, уряд, охорона здоров'я, це, правоохоронні органи, виробництво, маркетинг, роздрібна торгівля, фармацевтика.
Травень 2021 року.	6 травня Colonial Pipeline, найбільший паливопровід у Сполучених Штатах, став об'єктом атаки програм-вимагачів. Енергетична компанія перекрила трубопровід і згодом заплатила 5 мільйонів доларів викупу. Атаку приписують російськомовній хакерській групі DarkSide.
Травень 2021 року.	4 і 5 травня норвезька енергетична технологічна компанія Volue стала жертвою атаки програмного забезпечення-вимагача. Атака призвела до зупинки водопостачання та очисних споруд у 200 муніципалітетах, що постраждало приблизно 85% населення Норвегії.
Травень 2021 року.	Велика DDoS-атака вивела з ладу інтернет-провайдера, яким користується уряд Бельгії, що вплинуло на понад 200 організацій, що спричинило скасування кількох парламентських засідань.
Травень 2021 року.	Китайська хакерська група скомпрометувала російського оборонного підрядника, який займався розробкою атомних

	підводних човнів для російського флоту.
Квітень 2021 року.	Хакерська група зламала акаунти польських чиновників у соцмережах і використала їх для поширення критичних наративів щодо НАТО. Влада Німеччини повідомила, що ця ж група також намагалася скомпрометувати депутатів Бундестагу та державного парламенту.
Квітень 2021 року.	Хакери, пов'язані з китайськими військовими, провели шпигунську кампанію проти військових та урядових організацій у Південно-Східній Азії, починаючи з 2019 року.
Квітень 2021 року.	Шкідливе програмне забезпечення спричинило збій у роботі систем бронювання авіакомпаній, що призвело до збою мереж 20 лоукост авіакомпаній у всьому світі.
Квітень 2021 року.	Російські хакери атакували українських урядовців, намагаючись підшукати, оскільки на початку 2021 року напруга між двома країнами зросла.
Квітень 2021 року.	Хакери, пов'язані з палестинською розвідкою, провели кампанію кібершпигуну, в результаті якої було скомпрометовано близько 800 палестинських репортерів, активістів і дисидентів як у Палестині, так і на Близькому Сході.
Квітень 2021 року.	Дві підтримувані державою хакерські групи, одна з яких працює від імені китайського уряду, використали вразливості в службі VPN для націлювання на організації в США та Європі з особливим акцентом на американських оборонних підрядників.
Квітень 2021 року.	MI-5 попередила, що понад 10 000 британських професіоналів у сфері гоління стали мішенню ворожих держав протягом останніх п'яти років у рамках кампаній з підводного фішингу та соціальної інженерії на LinkedIn.
Квітень 2021 року.	Шведські чиновники розкрили, що Шведська спортивна конфедерація була зламана російською військовою розвідкою

	наприкінці 2017 та на початку 2018 року у відповідь на звинувачення у спонсованому російським урядом допінгу російським спортсменам.
Квітень 2021 року.	Управління міського транспорту Нью-Йорка (MTA) було зламано підтримуваними Китаєм акторами, але вони не змогли отримати доступ до даних користувачів або інформаційних систем.
Квітень 2021 року.	Французькі дослідники з питань безпеки виявили, що кількість атак, які вражають критичні французькі підприємства, у 2020 році зросла в чотири рази під час пандемії COVID-19.
Квітень 2021 року.	Європейська комісія оголосила, що ЄС та кілька інших організацій ЄС постраждали від масштабної кібератаки невідомих хакерів.
Квітень 2021 року.	У другій половині 2020 року китайські хакери розпочали багатомісячну кампанію кібершпигунства, спрямовану на державні установи у В'єтнамі з метою збору політичної розвідки.
Березень 2021 року.	Північнокорейська хакерська група, відповідальна за низку атак на дослідників кібербезпеки, у січні 2021 року запустила нову кампанію, націлену на професіоналів Infosec, використовуючи підроблені профілі в соціальних мережах і фальшивий веб-сайт для неіснуючої компанії, яка займається безпекою.
Березень 2021 року.	Підозрювані іранські хакери атакували медичних дослідників в Ізраїлі та США, намагаючись викрасти облікові дані генетиків, неврологів та онкологів у двох країнах.
Березень 2021 року.	Підозрювані російські хакери вкрали тисячі електронних листів після злому поштового сервера Державного департаменту США.

Березень 2021 року.	Підозрювані державні хакери атакували австралійську медіа-компанію Nine Entertainment за допомогою програмного забезпечення-вимагача, порушивши прямі трансляції та системи друку.
Березень 2021 року.	Підозрювані російські хакери намагалися отримати доступ до особистих облікових записів електронної пошти німецьких парламентарів напередодні національних виборів у Німеччині.
Березень 2021 року.	Кібер-командування США підтвердило, що надає допомогу Колумбії у реагуванні на втручання у вибори та операції впливу.
Березень 2021 року.	Глава кіберкомандування США засвідчив, що організація провела більше двох десятків операцій для протистояння іноземним загрозам напередодні виборів у США 2020 року, включаючи одинадцять передових операцій полювання в дев'яти різних країнах.
Березень 2021 року.	Група китайських хакерів використовувала Facebook, щоб надіслати шкідливі посилання на уйгурських активістів, журналістів і дисидентів, які перебувають за кордоном.
Березень 2021 року.	Індійська команда реагування на комп’ютерні надзвичайні ситуації знайшла докази того, що китайські хакери проводять кампанію кібершпигунства проти індійського транспортного сектора.
Березень 2021 року.	Польські служби безпеки повідомили, що підозрювані російські хакери ненадовго захопили веб-сайти Національного агентства з атомної енергії Польщі та Міністерства охорони здоров'я, щоб поширити помилкові повідомлення про неіснуючі радіоактивні загрози.
Березень 2021 року.	Як російські, так і китайські розвідувальні служби в 2020 році атакували Європейське медичне агентство в непов’язаних

	кампаніях, викрадаючи документи, що стосуються вакцин і ліків від COVID-19.
Березень 2021 року.	Служба державної безпеки України повідомила, що запобігла широкомасштабній атаці з боку хакерів ФСБ Росії, які намагалися отримати доступ до секретних державних даних.
Березень 2021 року.	Департамент державної безпеки Литви заявив, що в 2020 році російські хакери атакували вищих чиновників Литви та використовували IT-інфраструктуру країни для здійснення атак на організації, які займаються розробкою вакцини проти COVID-19.
Березень 2021 року.	Підозрювані іранські хакери атакували державні установи, наукові кола та туристичну індустрію в Азербайджані, Бахрейні, Ізраїлі, Саудівській Аравії та ОАЕ в рамках кампанії кібершпигунства.
Березень 2021 року.	Китайські урядові хакери атакували корпоративне програмне забезпечення електронної пошти Microsoft, щоб викрасти дані понад 30 000 організацій по всьому світу, включаючи державні установи, законодавчі органи, юридичні фірми, оборонних підрядників, дослідників інфекційних захворювань і аналітичні центри.
Березень 2021 року.	Підозрювані китайські хакери атакували операторів електромереж в Індії, очевидно, намагаючись закласти основу для можливих майбутніх атак.