МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

САВЧУК АЛІНА ВАЛЕНТИНІВНА

Допускається до захисту:
в.о. завідувача кафедри міжнародних відносин і зовнішньої політики,
д-р економічних наук, доцент
_____ В. В. Лимар
«____»_____ 20__ р.

СПОЛУЧЕНІ ШТАТИ АМЕРИКИ ТА РОСІЙСЬКА ФЕДЕРАЦІЯ: ПРОТИСТОЯННЯ У КІБЕРПРОСТОРІ

Спеціальність 291 Міжнародні відносини, суспільні комунікації та регіональні студії

Магістерська робота

Науковий керівник:
Лещенко Л.В., професор кафедри
міжнародних відносин і зовнішньої політики,
доктор політичних наук, професор

Оцінка:_____/ _____/ _____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК:
Кулявець В. Г., к.е.н., доцент
_____
(підпис)

Вінниця – 2023

Савчук А. В. Сполучені Штати Америки та Російська Федерація: протистояння у кіберпросторі. Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОП «Міжнародні комунікації та медіація в умовах конфліктного врегулювання», Донецький національний університет імені Василя Стуса, Вінниця, 2023.

У кваліфікаційній (магістерській) роботі досліджено стан відносин Сполучених Штатів Америки та Російської Федерації в кіберпросторі, проаналізовано законодавчу базу у галузі кібербезпеки, їх діяльність стосовно один одного у вигляді кібератак та ініціатив у сфері міжнародного права.

Ключові слова: кібербезпека, Росія, США, критична інфраструктура, кібероперації.

80 с. Бібліограф.: 98 найм.

Savchuk A. The United States of America and the Russian Federation: confrontation in cyberspace. Specialty 291 "International Relations, Public Communications and Regional Studies", EP "International Communications and Mediation in Conflict Resolution". Vasyl` Stus Donetsk National University, Vinnytsia, 2023.

In the qualification (master's) work the state of relations between the United States of America and the Russian Federation in cyberspace researched, the legislative framework in the field of cyber security was analyzed, their activities according to each other in the form of cyber-attacks and initiatives in the field of international law.

Keywords: cyber security, Russia, USA, critical infrastructure, cyber operations.

80 p. Bibliography: 98 items.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЗМІ – Засоби масової інформації

ІВ – інформаційна війна

ІДІЛ - Ісламська держава Іраку й Леванту

ІКТ – Інформаційно-комунікаційні технології

КНР – Китайська Народна Республіка

НАТО - Організація Північноатлантичного договору (North Atlantic Treaty Organization)

ООН – Організація Об'єднаних Націй

РФ – Російська Федерація

США – Сполучені Штати Америки

ФСБ - Федеральна служба безпеки (Російської Федерації)

ЦРУ - Центральне розвідувальне управління (США)

CIRCIA - Cyber Incident Reporting for Critical Infrastructure Act (Закон про звітність про кіберінциденти для критичної інфраструктури)

CISA – Cybersecurity & Infrastructure Security Agency (Агентство з кібербезпеки та безпеки інфраструктури)

DCCP - Digital Connectivity and Cybersecurity Partnership (Партнерство з цифрового підключення та кібербезпеки)

NCPI - National Cyber Power Index (Національний індекс кіберпотужності)

OEWG – Open-Ended Working Group (Робоча група відкритого складу ООН)

SEC – Securities and Exchange Commission (Комісія з цінних паперів і бірж США)

ВСТУП

Значення кіберпростору у останні десятиліття тільки зростає, а методи боротьби між державами у ньому і за нього стають більш жорсткими. Оскільки розвиток технологій відбувається постійно, а людство стає все більш залежним від штучного інтелекту, можливостей посіяти хаос усе більше, тим паче за наявності міжнародних акторів, які не дотримуються загальноприйнятих законів.

Актуальність теми. Поруч з традиційними засобами ведення війни на поле бою виходять і інформаційно-комунікаційні технології, використання яких іноді важко передбачити, а наслідки можуть бути досить руйнівними. У міру того, що війна в Україні все ще триває, давня боротьба між Російською Федерацією та Сполученими Штатами Америки за кіберпростір також загострюється. Сучасний стан відносин Росії та США відзначаються високим рівнем недовіри. Дипломатична верхівка Російської Федерації попереджає про «катастрофічні» наслідки, якщо Сполучені Штати або їхні союзники спровокують Росію кібератакою, хоча сама вона використовує кіберпростір на постійній основі, готуючи масштабні удари.

Одержимість Росії кіберпростором частково відображає думку російської влади про те, що США контролюють Інтернет і його управління. Росія прагне визнання великої держави та світового стандарту, тому критична інфраструктура США є постійною ціллю російських хакерів з надією отримати стратегічно важливу інформацію. Розуміння тенденцій у відносинах і поведінці Російської Федерації та Сполучених Штатів Америки щодо один одного в кіберберпросторі дасть можливість розраховувати ризики в процесі протистояння двох держав.

Об’єктом дослідження є відносини Сполучених Штатів Америки та Російської Федерації у кіберпросторі.

Предметом дослідження є динаміка розвитку відносин Сполучених Штатів Америки та Російської Федерації у сфері кібербезпеки.

Метою дослідження є з’ясувати, яким чином Російська Федерація та Сполучені Штати Америки діють у кіберпросторі стосовно один одного.

Виходячи з зазначеної мети, можна виокремити наступні **завдання**:

- проаналізувати правову базу, що регулює поведінку двох держав у кіберпросторі;
- порівняти реальні дії держав з позиціонуванням у нормативних документах;
- визначити, як розвивалась кібербезпека РФ та США впродовж визначеного періоду;
- визначити, яким чином стан кібербезпеки впливає на позиціонування держави на міжнародній арені.

Хронологічні рамки дослідження – 2000 – 2023. Ці рамки обґрунтовуються приходом президента В. Путіна до влади, оскільки саме з цього моменту в РФ починає розвиватися правова база кібербезпеки з Доктрини інформаційної безпеки РФ і формуватись окремі погляди на зовнішню політику держави. Таким чином, першу Доктрину інформаційної безпеки було затверджено Президентом Російської Федерації у вересні 2000 року.

Територіальні межі відсутні, оскільки технічною особливістю кіберпростору є те, що поняття кордонів стираються, а всесвітня мережа поширена без урахування чітких меж.

Гіпотеза дослідження – останнє десятиліття агресія РФ в кіберпросторі стосовно США та й інших держав тільки посилюється і не планує збавляти темп, натомість США займає більше оборонну позицію в кіберпросторі.

Теоретичне або практичне значення одержаних результатів – робота розкриває собою протиріччя та різноманітність підходів до дослідження кіберпростору. Також чіткіше вимальовуються образи держав з досить «нетрадиційного» ракурсу. Розуміння тенденцій відносин США та РФ у

кіберпросторі дає можливість прогнозування як ситуації між цими двома державами в інших сферах, так і клімат світового порядку денного загалом.

Апробація результатів дослідження – VI Міжнародна науково-практична конференція студентів, аспірантів і молодих учених «Актуальні проблеми гуманітарних, технічних і природничих наук» - “Relations between the Russian Federation and the United States in cyberspace”; V Міжнародна наукова конференція «Міжнародні конфлікти у сучасному світі: від регіонального протистояння до глобального суперництва» - “Актуальні тенденції політики США в сфері кібербезпеки в умовах збройної агресії Російської Федерації проти України”.

Структура кваліфікаційної (магістерської) роботи – робота містить в собі 8 основних частин з відповідним наповненням: вступ, 5 основних розділи зі своїми підрозділами, висновки та список використаних джерел. У першому розділі описано методологічні засади дослідження та характеристика використаної літератури. Другий розділ привячений ролі кібербезпеки для статусу держави на міжнародній арені. Третій розділ присвячений Сполученим Штатам Америки, аналізу законодавчої бази держави, що регулює кіберпростір та як він використовується у політичних цілях. У четвертому розділі натомість представлено спеціифіку РФ, її діяльність у кіберпросторі та як вона відрізняється від позиціонування в законодавчих документах. В п’ятому розділі розглядається конфронтаційна політика двох держав, а також звертається увага на взаємодію у кіберпросторі та прогнозуються перспективи майбутніх відносин.

У висновках звертається увага на рівень реалізації вказаної в праці мети, а також представлене підтвердження висунотої гіпотези.

РОЗДІЛ 1
СТАН ДОСЛІДЖЕННЯ, ДЖЕРЕЛЬНА БАЗА ТА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

1.1. Стан вивчення проблеми

Серед дослідників проблем міжнародної безпеки тема кіберпростору та міждержавних відносин в ньому стає все більше цікавою з огляду на безупинний розвиток технологій, адже нові можливості несуть з собою й нові загрози. До вивчення кіберпростору підходять з дуже різних сторін – технологічний аспект, які інструменти та програми використовуються для його функціонування; розвиток нормативно-правових засад, їх реалізація і дотримання; психологічні аспекти. Держави, в свою чергу, знайшли нове поле для геополітичного протистояння та самоствердження. Найбільш цікавими для дослідників, звичайно, стають ті держави, що демонструють певну активність в кіберпросторі, в більшій мірі агресивну, тому саме безпековий аспект та кібербезпека як фактор впливу на відносини є найбільш популярним серед літератури.

Акторів міжнародних відносин, що найчастіше фігурують в різних матеріалах можна поділити на два табори. Перший – США та ЄС (як загалом геополітична структура, так і окремі держави можуть згадуватися), що ведуть досить ліберальну політику в кіберпросторі та фокусують свою увагу впершу чергу на розбудові власної безпеки та співпраці. Другий – КНР, Російська Федерація, Іран, Північна Корея, держави чия діяльність в кіберпросторі майже завжди висвітлюється в контексті здійснених кібератак, шпигунських дій, та з ким пов’язують роботу різних груп хакерів. Примітно, що в періодичних виданнях висвітлюються випадки уже здійснених кібератак, де держави другої групи виступають кривдником, а держави першої – жертвою.

Загалом, дискусії про природу і закони кіберпростору серед науковців досить жваві і з багатьох питань так і не існує однієї, визначеної правильною думки. Ще

більш дискусійними є питання законодавства. Ситуація в цьому аспекті складається таким чином, що навіть при наявності ряду міжнародних нормативно-правових актів з приводу поведінки держав, то мало хто їх дотримується. Подібна дилема існує в розрізі і національного законодавства окремих держав. Наприклад, беручи за приклад Росію, 23 стаття Конституції [2] становить: «Кожен має право на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень», а наступна стаття зазначає, що «Збір, зберігання, використання та розповсюдження інформації про приватне життя особи без її згоди не допускаються». Паралельно доповнення до закону «Про протидію тероризму» [6] від липня 2016 року вказує наступне «Федеральний орган виконавчої влади у сфері забезпечення безпеки має право отримувати на безоплатній основі від державних органів та державних позабюджетних фондів необхідні для виконання покладених на нього обов'язків інформаційні системи та (або) бази даних, у тому числі шляхом отримання можливості віддаленого доступу до них». Тобто в даному випадку деякі закони суперечать одне одному і порушують права людини.

Наукова спільнота пильно відстежує динаміку відносин в кіберпросторі, зокрема питання кількості кібератак наскільки це можливо, реакція держав, що зазнали ударів, реакція міжнародної спільноти, розвиток національних законодавчих баз, ініціативи щодо навчання. Проте, будь-які дослідження в цьому напрямку не можуть давати повну картину ситуації. Більшість інформації зберігається державами в секреті, що логічно з точки зору національної безпеки. Якщо говорити про злочинну діяльність хакерських груп, то експерти не одразу можуть встановити, яка саме група здійснила напад та чи був він на замовлення уряду та якого. Цей процес іноді займає до року, а притягнення окремих осіб до відповідальності і судові справи тривають по декілька років.

США цікаві для дослідників з точки зору як заявленої технологічної першості, так і політичної ваги. Тому поведінка Штатів в кіберпросторі

знаходиться під постійною увагою як науковців, так і міжнародної спільноти. Варто зауважити, що помічається обмежена кількість інформації про кібератаки чи іншу агресивну активність в кіберпросорі з боку Америки. Помітно також, що ця інформація є у відкритому доступі значно в менших кількостях ніж про РФ чи Китай. Російська Федерація навпаки привертає увагу своєю активністю і креативністю. ЇЇ кібератаки - це щоденна робота хакерів, які часто працюють на замовлення уряду. Крім того, виконавці йдуть в ногу з часом і знаходять різні засоби як обійти системи безпеки. Тому, динаміка і складність атак з російської сторони цікава не лише з точки зору створення чіткої дорожньої карти і підходів до присутності РФ в кіберпросторі, а й безпекових аспектів, щоб розуміти до чого треба готуватися потенційним цілям. Говорячи про взаємодію США і РФ у кіберпросторі протягом останніх років, в більшості випадків прослідковується зв'язок з повномасштабним вторгненням Росії на територію України або з окупацією Криму в 2014. Напруженість між США та Росією через діяльність у кіберпросторі мала широкий вплив як на внутрішньому рівні держв, так і на міжнародному рівні. Міжнародні наслідки напруженості між США та Росією через кібер-діяльність, включають можливу ескалацію ситуації та її перетікання у звичайну війну.

1.2. Характеристика джерел

В ході дослідження було використано численні джерельні матеріали та література предмету авторства українських та іноземних дослідників. Найважливішою групою джерел були законодавчі акти США та Російської Федерації. На жаль, не до всіх документів РФ був доступ, тим не менше вдалось скористатись рядом нормативно-правових актів, які прямо чи опосередковано урегульовують поведінку Росії в кіберпросторі. Так, було використано Конституцію Російської Федерації, Федеральний закон «Про участь у міжнародному інформаційному обміні», Указ Президента Російської Федерації

«Про затвердження Доктрини інформаційної безпеки Російської Федерації» 2016 року, Федеральний закон «Про внесення змін до Федерального закону «Про протидію тероризму», тощо. Щодо законодавчої бази США, то найважливішим на сьогоднішній день є нова Стратегія кібербезпеки США 2023 року. Додатково було використано наступні документи: Федеральний закон «Про модернізацію інформаційної безпеки» 2014 року, закон Гремма-Ліча-Блайлі, виконавчий наказ «Про сприяння обміну інформацією про кібербезпеку в приватному секторі», виконавчий наказ «Покращення кібербезпеки критичної інфраструктури», погоджені бюджети на 2023 та 2024 роки та інші.

Іншою великою групою джерел стали звіти. Особливу увагу варто звернути на звіт про розслідування російського втручання у президентські вибори 2016 року, огляд кіберзагроз Росії та рекомендації від агентства кібербезпеки та безпеки інфраструктури, звіт щодо стратегії кібербезпеки Росії, опублікований Центром передового досвіду стратегічних комунікацій НАТО, звіт Міжнародного інституту стратегічних досліджень «Кіберможливості та національна сила: оцінка».

Важливою групою джерел стали статистичні дані. Так до дослідження було залучено дані Національного індексу кіберпотужності, лічильник кібероперацій, розроблений Радою з міжнародних відносин, аналітика від компанії CyberProof, що спеціалізується на програмному забезпеченні. Важливою, з точки зору, представленої теми, була також медійна інформація. Інформація щодо здійснених кібератак і їх деталей в основному висвітлюється в новинних стрічках. Тому використостовувались наступні видання: The Wall Street Journal, The Washington Post, The New York Times, Reuters, та інші.

Серед авторів були використані праці таких провідних сучасних дослідників у галузі кібербезпеки як Дж. Най, Д. Кюль, що зосереджують свої дослідження на вивчені природи кіберпростору та його роль в сучасній політиці. М. Лібіцкі, один з провідних дослідників питань кібербезпеки, сфокусований на

спроможностях США, їх відносинах з іншими державами в кіберпросторі. Суліван Л. та Джаілс К. сфокусований на протистоянні Російської Федерації США у різних сферах, в тому числі і кіберпросторі.

1.3 Методологічні засади дослідження

Тема кібербезпеки вимагає комплексного підходу до дослідження, паралельно, необхідно пам'ятати про її спорідненість з інформаційною безпекою. Словники визначають поняття *кібербезпеки* як заходи, вжиті для захисту комп'ютерних систем від несанкціонованого доступу або нападу (кібератак). В контексті даної роботи та взагалі міжнародних відносин мається на увазі комп'ютерні системи певної держави, що включають як державну інфраструктуру і її користувачів (громадян), так і внутрішні системи певних органів, що містять в собі стратегічну та секретну інформацію. Під «несанкціонованим доступом» та «кібератаками», вважаються зловмисні дії уряду держави «Б» або діяльність третіх осіб (хакерських груп), в тому числі на замовлення уряду, з метою отримання інформації, що зберігаються у системах держави «А», або втручання з метою здійснити збій в роботі державних систем та установ. Кібербезпека часто перетинається з поняттям інформаційної безпеки, проте вони не тотожні. Інформаційна безпека сфокусована більше на збереженні інформації і її достовірності, особливо тієї, яка доходить до громадян через медіа та телебачення. Звідси інформаційна війна - це тактичне та стратегічне використання інформації для отримання переваги.

