НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

Д. В. Дубов

КІБЕРПРОСТІР ЯК НОВИЙ ВИМІР ГЕОПОЛІТИЧНОГО СУПЕРНИЦТВА

Монографія

Київ 2014

УДК 044:327(075.8)(477:470+571:510:73)
Д 79

Рекомендовано до друку
Вченою радою Національного інституту стратегічних досліджень
(Протокол № 3 від 16.04.2014 р.)

Автор:

Д. В. Дубов – к. політ. н.

Рецензенти:

Грубов В. М. – д. політ. н., проф.;
Рижков М. М. – д. політ. н., проф.;
Храбан І. А. – д. політ. н., проф.

Електронна версія: http:/www.niss.gov.ua

Дубов Д. В.

Д 79 Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

ISBN 978-966-554-240-7

Досліджено питання кіберпростору як складової частини класичної й некласичної геополітики. Розглянуто геополітичне та геостратегічне значення кіберпростору, його роль у глобальному суперництві США та КНР, а також проблему забезпечення національних інтересів України в умовах зростання геополітичної ролі кіберпростору та протистоянь у ньому.

Орієнтовано на фахівців з міжнародних відносин, геополітики, безпекознавців, а також широке коло читачів, які цікавляться проблемами національної та міжнародної кібербезпеки.

ISBN 978-966-554-240-7

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 6

ВСТУП 9

РОЗДІЛ 1.
БЕЗПЕКА КІБЕРПРОСТОРУ
ЯК ПАРАДИГМА НОВОЇ ГЕОПОЛІТИКИ
ТА ГЕОСТРАТЕГІЇ 15

1.1. Зрушення сфер геополітичного протиборства:
від просторів географічних до просторів інформаційних
і кібернетичних 15

1.2. Кібермогутність і національна безпека держави 34

1.3. Кіберпростір як сфера глобальних конфронтацій 50

1.4. Спроби категоріально-понятійного осмислення
кібербезпекової політики у вимірах наукової теорії 68

1.5. Нормативно-правові проблеми розуміння
безпеки кібернетичного простору як відображення
геостратегічних суперечностей і зіткнень
національних інтересів великих держав 78

Висновки до розділу 88

РОЗДІЛ 2.
СУЧАСНІ КОНФЛІКТИ В КІБЕРПРОСТОРІ.
У ПЕРЕДЧУТТІ «ХОЛОДНОЇ ВІЙНИ *V*2.0.» 90

2.1. Відносини США – КНР як ключовий
геополітичний наратив початку XXI сторіччя:
співробітництво, суперництво, протистояння? 90

2.2. Суперництво США та КНР у кіберпросторі
як основа «холодної війни *v*2.0.» 106

2.3. Механізми реалізації кіберконфліктів
у міжнародній політиці XXI сторіччя:
хактивізм, кібершпигунство та кібердиверсії 115

Висновки до розділу 139

РОЗДІЛ 3.
ГЕОСТРАТЕГІЧНІ АЛЬТЕРНАТИВИ
КІБЕРНЕТИЧНОГО ПРОСТОРУ:
ЗБРОЙНІ КОНФРОНТАЦІЇ *VS* КОМПРОМІСИ
ТА СПІВРОБІТНИЦТВО 141

3.1. Альтернативні тренди кіберпростору:
мілітаризація *vs* демілітаризація 141

3.2. Проблематика міжнародної кібербезпеки:
пріоритет співробітництва та демілітаризації 158

3.3. Кібербезпекова політика
Сполучених Штатів Америки: від внутрішніх дискусій
до міжнародних стратегічних ініціатив 172

3.4. Кібербезпекова політика
Китайської Народної Республіки:
національно-державний і міжнародний аспекти 191

Висновки до розділу 208

РОЗДІЛ 4.
ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНИХ
ІНТЕРЕСІВ УКРАЇНИ В ГЛОБАЛЬНОМУ
ТА НАЦІОНАЛЬНОМУ КІБЕРПРОСТОРАХ 210

4.1. Ключові засади позиціювання України
щодо кібербезпекової проблематики 210

4.1.1. Україна у вимірі сучасних кіберзагроз 210

*4.1.2. Геостратегічні чинники впливу
на кібербезпекову політику України* 218

4.2. Пріоритети зовнішньополітичних стратегій України
в кіберпросторі за умов посилення суперництва
між основними геополітичними гравцями 226

4.3. Національні механізми протидії кіберзагрозам:
стан і проблеми нормативно-стратегічного
та організаційного забезпечення 240

4.4. Стан і напрями вдосконалення
нормативно-правової бази щодо розбудови
Національної системи кібернетичної безпеки 256

Висновки до розділу 268

ВИСНОВКИ 269

ВИКОРИСТАНА ЛІТЕРАТУРА 276

ГЛОСАРІЙ 315

ПОКАЖЧИК 318

ПЕРЕЛІК СКОРОЧЕНЬ

ACTA – *Anti-Counterfeiting Trade Agreement*, Торговельна угода щодо боротьби з контрафакцією

AIPAC – *The American Israel Public Affairs Committee*, Американсько-ізраїльський комітет у справах громадськості

BBC – *British Broadcasting Corporation*, Британська широкомовна корпорація

BISTF – *Bilateral Information Security Task Force*, Двостороння робоча група з питань інформаційної безпеки

CCD COE – *The NATO Cooperative Cyber Defence Centre of Excellence*, Центр кіберзахисту НАТО в м. Таллінні

CERT – *Computer Emergency Response Team*, команда реагування на комп'ютерні надзвичайні події

CERT-UA – *Computer Emergency Response Team of Ukraine* – команда реагування на комп'ютерні надзвичайні події України

CISPA – *Cyber Intelligence Sharing and Protection Act*

CNN – *Cable News Network* (телеканал)

CSIS – *Centre for Strategic and International Studies*, Центр стратегічних та міжнародних досліджень

DARPA – *Defense Advanced Research Projects Agency*, Агентство перспективних розробок Пентагону

DNS – *Domain Name System*, система доменних імен

ERP (система) – *Enterprise Resource Planning (System)*, планування ресурсів підприємства

FBI – *Federal Bureau of Investigation,* Федеральне бюро розслідувань, ФБР

FIRST – *Forum for Incident Response and Security Teams*, Форум команд реагування на інциденти інформаційної безпеки

FOIA – *Freedom of Information Act,* Закон про свободу інформації

GCHQ – *Government Communications Headquarters* (розвідувально-безпекова спецслужба Великобританії)

HADOPI low – *Haute Autorité pour la Diffusion des oeuvres et la Protection des droits d'auteur sur Internet*, Закон щодо сприяння поширенню та захисту авторського права в інтернеті (Закон «про три попередження»)

IAB – *Internet Architecture Board*, Рада з архітектури інтернету

IANA – *Internet Assigned Numbers Authority*, Адміністрація адресного простору інтернету

IBM – *International Business Machines Corporation*

ICANN – *Internet Corporation for Assigned Names and Numbers*, Корпорація з управління доменними іменами та *IP*-адресами

ID – *identifier*, розпізнавач

IETF – *Internet Engineering Task Force*, Інженерна Рада інтернету

IGF – *Internet Governance Forum*, Форум з управління Інтернетом

IPRED – *Intellectual Property Rights Enforcement Directive*, Директива щодо охорони прав на інтелектуальну власність (ЄС)

IT – *Information Technology*, інформаційні технології

LOAC – *Law of armed conflict*, закон воєнного конфлікту

MNP – *Military Network Protocol*

2MRC – *two major regional conflict*, концепція одночасного ведення війн у двох віддалених регіонах

NATO – *North Atlantic Treaty Organizat*ion, Організація Північноатлантичного договору

PIPA – *PROTECT Intellectual Property Act* (або*: PROTECT IP Act*; повна назва: *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of* 2011, Закон 2011 про запобігання реальним мережевим загрозам економічній творчості і крадіжці інтелектуальної власності

PRISM – *Program for Robotics, Intelligents Sensing and Mechatronics*

RT – *Russia Today*, Росія сьогодні

SCADA – *supervisory control and data acquisition*, диспетчерське управління і збір даних (програмний пакет)

SJAC – *Society of Japanese Aerospace Companies*, Товариство Японських компаній Аерокосмічної промисловості

SOPA – *Stop Online Piracy Act*, Акт про припинення онлайн-піратства

UKUSA – *United Kingdom – United States of America Agreement*

VBA – *VirusBlokAda* (антивірусна компанія)

WCIT – *World Conference on International Telecommunications*, Всесвітня конференція з регулювання міжнародних телекомунікацій

WSIS – *World Summit on the Information Society*, Всесвітній саміт з інформаційного суспільства

АЕС – атомна електростанція

АНБ – Агентство національної безпеки, *National Security Agency*

АСЕАН – Асоціація держав Південно-Східної Азії, *Association of SouthEast Asian Nations*

АТЕС – Азійсько-Тихоокеанське економічне співробітництво, *The Asia-Pacific Economic Cooperation*

БПЛА – безпілотний літальний апарат

БРІК – Бразилія, Росія, Індія, Китай; *Brazil, Russia, India, China* (група країн)

БРІКС – (група країн) Бразилія, Росія, Індія, Китай, Південно-Африканська Республіка; *Brazil, Russia, India, China, South Africa*

ВВП – валовий внутрішній продукт

ВПС – військово-повітряні сили

ВРУ – Верховна Рада України

ДВБ – Департамент (Міністерство) внутрішньої безпеки, *Department of Homeland Security*

ЄС – Європейський Союз

ЗМІ – засоби масової інформації

ЗС – збройні сили

ІКТ – інформаційно-комунікаційні технології
КЗМІБ – Конвенція про забезпечення міжнародної інформаційної безпеки
КК – Кримінальний кодекс
КМУ – Кабінет Міністрів України
КНДР – Корейська Народно-Демократична Республіка
КНР – Китайська Народна Республіка
КПК – Комуністична партія Китаю
ЛК – Лабораторія Касперського (антивірусна компанія)
МЗС – Міністерство закордонних справ
МІБ – міжнародна інформаційна безпека
МСЕ – Міжнародний союз електрозв'язку, *International Telecommunication Union, ITU*
НАСА – Національне управління з повітроплавання і дослідження космічного простору, *National Aeronautics and Space Administration, NASA*
НАТО – Організація Північноатлантичного договору, *North Atlantic Treaty Organization, NATO*
НДО – недержавне об'єднання
НІСД – Національний інститут стратегічних досліджень
ОБСЄ – Організація з безпеки і співробітництва в Європі, *Organization for Security and Co-operation in Europe, OSCE*
ОДКБ – Організація договору про колективну безпеку
ОЕСР – Організація економічного співробітництва та розвитку, *Organisation for Economic Co-operation and Developmet, OECD*
ООН – Організація Об'єднаних Націй, *United Nations Organisation*
ПМПК – Правила міжнародної поведінки в кіберпросторі
РНБОУ – Рада національної безпеки і оборони України
РФ – Російська Федерація
СБУ – Служба безпеки України
СРСР – Союз Радянських Соціалістичних Республік
США – Сполучені Штати Америки
ТНК – транснаціональна корпорація
ФБР – Федеральне бюро розслідувань, *Federal Bureau of Investigation, FBI*
ФСБ – Федеральна служба безпеки
ЦК – Центральний комітет
ЦРУ – Центральне розвідувальне управління, *Central Intelligence Agency, CIA*
ШОС – Шанхайська організація співробітництва
ШСД – широкосмуговий доступ
ЮНЕСКО – Організація Об'єднаних Націй з питань освіти, науки і культури, *United Nations Educational, Scientific and Cultural Organization, UNESCO*

Людство завжди прагнуло якнайповніше опанувати всі доступні йому простори. Об'єктивно це пов'язано з бажанням використати їх для цивілізаційного зростання, посилення економічних і політичних позицій держав, що з необхідністю призводило до виникнення протиріч. У результаті всі простори рано чи пізно перетворювалися на «території» запеклих протистоянь і конкурентної боротьби у сфері внутрішніх і зовнішніх відносин.

Щойно людина завдяки авіаційним і ракетним технологіям опанувала *повітря* й *космос* (третій і четвертий простори), розпочалася їх мілітаризація та внутрішня боротьба за гегемонію. Проте якщо з повітряними кордонами держав усе було більш-менш зрозуміло, то в космосі відсутні державні кордони, тому його мілітаризацію було заборонено відповідними міжнародними угодами. Разом з тим фактично мілітаризація й гонка космічних озброєнь мали двох основних акторів – головних суперників часів «холодної війни» – СРСР і США. Згодом до клубу космічних гравців долучилася КНР, яка нині намагається стати країною, що першою створить постійну базу на Місяці.