У сучасній науці про міжнародні відносини визначення суттєвих ознак сучасних наддержав залишається яблуком розбрату. Тим не менше в класичному розумінні «наддержавою» можна назвати таку, що має економічний потенціал, який значно перевищує потенціал інших країн, військову міць, критичні технології, розвинену науково-промислову базу, людський капітал. Саме за

рахунок комплексного поєднання цих факторів держава має значний вплив на хід справ на міжнародній арені.

Неореалісти, такі як Кеннет Уолц, стверджують, що міжнародна система перебуває в стані анархії, де держава має найвищу владу. Таким чином, немає гарантії, що держава не нападе на іншу державу, що дуже властиво кіберпростору сьогодні. Страх і невпевненість змушують держави максимізувати свій військовий потенціал, економічну спроможність та інші сили. Оскільки неореалізм також є державоцентричною парадигмою, це створює певні обмеження при дослідженнях кіберпростору. Наприклад, це ускладнює визначення того, хто є великою силою в кіберпросторі. Кожна держава має свій власний кіберпотенціал, включаючи малі держави, держави зі слабкою економікою та слабкою військовою силою. Проте, це зовсім не означає, що вони слабкі в кіберпросторі.

Для вирішення основних завдань дослідження використовувалися як кількісні, так і якісні методи, використання як вторинних, так і первинних джерел інформації. Якісні дані підтримують кількісний аналіз даних і результатів
Дослідження базується на наступних методах:

- аналізу і синтезу, методи індукції та дедукції – наприклад, при окресленні тенденцій політики РФ;
- порівняльно-правовому методі – тобто співставлення правових норм США та РФ, що стосуються кіберпростору та їх порівняння;
- системно-структурному методах – в контексті даної роботи кібербезпека є цілісним об’єктом, елементами якого є, нормативно-правова база обох держав, міжнародні договори, кібератаки та їх наслідки, а взаємозв’язок усіх цих аспектів дає розуміння цілісної картини ситуації між США і РФ;
- інтерпретації – використовувався при роботі зі статистичними даними;

- порівняльно-історичний – а саме, порівняння ситуації в кіберпросторі з року в рік, особливо починаючи з 2010-х, коли в інформаційному полі все більше і більше фіксуються певні кроки обох держав.

РОЗДІЛ 2
КІБЕРБЕЗПЕКА ЯК ФАКТОР СУЧАСНОЇ НАДДЕРЖАВИ

Потужності кібербезпеки поступово стають новим доповненням до сили країни, а відповідно, до її статусу. В 21 столітті кіберпотенціал як інструмент впливу все більше набирає значення. Усе частіше в новинній стрічці можна помітити повідомлення про втручання до комп'ютерних систем держави, викрадення даних, фішингові атаки на об'єкти критичної інфраструктури. Як приклад, можна згадати кібератаку в кінці 2015 на «Укренерго» [3], внаслідок якої було відключення електроенергії у Прикарпатті. Загалом, близько 700 000 мешканців Івано-Франківської області залишались без світла декілька годин. Інший показовий випадок стався у травні 2021, коли на управління охорони здоров'я Ірландії була здіснена атака за допомогою вірусу Conti. [77] Було виведено з ладу декілька систем, а для запобігання поширення шкідливого програмного забезпечення на усі інші системи, управлінням було прийнято рішення взагалі вимкнуті усі свої IT-системи. Це значно сповільнило роботу служб, які покладалися на цифрові процеси, як-от сканування, перенаправлення та надання діагностичних послуг, особливо в умовах пандемії. Або ж кібератака найбільший порт Японії Нагоя у червні 2023 [52], який відповідає за обробку деяких експортних поставок автомобілів Toyota Motor. Тоді робота порту призупинилась на дві доби, а оператор порту отримав вимогу викупу в обмін на відновлення систем.

Окрім використання цих технічних можливостей для викрадення державних таємниць одна в одної, як у традиційному шпигунстві, держави також використовували їх для низки інших, більш загрозливих цілей.

У 2000-х роках кібернетика ще розвивалась у більшості країнах, і тоді ще не була гострою потребою, на відміну від проблем, пов'язаних безпосередньо з тероризмом [50]. Серед науковців немає чітко визначеного чи загальновизнаного

визначення кіберсили (cyber power). Більш простіший погляд на кіберпотужність полягає у трьох факторах: наскільки добре організована кожна країна – стратегії та доктрини, командування та контроль; наскільки добре вона може захистити себе за допомогою власної кібербезпеки або через міжнародне партнерство; а також наскільки ефективно її цифрова економіка може підтримувати її кіберпотреби та амбіції. [18] Один з популярних дослідників кібербезпеки Джозеф Най [72] визначає кіберпотужність як «здатність отримувати бажані результати шляхом використання електронних взаємопов'язаних інформаційних ресурсів кібердомену». У цьому підході Най підкреслює, що кіберпотужність можна використовувати для створення бажаного впливу як у звичайній, так і в кіберсфері. Відповідно до Джона Шелдона [86], кіберпростір визначається проведеними кібероперaціями, а кіберпотужності – вплив від цих операцій, а наслідки можуть бути відчутні не лише у віртуальному просторі, а й в фізичному, тобто на землі, в повтрі, воді, космосі.

Натомість, вивчаючи Національний індекс кіберпотужності (далі NCPI) [95], цей термін виявляється більш комплексним та включає в себе значно більше факторів. За словами авторів цього звіту, «Кіберпотужність багатогранна і вимагає загальнонаціонального підходу, щоб використовувати її». Проаналізувавши 30 держав [94] (через обмежені ресурси та доступ до відкритих джерел даних автори не змогли включити багато інших країн), держави прагнуть не лише знищити та вивести з ладу інфраструктуру та можливості супротивника (традиційне, але вузьке та оманливе уявлення про кіберпотужність), а й зміцнити та посилити національний кіберзахист, збирати розвідувальні дані в інших країнах, розвивати національні кібернетичні та комерційні технології, контролювати та маніпулювати інформаційним середовищем, а також розширювати свій вплив шляхом визначення міжнародних кібернорм і технічних стандартів. Кіберпотужність слід розглядати в контексті національних цілей держави. Знищення або виведення з ладу інфраструктури супротивника є лише

однією з восьми цілей виділених авторами, які країни переслідують за допомогою кіберзасобів.

Представлений звіт дає підстави стверджувати, що США є сучасною кібердержавою. Якщо більшість країн надають перевагу найбільше покривати одну, дві, рідше три цілі одночасно, то США намагається віддати максимум потужностей на шість з восьми цілей. Росія займає 2 місце після США в цілях «Контроль інформації» та «Наступальні дії».

Зі свого боку, Китай очолює рейтинг можливостей кіберзахисту. Загалом ця країна входить до ТОП-5 за кожною ціллю. З початку 1990-х років Китай інвестував значні кошти в дослідження та розробку технологій, які розвивають можливості ведення кібервійни. Військова доктрина Китаю включає кібератаку як складову стратегії, спрямовану на перемогу над ворогом, який є краще оснащеним або переважає за чисельністю. [79]

Термін «кібернаддержава» застосовувався до Китаю, Ізраїлю, Росії, Великобританії та США такими впливовими організаціями, як Всесвітній економічний форум. [15] Однак це звання було присвоєно без будь-якого чіткого пояснення критеріїв того, на що «кібердержава» або «кібернаддержава» здатна. Виокремлення саме цих акторів здійснилось на підставі загальноприйнятого погляду на стан розвитку кіберпотужностей. Варто зауважити, що спроби РФ презентувати себе у якості наддержави з якою варто рахуватися, були повністю зруйновані вторгненням в Україну. Економічний потенціал і до цього підводив Росію, проте зараз він тільки погіршується за рахунок санкцій західного світу. Демографічний потенціал теж значно страждає, а загальна репутація на міжнародній арені спаплюжена неодноразовим повторенням інцидентів різного характеру.

Кіберпотужність слід розглядати як окрему сферу, а не лише як доповнення або підсилювач інших форм влади. Кіберпростір уже вважається п’ятою сферою після космосу, моря, землі та повітря. [65] У книзі «Необмежена війна» [59] двох

колишніх полковників Народно-визвольної армії Цяо Ляна та Ван Сянсуя пояснюється, як перемогти технологічно вищого супротивника (у цьому випадку Сполучені Штати), покладаючись на різні засоби, окрім прямого військового протистояння. Автори проаналізували, яким чином країни, що розвиваються, можуть діяти проти більш технологічно розвинутих держав у разі відкритого спалаху військових дій, маючи на увазі, що такі заходи повинні використовуватися для визначення курсу, який Китаю довелося взяти, щоб компенсувати свою тодішню військову непереможність перед Сполученими Штатами Америки. Вони окреслюють синхронне застосування безлічі засобів, які будуть використовуватися одночасно з військовою силою для перемоги в конфлікті, включаючи злом урядових веб-сайтів, які підтримують управління урядом опонента, підрив фінансових установ, використання відкритих ЗМІ Заходу, сприяння соціальному розбрату та проведен. «На даний момент американці, які запропонували концепцію «повітряно-земляного бою», вже пішли трохи далі, але, незважаючи на це, їм все одно доведеться чекати кілька років, перш ніж вони зрозуміють це, як тільки вони вдадуться до теорії інтегрованих операцій в реальних боях, масштаби виходитимуть далеко за межі того, що вони передбачали спочатку, поширюючись на широкий і всеохоплюючий діапазон, який охоплює землю, море, повітря, космос і кіберсфери».

Оголошення Сполучених Штатів про те, що вони використовують своє військове кіберкомандування для здійснення атак на комп'ютерну мережу проти Ісламської держави, є демонстрацією того, наскільки значним став цей новий бойовий фронт. Сполучені Штати є лише однією з багатьох країн, які інвестували значні суми грошей у розробку не лише засобів захисту від атак, але й здатності організовувати руйнівні кібервійни. [15]

У випадку США, їх кіберпотенціал слід розглядати як такий, що дорівнює їх наземній, повітряній чи морській силі. Крім того, у випадку Китаю та Росії їхня

кіберпотужність є більш ефективною, ніж їхні можливості у контексті традиційних засобів війни. Крім того, хоча й не є рівними трьом «кібернаддержавам», у кіберпросторі є інші важливі гравці, зокрема Естонія, Франція, Індія, Іран, Ізраїль та Північна Корея. [21]

Тим не менш, кібернетика швидко стає стратегічним інструментом для країн. Все більше країн розвивають наступальний потенціал, а кіберпростір стає сферою постійної суперечки. Країни виділяють більше ресурсів на кіберзахист і напади. На початку березня 2023 адміністрація Байдена оприлюднила бюджет [17] на 2024 рік. Кібербезпека в ньому стала провідною сферою для інвестицій. У державному бюджеті передбачається виділення 3,1 мільярда доларів на Агентство з кібербезпеки та безпеки інфраструктури (CISA), що на 145 мільйонів доларів більше від виділеної суми у 2023. [16] У 2023 бюджет передбачає 2,5 мільярда доларів США, що на 486 мільйонів доларів більше, ніж рівень, прийнятий у 2021 році. Згідно з новими пропозиціями на 2024, фінансування включатиме 98 мільйонів доларів на реалізацію Закону про звітність про кіберінциденти для критичної інфраструктури, а також 425 мільйонів доларів на покращення внутрішньої кібербезпеки та аналітичних можливостей.

Китай має передові кібер-можливості, але, принаймні досі, він був зосереджений на експлуатації мережі, а не на мережевих атаках. Невпинне використання Китаєм кібершпигунства розлютило Сполучені Штати, оскільки завдяки атакам Китаю вдалось викрасти величезну кількість даних для розвитку розвідувальних і військових можливостей Китаю, а також для того, щоб принести користь китайській економіці та корпораціям, дозволивши їм скоротити дослідження та витрати на розробку. Китайці успішно змогли проникнути в найсучасніші системи озброєння. Природно, вони зосередилися, зокрема, на оборонних підрядниках США та використали викрадені дані, щоб закрити прогалину в можливостях традиційної зброї. Китай розсунув межі, і навіть перевищив їх, нормативної поведінки щодо посягань на мережі. Серед публічно

відомих подій однією з найбільш значущих і згубних для Америки став витік даних Китаєм у 2015 році в Управлінні управління персоналом США. Це проникнення включало компрометацію особистих даних понад 20 мільйонів людей, у тому числі багатьох представників розвідувального співтовариства. [31]

Окрім Китаю державою, яка часто фігурує в звинуваченнях про здійсненні кібератаки є Російська Федерація. Згідно з базою даних відстеження кібероперацій [24], розробленим Council on Foreign Relations, лише за 2023 рік Росією було здійснено 15 кібероперацій, а Китаєм - 18. Необхідно зуважити, що цей інструмент фіксує лише інциденти, які були здійсненні на замовлення певної держави. Звіти про недержавні суб'єкти, як-от хактивістські групи, як правило, важчі для ідентифікації та роблять дані менш надійними. Більшість кібератак Росія використовувала в асиметричних конфліктах, де вона домінувала в ескалації, що означає, що інші країни не можуть або не мають стимулу до ескалації конфлікту на вищий рівень. Примітно, що хакерська кампанія під час президентських виборів у Сполучених Штатах 2016 року була іншою в тому сенсі, що Росія не була в позиції домінування ескалації. Замість використання своїх кіберможливостей, щоб примусити або покарати слабшу державу, вона мала на меті використовувати кіберможливості, щоб вплинути на вибори в США — як тепер добре відомо — за допомогою винятковий навичок хакерства, щоб проникнути в політично чутливу інформацію, використовувати її таємно або ж злити у відкритий доступ. Про вплив кібератак на результати виборів можна сперечатися, а їх ефективність у кращому випадку неоднозначна, але безсумнівно, що атаки підкреслили використання Росією кіберзброї для впливу на вибори та, без сумніву, на інші цілі. Все це було зроблено як операція впливу — ще одна стріла в їхньому сагайдаку прихованої дії. Можливо, найбільшим активом Росії в її кібер-арсеналі є її інновації та готовність здійснювати кібератаки проти своїх ворогів.

Звичайно, можливості Росії також мають межі. На досвіді Америки та Ізраїлю зі Stuxnet [43] (комп'ютерний хробак), як тільки Росія використає певну стратегію, інші потенційні супротивники отримають можливість краще підготуватися. Хоча російські кібератаки в Україні можна розглядати як тестування кібер-можливостей та їх корекція, вони також дають Заходу можливість вивчити новітні можливості Росії. Коли певні можливості та тактика відомі, легше покращити захисні можливості. Наприклад, російський злом виборів не був таким ефективним на виборах у Нідерландах, Франції, Німеччині чи Італії, як це могло бути в попередніх випадках. Нарешті, російська атака на Естонію демонструє, що розгортання кіберзброї, як і кінетичної зброї, генерує значні контрзаходи та підвищує рішучість захисника забезпечити зниження своєї вразливості через кіберзахист і, що більш важливо, через мобілізацію населення для усунення загрози.

Одночасно, команда CyberProof [32], що є постачальником цифрових і інформаційних технологій і послуг, здійснила аналіз найнебезпечніших країн 2021 року з точки зору походження кібератак. Згідно з цим дослідженням, більш ніж 18% усіх кібератак було здійсненно з території КНР, а на другому місці – США з показником в 17%. Але у світових ЗМІ атаки скоєні США майже не висвітлюються, натомість навпаки Штати в більшості випадків стають жертвою. Таким чином, політична першість Штатів все таки впливає не так на ситуацію в кіберпросторі, скільки на публічність протистояння з іншими державами.

Не менше кіберпотужності впливають на імідж держави. Одна справа, коли держава займається розвитком ІКТ для покращення умов життєдіяльності людства і свого населення, а інша – коли у намірах є дестабілізація ситуації в іншій державі, втрутитись у внутрішню справи. У новинах про використання кіберпростору окремих держав у своїх інтересах у негативиному контексті (злом, викрадення даних, тощо) найчастіше фігурують держави з авторитарними режимами. Зокрема зазначаються РФ, Іран, КНР.