На простір мілітарної змагальності перетворюється і п'ятий – кіберпростір – буття, винятковість якого пов'язана з тим, що він єдиний з усіх п'яти наразі опанованих людиною просторів є екстериторіальним, адже практично позбавлений географічних обмежень.

При цьому залежність сучасної людини від кіберпростору є лише трохи меншою, ніж від інших. Саме від кіберпростору, від його стану, функціональності, передбачуваності та прогнозованості залежить стабільність світової економіки, безпека людей, всезагальне зростання добробуту, суспільний розвиток. Хоча ніхто не га-

рантує, що розвиток кіберпростору може відбутися (й, на великий жаль, уже відбувається) у зворотному напрямі: до нестабільності й розбалансованості економічних, фінансових і політичних процесів, створення дедалі нових викликів і загроз, деградації людської особистості, відсутності реального суспільного розвитку й тотального контролю та шпигунства, декорованого пропагандистським флером перевернутих утопій (дистоній) у стилі романів Дж. Оруелла, О. Хакслі чи Є. Замятіна.

Проте попри всю реальність згаданих викликів і загроз, людство не поспішає зі встановленням чітких принципів і правил поведінки в кіберпросторі. І хоча певні кроки в цьому напрямі вже зроблено[1], сучасний кіберпростір досі перебуває у стані своєрідного хаосу, нагадуючи, радше, первісний додержавний світ «війни всіх проти всіх» Т. Гоббса.

Відсутність принципів існування та використання кіберпростору, пріоритет практичних міркувань над правилами співіснування людей характеризують політику використання кіберпростору як своєрідну *realpolitik,* яку часто намагаються поєднати з радикальними ліберальними теоріями, створюючи химери уявного світу, який нібито регулюється загальноприйнятими нормами на кшталт Вестфальського миру та міжнародним законодавством. Попри всі публічні заклики до мирного використання кіберпростору в інтересах усіх людей і держав, уряди тих самих країн, які до цього закликають, активно долучилися до гонки кіберозброєнь, відтворюючи класичну «дилему безпеки» на якісно новій основі. А це означає, що на тлі розгортання складних і суперечливих глобальних процесів політичного, економічного та соціального розвитку кіберпростір перетворюється на простір виникнення «холодної війни *v*2.0.», тобто основу нового протистояння ключових геополітичних суб'єктів, яке відбуватиметься переважно в кіберпросторі.

Оскільки політична й геополітична змагальність у кіберпросторі є віртуальною і, швидше, вторинною щодо інших просторів, для її адекватної оцінки доречно скористатися алегорією Платона про печеру: на віртуальній «стіні» «печери» кіберпростору можна бачити «тіні» реального протиборства держав (у найближчій перспективі й недержавних

[1] Виступаючи у 2011 році з нагоди оприлюднення Міжнародної стратегії дій у кіберпросторі, Президент США Б. Обама зазначив, що «цифровий простір не є більше фронтіром без закону» [325]. Під «фронтіром» в історії США XVII–XIX століть розуміється перехідна територія дикої експансії, яку зазвичай виразно, з елементами невиправданої романтизації, зображають у голлівудських вестернах. «Фронтір» був територією беззаконня й конфліктів «нових» американців (колонізаторів) зі «старими» (аборигенами-індіанцями). З наведеного порівняння фактично випливає, що кіберпростір у його нинішньому неврегульованому стані – це феномен, синонімічний Дикому Заходу з усіма його тодішніми проблемами, спроектованими на сьогодення.

суб'єктів). Унікальність ситуації полягає в тім, що «тіні» цілком можуть взаємодіяти з «реальною реальністю» і не є цілковито ефемерною конструкцією, про що, зокрема, свідчить ескалація напруження в кіберпросторі між США та КНР, а також між США та Російською Федерацією.

Не залишається осторонь цих питань і Європейський Союз, інтеграцію до якого проголошено зовнішньополітичним пріоритетом України. Причому наразі ЄС фундаментально переосмислює кібербезпекову дійсність [243] і переходить від розуміння кіберзагроз виключно як кіберзлочинів до військових і геополітичних трактувань цього явища.

Отже, держави загалом мають принципово переосмислити пріоритети національних інтересів і саморозуміння, зважаючи на те, що захист інтересів держави та нації в інформаційному суспільстві якісно вирізняється від традиційного розуміння безпеки як «стану захищеності». Оскільки світ перманентно перебуватиме під впливом різноманітних криз, то й про жодну «захищеність» у цьому світі не можна ставити питання. Ітиметься, вочевидь, лише про послаблення загроз та зниження вразливості до прийнятного рівня. Хоча цифрові кордони держав дедалі менше збігаються з їх географічними кордонами, захист цих кордонів і цифрового суверенітету стає проблемою дедалі актуальнішою.

Україна інтегрована у світовий цифровий простір і відповідно зазнає різних загроз і негативних впливів, пов'язаних з розвитком кіберпростору (зокрема від наслідків суперництва США та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Йдеться про необхідність концептуально зрозуміти нову безпекову (кібербезпекову) реальність та вирішити суто практичні питання впорядкування внутрішнього нормативно-правового поля, зон відповідальності відомств, задіяних у забезпеченні кібербезпеки держави, загалом весь комплекс проблем, пов'язаних з розбудовою ефективної національної системи кібербезпеки. Надто вже зараз Україна потерпає не лише від «традиційних» кіберзлочинів, а й від складніших кібератак.

Україна має не просто сформулювати на загальнодержавному рівні власне бачення глобальних процесів, пов'язаних з розвитком кіберпростору, вона мусить *віднайти себе* в цих процесах. В іншому разі питанням стають перспективи державного буття Української держави в умовах «нового цифрового порядку» з його агресивно-гегемоністською компонентою «холодної війни *v*2.0.».

Стан наукової розробленості теми. Незважаючи на значний суспільний і науковий інтерес до взаємозв'язку між проблемами геополітики та світовою й національною політикою розвитку кіберпростору,

ця тема досліджена вельми фрагментарно. Лише щодо окремих аспектів і напрямів існують достатні напрацювання, які кореспондують із традиціями й новаціями геополітики як науки та політичної практики.