При тому, в дискусійних колах підіймається ідея розвитку наступальних сил у сфері кібербезпеки як гарантія захисту. Тобто, за умови, що держава становить загрозу іншим, це зменшує ризик наступу на неї саму. Але можливості не обов'язково означають використання. Таким чином, Сполучені Штати є найбільш просунутими, але не обов'язково найактивнішими на рівні наступу, навіть якщо в новинних стрічках з'являються повідомлення, що вони вжили заходів проти Ірану чи Північної Кореї. [58] Суть стримування полягає в тому, щоб мати можливість заподіяти своєму опонентові те, що він намагається зробити з вами. У ядерну епоху це називали «рівновагою терору», коли американці та радянські війська мали можливість знищити один одного. Кібервсесвіт ще не дійшов до подібного стану. Але важливо вміти правильно оцінити можливості гравців у сфері.

Розвиток кіберзброї нині змушує розглядати та оцінювати кібербаланс сил як головну характеристику міжнародної влади. Відносна легкість збору розвідувальних даних і атаки, труднощі у встановленні масштабу атаки та її приписування, а також продемонстрована ефективність кібервійни роблять кіберзброю корисною для тих, хто приймає рішення щодо національної безпеки. У свою чергу, це гарантує, що кібернетичні засоби й надалі будуть інструментом збору розвідувальних даних і що кіберзброя буде розгортатися великими державами як у мирний час, так і під час майбутніх криз і воєн.

Проте, серед особливостей кіберпотужностей прослідковується така характеристика як «одноразовість» атак, оскільки як тільки будь-яка держава Росія, Китай, США використає певну стратегію, інші потенційні супротивники отримають можливість краще підготуватися або використати ті самі прийоми. Таким чином, інноваційність вимагає багато ресурсів: підготувка якісної атаки іноді займає роки. Поки що, кіберпотужності, як такі не впливають на вагомість країни. Можна припустити, що більшої значимості сили у кіберпросторі як фактор наддержави отримають тоді, коли традиційні засоби війни віддійдуть на

задній план і не приноситимуть очевидної переваги. Але якщо держава визначається першістю в міжнародній спільноті у політичному та безпековому вимірі, кіберпростір стає інструментом впливу.

РОЗДІЛ 3
СПОЛУЧЕНІ ШТАТИ АМЕРИКИ ЯК ЛІДЕР У ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

3.1. Законодавче врегулювання кіберпростору

Технології сприяли демократії, свободі слова, інноваціям і рівності. Але ними також зловживали для транснаціональних репресій і цифрового авторитаризму, викрадення даних та інтелектуальної власності, поширення дезінформації, порушення критичної інфраструктури; поширюються такі явища, як онлайн-переслідування та експлуатація, сприяння злочинцям і насильницькому екстремізму, що загрожує миру та стабільності.

У 2023 році ризик кібератак залишається високим для урядів та компаній через уразливості, спричинені віддаленою роботою, дедалі більшою залежністю від електронної комерції та більш досвідченими зловмисниками. Кібератаки призводили до перерви у виплаті допомоги з безробіття в кількох штатах Америки, а атаки програм-вимагачів продовжують припиняти діяльність або спричиняти величезні витрати урядам, школам, корпораціям і підприємствам. Нещодавнім гучним і показовим інцидентом впливу новітніх технологій стала атака програми-вимагача на системи корпорації Colonial Pipeline, що займається доставкою нафтопродукції у США. [53] Кібератака змусила кампанію припинити тимчасово подачу продукції, внаслідок чого серед американців поширилась паніка, а до заправок з’явилися великі черги.

Інциденти з кібербезпекою відбуваються роками, але більшість з них залишалися поза увагою громадськості до останнього десятиліття. Нещодавні резонансні інциденти, які торкнулися великої кількості звичайних громадян, вивернули це питання в національний дискурс і в центр уваги законодавчих і регуляторних органів. Зараз світ вступає в нову еру кібербезпеки, коли уряди та компанії працюють над посиленням нагляду за інцидентами кібербезпеки.

Федеральних нормативних актів щодо кібербезпеки небагато, а ті, що існують, зосереджені на конкретних галузях. Трьома основними правилами кібербезпеки є Закон про перенесення та підзвітність медичного страхування 1996 року (HIPAA), Закон Грамма-Ліча-Блілі [49] 1999 року та Закон про національну безпеку 2002 року, який включає Федеральний закон про управління безпекою інформації (FISMA). [84] Ці три правила зобов'язують організації охорони здоров'я, фінансові установи та федеральні агентства захищати свої системи та інформацію. Наприклад, FISMA, яка поширюється на кожну державну установу, «вимагає розробки та впровадження обов'язкових політик, принципів, стандартів і вказівок щодо інформаційної безпеки». Однак положення не стосуються численних пов'язаних з комп'ютерами галузей, таких як Інтернет-провайдери (ISP) і компанії, що займаються програмним забезпеченням. [70] Крім того, нормативні акти не вказують, які заходи кібербезпеки мають бути впроваджені, і вимагають лише «розумного» рівня безпеки. Нечітка мова цих нормативних актів залишає багато можливостей для тлумачення.

«Національна стратегія безпеки кіберпростору» 2003 року значною мірою відмовляється від зобов'язання компаній вживати певних заходів. [57] Натомість основна ідея документу, щоб уряд співпрацював з приватним сектором для створення системи екстреного реагування на кібератаки та зменшити вразливість країни до таких загроз.

Уряди штатів намагалися покращити кібербезпеку, збільшивши публічну видимість фірм із слабкою безпекою. У тому ж 2003 році Каліфорнія прийняла Закон про повідомлення про порушення безпеки, який вимагає, щоб будь-яка компанія, яка зберігає особисту інформацію громадян Каліфорнії та має порушення безпеки, повинна розкривати подробиці події. [46]

Кілька інших штатів наслідували приклад Каліфорнії та прийняли подібні правила сповіщення про порушення безпеки. Такі правила сповіщення про порушення безпеки карають фірми за їхні збої в кібербезпеці, надаючи їм свободу

вибору способів захисту своїх систем. Крім того, положення створює стимул для компаній добровільно інвестувати в кібербезпеку, щоб уникнути потенційної втрати репутації та відповідних економічних втрат, які можуть виникнути в результаті успішної кібератаки. [54]

Конгрес США запропонував численні законопроекти, які розширюють регулювання кібербезпеки. Закон про безпеку та сповіщення даних споживачів вносить зміни до Закону Грамма-Ліча-Блілі, які вимагають розкриття фактів порушення безпеки фінансовими установами. Конгресмени також запропонували «розширити Закону Грамма-Ліча-Блілі на всі галузі, які торкаються фінансової інформації споживачів, включаючи будь-яку фірму, яка приймає оплату кредитною карткою». [91]

12 травня 2011 року президент США Барак Обама запропонував пакет законодавчих реформ у сфері кібербезпеки для покращення безпеки громадян США, федерального уряду та критичної інфраструктури. Послідував рік публічних дебатів і слухань у Конгресі, в результаті чого Палата представників прийняла законопроект про обмін інформацією, а Сенат розробив компромісний законопроект, спрямований на баланс між національною безпекою, конфіденційністю та інтересами бізнесу.

У липні 2012 року сенатори Джозеф Ліберман і Сьюзен Коллінз запропонували Закон про кібербезпеку 2012 року. [7] Законопроект передбачав створення добровільних «стандартів найкращої практики» для захисту ключової інфраструктури від кібератак, до прийняття яких підприємства заохочували б за допомогою таких стимулів, як захист від відповідальності. Законопроект був поставлений на голосування в Сенаті, але не був прийнятий. Обама висловив свою підтримку Закону і його також підтримали офіційні особи в армії та національній безпеці. Як повідомляє The Washington Post, експерти заявили, що неприйняття закону може зробити Сполучені Штати «вразливими для широкого хакерства або серйозної кібератаки». [73]

У лютому 2013 року Обама запропонував Указ про покращення кібербезпеки критичної інфраструктури. [47] Розпорядження розроблено для підвищення рівня основних можливостей критичної інфраструктури для управління кіберризиками. Це робиться, зосереджуючись на трьох ключових сферах: обмін інформацією, конфіденційність і впровадження практик кібербезпеки. доручив Національному інституту стандартів і технологій (NIST) співпрацювати з приватним сектором, щоб визначити існуючі добровільні узгоджені стандарти та найкращі галузеві практики та включити їх у структуру кібербезпеки. [25] Адміністрація визнає, що є кібер-лідери приватного сектора, які вже впроваджують жорсткі засоби контролю, політики, процедури та інновації в галузі кібербезпеки, і попросила ці компанії допомогти нам сформувати найкращі практики в критичній інфраструктурі.

У січні 2015 року Обама оголосив про нову законодавчу пропозицію щодо кібербезпеки. Виконавчий наказ 13691 «Сприяння обміну інформацією про кібербезпеку в приватному секторі» [48], також визнає, що організації, які займаються обміном інформацією про ризики та інциденти в кібербезпеці, відіграють неоціненну роль у колективній кібербезпеці Сполучених Штатів. Цей виконавчий наказ заохочує розвиток організацій з аналізу обміну інформацією (Information Sharing Analysis Organizations - ISAO), які слугуватимуть координаційними центрами для обміну інформацією з кібербезпеки та співпраці в приватному секторі, а також між приватним сектором і урядом. Наказ також вимагає, щоб організації «захищали конфіденційність і громадянські свободи осіб, зберігаючи ділову конфіденційність, захищаючи інформацію, яка передається...». Метою організацій є збір та аналіз інформації про критичну інфраструктуру, щоб краще зрозуміти проблеми кібербезпеки та взаємозалежності, повідомляють або розкривають інформацію про критичну інфраструктуру, щоб допомогти запобігти, виявити, пом’якшити або відновити наслідки кіберзагроз, або добровільно поширювати інформацію про критичну

інфраструктуру своїм членам або інші залучені до виявлення та реагування на проблеми кібербезпеки.

Щонайменше 40 штатів представили або розглянули понад 250 законопроектів або резолюцій, які значною мірою стосуються кібербезпеки. 24 штати прийняли принаймні 41 законопроект у 2022 році. Найпоширенішими нормативними актами у 2022 році були: [26]

- вимагати від державних установ впровадження навчання з кібербезпеки;
- створювати та дотримуватися формальної політики, стандартів і практик безпеки;
- мати плани реагування на інциденти;
- забезпечити обов'язкове навчання працівників;
- повідомляти про інциденти безпеки, включаючи атаки програм-вимагачів.

Компанії можуть розглядати нові правила як можливість підготуватися до більшої прозорості кібербезпеки. У Сполучених Штатах два правила кібербезпеки, ймовірно, вплинуть на кілька галузей комерційного сектора. По-перше, Закон про звітність про кіберінциденти для критичної інфраструктури (CIRCIA) [23], підписаний у березні 2022 року, вимагатиме від компаній критичної інфраструктури, включаючи фінансові послуги, повідомляти про інциденти кібербезпеки, такі як атаки програм-вимагачів, до Агентства з кібербезпеки та безпеки інфраструктури (CISA). Крім того, Комісія з цінних паперів і бірж США (SEC) у березні 2022 року запропонувала правило, яке вимагає від публічно зареєстрованих компаній повідомляти SEC про інциденти кібербезпеки, їхні можливості кібербезпеки, а також досвід і нагляд у сфері кібербезпеки з боку правління (див. бічну панель, «CISA та SEC будуть створити вимоги США щодо звітності щодо кібербезпеки»). [11]

Відповідно до CIRCIA [23], компанії в секторах критичної інфраструктури повинні будуть створити та підтримувати можливість повідомляти про інциденти протягом необхідних часових рамок (24 або 72 години, залежно від події). Вимоги щодо звітності унеможливлять спокійну оплату викупу під час нападу. Тому буде важливо створити єдину стратегію захисту та реагування на кібербезпеку.

Згідно з правилами SEC, усі публічні компанії повинні розкривати інформацію про свої інциденти та захист своїм інвесторам та акціонерам. Тому члени правління повинні розуміти та вміти описати — і, ймовірно, захистити — положення своєї компанії щодо кібербезпеки. Для цього радам директорів, ймовірно, доведеться більше, ніж будь-коли, займатися питаннями кібербезпеки.

У майбутньому компанії можуть отримати вигоду від посилення захисту та реагування на кібербезпеку, одночасно розглядаючи кроки для підготовки до дотримання чинних нормативних актів. На нинішньому етапі нормотворчого процесу SEC запропоноване правило не має жорсткого порогу для суттєвості інцидентів кібербезпеки. Компаніям, ймовірно, доведеться попрацювати з усіма відділами інформаційної безпеки та юридичними відділами, щоб встановити порогове значення для звітності. В ідеалі вони мали б розглянути потенційну потребу повідомляти про серйозні кіберінциденти, але мати можливість уникнути надмірного обміну інформацією, яка не вимагається положеннями про розкриття інформації, і керувати ризиком для репутації.

Подібним чином, оскільки компанії дотримуються нових вимог до звітності щодо можливостей реагування на інциденти кібербезпеки, їм потрібно керувати ризиком надмірного використання своєї інтелектуальної власності та своєї позиції кіберзахисту. Завищене повідомлення про інтелектуальну власність ризикує розголошенням корпоративних секретів може дозволити конкурентам отримати потенційну перевагу; надмірний обмін інформацією про кіберзахист

може дати хакерам можливість використовувати розкриту інформацію для компрометації мереж компанії. IT та кібербезпека повинні співпрацювати з керівництвом компанії, особливо з керівниками ризиків і юристами, щоб забезпечити дотримання нормативних вимог, не наражаючи компанію на подальший ризик. [11]

Оскільки розвиток технологій рухається невпинно, державне законодавство теж має відповідати сучасним реаліям, аби державу було важко дестабілізувати. У березні 2023 року адміністрація президента Байдена презентувала Національну стратегію кібербезпеки. Аналізуючи її, можна зрозуміти, що Сполучені Штати налаштовані досить серйозно з приводу захисту своїх комунікацій: «Наша ціль — надійна, стійка цифрова екосистема, де атакувати системи обходиться дорожче, ніж захищати їх, де конфіденційна або приватна інформація безпечна та захищена, і де ані інциденти, ані помилки не призводять до катастрофічних системних наслідків».

Існує велика кількість досліджень того, як політики вживають займенники, зазвичай стратегічно, щоб продемонструвати силу, солідарність або авторитет. [61] Проаналізувавши «Вступ» Стратегії, що загалом налічує 2681 слів, слово «МИ» було зазначено 17 разів, слово «НАШ» - 27, та слово «США» у варіяціях «U.S», «The United States», «The Federal Government» - 13.

«*Ми* (1) закладаємо основу для глобальної співпраці в режимі реального часу, використовуючи величезні обсяги даних і обчислювальну потужність, які дозволять розблокувати наукові відкриття та інші суспільні блага, про які *Ми (2)* ще не можемо уявити. Досягнення цього бачення процвітаючого, пов'язаного майбутнього залежатиме від кібербезпеки та стійкості базових технологій і систем. *Ми* (3) засвоїли важкі уроки та досягли значного прогресу у спільному захисті нашої цифрової екосистеми».

У дослідженні політичної мови опора на «ми» є ще більш яскравою щодо того, як вона може маніпулювати та що вона може приховати. Часто це передбачає

консенсус або колективний мандат, коли його насправді не існує. Використання «ми» може бути методом, за допомогою якого лідери прагнуть отримати легітимність. «Ми» є важливим займенником у політичних промовах у тому сенсі, що він виражає «інституційну ідентичність», тобто коли одна особа говорить як представник або від імені установи. «Ми» також використовується, щоб відокремити нас від них, наприклад, між двома політичними групами, такими як політичні партії. [51] У всіх випадках в вище зазначеному уривку слово «Ми» зазначається зі сторони адміністрації Президента і одночасно об'єднує народ держави, адже використовуючи «Ми» (1), підкреслюється першість США у формуванні укладу відносин у кіберпросторі. У випадку (3) «важкі уроки» були засвоєні і урядом США і громадянами, наприклад, з втручання у президентські вибори.

3.2. Партнерство США у забезпеченні безпечного використання ІКТ

Оскільки впровадження цифрових технологій стрімко поширюється по всьому світу, а зростання економічного добробуту в багатьох країнах стає тісно пов’язаним із підключенням до Інтернету, з’являється інше важливе питання. Яким чином можна гарантувати, що ця цифрова трансформація базується на відкритих і безпечних технологіях, сприяє всеохоплюючому зростанню, сприяє створенню стійких і демократичних суспільств і розширює можливості для всіх, включаючи найбільш вразливих? Як можна переконатися, що технології не використовуються для моніторингу населення, обмеження доступу громадян до інформації та використання вразливості робочої сили, яка не навчена боротися з витоками даних і кібератаками?

Незважаючи на те, що США є однією з найбільш розвинених технологічно держав, Америка все одно сприяє міжнародній співпраці в галузі мережевих технологій і законодавства, щоб запобігти атакам і збиткам від міжнародного тероризму через мережу. Так, започатковане в липні 2018 року Партнерство з

цифрового підключення та кібербезпеки (DCCP) [33] є загальноурядовою ініціативою, яка спрямована на:

- Розширення та збільшення безпечного доступу до Інтернету на цільових ринках, що розвиваються, забезпечивши вихід на ринок технологічних компаній, зокрема американських;
- Збільшення прийняття політики та регуляторних позицій, які заохочують відкриту, сумісну, надійну та безпечну цифрову інфраструктуру;
- Сприяння експорту товарів і послуг у сфері інформаційно-комунікаційних технологій (ІКТ) США та збільшення ринкової частки компаній США на цільових ринках;
- Збільшення впровадження найкращих практик кібербезпеки в цільових країнах.

Під керівництвом Агентства США з міжнародного розвитку (USAID) і Державного департаменту США DCCP співпрацює з країнами-партнерами для підтримки розвитку комунікаційної інфраструктури, сприяння прозорій регуляторній політиці для відкритих конкурентних ринків, і нарощування потенціалу партнерів у сфері кібербезпеки для протидії спільним загрозам шляхом взаємодії з приватним сектором, урядом і громадянським суспільством.

Проте, в напрямку розвитку ІКТ, США більше працює в двосторонньому форматі з різними державами в рамках розбудови більш всеосяжної підтримки. Більш того, розширення співпраці з чималою кількістю партнерів відбулось у 2022 році. Наприклад, 7 березня 2022 Сполучені Штати та Танзанія підписали Меморандум про взаєморозуміння [41], який встановлює партнерство для нарощування потенціалу та співпраці у сфері 5G, кібербезпеки та пов’язаної нормативної політики та механізмів. Під час двосторонньої зустрічі у квітні 2022 року президент Самія та віце-президент Гарріс зобов’язалися зосередитися на зміцненні партнерства США та Танзанії у сфері кібербезпеки та інформаційно-

комунікаційних технологій (ІКТ). Відтоді Сполучені Штати тісно співпрацювали з урядом Танзанії, щоб провести регіональний семінар з ІКТ; надано технічну допомогу з питань 5G, кібербезпеки та боротьби з кіберзлочинністю; і сприяв збільшенню інвестицій США в сектор ІКТ Танзанії.

Протягом 2021-2022 США та Японія поступово розширюють співпрацю у різних напрямах: економіка, енергетика, торгівля, тощо. Обидві держави визнали одна одну лідерами інноваційних технологій. Тому у 2022 вони об'єднали свої зусилля у зміцненні конкурентоспроможності в цифровій сфері шляхом інвестування в дослідження, розробку, тестування та розгортання безпечних мереж і передових ІКТ, включаючи 5G і мобільні мережі наступного покоління («6G» або «Beyond 5G»). [39] Сполучені Штати виділили 2,5 мільярда доларів на ці зусилля, а Японія виділила 2 мільярди доларів. Також, було окреслено розвиток співробітництва між США та Японією в третіх країнах і запуск Глобального партнерства з цифрового підключення, щоб сприяти безпечному підключенню та жвавій цифровій економіці, одночасно зміцнюючи потенціал партнерів у сфері кібербезпеки для боротьби зі спільними загрозами; посилення співпраці та обмін інформацією між американськими та японськими експертами з ІКТ у розробці глобальних стандартів.

На саміті G7 у 2023 році в Хіросімі, Японія, лідери G7 підтвердили свою прихильність визначати нові можливості для розширення Партнерства для глобальної інфраструктури та інвестицій. [37] Сполучені Штати співпрацюють з урядом Коста-Ріки над підвищенням цифрової безпеки та підключення в країні. Державний департамент виділить приблизно 25 мільйонів доларів США на зміцнення можливостей кіберзахисту Коста-Ріки, включно з навчальними операціями, обладнанням, програмним забезпеченням і довгостроковим розвитком потенціалу.

У травні 2022 року президент Байден і прем'єр-міністр Моді оголосили про американсько-індійську ініціативу щодо критично важливих і нових технологій

(iCET) [40], спрямовану на підвищення та розширення нашого стратегічного технологічного партнерства та оборонно-промислового співробітництва між урядами, підприємствами та науковими установами наших двох країн. В рамках цієї ініціативи було підписано Угоду про впровадження партнерства дослідницького агентства між Національним науковим фондом та індійськими науковими агенціями [71] з метою розширення міжнародної співпраці в низці сфер, включаючи штучний інтелект, квантові технології та передовий бездротовий зв'язок, для побудови надійної інноваційної екосистеми між нашими країнами.

Проте, США не менш зосереджені і на розвитку внутрішньої системи ІКТ. Щоб зміцнити лідерство США та сприяти інтересам національної безпеки, Конгрес схвалив виділення Державному департаменту США 500 мільйонів доларів США протягом п'яти років через Закон CHIPS для вирішення ключових проблем у галузі інформаційно-комунікаційних технологій (ІКТ) і напівпровідникової промисловості. [67] Цей Міжнародний фонд технологічної безпеки та інновацій (ITSI) має амбітні цілі щодо диверсифікації ланцюгів постачання, захисту кібермереж, а також надання потенціалу та технічної допомоги в цьому просторі — і все це з відносно невеликим капіталом. Щоб максимізувати вплив фонду, Державний департамент повинен ефективно координувати роботу з іншими департаментами та відомствами США, партнерами та союзниками, а також приватним сектором. Він також має зосередити фонд як географічно, так і в ключових видах діяльності, таких як підвищення банківської спроможності проекту, сприяння розвитку робочої сили, моніторинг ланцюгів постачання та підтримка зусиль із розширення надійних, економічно ефективних технологій і продуктів.

3.3. Використання кіберпростору у політичних цілях

Глобальний відкритий Інтернет служить стратегічним, економічним, політичним і зовнішньополітичним інтересам держав. Сполучені Штати є асиметрично вразливими через високий рівень оцифрування та сильний захист свободи слова. Противники адаптувалися швидше, ніж очікувалося. Вони мають чітке бачення своїх цілей у кіберпросторі, розробляють і впроваджують стратегії, що відповідають їхнім інтересам, і ускладнюють роботу Сполучених Штатів у цій сфері.

У всьому світі держави з будь-яким режимом примусово локалізують дані, а також блокують і модерують вміст. Ранні лідерські позиції Сполучених Штатів в Інтернет-технологіях спонукали багато країн сприяти резидентності даних (збереження даних користувачів, відповідно до їх місцезнаходження) та іншим нормам для захисту національних компаній. Китай деякий час блокував доступ до іноземних веб-сайтів, створював торговельні бар'єри для американських технологічних компаній і віддавав перевагу вітчизняним компаніям, які зараз працюють по всьому світу. [67] Європейські політики все більше зосереджуються на необхідності передбачуваної цифрової самодостатності та конфіденційності даних. Війна між Росією та Україною сприяла розколу: Москва спочатку придушила, а потім заборонила американські соціальні мережі, а американські компанії, що займаються апаратним і програмним забезпеченням, пішли з російського ринку. [85]

Дослідники, що цікавляться наступальними кібероперaціями США, стикаються з певними труднощами у цьому напрямку, оскільки уряд незацікавлений в тому, аби така інформація виходила назовні. У публічному доступі існує інформація про кілька викритих кібероперацій, які були в основному низького рівня та здебільшого не ескалаційними (націленими на Китай, Іран, Північну Корею та Росію). Проте майже немає інформації – за винятком найзагальніших – про кібератаки вищої інтенсивності, які

передбачають багатохвильові, багатовекторні, багатотеатральні та широкомасштабні напади. Американський кібернауковець Мартін Лібікі [60] стверджує, що Сполучені Штати ще не відповіли на жодну кібератаку з дійсно серйозними наслідками, які може побачити решта світу. Проте, це може бути пов'язане з небажанням підірвати довіру партнерів.

У США є добре розвинена стратегія кібероперацій, яка напрацьовувалась протягом трьох-чотирьох десятиліть. У розробці стратегії та доктрини операцій США в кіберпросторі існує п'ять широких напрямків: шпигунство, політика сили, внутрішня безпека в кіберпросторі, конфлікти низької інтенсивності та війни високої інтенсивності. Політики та можливості мали, як правило, нерівномірну еволюцію, іноді позначаючись прогресом, а часто – паузою. Це шлях, який часто спостерігається, коли країна вирішує застосувати надзвичайно руйнівні технології для задоволення традиційних політичних потреб. Процес інституціоналізації наступальних кібероперацій (нові доктрини, нові організаційні структури, масштабні програми набору та навчання) майже завжди відставав від оперативного використання можливостей у скромних формах або на пробній основі.

Спроможність Сполучених Штатів проводити глобальні інформаційні операції демонструє досить послідовну траєкторію зростання з початку 1980-х років. З поширенням кібертехнологій у цьому десятилітті США перейшли до наступальних застосувань цих технологій принаймні ще в 1990 році. До 1996 року цей інтерес дозрів і почав формуватися, оскільки лідери почали розглядати кіберкампанії як потужний і необхідний елемент національної стратегії. Урядовий інтерес був підкріплений усвідомленням того, що США можуть отримати стратегічну перевагу. Це була єдина наддержава в базових технологіях, яка мала кіберпромисловий комплекс, з яким не міг би зрівнятися жодний потенційний супротивник. У 2021 році IISS оцінив, що «наступальні

кіберпотенціали США розвинені більше, ніж у будь-якій іншій країні», значною мірою через «здатність використовувати складні можливості в масштабі». [28]

Хоча більшість загальнодоступної інформації про кіберкампанії США стосується Міністерства оборони (DoD), Агентства національної безпеки (NSA) і кіберкомандування США, ЦРУ є головним актором і зацікавленою стороною, навіть якщо про його кібероперації мало що відомо. На одному рівні можна розподілити відповідальність за різні аспекти наступальних кібероперацій Сполучених Штатів між цими організаціями, при цьому Міністерство оборони та Кіберкомандування візьмуть на себе відповідальність за місії, орієнтовані більше на кібердиверсійні операції, а ЦРУ — за операції кібервпливу (насамперед політичного впливу). Проте його відзнака погано відображатиме те, наскільки тісно ці агенції співпрацюють і залежать одна від одної для аналізу розвідданих та оперативної підтримки в наступальних операціях. Міністерство оборони має високорозвинені стратегії та механізми відкритого політичного впливу, які іноді мають таємні елементи. ЦРУ має власні внутрішні можливості кібердиверсій, яким позаздрили б більшість урядів. Крім того, інституційна практика кіберкампаній часто передбачала створення робочих груп із залученням команд із різних установ, які працюють разом. Помітним успіхом такого процесу стала Робоча група з активних заходів, координована Радою національної безпеки (NSC) у 1981 році для протидії радянській дезінформації, яка передбачала публічні чи таємні дії зацікавлених агенцій або відповідних можливостей (включаючи ЦРУ, Міністерство оборони та Державний департамент). Більш свіжим прикладом є «російська група», очолювана кіберкомандуванням, спрямована на протидію операціям російського впливу, до складу якої входять представники ФБР, ЦРУ та Департаменту внутрішньої безпеки.

Під час проведення наступальних кібероперацій учасники бойових дій повинні дотримуватися правил, викладених у Спільній публікації 3-12. [27] Цей документ визначає наступальні кібероперації як сплановані дії, що виконуються

організованою групою з визначеною метою в апаратному та програмному забезпеченні та за допомогою них, що використовується для створення, обробки, зберігання, отримання та розповсюдження інформації в різних типах взаємопов'язаних мереж, які створюють велику глобальну мережу, побудовану та використовувану дуже різноманітними людьми. Вкрай важливо, щоб у міру переходу війни з традиційного поля бою на цифрове кібервоїни визначили правила бойових дій, за якими діяти. У відповідь на збиття MQ-4 Triton, військового безпілотника вартістю 240 мільйонів доларів США, кіберкомандування США провело наступальну кібероперацію, націлену на базу даних, яка використовувалася «іранською шпигунською групою… для відстеження та націлювання на військові та цивільні кораблі, що проходять через економічну зону Важливо відзначити, що перед нападом у червні 2019 року колишній президент США Трамп повернувся до кібервідповіді на відміну від кінетичної реакції, коли він дізнався, що в результаті останньої загине кілька іранців. [12] Незважаючи на те, що наступальні кібероперації не спрямовані на загибель людей, вони можуть призвести до супутніх збитків, через що кібероператори стають ціллю як цифрових, так і фізичних.

У разі кібератаки на критично важливу інфраструктуру США основним агенством у відповідь буде Агентство з кібербезпеки та безпеки інфраструктури США (CISA). CISA доручено захистити 16 критичних секторів інфраструктури у співпраці з іншими галузевими агентствами, такими як міністерства сільського господарства, енергетики, оборони та фінансів США. Активи, системи та мережі цих 16 секторів, чи то фізичні чи віртуальні, є дуже важливими для Сполучених Штатів, що у разі їх виведення з ладу або знищення матиме виснажливий вплив на національну безпеку, економіку, громадське здоров'я та безпеку. 16 секторів є хімічними; комерційні об'єкти; комунікації; критичне виробництво; дамби; оборонно-промислова база; екстрені служби; енергія; фінансові послуги; сільське господарство та продовольство; державні установи; IT; ядерні реактори,

матеріали та відходи; громадське здоров'я та охорона здоров'я; транспортні системи; системи водопостачання та водовідведення.

Наприклад, виборча інфраструктура, яка відноситься до сектору державних установ, включає широкий спектр фізичних та електронних активів, таких як сховища, виборчі дільниці та централізовані місця підрахунку голосів, на додаток до інформаційно-комунікаційних технологій (ІКТ), таких як виборці реєстраційні бази даних, машини для голосування та інші системи, необхідні для управління виборчим процесом, звітування та відображення результатів від імені державних і місцевих органів влади.9 Одним із найважливіших завдань у захисті національної безпеки США є запобігання втручанню в демократичний процес і, хоча федеральний виборам у цьому відношенні приділяється більше уваги, захист державних і місцевих виборів є не менш важливим. [35]

Сполучені Штати організаційно добре підготовлені до проекції влади в кіберпросторі та через нього. Основним обмеженням, здається, є низький рівень консенсусу керівництва щодо політичної користі кібердиверсійних операцій для стратегічного ефекту – обмеження, яке, ймовірно, не є фактором для операцій політичного впливу чи втручання. Відсутність консенсусу щодо кібердиверсійних операцій посилюється відносно низьким рівнем знань еліт щодо їхнього потенціалу. Загальнодоступні відомості про операції США свідчать лише про епізодичні кампанії кібердиверсій, найвідомішою з яких є знищення Stuxnet тисяч іранських центрифуг для ядерного збагачення. [68] Ця кампанія мала дві мети: показати, що можливі значні некінетичні атаки проти Ірану, і надати Тегерану чітке повідомлення про те, що він не може продовжувати свою політику поза межами міжнародного нагляду. В іншому випадку США діяли досить обережно щодо можливих негативних наслідків таких кампаній і не сподівалися серед політичних лідерів, що кібероперації можуть дати стратегічно важливі результати.

Американські фахівці деякий час обдумували (через вагомі оперативні та юридичні причини), перш ніж застосувати кібердиверсійні операції проти Ісламської держави (ІДІЛ) у 2016 році, і робили це лише в обмеженому порядку. Операцію координувала міжвідомча оперативна група під керівництвом кіберкомандування. [74] Загалом США використовували наступальні кібердиверсійні операції пізніше в ході політичного конфлікту, ніж Росія. Звіти про операції кібервпливу США були менш суттєвими в деталях, але можна припустити, що використання таких інструментів було незмінною частиною політики США і проводилося головним чином Центральним розвідувальним управлінням, в основному покладаючись на підтримку Національного управління США. Кіберкомандування бере участь у наступальних кібероперациях переважно через свою стратегію «захищатися вперед», згідно з якою воно працює в мережах противника, щоб перешкоджати поточним атакам.

США використовували наступальні кібероперації досить обережно щодо можливих негативних наслідків і без сильного очікування серед політичних лідерів, що кібероперації можуть дати стратегічно важливі результати. Найагресивніша кампанія США – проти ІДІЛ – ймовірно, сприяла її поразці на землі, але оцінити її вплив важко. Найважливіший висновок із тематичних досліджень полягає в тому, що лідери США наразі використовували кіберкампанії не для досягнення стратегічних результатів, а радше як допоміжний захід, щоб зірвати чи створити додатковий тиск на цільові країни.