Питання загальної геополітичної теорії знайшли відображення передусім у працях її засновників, до яких слід віднести насамперед Ф. Ратцеля, Р. Челлена, К. Хаусхофера, А. Мехена, Х. Маккіндера, Н. Спайкмена. Згодом з'явилися праці таких представників нетрадиційних напрямів геополітики, як А. Шупраде, П. Галлуа, Ж. Туатайль, Дж. Егню, І. Лакосте, П. Відаль де ла Блаш, Р. Арон, Е. Долман, Ф. Макдоналд, С. Делбі, К. Доддс.

Оскільки після Другої світової війни геополітику в СРСР було проголошено «нацистською наукою», тобто на неї де-факто було накладено табу, то її розвиток на теренах України й інших пострадянських республік розпочався тільки за років горбачовської Перебудови. З-поміж українських і російських дослідників новітньої доби проблеми геополітики досліджували Т. Михайлов, В. Цимбурський, Я. Волков, І. Кефелі, П. Циганков, В. Якунін, М. Ільїн, В. Адріанов, І. Василенко, К. Гаджієв, В. Куткін, В. Дергачов, Б. Парахонський, Г. Яворська, М. Єжеєв, О. Волошин, А. Соболєв, О. Резнікова, В. Шахов, Д. Міхель, Ж. Панченко, С. Василенко, Ю. Шмаленко, А. Бутузова.

У межах загальної теорії геополітики як окремий напрям успішно розвивається геостратегування. З-поміж іноземних дослідників на цих проблемах зосереджувалися К. Міна, Дж. Паркер, Зб. Бжезинський. З-поміж пострадянських – Ю. Вознюк, В. Цимбурський, П. Масляк, А. Гольцов, М. Русанова, М. Рижков, С. Юрченко, О. Ірхін, М. Гнатюк.

Упродовж останнього десятиліття істотно зросла кількість досліджень, присвячених геополітичному й військовому значенню кіберпростору та пов'язаним з цим ключовими питаннями. На особливу увагу заслуговують праці Г. Раттрея, Д. Шелдона, К. Демчака, П. Домбровського, Дж. Ная-мол., С. Старра, Лі Джанга, А. Клімбурга.

Термінологічні дослідження з кібербезпекової проблематики знайшли належне відображення у працях Дж. Ліпмана, Д. Фахренкурга, Ф. Крамера, Л. Вентца, Дж. Льюїса, М. Лібіцкі, Д. Куела, С. Бейделмана, Л. Жанчевскі, А. Коларіка, М. Каветлі. Віддали належне цій тематиці й вітчизняні дослідники: О. Порфимович, А. Марченко, Ю. Федорова, М. Погорецький, В. Шеломенцев, О. Манжай, В. Петров, М. Ожеван, В. Пилипчук.

До критично важливих для нашої роботи досліджень варто віднести праці з нормативно-правової проблематики кібербезпеки, зокрема

дослідження Дж. Ліпмана, Дж. Льюїса, Ф. Крамера, Л. Вентца, К. Александера, Р. Олдріча, В. Шарпа, Т. Вінгфілда, М. Шмітта, Дж. Міхаельї, Д. Віджесекера, Д. Аддікотта, Б. Шнаєра, Дж. Чарльза, Л. Мюїра, Ш. Лоусона, Дж. Ліндсея, Д. Брауна.

Серед вітчизняних досліджень нормативно-правових проблем кібербезпеки на особливу увагу заслуговують праці М. Ожевана, О. Дзьобаня, В. Пилипчука, В. Петрова.

Концептуальну рамку досліджень проблем кіберпростору в геополітичному сенсі створюють дослідження інформаційного суспільства та його похідних. Крім «класичних» робіт Е. Тоффлера, Ф. Махлупа, Ф. Фукуями, Ю. Хаясі, М. Бангеманна, М. Маклюена, Г. Рейнгольда, на увагу заслуговують роботи М. Ожевана, І. Педака, Ю. Павленка, І. Даніліна, Р. Барбрука, Д. Камерона, Ф. Міллраха, М. Капура, Н. Гінгріча, Дж. Ная-мол., Т. Вадена, Й. Суоранта, С. Жижека, А. Крокера, А. Вайнштайна, В. Скалацького.

У дослідженні ми будемо виходити з того, що ключовим геополітичним суперництвом, яке визначатиме природу загального геополітичного ландшафту міжнародних відносин у стратегічній перспективі, буде суперництво між США та КНР. Саме їх відносини (передусім щодо кіберпростору) покладено в основу роботи. Отже, важливими для цілей дослідження є праці, присвячені сучасному стану й розвитку політичних систем США та КНР, а також дослідження взаємовідносин цих провідних країн. У даному зв'язку привертають увагу роботи Р. Беттса, Г. Кіссинджера, Е. Долмана, Ся Ліпіна, Цзянь Сіюаня, Д. Мульвенона, Г. Вакера, Р. Маккінона, Р. Пітерса. З-поміж вітчизняних і російських досліджень слід виокремити роботи Є. Євдокимова, А. Ломанова, І. Зевельова, М. Гримської, Я. Єрьоміна, П. Ленського, О. Шевчука, Н. Жданова.

Частина досліджень із проблематики суперництва США та КНР у кіберпросторі присвячена перспективам імовірного переходу цих країн до суперництва «холодна війна *v*2.0.». З-поміж дослідників, які вказують на таку перспективу й активно її досліджують, доречно назвати Я. Бремора, Д. Роткопфа, Р. Діперта, Д. Редкліфа, Є. Черненко, А. Раффа, Е. Джелленка, Х. Ліна.

Водночас наразі в науковій літературі відсутні системні наукові дослідження, присвячені геополітичному виміру глобальних суперництв (зокрема США та КНР) у кіберпросторі, а також наслідкам такого використання кіберпростору для інших учасників міжнародних відносин, передусім для України.

Об'єктом дослідження є геополітичне суперництво.

Предметом дослідження є кіберпростір як новий вимір геополітичного суперництва.

Метою дослідження є встановлення ролі кіберпростору як арени нових геополітичних суперництв і протиборств, його ролі в геополітичному суперництві США та КНР, а також обґрунтуванні пріоритетних заходів Української держави в умовах перетворення кіберпростору на арену геополітичних протиборств.