РОЗДІЛ 4
КІБЕРПРОСТІР РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ТА ЙОГО МОЖЛИВОСТІ

4.1. Самопозиціонування згідно з законодавчою базою

Оцінки кіберпотуги Росії, висловлені ключовими офіційними особами США, класифікують Російську Федерацію як одну з провідних держав у кіберпросторі. [9] Російські погляди на природу, потенціал і використання кіберпростору суттєво відрізняються від західного консенсусу. Зокрема, Росія глибоко стурбована принципом неконтрольованого обміну інформацією в кіберпросторі та презумпцією, що національні кордони мають там обмежене значення. Розповсюдження інформації, яка створює передбачувану загрозу суспільству чи державі та суверенітету «національного Інтернету» є ключовими проблемами безпеки в Росії. Ця розбіжність підриває спроби досягти згоди щодо спільних принципів або правил поведінки в кіберпросторі з Росією, незважаючи на неодноразові спроби Росії представити подібні норми, до яких інші держави запрошуються приєднатися. [45]

Внутрішнє законодавство Російської Федерації, що стосується регулювання кіберпростору, можна згрупувати за трьома заголовками: (1) відповідні конституційні положення; (2) закони та нормативні акти, що стосуються саме питань кіберпростору; (3) Кримінальний кодекс і Кодекс про адміністративні правопорушення. Конституція Російської Федерації була прийнята 12 грудня 1993 року і набула чинності 25 грудня 1993 року. До неї кілька разів вносилися зміни, найбільш суттєві – у 2020 році. Конституція містить кілька положень, які прямо чи опосередковано стосуються кіберпростору. Конституційні положення, що стосуються прав людини та основних свобод, застосовуються як офлайн, так і в кіберпросторі. Згідно зі статтею 23(1), «кожен має право на недоторканність приватного життя, особистої та сімейної таємниці, захист своєї честі та доброго імені», а другий абзац цієї ж статті передбачає, що «кожна має право на таємницю

листування, телефонних розмов, поштових, телеграфних та інших повідомлень. [2] Обмеження цього права допускається лише на підставі рішення суду». Крім того, згідно зі статтею 24(1), «збирання, зберігання, використання та поширення інформації про особисте життя особи без її згоди не допускається». Стаття 29(4) передбачає, що «кожен має право вільно шукати, отримувати, передавати, виробляти та поширювати інформацію будь-яким законним способом», а стаття 29(5) визначає, що «свобода ЗМІ гарантується» та «цензура заборонена». Стаття 43(5) пояснює, що Російська Федерація «підтримує різні форми освіти та самоосвіти», що набуло нового практичного значення в умовах пандемії COVID-19. Так само тимчасовий перехід судової діяльності в онлайн-формат надав нового змісту статті 46(1) (яка передбачає, що «кожному гарантується судовий захист його прав і свобод») та статтям 47–54 (які стосуються право на справедливий суд).

Законодавчий орган РФ - Державна дума прийняла кілька законів, що стосуються кіберпростору. Примітно, що більшість цих нормативних документів загалом не посилаються на міжнародне право, а натомість зосереджуються на національних інтересах і безпеці Росії. Варто зауважити, що лише один із цих документів містить визначення, яке близьке до визначення «кіберпростору» як такого. Федеральний закон № 85-ФЗ «Про участь у міжнародному обміні інформацією» був прийнятий 5 червня 1996 року зі змінами і доповненнями в 2003 і 2004 роках. [5] Федеральний закон складається з 23 статей, об'єднаних в чотири глави. Відповідно до частини першої статті 1, цілями Федерального закону є «створення умов для ефективної участі Росії в міжнародному інформаційному обміні в рамках єдиного світового інформаційного простору, захисту інтересів Російської Федерації, суб'єктів Російської Федерації». Федерація і муніципалітети під час міжнародного інформаційного обміну, захист інтересів, прав і свобод фізичних і юридичних осіб під час міжнародного інформаційного обміну». Серед іншого, основні положення Закону регулюють

обмеження у здійсненні міжнародного обміну інформацією (ст. 8); доступ до засобів міжнародного інформаційного обміну та іноземної інформаційної продукції (ст. 12); та координація діяльності у сфері міжнародного обміну інформацією (ст. 15). Той факт, що з 1996 року цей Федеральний закон змінювався лише двічі, ймовірно, означає, що більшу практичну вагу в регулюванні Інтернету надають підзаконні акти, такі як Доктрина інформаційної безпеки.

9 жовтня 2000 року Президент Російської Федерації затвердив Доктрину інформаційної безпеки Російської Федерації. 5 грудня 2016 року Указом № 646 набула чинності нова Доктрина інформаційної безпеки. [4] Відповідно до пункту 5, Доктрина розвиває відповідні положення Стратегії національної безпеки від 31 грудня 2015 року та є нормативною основою державної політики у сфері інформаційної безпеки. Він не визначає кіберпростір як такий і зосереджується на методах і засобах забезпечення інформаційної безпеки країни. У Доктрині, серед іншого, перераховуються національні інтереси Росії в інформаційній сфері, розглядаються основні інформаційні загрози (частина III), окреслюються основні напрями інформаційної політики Росії у військовій, економічній, науково-технічній та освітній сферах.

Частина V визначає організацію інформаційної безпеки, зокрема, що стосується функцій законодавчої, виконавчої та судової влади. Важливо, що в 19 пункті звертається увага на: «Відсутність міжнародно-правових норм, що регулюють міждержавні відносини в інформаційному просторі, а також механізмів і процедур їх застосування, які б враховували специфіку інформаційних технологій, ускладнює формування системи міжнародної інформаційної безпеки, спрямованої на досягнення стратегічної стабільності та рівноправного стратегічного партнерства». Цей підхід є досить зручним з практичної точки зору, оскільки нібито відсутність міжнародно-правового

регулювання в кіберпросторі передбачає більшу свободу дій як для державних, так і для недержавних суб'єктів з відносною безкарністю.

Паралельно з розвитком нормативно-правової бази, що застосовується до кіберпростору, створювалась і система органів, які б могли здіснювати відповідні повноваження. Таким чином, російські кібератори включають [88]:

- Федеральна служба безпеки (ФСБ) є основним внутрішнім органом безпеки та розвідки. У кібернетичному просторі можливості ФСБ розподіляються між тими, які агентство створювало з кінця 1990-х років (18-й центр, або Центр інформаційної безпеки), і можливостями, які ФСБ придбала в 2003 році, коли поглинула кілька відділів російської електронної розвідки (ELINT). Федеральне агентство урядового зв'язку та інформації або FAPSI (16-й центр ФСБ або Центр радіоелектронної розвідки у зв'язку).
- Служба зовнішньої розвідки (СЗР) — російське розвідувальне агентство, прямий спадкоємець відділу зовнішньої розвідки КДБ. Агентство ніколи не проходило структурних реформ, але в 2010-х його можливості були значно розширені, в тому числі в кіберсфері.
- Військові: кіберпотенціал російської армії управляється двома управліннями в російському Генеральному штабі: ГУ (або Головне розвідувальне управління та 8-е управління). не було запущено, незважаючи на кілька спроб на початку 2010-х років.
- Адміністрація президента: прямий спадкоємець ЦК Комуністичної партії, адміністрація президента контролює розвідку та служби безпеки Росії. Невід'ємною частиною управління є Рада безпеки Росії, яка забезпечує стратегічне мислення в усіх сферах національної безпеки, включаючи кібернетичну; це також урядовий орган, якому доручено підтримувати контакт із західними партнерами, включаючи кібер-«червону лінію» між Москвою та Вашингтоном.

- Приватні компанії з кібербезпеки: ці компанії пов’язані з кіберзаходами Росії через мережі офіційних і неофіційних контактів. Їхня роль полягає в тому, щоб надати експертні знання та допомогти у працевлаштуванні.

Військова діяльність Росії в інформаційному просторі «включає заходи штабів і дії військ із збору розвідувальної інформації, оперативного обману, радіоелектронної боротьби, зв’язку, прихованого й автоматизованого управління, інформаційної роботи штабів, захисту інформаційних систем від радіоелектронних, комп’ютерних засобів. та інші впливи». Як і в інших публічних заявах Росії та на відміну від подібних заяв інших країн і відкритої підготовки цих держав, у Поглядах немає жодної згадки про наступальну кіберактивність. У Росії термін «інформатизація», який відноситься до інтенсивного дослідження та використання цифрових інструментів для соціального та економічного прогресу, часто використовується владою, тоді як термін «кібер» зазвичай зарезервований для медичного та академічного секторів. Незважаючи на те, що терміни «кіберзлочинність» і «кібервійна» чи «кібератака» не зустрічаються в жодному з офіційних публічних документів, використання таких термінів, як інформаційна безпека, комп’ютерна інформаційна злочинність, комп’ютерна злочинність та інформаційний опір, дає зрозуміти, що уряд розрізняє звичайні кіберзлочини та кібервійну. У Росії кількість позовів, пов’язаних із конфіденційністю даних, зростає, і в цьому регіоні очікуються подальші дії щодо відповідності, а також більше судових роз’яснень. [92]

4.2. Російська агресія в кіберпросторі

Росія володіє цілим набором інструментів для дій у кіберпросторі, які є як інформаційно-технічними, так і інформаційно-психологічними та залучають державних акторів. Тим не менш, кожен інструмент підходить для окремих цілей, які варіюються від збору інформації для впливу на прийняття рішень до

доповнення кінетичних операцій. Також важливо розрізняти дії, спрямовані на внутрішню аудиторію, і дії, спрямовані на іноземні країни та різні групи в них.

Росія має довгу історію конфлікту з Грузією, особливо війна в серпні 2008 року, після якої Грузія втратила контроль над приблизно однією п'ятою своєї території. Грузія є одним із перших прикладів, де військові операції та кібератаки/інформаційні атаки використовувалися разом. Наприкінці липня 2008 року хакери зламали веб-сайт президента Грузії Михайла Саакашвілі, і до того, як російські війська вступили в прямий конфлікт, багато урядових сайтів вийшли з ладу. Хакери вивели з ладу найбільший комерційний банк країни та ЗМІ і зіпсували веб-сайти президента Грузії та Міністерства закордонних справ. Атаки координувалися на публічних форумах, які розповсюджували інструкції щодо затоплення веб-сайтів і надавали список цілей. Сайт StopGeorgia.ru оприлюднив повний список цілей лише через кілька годин після того, як російські війська перетнули кордон. Для цього знадобилася підготовка, і це свідчить про те, що організаторам сайту було повідомлено про час військових дій. [76]

Більш свіжим прикладом є масштабна кібератака проти Грузії в жовтні 2019 року, яка є прикладом невіддільності технічних і психологічних елементів підходу Росії до націлювання на своїх опонентів. Атака пошкодила сервери в офісі президента Грузії, судовій системі, урядових муніципалітетах і неурядових організаціях, зіпсувала веб-сайти та порушила трансляцію телевізійних станцій. 28 жовтня 2019 року понад 2000 сайтів державних (включно з Адміністрацією президента), приватних і громадських ЗМІ були зіпсовані з натяками на екс-президента Михайла Саакашвілі (зловмисники розмістили зображення Саакашвілі з текстом «Я повернуся»). Крім того, було зірвано мовлення двох приватних телеканалів – «Імеді» та «Маестро».

Злочинна кіберактивність, пов’язана з Росією, охопила останнє десятиліття. Зловмисна діяльність, пов’язана з російськими злочинними організаціями, становить значний кібернетичний потенціал. Російські злочинці володіють

помірно складними технологіями, але контролюють величезні онлайн-ресурси. Росія стоїть за серією кібератак з початку нового вторгнення в Україну, про це оголосили Великобританія та міжнародні союзники. [81]

З 2014 року адміністрація президента Барака Обами покарала три з чотирьох держав, які вважаються найбільшими кіберзагрозами комп'ютерним мережам США: Китай, Іран і Північну Корею. Цікавим винятком є Росія. У той час як високопоставлені чиновники США широко критикували Росію за її все більш агресивну поведінку в кіберпросторі США, ця держава не завжди офіційно прив'язує Росію до конкретної атаки. Вперше це було в 2015 році, коли міністр оборони Еш Картер звинуватив Москву в дослідженні системи Пентагону. [56]

Було виявлено втручання Росії у вибори в кількох країнах. Втручання у президентські вибори в США 2016 року є найбільш задокументованим випадком, який показує, як Росія використовує як інфотехнічні, так і інфопсихологічні інструменти. Це втручання передбачало атаки на виборчу інфраструктуру США, отримання та подальший витік даних Комітету з питань кампанії в Конгресі Демократичної партії (DCCC) і Національного комітету Демократичної партії (DNC), включно з електронною поштою кандидата від партії Гілларі Клінтон, а також широку інформаційну кампанію, проведену IRA та афілійованими з Росією ЗМІ. [78]

Втручання у президентські вибори у Франції 2017 року було скоординованою спробою дискредитувати Еммануеля Макрона за допомогою широкомасштабної кампанії з дезінформації, а також операції по злому та витоку інформації щодо штабу кампанії Макрона – так звані «витоки даних Макрона». [10] Фішингові атаки були спрямовані проти штабу кампанії Макрона з грудня 2016 року. У результаті облікові записи електронної пошти щонайменше п'яти близьких співробітників Макрона були зламані, зловмисники вкрали 15 гігабайт (ГБ) даних, включаючи 21 075 електронних листів, і оприлюднили їх. 5 травня — лише за два дні до другого й останнього раунду виборів.

Кібероперації використовувалися як частина більших кампаній, щоб перешкодити процесу розширення НАТО, який Кремль сприймає як агресивний і загрозливий. Це було у випадку Чорногорії, коли вона проходила свою останню фазу переговорів про вступ до НАТО наприкінці 2016 року. Росія здійснила кілька форм нападу: Чорногорія зазнала інформаційної кампанії російських ЗМІ, погроз ембарго на виробництво вина та іншої продукції, спроби державного перевороту під час парламентських виборів у жовтні 2016 року, а також кібератаки, які можна приписати російським спецслужбам (APT28 або Fancy Bear). За цей період у Чорногорії різко зросла кількість кібератак (проте не всі можна віднести до Росії), в основному проти державних установ і ЗМІ. [55]

Останні 2 роки кібероперації, ймовірно, зайняли перше місце в порядку денному США і Росії. Протягом багатьох років кількість і потужність російських кібероперацій, якими займаються як російські служби безпеки та розвідки, так і кіберзлочинці, зростали. У 2021 році Програмне забезпечення-вимагач, націлене на оператора нафтопроводу та виробника м'яса перед самітом у Женеві, змусило президента Байдена попередити президента Путіна, що США дадуть рішучу відповідь, якщо атаки з боку Росії будуть спрямовані на будь-який із 16 критичних секторів інфраструктури Сполучених Штатів. Через кілька тижнів після зустрічі інше злочинне угруповання розпочало ще одну широко розповсюджену атаку програм-вимагачів, націлену на сотні компаній у всьому світі. Це змусило Байдена зробити ще одне попередження Путіну під час телефонної розмови через тиждень після нападів, заявивши, що США вживуть «будь-яких необхідних заходів», щоб захистити себе. [82]

Росія ще не зіткнулася з масштабними наслідками своєї агресивної поведінки. Але враховуючи зростаючий консенсус серед експертів як в уряді США, так і за його межами, Росія стоїть принаймні за зломом Національного комітету Демократичної партії (якщо не за публічним оприлюдненням

викрадених документів через WikiLeaks), зростає тиск на Білий дім, щоб спробувати обмежити стримування кіберагресії Росії.