Реалізація зазначеної мети передбачала розв'язання цілої низки **завдань:**

• визначення ролі та місця проблематики кіберпростору в теорії геополітики;

• концептуалізації емпіричного матеріалу, що стосується трансформації пріоритетів національних інтересів розвинутих країн в умовах глобалізації кіберпростору;

• формулювання ключових проблем термінологічної й нормативно-правової невизначеності кібербезпекової проблематики на національному та міжнародному рівнях;

• характеристики геополітичного суперництва США та КНР у кіберпросторі у форматі «холодної війни *v*2.0.», що перетворюється на домінантний зовнішньополітичний наратив XXI сторіччя;

• опису й уточнення основних механізмів кіберпротистоянь: політичного хактивізму, кібершпигунства, кібердиверсій;

• характеристики підходів ключових геополітичних гравців до проблем мілітаризації кіберпростору («гонки кіберозброєнь») та його демілітаризації;

• формулювання пропозицій для органів державної влади стосовно приведення у відповідність до національно-державних інтересів системи кібербезпеки України з урахуванням зовнішньополітичної й геополітичної сфер та актуальних питань вдосконалення механізмів реагування на кіберзагрози та кібервиклики з боку системи національної безпеки та оборони держави.

Методологічні підходи й методи дослідження. Відповідно до конкретних завдань на різних етапах дослідження використано такі методологічні підходи й методи, як системно-структурний, кібернетичний, синергетичний, структурно-функціональний, порівняльно-історичний, герменевтичний, аналогії, аналізу й синтезу, сходження від абстрактного до конкретного, структурно-логічного моделювання, індукції та дедукції, інтерпретації тощо.

БЕЗПЕКА КІБЕРПРОСТОРУ ЯК ПАРАДИГМА НОВОЇ ГЕОПОЛІТИКИ ТА ГЕОСТРАТЕГІЇ

1.1. Зрушення сфер геополітичного протиборства: від просторів географічних до просторів інформаційних і кібернетичних

Протягом історії людства доступні йому «простори» завжди були джерелом могутності й більшості міжнародних конфліктів, одночасно надаючи, проте, засоби їх розв'язання.

Ця проблема з необхідністю відобразилася в загальнонаукових і практично значущих концептуалізаціях, що згодом спричинило дослідження принципів та ефективності використання можливостей того чи іншого «простору», його значення й сутнісних характеристик у межах геополітики. Як науковий напрям геополітика спроможна більш-менш чітко визначити роль і значення «кіберпростору» в сучасних міжнародних відносинах та за допомогою своєї практичної частини – геостратегії – вказати на необхідні засоби для аналізу поточної політики провідних держав світу щодо політичної практики за умов виникнення й утвердження нової «просторової реальності».

При цьому слід погодитися з Дж. Наєммол. (*Joseph S. Nye, Jr.*[2]), розробником концепції «м'якої сили», що інформаційний простір і кіберпростір не можуть замінити простір географічний і не провіщають скасування державних суверенітетів [383]. Ідеться, радше, про нові ін-

[2] Тут і далі з метою уникнення проблем, пов'язаних з різночитанням, при першому згадуванні прізвища іноземних дослідників, державних, громадських діячів тощо дублюються в дужках латиницею. Винятком із цього правила є написання прізвищ російських, білоруських дослідників і діячів, а також вищих посадових осіб різних країн (Б. Обама, Ху Цзіньтао, Дж. Буш, М. Ахмедініжад, Лі Куан Ю та інші) – *Прим. ред.*

струменти посилення/послаблення державної могутності й державних суверенітетів, про істотні впливи інформаційно-комунікативних технологій (ІКТ) на політику й геополітику, похідними яких є сфери технополітики й техногеополітики [453].

Телеграф і телефон, щойно з'явившись у XIX сторіччі, значною мірою «ущільнили» географічний простір і детермінували масові рухи за скасування рабства та колоніалізму в їх найбільш одіозних формах і виявах. Радіо й телебачення посилили тренд «комунікативного ущільнення» та перетворили наступне XX сторіччя на пропагандистський час «промивання мізків».

Порівняно з іншими напрямами політичної думки геополітика є відносно молодою наукою. Більшість фахівців з геополітики впевнено називають її батьком-засновником німецького географа Ф. Ратцеля (*Friedrich Ratzel*), який одним з перших здійснив спробу поєднати політику й географію та вивчати політику держави, орієнтуючись на її географічне розташування.

Водночас варто зазначити, що сам Ф. Ратцель не застосовував терміна *геополітика*. Його засаднича праця мала назву «Політична географія». З огляду на те, що значну частину свого життя він присвятив етнології, логічною є його ключова сентенція: держава є живим організмом, однак організмом, закоріненим у природному «ґрунті», усвідомлення якого є тим ключем, який може вважатися основою для розуміння позиції й ролі держави на світовій арені, оцінювання її потенціалу та перспектив еволюційного розвитку.

Наполягаючи на сутнісному «географічному» розумінні держав, Ф. Ратцель разом з тим звертав увагу на те, що обсяг поняття *простір* є ширшим, аніж визначення його відповідно до суто географічних меж. А одне із запроваджених дослідником основних понять – *життєвий простір* – узагалі неоднозначно поєднує геота біосередовище.

Ідея держави-організма, запропонована Ф. Ратцелем, робить природним прагнення будь-якої держави до територіального розширення. Фактично він чи не вперше переконливо довів, що будь-яка держава, яка прагне «величі», має здійснювати експансію. Таке розуміння політики «великих держав» частково пояснює поступову мілітаризацію будь-якого «простору», здатного забезпечити державі виграшні умови на міжнародній арені.

Уперше термін *геополітика* був використаний шведським дослідником Р. Челленом, який вважав себе учнем Ф. Ратцеля.

Цікавою особливістю перших теоретичних розробок у сфері геополітики були, власне, ті вихідні мотиви, які рухали як Ф. Ратцелем, так і Р. Челленом (*Johan Rudolf Kjellén*) в їхніх дослідженнях геополітики. Обидва вважали свою роботу не стільки науковою, скільки політично значущою та мали на меті передусім привернути увагу політичних діячів до ролі географічних характеристик в управлінні державою [218]. Наразі геополітика зберігає такий подвійний теоретико-практичний зміст.

Починаючи від розквіту на початку та в першій половині XX сторіччя геополітика подолала доволі складний шлях, зазнавши в перші роки після завершення Другої світової війни тимчасового занепаду. У Радянському Союзі геополітика взагалі опинилася під забороною й лише на початку 90-х років отримала новий стимул разом зі становленням критичної геополітики та глобальної геополітики. Е. Долман (*Everett C. Dolman*) слушно зазначає, що «період певного «занепаду» геополітики закінчується, і вона після доопрацювання ключового поняття *простір* знову перетворюється на мейнстрім наукового мислення. Ренесанс геополітики означає, що, пройшовши крізь немилість і занепад, вона знову вимагає подальшого вивчення» [294, с. 79].

Однією з вихідних проблем дослідження є ствердження сучасного кібернетичного (чи інформаційного) простору як предмета геополітики та з'ясування підходів щодо врахування цього «простору» в геостратегіях держав.

Їх розв'язання ускладнене передусім відсутністю усталеного визначення самого поняття *геополітика*. Незрозумілою, власне, є відповідь на запитання, що вона досліджує за сучасних умов та яким чином співвідноситься з різними «геостратегіями». Загальна множина пропонованих дослідниками визначень предметної сфери геополітики, з одного боку, відображає нюанси розвитку цієї науки як класиками, так і сучасними дослідниками, а з іншого – свідчить про складну динамічну природу предмета вивчення.

У цьому сенсі показовим є дослідження проблем взаємозв'язку космосу та геополітики Ф. Макдоналдом (*Fraser MacDonald*), який констатує, що «незважаючи на більш ніж 50-річну експлуатацію людиною космосу, нам досі не вдалося внести необхідні зміни у критичну географію щодо цього простору» [359, с. 593]. Тобто з погляду класичної геополітики навіть така вже звична для нас проблема, як роль космосу в загальному балансі сил, дотепер є неоднозначною.

На нашу думку, суттєву проблему у вирішенні взаємозв'язку кіберпростору та геополітики становить надмірна прив'язаність класичного розуміння геополітики до землі (*land*) та географії. Зокрема, в розумінні класиків і сучасних теоретиків геополітика це:

• теорія про державу як географічний організм або феномен у просторі (*phenomenon in space*) (Р. Челлен [73]);

• вчення про просторовий детермінізм усіх політичних процесів, засноване на широкій географічній базі, особливо базі політичної географії (К. Хаусхофер (*Karl Haushofer*) [296]);

• наука, що здійснює пошук розуміння геополітичних реалій та їх майбутнього на основі вивчення профілів, даних і геополітичного устрою (А. Шупраде (*Aymeric Chauprade*) [Там само]);

• напрям, що вивчає взаємозалежність зовнішньої політики держав, міжнародних відносин і систем політичних, економічних, екологічних, воєнно-стратегічних та інших взаємозв'язків, зумовлену географічним положенням країни (регіону) та іншими фізико- й економіко-географічними чинниками (Т. Михайлов [129, с. 22]);

• політична практика держави через раціоналізацію національних інтересів у часі та просторі (Я. Волков [36]).

Попри таке багатоманіття визначень, більшість з них насправді лише частково відповідає сучасним реаліям геополітичного протиборства, адже, як справедливо зазначив російський дослідник І. Кефелі, «більшість конструкцій засновниками геополітики будувалася на достатньо обмеженому понятійному апараті – географічний простір, держава, сила» [87, с. 9]. Оскільки більшість предметних визначень геополітики дійсно надмірно апелює до суто географічного чинника, ігноруючи ключові для предмета дослідження процеси інформатизації та глобалізації або не надаючи цим процесам належної уваги, вони не можуть бути використані (у запропонованому їх авторами вигляді) для потреб дослідження.

Як слушно зазначав на початку 90-х років XX сторіччя російський дослідник П. Циганков, в епоху постіндустріальної революції руйнуються майже всі традиційні «імперативи» «класичної геополітики». Відповідно наївно думати, що геополітика – це передусім «суперечки між державами з приводу територій» [218]. Російський політичний діяч В. Якунін також звертає увагу на те, що за сучасних умов «геополітика виступає як комплексна форма налагодження економічних (фінансових, торговельних), соціальних, культурних чи інших аналогічних форм владного впливу, не обумовлених при цьому доміную-

чими образами територіального проникнення (так само, як і відповідною риторикою, символами та іншими інструментами такого типу впливу)» [230].

У роботі «Геополітика. Витоки могутності» П. Галлуа (*Patrick Gallois*) зауважує такі риси сучасної геополітики [Цит. за: 218]:

• по-перше, вона не має нічого спільного як з географічним детермінізмом, так і з нацистською інтерпретацією цього терміна;

• по-друге, її слід відрізняти від політичної географії, яка пояснює міжнародну політику впливом зовнішнього середовища;

• по-третє, до її традиційних елементів – просторово-територіальних характеристик держав (географічного положення, довжини кордонів, запасів корисних копалин, структури населення тощо) – сьогодні додаються нові, такі, що перевертають наші уявлення про силу держав, змінюють пріоритети врахування чинників впливу на міжнародну політику. Передусім ідеться про зброю масового ураження та засоби її доставки, освоєння космічного простору, здатне впливати на стан світової політики.

У більш широкому сенсі можна говорити про глибинну кризу «державоцентричної оцінки спатіальності[3]», на що звертає увагу британський дослідник Дж. Егню (*John Agnew*). Ця криза характеризується переоцінюванням трьох географічних постулатів, які впродовж тривалого часу вважалися основою не лише геополітики, а й самого світопорядку: 1) держави мають виключний суверенітет над власною територією; 2) «внутрішні» та «зовнішні» сфери чітко розділені між собою; 3) кордони держав визначають кордони «суспільства» [Цит. за: 139].

Важливим поштовхом до кризи класичної теорії геополітики та геостратегії стала так звана ера балістичних ракет, яка розпочалася з 1960-х років XX сторіччя і здійснила переворот в ієрархії стратегічних сил. Більшість географічних чинників (острівне положення, геоморфологічні особливості тощо) втратили для світової та геополітичної стратегії держав свій початковий, традиційний, сенс [35]. Це своєю чергою сприяло поступовій зміні геостратегічних підходів індустріальної епохи. Вони ґрунтувалися на геополітичній парадигмі міжнародних відносин, що передбачала планомірне широкомасштабне вжиття заходів щодо концентрування управління в регіонах світу з метою встановлення прямого військового та політичного контролю над планетарними ресурсами [225].

[3] Просторовості – *Прим. авт.*

На нашу думку, згадана робота П. Галлуа відобразила доволі жорстку дискусію між прибічниками «вузького» та «широкого» підходів до геополітики, стала своєрідним проміжним етапом переосмислення більшості положень «класичної» геополітики.