«З початку війни російські напади [на союзників України] були успішними у 29% випадків», — написав президент Microsoft Бред Сміт, причому дані були викрадені принаймні в одній чверті успішних мережевих вторгнень. «Оскільки коаліція країн об’єдналася, щоб захистити Україну, російські спецслужби активізували проникнення в мережу та шпигунську діяльність, націлену на уряди союзників за межами України», – сказав Сміт. Майже дві третини цілей кібершпигунства стосувалися членів НАТО. Сполучені Штати були головною ціллю, а Польща, основний канал військової допомоги, що надходить до України, була на другому місці. У 2022 Данію, Норвегію, Фінляндію, Швецію та Туреччину супроводжували посилені напади. Яскравим винятком є Естонія, де Microsoft заявила, що не виявила жодних російських кібервторгнень після того, як Росія вторглася в Україну 24 лютого. Компанія вважає заслугою впровадження Естонією хмарних обчислень, де легше виявити зловмисників. У деяких інших європейських урядів "зберігаються значні слабкості колективного захисту", заявила Microsoft, не називаючи їх. [63]

Російська діяльність у сфері кіберзагроз скоригувала націлювання та методи, розширивши доступ для підтримки збору розвідувальної інформації про Україну та підтримки цивільних і військових активів нації, а також створення передумов для руйнівних атак в Україні та за її межами. Розробка нових форм програм-вимагачів є прикладом цього, але інші форми включають використання соціальних медіа для просування піратського програмного забезпечення серед української аудиторії, яке потім забезпечує початковий доступ до організацій, а також кампанії підману, націлені на вразливі локальні сервери в уряді, ІТ та стихійних лихах. Також немає жодних географічних кордонів, які забороняють спроби здійснення російських атак. Актори, які займаються кіберзагрозами, які мають відомі або підозрювані зв’язки з російськими спецслужбами, намагалися

отримати початковий доступ до урядових і пов'язаних з обороною організацій не лише в Центральній та Східній Європі, але й в Америці. [96]

4.3. Російська кібервійна та боротьба з нею

Росія залишатиметься головною кіберзагрозою, оскільки вона вдосконалює та використовує свій потенціал для шпигунства, впливу та атак. Росія особливо зосереджена на покращенні своєї здатності націлюватися на критичну інфраструктуру, включаючи підводні кабелі та промислові системи управління, у Сполучених Штатах Америки. Держави, а також країни-союзники та партнери, тому що компрометація такої інфраструктури покращує та демонструє її здатність завдати шкоди інфраструктурі під час кризи. [83]

Лютий 2022 року став кульмінацією однієї з найбільш тривалих і масштабних інформаційних атак однієї держави на іншу в історії. Після 2014 року Україну можна вважати полігоном для випробувань Росії для наступальних кібер- та інформаційних операцій — головним чином для ведення політичної війни. Україна продемонструвала величезну оборонну силу та стійкість на фізичному полі бою, і те саме стосується й кіберпростору. Низький кіберуспіх Росії був надмірно визначеним результатом багатьох факторів, у тому числі недостатньої кіберпотужності та виняткових оборонних зусиль України та її партнерів. Щоб суттєво вплинути на війну такого масштабу, кібероперації повинні проводитися в такому темпі, який Росія, очевидно, могла б підтримувати щонайбільше декілька тижнів. Москва погіршила свою проблему потужності, вирішивши зберегти або навіть збільшити свою глобальну кіберактивність проти інших цілей і не повністю використавши кіберзлочинців як допоміжну силу проти України. Тим часом Росія, схоже, не бажає або не в змозі планувати та вести війну таким точним, керованим розвідкою способом, який є оптимальним для кібероперацій. Україна, зі свого боку, скористалася стійкою цифровою екосистемою, роками попередніх інвестицій у кібербезпеку та безпрецедентним

сплеском кіберпідтримки з боку найздатніших компаній і урядів світу. Деякі інші часто цитовані пояснення, як-от погане планування чи стриманість Росії, менш переконливі. Дев'ять місяців війни дали російським хакерам достатньо часу, щоб зрозуміти воєнні цілі Москви, але темпи згубних кібератак з часом упали, а не зросли. І оскільки російські війська наполегливо працюють над знищенням інфраструктури України та знущанням над населенням, російським хакерам не буде сенсу стримуватися.

Західні уряди спільно попередили в квітні 2022 про потенційну загрозу посилення зловмисної кіберактивності з боку Росії проти критичної інфраструктури у відповідь на санкції, запроваджені як покарання за її вторгнення в Україну. Агентства з кібербезпеки Сполучених Штатів, Британії, Австралії, Канади та Нової Зеландії, які разом утворюють альянс з обміну розвідувальною інформацією «П'ять очей», заявили, що війна може поставити організації в усьому світі під вплив кіберзлочинності. [75] 7 березня 2023 року Росія подала своє бачення Конвенції ООН про забезпечення міжнародної інформаційної безпеки до Робочої групи відкритого складу ООН з безпеки та використання інформаційно-комунікаційних технологій (OEWG). Якщо дев'ятисторінковий документ отримає популярність в ООН, він може підірвати відповідальність за дії держави в кіберпросторі та серйозно зашкодити цифровим правам людини.

OEWG – це форум, який сприяє обговоренню питань міжнародної кібербезпеки під егідою першого комітету Генеральної Асамблеї ООН. Процес був ініційований Росією, щоб конкурувати з Урядовою групою експертів ООН, яка складалася з обраної групи країн, але які займалися тими самими питаннями. З 2019 року в рамках OEWG делегати держав-членів ООН кожні два та три роки ділилися своїм баченням поточних і нових загроз, способів розбудови потенціалу кібербезпеки, встановлення заходів зміцнення довіри та розуміння того, як

міжнародне право застосовується до кіберпростору. Під час засідання OEWG Росія неодноразово закликала до укладення договору.

Російська концептуальна записка закликає до суверенної рівності, територіальної цілісності держав і невтручання у внутрішні справи інших шляхом пропаганди та інших засобів. Враховуючи незліченні кібероперації Росії проти України та її тролінгову діяльність за кордоном, це чисте лицемірство. Росія закликає до неприпустимості необґрунтованих приписок, зокрема, якщо вони використовуються для виправдання санкцій. Однак приписування та накладення санкцій є національною прерогативою держав і відіграє важливу роль у створенні підзвітності в кіберпросторі. Звичайно, більше доказів – краще, і Сполучені Штати особливо прозоро надавали докази для своїх заяв про приписування. За іронією долі, саме російському приписуванню кібероперацій не вистачає доказів. [97] Хоча в документі йдеться про права людини та фундаментальні свободи, він лише конкретизує свободу вираження поглядів і закликає до можливості її обмеження з міркувань національної безпеки, громадського порядку та моралі. Згадка про права людини врівноважується формулюванням безпеки.

Як Росія може адаптуватися в кіберпросторі в майбутньому? Відтік західних технологій з російського ринку означає, що російські державні актори тепер можуть потерпати від відсутності необхідного апаратного забезпечення до оновлень програмного забезпечення, або вдаватися до менш надійних китайських варіантів. З часом це може знизити безпеку та функціональність усього, від внутрішньої телекомунікаційної (і, отже, спостереження) інфраструктури до високотехнологічних дослідницьких організацій, які розробляють складні кіберексплойти. Тим часом Москва, ймовірно, зіткнеться зі стрімким зменшенням обсягів фінансування науково-дослідних розробок і особливо технічних талантів, більшість з яких, за всіма даними, почали шукати більш гостинні домівки в таких країнах, як Грузія, Казахстан, Туреччина та Ізраїль. У

найближчій перспективі можна очікувати подвоєння кількості одноразових, руйнівних, але не вирішальних кібернападів зі сторони Росії. [13]

РОЗДІЛ 5
РОСІЙСЬКО-АМЕРИКАНСЬКЕ ПРОТИСТОЯННЯ В КІБЕРПРОСТОРІ ПІСЛЯ РОСІЙСЬКОЇ АГРЕСІЇ НА УКРАЇНУ

5.1 Протидія США російській кібервійні

Риторика США полягає в тому, що кібератаки, яких зазнає їхня країна, здебільшого спонсорують ворожі держави, такі як Іран, Північна Корея, Китай і Росія. З іншого боку, США теж здійснюють заходи з кібершпигунства та кібератаки, наприклад Stuxnet, проти інших. [42] З 2015 року між США та Китаєм діє угода про кібербезпеку, [38] яка призвела до значного зниження частоти та серйозності кібератак між двома країнами. Однак за відсутності такої угоди між США та Росією кібервідносини між ними залишаються напруженими та невизначеними.

Адміністрація Байдена-Гарріс неодноразово попереджала про те, що Росія може розгортати зловмисну кіберактивність проти Сполучених Штатів у відповідь на запроваджені економічні санкції та допомогу Україні через повномасштабне вторгнення РФ. Так, ще до початку повномасштабного вторгнення РФ в Україну Президент Джо Байден попередив, що якщо Росія почне кібератаки на американські компанії та критичну інфраструктуру в рамках своєї кампанії гібридної війни проти України, «ми готові відповісти», але не уточнив, яким саме шляхом. [62] Майк Роджерс, колишній член Конгресу, який нині є старшим науковим співробітником проекту розвідки в Центрі науки та міжнародних відносин Белфера Гарвардського університету, стверджує, що якби була здійснена справжня серйозна атака на інфраструктуру, то США програли б: «Наразі ми уникнули цифрової катастрофи не завдяки вмінню. Це завдяки сліпому везінню і стриманості наших супротивників». Щодо інциденту Solar Winds російські хакери сиділи в американських мережах майже рік, перш ніж їх

ідентифікували, скориставшись як законом, так і стратегією кібербезпеки. Стартегія кібербезпеки 2023 заохочує активну участь і приватного сектору. [80]

Повертаючись до раніше згадуваної Стратегії кібербезпеки США, [69] то в ній якраз прослідковується новий погляд на баланс між урядом і приватним сектором з точки зору ролей і обов'язків щодо пом'якшення кіберризиків. Стратегія шукає нові механізми для забезпечення основних стандартів безпеки на рівні пересічного користувача та постачальника послуг. Документ наголошує на потребі приватних організацій захищати свої системи, підкреслюючи роль уряду щодо захисту власних систем і участі в дипломатії, правоохоронній діяльності та зборі розвідданих, стратегія наголошує на потребі приватних організацій захищати свої системи.

Адміністрація США вже сфокусувалась на посиленні власної кібербезпеки, щоб зменшити ризики для своїх структур. 21 березня 2022 Байден закликав лідерів американського бізнесу негайно посилити кіберзахист своїх компаній. Він сказав, що президент Росії Путін, «імовірно, використовуватиме кібератаки як форму відплати» за дії США щодо протидії російському вторгненню в Україну. [93] Більша частина критично важливої інфраструктури країни належить і управляється приватним сектором, і приватний сектор повинен діяти, щоб захистити критично важливі служби, на які покладаються всі американці. Тому уряд США працює над наданням ресурсів та інструментів приватному сектору, зокрема через кампанію CISA. Приватним компаніям був наданний ряд «приземленних» рекомендацій, наприклад, створювати резервні копії даних, переконатися в справності своїх внутрішніх систем, створити і використовувати багатофакторну автентифікацію, щоб зловмисникам було складніше проникнути у систему. [36]

Президенту Джо Байдену було надано список варіантів для США щодо здійснення масових кібератак, спрямованих на те, щоб порушити здатність Росії підтримувати військові операції в Україні. Проте, будь-яке використання

кіберзброї у відповідь на російське вторгнення в Україну стане поворотним моментом для кібероперацій США, які в основному були зосереджені на зборі розвідданих, інформаційних операціях і цілеспрямованих ударах, багато з яких з антитерористичною метою. Представники розвідки заявили, що остаточних рішень не прийнято, але вони кажуть, що розвідка США пропонує використовувати американську кіберзброю в масштабах, які раніше не передбачалися. [34] Серед варіантів: зрив інтернет-з'єднання по всій Росії, відключення електроенергії та втручання в роботу стрілочних переводів, щоб перешкодити здатності Росії поповнювати свої сили. Проте адміністрція Байдена рішуче заперечує прийняття саме такої форми використання кіберпотужностей. «Ми надзвичайно стурбовані тим, що будь-яка відповідь натуральним або кінетичним шляхом на російську атаку на критичну інфраструктуру вийде з-під контролю», — сказав Джош Лоспіносо, генеральний директор і співзасновник компанії з кібербезпеки Shift5 і колишній високопосадовець компанії як Кіберкомандування США. [64] Минулого року Байден наклав на Росію санкції за її причетність до злому Solarwinds, після чого Міністерство юстиції висунуло обвинувачення проти багатьох передбачуваних російських хакерів, але хакерські операції Москви тривають досі. Росія дослідила та проникла в критичні сектори цифрової інфраструктури США, від банків до електричних мереж і виборчих систем. Подібним чином офіційні особи США натякнули, що американський уряд має значний доступ і повноваження, щоб зробити те саме або навіть завдати кіберударів безпосередньо проти хакерських операцій Москви. Визначити, що вважатиметься ескалацією у кіберпросторі дуже важко. Законодавці вже давно вимагають більшої ясності щодо того, як може виглядати відповідь США у разі серйозного нападу Росії. Адміністрація рішуче відмовлялася оприлюднювати такі подробиці, заявляючи, що це дасть Росії надто повне уявлення про стратегії США.

В теорії для Президента Байдена існує кілька опцій у боротьбі США проти кібервійни Росії. Перший варіант, який скоріше за все використає Байден, – це запровадження нових санкцій проти Росії. Санкції розглядаються як легший спосіб розправитися з іноземним урядом, ніж прямі наступальні кібер-акції, і вони вже були ключовою зброєю, використаною адміністрацією Байдена для покарання Росії за вторгнення в Україну. Проте, враховуючи кількість санкцій, які вже діють, додаткові покарання можуть не сильно вплинути.

Наступна ідея - це націлити деструктивні атаки на інфраструктуру, яка використовується для проведення російських кібероперацій, або розповсюдити російське шкідливе програмне забезпечення серед експертів з безпеки, щоб обмежити їхню можливість його використання. Це була б більш масштабна версія ліквідації американськими кіберзасобами російських ферм тролів. Колишній президент Дональд Трамп підтвердив The Washington Post у 2020 році, що він санкціонував атаку Кіберкомандування США на розташоване в Санкт-Петербурзі Агентство інтернет-досліджень перед проміжними виборами 2018 року, щоб зупинити групу від втручання у виборчий процес. [90]

Інший варіант стане найгучнішим повідомленням РФ, але також підвищить ставки на ескалаційну відповідь. США мають передові кіберпотенціали, які перевищують російські, включаючи здатність втручатися у функціонування критичної інфраструктури в інших країнах. У звіті, опублікованому минулого року Міжнародним інститутом стратегічних досліджень [22], зроблено висновок, що наступальні кіберпотенціали США «більш розвинені, ніж у будь-якої іншої країни», і включають здатність відключати системи командування й контролю супротивників і порушувати системи зброї. Але атака, яка завдає шкоди фізичним системам у Росії чи деінде, буде масовою ескалацією та майже гарантуватиме відповідь Москви.

5.2 Російська кібервійна як складова зовнішньої політики

Росіяни зазвичай не використовують термін «кібервійна», за винятком випадків, коли вони посилаються на західні чи інші іноземні твори на цю тему. Натомість, як і китайці, вони схильні використовувати слово інформатизація, таким чином концептуалізуючи кібероперації в рамках ширшої категорії інформаційної війни. Інформаційна війна, як цей термін використовують російські військові теоретики, є цілісною концепцією, що включає операції комп'ютерної мережі, психологічні операції та інформаційні операції. [44]

Кіберінформаційна війна — річ неоднозначна. З одного боку, держави можуть використовувати її для формування мислення іноземних суспільств і політиків. З іншого боку, держави також схильні до зовнішнього впливу через інформаційну війну. У двадцять першому столітті замість того, щоб боротися з жорсткою силою за допомогою жорсткої сили, Росія використовує розумну силу та інформаційну війну для досягнення своїх стратегічних цілей. Зараз Росія використовує операції кібервпливу та гібридної війни на повну потужність.

Однак інформаційна війна — це не просто частина гібридної війни, це окрема стратегія просування політики та стратегій тиску на супротивника без застосування грубої сили. Російське кібершпигунство та інформаційна війна є тривалим методом мислення з радянських часів правління, оскільки радянські лідери розуміли цінність інформації та силу впливу. [30] Радянський або російський термін для ІВ означає приховані та відкриті методи впливу на події та поведінку в інших країнах. У цих випадках інформація маніпулювалася та поширювалася підставними організаціями, які підтримували Радянський Союз, агентами впливу, такими як місцеві політики чи навіть шпигуни, за допомогою фейкових історій і підробок у нерадянських ЗМІ. [29] Російська влада сприймає кіберпростір не лише як можливість керувати інформаційними війнами проти Заходу, а й як серйозну загрозу національній безпеці, стабільності та легітимності режиму Росії, оскільки вільний потік інформації в кіберпросторі може підірвати

режим і сприяти протестам і повстаням. [1] Щоб проводити операції ІВ, не боячись стати самим їх жертвою, російська влада прагнула забезпечити безпеку та захист російської інформаційної сфери від іноземних впливів. Російська влада за допомогою законодавства та кіберрегуляції прагне контролювати російський кіберпростір, щоб запобігти або стримати, наскільки це можливо, поширення інформації, яка може зіпсувати позитивне уявлення про режим Володимира Путіна, або будь-яку діяльність, яка може поставити під загрозу стабільність режиму. [4] Тому російська влада прагне взяти під контроль зміст інформації, що циркулює в російському кіберпросторі. Закон Ярової, прийнятий у 2016 р., вимагає надання ключів шифрування/дешифрування на запит розповсюджувачам інформації, таким як інтернет- і телекомунікаційні компанії, месенджери, служби електронної пошти, форуми, та інші платформи, які дозволяють обмінюватися інформацією з російськими спецслужбами, такими як Федеральна служба безпеки (ФСБ). Ключі шифрування/дешифрування необхідні для декодування отриманих, переданих, доставлених та/або оброблених електронних повідомлень та інформації. [6] Крім того, згідно з цим законом, великі дані, пов’язані з діяльністю в російському кіберпросторі, повинні зберігатися на території Росії, а спецслужби повинні мати необмежений доступ до цих даних. На практиці цей закон дозволяє російським спецслужбам отримувати доступ до приватної та корпоративної інформації, що циркулює в Російський сегмент кіберпростору. Наприклад, такі компанії, як Facebook або Google, повинні зберігати інформацію про дані та діяльність своїх російських користувачів на території Росії та надавати необмежений доступ російським спецслужбам.