У «вузькому» («класичному») розумінні геополітики досі переважають доволі спрощені географічні підходи, які базуються насамперед на аналізі географічних чинників у контексті протистояння континентальних і морських держав. Основний закон «класичної» геополітики зводиться до фундаментального дуалізму двох стихій – «телурократії» (суходільної могутності) і «таласократії» (морської могутності).

Прибічників традиційного підходу предостатньо. На їхню думку, предметом геополітики може бути лише «з'ясування взаємодії природних та, ширше, географічних чинників з різними системами та способами політичної організації» [83, с. 82]. Будь-які спроби трактувати геополітику більш широко вони називають виявами «геополітичного марення»: «ані високий рівень технологічного розвитку, ані економічне процвітання суспільства, ані масштабні фінансові ресурси не виводять державу поміж великих держав, якщо у неї немає для цього геополітичної основи. Лише наявність великої території з цінними ресурсами та численним населенням є своєрідним резервуаром могутності й безпеки держави і є, хоч і не достатньою, проте необхідною умовою перетворення держави на світовий центр сили, до якого схилятимуться та довкола якого групуватимуться країни та народи» [7].

Думка В. Адріанова в контексті дослідження феномену кіберпростору та його геополітичного значення дійсно є сенсовою, однак в іншому розумінні, ніж це формулюють прихильники «вузького» підходу. У феномені кібермогутності ключовим чинником є не стільки технологічна, скільки кадрова перевага – наявність достатньої кількості фахівців, які зможуть забезпечити інтереси держави в кіберпросторі. Відповідно, держави з більшою кількістю населення отримують очевидні латентні переваги у використанні потенціалу цього нового простору. Наразі КНР має один з найпотужніших *IT*-комплексів (починаючи від проектування і закінчуючи виробництвом), а Індія є одним зі світових лідерів з підготовки програмістів.

Водночас, на нашу думку, стверджувати можливість використання постулатів повноцінної «класичної» геополітики в сучасному світі можна лише з неабиякими застереженнями. І обумовлено це навіть

не вже згаданими стрімкими технологічними змінами (наприклад, розвитком ракетної техніки), а й іншими, суттєвішими, обставинами. Наприклад, базова теза «класичних» геополітиків, зокрема Ф. Ратцеля, Р. Челлена чи П. Відаля де ла Блаша (*Paul Vidal de la Blache*), полягає у визначній ролі (у кожного в різній пропорції) напівмістичного взаємозв'язку «землі» та «людини». По суті ж ідеться про так звані довгі ідентичності, до яких, власне, відноситься і національна ідентичність. Однак саме вона є чи не першою жертвою сучасних процесів глобалізації й інформатизації. Сучасна людина значно менше «психологічно» пов'язана з територією проживання, ніж це було навіть 20–30 років тому.

Сучасні інформаційні технології роблять кордони політичною умовністю, а поява нових форм трансграничної соціалізації (через розваги, роботу, приналежність до груп інтересів тощо) робить зв'язок із «землею» дедалі примарнішим. Очевидно, цьому сприяють і масштабні міграційні процеси, які значно інтенсифікувалися протягом останніх десятиріч. У цьому новому «великому переселенні народів» (іноді без їх фізичного переміщення) щороку дедалі складніше зрозуміти, про яку, власне, Батьківщину йдеться. І такі складнощі виникають майже за всіма параметрами сучасного розуміння сили, могутності і впливовості держави чи групи держав.

При цьому окремі концептуальні тези «класичної» геополітики цілковито можуть бути адаптовані до потреб розуміння нових видів простору. Наприклад, концепція А. Мехена (*Alfred Thayer Mahan*) щодо набуття США статусу світової держави передбачала виконання чотирьох ключових пунктів.

1. Активне співробітництво з Британською (морською) державою.

2. Протидія морським претензіям з боку Німеччини.

3. Уважне спостереження за експансією Японії в Тихому океані та протидія цій експансії.

4. Координування спільних з європейцями дій проти народів Азії.

Якщо ж оцінювати реальність сучасного протистояння у кіберпросторі (про що йтиметься у наступних розділах роботи), то нескладно помітити, що ці пункти, хоча й зазнали часткового коригування, проте досі визначають напрям американської зовнішньої політики, про що свідчать такі факти.

1. Активне співробітництво з Британією у сфері кібербезпеки.

2. Протидія російсько-китайським претензіям щодо функціонування глобального кіберпростору.

3. Уважне спостереження за експансією союзних європейських держав (особливо Німеччини та Франції) у кіберпростір і протидія цій експансії.

4. Координування спільних з європейцями дій у кіберпросторі проти народів Азії.

На противагу «вузькому» підходу до тлумачення терміна геополітика «широкий» підхід, який зазнав серйозного розвитку лише наприкінці 80-х – початку 90-х років XX сторіччя, передбачає певний відхід від «класичного», базового розуміння геополітики як науки, ґрунтованій на географії як такій.

Зокрема, Ж. Туатайль (*Gearoid O'Tuathail*) зазначає: «глобалізація, інформаціоналізація, суспільство ризику викликали умови геополітики постмодерну у світовій політиці. Ці взаємозалежні процеси безпосередньо кидають виклик і знищують кордони сучасної міждержавної системи, створюючи нові режими взаємопов'язаності між просторами по всій земній кулі; трансформуючи скалярні відносини між локальним, національним і глобальним; запроваджуючи безпрецедентні швидкості взаємодії та комунікації; створюючи посилену взаємозалежність та уразливість від небезпек по всьому світу» [139]. А оскільки інформатизація суспільства є глобальним соціальним процесом виробництва і повсюдного використання інформації як суспільного ресурсу, то вона перетворилася «з об'єкта теоретичного аналізу вчених <...> на критерій оцінки могутності держав, стала найважливішим чинником у боротьбі тієї або іншої країни за економічну, політичну, культурну і військову перевагу, а також чинником виживання всього людства в цілому» [130, с. 68–69].

Український дослідник П. Федорук зазначає із цього приводу: «інформаційний простір стає тим майданчиком, через який зовнішні гравці нав'язують своє «геополітичне бачення», свої уявлення про «геополітичні коди» країн і регіонів, за допомогою яких сучасна геополітика фактично ототожнює реальні (які існують фізично) і віртуальні (концептуальні) простори» [210, с. 184]. У цілому погоджуючись із цим твердженням, ми застерігаємо від надмірної уваги до слабко окресленого «інформаційного простору», введення якого до сфери геополітичних розробок (принаймні їх гуманітарного складника) має для науки не менші загрози, ніж розмивання предмета науки в цілому.