Після здійснення кібератак, кібершпигунства та постійного використання інформаційної війни з кінця 1990-х років операції Росії вплинули на демократії, пропагували екстремізм, підтримували антидемократичних лідерів і похитнули вплив Заходу. Хоча всі ці наслідки російської агресії є правдивими, Конор

Каннінгем [30] визначає три цілі Росії для подальшого використання кібершпигунства та інформаційної війни:

- Відтворення єдиної російської Євразії.
- Війна проти ліберальної демократії та домінування Заходу, включаючи НАТО та США.
- Повторне підтвердження Росії як глобальної держави за допомогою швидких і серйозних кібератак.

Розширене використання кібернетичних засобів у Росії не є ізольованою загрозою. Російський план кібершпигунства та інформаційної війни впливає на кожен регіон світу через його розмір, масу та складність. Росія використовує свої кіберпотенціали, щоб стримувати, примушувати або дезорієнтувати своїх супротивників, Кремль також використовує кібернетичні засоби в сенсі м'якої сили — для поширення проросійської пропаганди та підриву підтримки урядів супротивників. Його зусилля в цьому відношенні можна розділити на три великі категорії: [20]

1. Використання фінансованих державою проросійських ЗМІ, таких як Sputnik і RT (~~раніше~~ Russia Today)

2. Поширення несприятливої або оманливої інформації про іноземні уряди та установи через витік документів, які часто були отримані за допомогою хакерів, фішингу чи інших форм кібершпигунства.

3. Використання Росією інтернет-«тролів» (тобто осіб, яким платять за створення фальшивих блогів і онлайн-профілів, щоб заповнювати розділи коментарів новин оманливими, фальшивими або проросійськими точками зору).

Основними кіберінструментами, які Росія використовує для м'якої сили, є хакерські групи та інтернет-тролі. Хакерські угруповання надають Росії приховану можливість отримання даних і документів, які можуть бути використані в кампаніях з дезінформації та інформаційних операціях. Вони здійснюють низку кібердій, від DDoS-атак і кібершпигунства до викрадання

даних/документів і цифрового саботажу. Документи, викрадені хакерськими групами, оприлюднюються через такі платформи, як WikiLeaks, або офіційні сайти ЗМІ. Документи часто містять незручну особисту інформацію про іноземних політичних чи опозиційних лідерів, викривають сумнівну державну політику чи бізнес-практику або містять інформацію, яка дискредитує уряд чи установу. Дії Росії можна частково пояснити іншим розумінням війни. У той час як американські військові мають концепцію «нульової фази», російські стратеги бачать себе в постійному і тривалому конфлікті. Це особливо актуально для кіберпростору, де стратегія радянської епохи «політичної війни» послужила основою для нинішньої російської стратегії інформаційної війни. [14]

5.3 Перспективи розбудови відносин у майбутньому

Незважаючи на певні непорозуміння та напругу у відносинах між США та Російською Федерацією в кіберпросторі, в будь-якому випадку необхідно буде намагтися співіснувати і надалі, а отже будувати подальшу політику. Протягом перших двадцяти п’яти років періоду після холодної війни американсько-російські відносини характеризувалися поєднанням конкуренції та співпраці. З 2014 року баланс між цими елементами різко змінився в бік конкуренції, і ця тенденція, ймовірно, збережеться на невизначений термін. Тим не менш, мінливі глобальні тенденції та внутрішня політична динаміка можуть відкрити двері для більших можливостей для співпраці. [87]

Накопичені образи з обох сторін і глибокі відмінності в інтересах, цінностях і концепціях глобального порядку майже виключать будь-які ідеї сталого партнерства, перезавантаження чи значного покращення зв’язків. Зовнішньополітична спільнота США розглядає Росію як ворожого актора, і ця точка зору, ймовірно, переважатиме в осяжному майбутньому. Політики США обурюються глобальною активністю Росії та дедалі більше стурбовані її партнерством з Китаєм. Подібним чином зовнішньополітичне співтовариство

Москви розглядає Сполучені Штати як агресивного, одностороннього, ворожого актора та загрозу внутрішній стабільності Росії та її претензіям на визначну позицію на світовій арені. Провідна російська точка зору на співпрацю у сфері кібербезпеки свідчить про те, що подальший двосторонній діалог має бути розбитий на два напрямки, [89] військовий і дипломатичний, щоб дозволити укладати угоди, незважаючи на великі розбіжності щодо ключових принципів кібербезпеки. Проте, для укладання договорів необхідно прийти до офіційно узгоджених термінів і визначень основних принципів кібербезпеки, що стане важливим першим кроком до створення структури співпраці. Військовий шлях має бути зосереджений на встановленні чітких червоних ліній, перетин яких гарантував би відповідь у кіберпрсторі і встановлював основні правила кіберактивності, особливо на ядерних об'єктах. Дипломатичний шлях має бути зосереджений на досягненні більшої прозорості та стабільності в кіберпросторі. Одним із запропонованих методів досягнення цього є зосередження на сферах, що викликають спільний інтерес, таких як кіберзлочинність або вербування терористів онлайн. США та Росія могли б працювати над розширенням обміну інформацією та єдиною відповіддю в цих сферах. Однак існує висока ймовірність того, що США не зможуть і не захочуть довіряти Росії в питаннях кіберзлочинності з огляду на заяви пов'язані з російським вторгненням на територію України.

Пріоритетність міжнародної інформаційної безпеки для Росії закріплена в ряді документів стратегічного планування, таких як «Основи національної політики Росії в галузі міжнародної інформаційної безпеки до 2021 року», «Стратегія національної безпеки до 2021 року» та ін. Відповідно до цих документів, Росія проводить політику щодо формування мирного та стабільного ІКТ-середовища. США вже давно насторожено ставляться до пропозицій Росії, розглядаючи їх як спробу обмежити розвиток ІКТ і кинути виклик американському лідерству. У квітні 2022 року США опублікували Декларацію

майбутнього Інтернету, [8] в якій пропонують боротися за свободу передачі інформації, а авторитарні держави Росію та Китай називають антагоністами вільного Інтернету. Навіть криза в американсько-російських відносинах, що виникла після початку російської операції в Україні, не змінила діяльність майданчиків ООН – діалог залишився непорушним. [98] Робоча група відкритого складу, як переговорний майданчик з міжнародної інформаційної безпеки, витримала випробування в складних умовах, довівши актуальність таких майданчиків, а також глобальних ініціатив Росії. У довгостроковій перспективі важливими будуть неформальні канали комунікації, зокрема експертні, академічні та ділові зустрічі, де стане можливим пошук шляхів розвитку двосторонніх відносин у кіберпросторі.

Як можна прогнозувати, «Гонка озброєнь» у кіберпросторі призведе до різкого збільшення потенціалу обох держав. Уразливість США, швидше за все, випередить вразливість Росії через більшу економічну та соціальну залежність Америки від Інтернету. Умови для встановлення норм поведінки, перевірки або заходів зміцнення довіри, а також будь-яке відчуття «спільної мети» будуть небезпечно повільними. Ймовірно, відносини в кіберпросторі між двома державами будуть розвиватися лінійно: Росія продовжуватиме здійснювати незначні розвідувальні кібератаки, а США запроваджувати санкції у відповідь. РФ наврядчи втримається від того, аби не втрутитись до процесу президентських виборів США. Дуже ймовірно, що жоден з них не впевнений в наявному кіберпотенціалі іншого, що й стає фактором стримування для потужних кібератак, які мали б довгострокові наслідки як для урядових структур, так і пересічних громадян.

ВИСНОВКИ

Кіберпростір у сучасному світі стає все більш багатофункціональним. Розбудова кіберпотенціалу стає для держави своєрідною гарантією безпеки та фактором стримування для інших. Сполучені Штати Америки почали розвиток законодавства значно раніше за Російську Федерацію – з 1986 року, [19] коли був ухвалений Закон про комп'ютерне шахрайство та зловживання. Натомість перший закон, що стосувався кіберпростору в Росії з'явився 1996 року. За такий проміжок часу США мали значну перевагу в напрацьовувані як нормативно-правової бази, так і технологічному розвитку. Вказані обставини дають можливість США-заявляти про свою технологічну першість.

Національна стратегія кібербезпеки США 2023 року є важливим документом з точки зору визнання РФ однією з основних загроз безпеці. Документ змінює погляд на механізм забезпечення кібербезпеки, покладаючи відповідальність не лише на державу, а й на приватний сектор, наголошуючи на їхній взаємодії. В нормативно-правовій базі Росії існує підміна понять, тому кіберпростір, кібербезпека розглядаються в контексті інформаційної безпеки та політики. Це створює проблеми в взаєморозумінні з іншими державами або в процесі розробки міжнародних угод, що стосуються поведінки в кіберпросторі. Кіберпростір дає можливість Російській Федерації

Відносини США та РФ у сфері кібербезпеки зберігали певну напруженність і до початку війни в Україні, проте залежать від керуючої адміністрації. Кількість публічних попереждень та погроз один одному дещо збільшилась з початком війни. Але, за наявності спільної цілі у кіберпросторі, обидві держави готові поєднати зусилля аби знищити загрозу для себе, не дивлячись на інші «тріщини» у відносинах. Розуміючи, які насліки можуть принести занадто агресивні кібератаки, США утримується від різких рухів у цьому напрямку, обмежуючись попередженнями, санкціями, а іноді й полюванням за окремими особами чи

угруповуванями. Одночасно Сполучені Штати готові ділитися своїми технологічними надбаннями і активно співпрацюють з іншими державами, зокрема Європейського Союзу, задля розбудови спроможності і формування колективної безпеки у кіберпросторі, проводячи різні навчання.

Натомість Росія значно збільшила кількість кібератак з початком повномасштабного вторгнення на територію України, але використовує свої сили в більшій мірі з метою шпигунства та отримання важливих даних стосовно й інших держав. Якісна і потужна кібератака займає багато часу для її підготовки. Дуже ймовірно, що найбільші за масштабами кібератаки, підготовлені РФ, вже були здіснені напередодні вторгнення та протягом перших 1-2 місяців. Проте, не виключення, що інші потужні кібератаки можуть готуватись паралельно. Демонструючи певну активність, Росія випробовує та провокує США, тим не менше теж утримується від занадто руйнівних атак. Таку стриманність Росії можна пояснити тим, що у кіберпросторі легко втратити контроль над шкідливим забезпеченням чи вірусами, і тоді шкода буде нанесена також тим державам, які кривдник не планував атакувати, а тому є ризик серйозної відповіді. Для Росії це додатковий спосіб заявити про себе, як про наддержаву, але цим лише погіршує свою репутацію серед цивілізованого світу.

Майбутнє кіберпростору безумовно залежить в великій мірі від внутрішніх та зовнішніх чинників. Поведінка в кіберпросторі все більше нагадує ігри сьогодення з ядерним озброєнням: хтось усвідомлює наслідки його застосування, а хтось цим користується для здобуття хоч якогось визнання на геополітичній арені. Через постійне збільшення залежності сучасного суспільства від технологій, Інтернету та електики воно стає більш вразливим, а тому пропорційно ростуть і загрози, а традиційна фізична війна вже частково перейшла у віртуальний світ.

Загалом мета дослідження, а саме вивчити поведінку США та РФ стосовно одна одної була досягнута, хоча питань для вивчення залишається чимало. Це

пов'язано з доступністю інформації, оскільки документи, які держави зберігають під грифом «Секретно», з часом можуть бути оприлюднені, а отже нові грані відносин будуть розкриті. Уся інформація, що є в доступі виглядає однобоко, а саме, є «злодій» у вигляді Російської Федерації, яка в більшості фігурує причетною до кібератак, і є «благодійник» - США, які намагаються зберегти баланс в кіберпросторі. З цим пов'язані і складнощі цього дослідження, наприклад, у відкритому доступі майже немає інформації про зловмисні дії в кіберпросторі з боку США. З цього огляду не можна на сто відстотків покладатися і на статистику та звіти, адже сумнівно, що й інші дослідники мають більш детальні дані.

Іншою складністю стало дотримання часових рамок дослідження. Нами було виокремлено рамки 2000 – 2023 роки, опираючись на прихід Володимира Путіна до влади. Проте суспільство, в тому числі і наукова спільнота, почало масово звертати увагу на проблеми кіберпростору лише на початку 2010-х, а самий сплеск почався в 2014 році після окупації Росією Автономної Республіки Крим. До цього моменту можна спиратись в більшості лише на законодавчі базу держав, а відслідковування динаміки злочинних дій у вигляді кібератак взагалі відсутнє.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Военная доктрина Российской Федерации. 05.02.2010. URL: http://www.kremlin.ru/supplement/461. (Дата звернення: 19.10.2023)
2. Конституция Российской Федерации. *Президент России*. URL: http://www.kremlin.ru/acts/constitution. (Дата звернення: 02.08.2023)
3. На "Укренерго" здійснюються нові хакерські атаки. *Економічна правда*. 20.01.2016. URL: https://www.epravda.com.ua/news/2016/01/20/577551/. (Дата звернення: 20.09.2023)
4. Указ Президента Российской Федерации от 05.12.2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации. *Президент России*. URL: http://kremlin.ru/acts/bank/41460 (Дата звернення: 05.08.2023)
5. Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) Об участии в международном информационном обмене. *Судебные и нормативные акты РФ.* URL: https://sudact.ru/law/federalnyi-zakon-ot-04071996-n-85-fz-ob/. (Дата звернення: 02.08.2023)
6. Федеральный закон от 06.07.2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». *Президент России*. URL: http://www.kremlin.ru/acts/bank/41108. (Дата звернення: 19.10.2023)
7. A Bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States. S.2105. In the senate of the United States. 112th congress 2d session. 14.02.2012. URL: https://www.govinfo.gov/content/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf. (Дата звернення: 28.05.2023)

8. A Declaration for the Future of the Internet. *The White House*. 04.2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf. (Дата звернення: 26.10.2023)
9. Alexander K. House Armed Services Subcommittee, Cyberspace Operations Testimony. The Cyber Domain. U.S. Department of Defense. 23.09.2010. URL: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf. (Дата звернення: 02.08.2023)
10. Auchard E. Macron campaign was target of cyber attacks by spy-linked group. *Reuters*. 24.04.2017. URL: https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200. (Дата звернення: 19.08.2023)
11. Bailey T., Greis J., Watters M., Welle J. Cybersecurity legislation: Preparing for increased reporting and transparency. McKisney & Company. 17.06.2022. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency. (Дата звернення: 08.06.2023)
12. Barnes J., Gibbons-Neff T. U.S. Carried Out Cyberattacks on Iran. *The New York Times*. 22.06.2019. URL: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html?module=inline. (Дата звернення: 30.06.2023)
13. Bateman J., Beecroft N., Wilde G. What the Russian Invasion Reveals About the Future of Cyber Warfare. Carnegie. 19.12.2022. URL: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667. (Дата звернення: 21.09.2023)
14. Blank S. Cyber War and Information War à la Russe. Understanding cyber conflict. 2017. P. 81-99. URL:

https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_FullText.pdf. (Дата звернення: 22.10.2023)

15. Breene K. Who are the cyberwar superpowers? *World Economic Forum*. 04.05.2016. URL: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/. (Дата звернення: 25.04.2023)
16. Budget of the U.S. Government Fiscal Year 2023. Office of management and budget. U.s. government publishing office, Washington 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf. (Дата звернення: 01.05.2023)
17. Budget of the U.S. Government Fiscal Year 2024. Office of management and budget. Washington: U.S. Government publishing office, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/budget_fy2024.pdf. (Дата звернення: 01.05.2023)
18. China not cyber superpower as portrayed, US is far ahead. *Telecom.com*. 01.07.2021. URL: https://telecom.economictimes.indiatimes.com/news/china-not-cyber-superpower-as-portrayed-us-is-far-ahead/84011651. (Дата звернення: 04.04.2023)
19. Computer Fraud and Abuse Act. *Central Intelligence Agency*. 03.06.1986. URL: https://www.cia.gov/readingroom/docs/CIA-RDP87B00858R000400470004-7.pdf. (Дата звернення: 30.10.2023)
20. Connel M., Vogler S. Russia's Approach to Cyber Warfare. CNA. 09.2016. 22 p. URL: https://apps.dtic.mil/sti/pdfs/AD1019062.pdf. (Дата звернення: 21.10.2023)
21. Crandal M., Thayer B. The Balance of Cyberpower. *The National Interest*. 25.11.2018. URL: https://nationalinterest.org/feature/balance-cyberpower-36637. (Дата звернення: 01.05.2023)
22. Cyber Capabilities and National Power: A Net Assessment. The international institute for strategic studies. 28.07.2021. 174 p. URL:

https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf. (Дата звернення: 14.10.2023)

23. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Public Law 117–103. 117th Congress. URL: https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf. (Дата звернення: 08.06.2023)
24. Cyber Operations Tracker. Council on Foreign Relations. URL: https://www.cfr.org/cyber-operations/#OurMethodology. (Дата звернення: 04.05.2023)
25. Cybersecurity — Executive Order 13636. The White House President Barack Obama. URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636. (Дата звернення: 06.06.2023)
26. Cybersecurity legislation 2022. National conference of state legislatures. 22.07.2022. URL: https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2022. (Дата звернення: 08.06.2023)
27. Cyberspace Operations. Joint Chiefs of Staff. Joint Publication 3-12. 08.06.2018. URL: https://irp.fas.org/doddir/dod/jp3_12.pdf. (Дата звернення: 30.06.2023)
28. Cyber Power – Tier One. IISS. 28.06.2021. URL: https://www.iiss.org/research-paper/2021/06/cyber-power---tier-one/. (Дата звернення: 26.06.2023)
29. Cull N. J., Gatov V., Pomerantsev P. et al. Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it. *Institute of Global Affairs*. 10.2017. 81 p. URL: https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf. (Дата звернення: 20.10.2023)
30. Cunningham C. A Russian Federation Information Warfare Primer. The Henry M. Jackson school of international studies. 12.11.2020. URL:

https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/. (Дата звернення: 16.10.2023)

31. Daniels F. Chinese theft of sensitive US military technology is still a 'huge problem,' says defense analyst. *CNBS*. 08.11.2017. URL:https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html. (Дата звернення: 03.05.2023)
32. DavidPur. N. Which Countries are Most Dangerous? Cyber Attack Origin – by Country. *Cyberproof*. 04.01.2023. URL: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous. (Дата звернення: 07.05.2023)
33. Digital Connectivity and Cybersecurity Partnership (DCCP). USAID. 2018. URL: https://www.usaid.gov/sites/default/files/2023-01/DCCP%20Factsheet.pdf. (Дата звернення: 15.06.2023)
34. Dilanian K., Kube C. Biden has been presented with options for massive cyberattacks against Russia. *NBC News*. 24.02.2022. URL: https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558. (Дата звернення: 07.10.2023)
35. Etame-Ese R., Odei D., Manning S., Mavakala E., Hall A. US Policy on the Use of Force in Cyberspace. *ISAKA*. 05.10.2022. URL: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/us-policy-on-the-use-of-force-in-cyberspace. (Дата звернення: 10.07.2023)
36. Fact sheet: Act Now to Protect Against Potential Cyberattacks. The White House. 21.03.2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/. (Дата звернення: 07.10.2023)
37. Fact sheet: Partnership for Global Infrastructure and Investment at the G7 Summit. The White House. 20.05.2023. URL: https://www.whitehouse.gov/briefing-room/statements-

releases/2023/05/20/fact-sheet-partnership-for-global-infrastructure-and-investment-at-the-g7-summit/. (Дата звернення: 17.06.2023)

38. Fact sheet: President Xi Jinping's State Visit to the United States. The White House. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. (Дата звернення: 05.10.2023)
39. Fact sheet: The U.S.-Japan Competitiveness and Resilience (CoRe) Partnership. The White House. 23.03.2022. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-the-u-s-japan-competitiveness-and-resilience-core-partnership/. (Дата звернення: 17.06.2023)
40. Fact sheet: United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology (iCET). The White House. 31.01.2023. URL: https://whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/. (Дата звернення: 17.06.2023)
41. Fact sheet: Vice President Harris Announces Initiatives to Deepen the U.S. Partnership with Tanzania. The White House. 30.03.2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/fact-sheet-vice-president-harris-announces-initiatives-to-deepen-the-u-s-partnership-with-tanzania-2/. (Дата звернення: 17.06.2023)
42. Ferdinando L. Cybercom to Elevate to Combatant Command. U.S. Department of Defense. 03.05.2018. URL: https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-tocombatant-command/. (Дата звернення: 05.10.2023)
43. Fruhlinger J. Stuxnet explained: The first known cyberweapon. CSO. 31.08.2022. URL: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html. (Дата звернення: 07.05.2023)

44. Giles K. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. Chatham House. 21.03.2016. URL: https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power. (Дата звернення: 16.10.2023)
45. Giles K. Russia's Public Stance on Cyberspace Issues. Conflict Studies Research Centre. Oxford, UK. 4th International Conference on Cyber Conflict. 2012. URL: https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf. (Дата звернення: 02.08.2023)
46. Gordon L., Loeb M., Lucyshyn W., Richardson R. CSI\FBI Computer crime and security survey. Computer Security Institute. 2005. URL: https://www.researchgate.net/publication/243784811_CSIFBI_Computer_Crime_and_Security_Survey. (Дата звернення: 23.05.2023)
47. Executive Order - Improving Critical Infrastructure Cybersecurity. The White House, President, Barack Obama. 12.02.2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. (Дата звернення: 06.06.2023)
48. Executive Order -- Promoting Private Sector Cybersecurity Information Sharing. The White House, President Barack Obama. 13.02.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. (Дата звернення: 06.06.2023)
49. Gramm-Leach-Bliley Act. Federal Trade Commission. URL: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act. (Дата звернення: 18.05.2023)

50. Gray C. S. Making strategic sense of cyber power: why the sky is not falling. U.S. Army war college. 04.2013. 82 p. URL: https://www.files.ethz.ch/isn/163664/pub1147.pdf. (Дата звернення: 13.04.2023)
51. Håkansson J. The Use of Personal Pronouns in Political Speeches. Linnaeus University. 12.05.2012. URL: https://www.diva-portal.org/smash/get/diva2:531167/fulltext01.pdf. (Дата звернення: 15.06.2023)
52. Japan's biggest port, Nagoya, hit by suspected cyberattack. *Nikkei Asia*. 05.07.2023. URL: https://asia.nikkei.com/Business/Technology/Japan-s-biggest-port-Nagoya-hit-by-suspected-cyberattack. (Дата звернення: 20.09.2023)
53. Kelly S., Resnick-ault J. One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. *Reuters*. 09.06.2021. URL: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/. (Дата звернення: 18.05.2023)
54. Kirby C. Forum focuses on cyber-security. *SF Gate*. 04.12.2003. URL: https://www.sfgate.com/business/article/forum-focuses-on-cyber-security-2510105.php (Дата звернення: 23.05.2023)
55. Kovacs E. Russian Hackers Target Montenegro as Country Joins NATO. *Security Week*. 07.07.2017. URL:https://www.securityweek.com/russian-hackers-target-montenegro-country-joins-nato/. (Дата звернення: 10.08.2023)
56. Lake E. Russian hackers' aggression in cyberspace. NorthWest Arkansas. *Democrat Gazette*. 07.08.2016. URL: https://www.nwaonline.com/news/2016/aug/07/russian-hackers-aggression-in-cyberspac/. (Дата звернення: 17.08.2023)

57. Lemos R. Bush unveils final cybersecurity plan. CNET. 13.11.2003. URL: https://www.cnet.com/tech/tech-industry/bush-unveils-final-cybersecurity-plan/. (Дата звернення: 22.05.2023)
58. Les États-Unis, seule superpuissance cyber-militaire, selon une étude. Radiofrance. 29.06.2021. URL: https://www.radiofrance.fr/franceinter/podcasts/geopolitique/geopolitique-du-mardi-29-juin-2021-1423650. (Дата звернення: 07.05.2023)
59. Liang Q., Xiangsui W. Unrestricted warfare. Beijing: PLA Literature and Arts Publishing House, 1999. 228 p. URL: https://www.c4i.org/unrestricted.pdf. (Дата звернення: 27.04.2023)
60. Libicki M. It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture. RAND Corporation. 01.03.2017. URL: https://www.rand.org/pubs/testimonies/CT465.html. (Дата звернення: 26.06.2023)
61. McHale L. The politics of pronouns. Palgrave Macmillan. 07.01.2022. URL: https://www.bps.org.uk/psychologist/politics-pronouns. (Дата звернення: 15.06.2023)
62. Meyer J. Biden says 'we are prepared to respond' if Russia launches cyberattack against US. *USA Today News*. URL: https://eu.usatoday.com/story/news/politics/2022/02/18/biden-administration-goes-shields-up-protect-u-s-russian-cyber-attack/6853643001/. (Дата звернення: 05.10.2023)
63. Microsoft: Russian Cyber Spying Targets 42 Ukraine Allies. *VOA*. 22.06.2022. URL: https://www.voanews.com/a/microsoft-russian-cyber-spying-targets-42-ukraine-allies/6628417.html. (Дата звернення: 16.08.2023)
64. Miller M. Biden’s options if Russia hacks U.S. infrastructure. *Politico*. 20.04.2022. URL: https://www.politico.com/news/2022/04/20/biden-russia-hacks-00026384 (Дата звернення: 10.10.2023)

65. Minárik T. NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit. CCDCOE. 2016. URL: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/. (Дата звернення: 27.04.2023)
66. Mozur P. U.S. Adds China’s Internet Controls to List of Trade Barriers. *The New York Times*. 07.04.2016. URL: https://www.nytimes.com/2016/04/08/business/international/china-internet-controls-us.html. (Дата звернення: 25.06.2023)
67. Murphy E. Protect, Promote, Secure: Maximizing the International Technology Security and Innovation Fund. CSIS. 15.05.2023 https://www.csis.org/analysis/protect-promote-secure-maximizing-international-technology-security-and-innovation-fund-0. (Дата звернення: 24.06.2023)
68. Nakashima E., Warrick J. Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*. 02.06.2012. URL: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. (Дата звернення: 10.07.2023)
69. National cybersecurity strategy. The White House. 03.2023. 35 p. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. (Дата звернення: 15.06.2023)
70. National Strategy to Secure Cyberspace. U.S. Department of Justice. Office of Justice Programs. 02.2003. 76 p. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-strategy-secure-cyberspace. (Дата звернення: 18.05.2023)
71. NSF signs U.S.-India implementation arrangement to streamline the process of funding projects between the two nations. U.S. National Science Foundation.

01.02.2023. URL: https://new.nsf.gov/news/nsf-signs-us-india-implementation-arrangement. (Дата звернення: 24.06.2023)

72. Nye J. Cyber Power. Belfer Center for Science and International Affairs. Harvard Kennedy School, 2010. 27 p. URL: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. (Дата звернення: 05.04.2023)
73. O'Keefe E. Cybersecurity bill fails in the Senate. *The Washington Post*. 02.08.2012. URL: https://www.washingtonpost.com/blogs/2chambers/post/cybersecurity-bill-fails-in-the-senate/2012/08/02/gJQABofxRX_blog.html. (Дата звернення: 06.06.2023)
74. Operation Glowing Symphony (2016). Cyber Law Toolkit. URL: https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016). (Дата звернення: 10.07.2023)
75. Pearson J. West warns of Russian cyberattacks on critical infrastructure. *Reuters*. 20.04.2022. https://www.reuters.com/world/europe/west-warns-russian-cyberattacks-critical-infrastructure-2022-04-20/. (Дата звернення: 16.09.2023)
76. Pernik P. The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine, in: Hacks, leaks and disruptions: Russia’s cyber strategies. EU ISS. 10.2018. pp.59 – 60. URL: https://www.jstor.org/stable/resrep21140.9. (Дата звернення: 14.08.2023)
77. Rees D. Cyber attacks in healthcare: the position across Europe. Pinsent Masons. 18.06.2021. URL: https://www.pinsentmasons.com/out-law/analysis/cyber-attacks-healthcare-europe. (Дата звернення: 20.09.2023)
78. Report on the Investigation Into Russian Interference In The 2016 Presidential Election. US Department of Justice. Vol. 1. 03.2019. URL: https://www.justice.gov/archives/sco/file/1373816/download. (Дата звернення: 18.08.2023)

79. Richard P. Cyberpuissance: les pays montrent leurs muscles. Techniques de l'ingénieur. 01.10.2020. URL: https://www.techniques-ingenieur.fr/actualite/articles/cyberpuissance-les-pays-montrent-leurs-muscles-84408/ (Дата звернення: 25.04.2023)
80. Rogers M. Why America would not survive a real first strike cyberattack today. *The Hill*. 22.02.2021. URL: https://thehill.com/opinion/cybersecurity/539826-we-would-not-survive-true-first-strike-cyberattack/. (Дата звернення: 07.10.2023)
81. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. Gov.UK. 10.05.2022. URL: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion. (Дата звернення: 17.08.2023)
82. Russia, cybercrime, and a new phase in US-Russian cybersecurity. Atlantic Council. 22.07.2021. URL: https://www.atlanticcouncil.org/event/russia-cybercrime-and-a-new-phase-in-us-russian-cybersecurity/. (Дата звернення: 21 .08.2023)
83. Russia Cyber Threat Overview and Advisories. Cybersecurity & Infrastructure security agency. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia. (Дата звернення: 20.09.2023)
84. S.2521 - Federal Information Security Modernization Act of 2014. Congress.gov. 2014. URL: https://www.congress.gov/bill/113th-congress/senate-bill/2521. (Дата звернення: 18.05.2023)
85. Segal A. A New U.S. Foreign Policy for Cyberspace. Council on Foreign Relations. 12.07.2022. URL: https://www.cfr.org/blog/new-us-foreign-policy-cyberspace. (Дата звернення: 25.06.2023)
86. Sheldon J. Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*. 2011. 95-112 p. URL:

https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf (Дата звернення: 09.04.2023)

87. Sokolsky R., Rumer E. U.S.-Russian Relations in 2030. 06.2020. 18 p. URL: https://carnegieendowment.org/files/SokolskyRumer_US-Russia-2030_final1.pdf. (Дата звернення: 28.10.2023)
88. Soldatov A., Borogan I. Russian Cyberwarfare: Unpacking the Kremlin's Capabilities. CEPA. 08.09.2022. URL: https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/. (Дата звернення: 05.08.2023)
89. Sullivan. L. US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective. 04.12.2021. URL: https://geohistory.today/us-russia-cybersecurity-cooperation/#History_of_US-Russia_Cybersecurity_Cooperation. (Дата звернення: 26.10.2023)
90. Thiessen M. A. Trump confirms, in an interview, a U.S. cyberattack on Russia. *The Washington Post*. 10.07.2020. URL: https://www.washingtonpost.com/opinions/2020/07/10/trump-confirms-an-interview-us-cyberattack-russia/. (Дата звернення: 14.10.2023)
91. Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements. Federal Student Aid. 09.02.2023. URL: https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements. (Дата звернення: 28.05.2023)
92. Vatsaraj D. A comparative analysis of cyber laws in Russia and India. *Pleaders*. 25.03.2021. URL: https://blog.ipleaders.in/comparative-analysis-cyber-laws-russia-india/#Russia%E2%80%99s_take_on_cyber_laws. (Дата звернення: 08.08.2023)
93. Vazquez M., Judd D., Lyngaas S. et al. Biden warns business leaders to prepare for Russian cyberattacks. CNN. 21.03.2022. URL:

https://edition.cnn.com/2022/03/21/politics/biden-russia-cyber-activity/index.html. (Дата звернення: 07.10.2023)

94. Voo J., Hemani I., Jones S. etc. National Cyber Power Index 2020. Belfer Center for Science and International Affairs. Harvard Kennedy School, 2020. URL: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf. (Дата звернення: 20.04.2023)
95. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Belfer Center for Science and International Affairs. Harvard Kennedy School. 09.2022. 53 p. URL: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf. (Дата звернення: 20.04.2023)
96. Watts C. Is Russia regrouping for renewed cyberwar? Microsoft Threat Analysis Center. 15.03.2023. URL: https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/. (Дата звернення: 16.08.2023)
97. Weber V. The Dangers of a New Russian Proposal for a UN Convention on International Information Security. Council on Foreign Relations. 21.03.2023. URL: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security (Дата звернення: 21.09.2023)
98. Zinovieva E. International Information Security in US-Russian Bilateral Relations. *Modern Diplomacy*. 22.05.2023 URL: https://moderndiplomacy.eu/2023/05/22/international-information-security-in-us-russian-bilateral-relations/. (Дата звернення: 26.10.2023)