Сучасні вельми суперечливі інформаційні процеси суттєво впливають на розуміння геополітики як такої, на що вказує французький

дослідник І. Лакосте (*Yves Lacoste*), який займається питаннями геополітики з 70-х років XX сторіччя.

Він слушно зауважує, що термін *геополітика* насправді «має справу з усім, що стосується суперництва держав або впливу на території та людей, які там проживають: суперництва між політичними силами всіх видів – і не тільки між державами, а й між політичними рухами та озброєними групами» [296]. У такому розумінні геополітика значно відходить від суб'єктності Вестфальської системи з державою як центральним елементом, оскільки включає і недержавних (позадержавних) суб'єктів.

Звичайно, неможливо заперечувати вплив соціоприродних географічних чинників на політичну організацію суспільства, так само, як і те, що ці чинники можуть бути щонайефективніше використані у практичній політиці й у жодному разі не можуть бути повністю відкинуті. Відповідно вони й надалі залишаються важливими об'єктами дослідження геополітики, але для новітнього переосмислення предмета геополітики дедалі важливішими стають питання взаємодії та взаємовпливу зовнішніх і внутрішніх аспектів розвитку цивілізації. Наприклад, дедалі тіснішим стає переплетення геополітики зі «світсистемним» підходом.

У сенсі глобального переосмислення геополітики дослідник К. Гаджієв закликає інакше поглянути на частину *гео*, пропонуючи розуміти її не як географічний чи просторово-територіального аспект політики, а як аспект загальнопланетарний, тобто з урахуванням параметрів і вимірів, правил і норм політичної поведінки в цілому, а також поведінки окремих держав, союзів, блоків у загальносвітовому контексті [42].

Однак, як ми вже зазначали вище, за такого надто широкого трактування геополітики існує реальний ризик втрати її предметної самобутності та перетворення на синонім світової політики або глобалістики.

Усі зазначені термінологічні трансформації спричинили до оформлення на межі 80-х і 90-х років XX сторіччя терміна *критична геополітика*. Його поява пов'язана передусім із дослідженням двох ірландських політичних географів – С. Делбі (*Simon Dalby*) і Ж. Туатайля.

Ж. Туатайль визначав новий напрям у геополітиці таким чином: «Критична геополітика – це підхід, який намагається проблематизувати наявні епістемологічні припущення та онтологічні орієнтації загальноприйнятої геополітики (класичної). Вона деконструює оку-

ляроцентризм (критика візуальної метафорики) об'єктивації світової політики класичною геополітикою, а також кидає виклик її відданості (певним державоцентричним політичним практикам) державоцентризму. У такий спосіб критична геополітика сама постає як форма геополітики, втягнена у гру опису геополітичних умов, однак такою, яка намагається деконструювати гегемонію геополітичного дискурсу та поставити під сумнів взаємовідносини сил у визначених геополітичних практиках домінуючих держав» [139].

У своїй книзі, що вийшла друком 2006 року, Ж. Туатайль зазначив, що геополітика – це передусім «дискурс щодо світової політики з особливим акцентом на змагальності держав у географічному вимірі їх могутності» [385]. Акцент на понятті *дискурс* відсилає до практик постмодерністської філософії, де саме дискурс є одним із центральних понять. Піддаючи геополітику постмодерністському переосмисленню, Ж. Туатайль вважає, що вона постає надзвичайно привабливою наукою, оскільки претендує на пояснення складних речей у простих термінах.

Критична геополітика в контексті запропонованого дослідження є особливо цікавим мейнстрімом переосмислення «класичної» геополітики, адже постулює ототожнення реального (фізичного) і концептуальних «просторів», поєднуючи елементи політичної економії й геополітичної практики, культурології й народної (фольклорної) геополітики, видової ідентичності й геополітичного дискурсу, психоаналітики й геополітичної уяви, образів телекомунікаційних мереж і геополітичних кіберорганізацій, кібернетичних війн і віртуальної геополітики, глобалізації й реструктурування геополітичних регіонів. За таких умов модерністську *гео-графію* замінює постмодерністська *інфо-графія*, оскільки дедалі більше великих груп людей інтегруються в глобальні мережі, тоді як пришвидшений простір інформаційних потоків розмиває традиційні поділи між місцевим, національним і глобальним [154].

Незважаючи на порівняно недавнє виокремлення нового напряму геополітики, вона вже сама розділилася на кілька генеральних напрямів, або предметно-проблемних полів. Британський дослідник К. Доддс (*Klaus Dodds*) наводить таку їх структуризацію:

• геополітичні практики: дослідження шляхів та способів географічних і геополітичних міркувань, поширених у реальній практиці світової політики (до цього напряму належать такі дослідники, як Ж. Туатайль і М. Хеффернан (*Michael Heffernan*);

• геополітичні традиції: переосмислення історичного та географічного контексту ідей, які стосуються географії, політики і стратегії (К. Доддс і Д. Аткінсон (*David Atkinson*);

• геополітика та популярна культура (*popular culture*): репрезентація світової політики на рівні образів масової культури;

• структурна геополітика: осмислення зв'язку практичних проблем державотворення (*statecraft*) із процесами глобалізації; процеси творення інформаційних мереж та економічні трансформації [292].

Концептуалізуючи наведені вище особливості розвитку геополітики як науки і власне те, чим вона наразі постає, зазначимо, що найбільш відповідним сучасному розумінню геополітики є визначення, запропоноване російською дослідницею І. Василенко: «Геополітика – це наука про закономірності розвитку влади людини над простором, що пояснює глобальні процеси, спираючись на комплекс гуманітарних, військових і політичних чинників» [31, с. 32].

Принциповим тут є акцент на просторі як такому, оскільки технічний розвиток людства останніх 50 років довів, що новітні технології спроможні не лише забезпечити освоєння нових просторів, до цього часу недоступних людині (космос), а й фактично створити нові (кіберпростір). Відповідно геополітика як наука про глобальні процеси не має права обмежувати себе в тім, які власне простори розглядатимуться нею в контексті забезпечення глобального балансу сил.

Однак наведені міркування наразі не надають вичерпної відповіді на запитання, яким чином проблема кіберпростору (або глобального кіберпростору) потрапляє у фокус уваги сучасної геополітики. Одна з можливих відповідей полягає в тому, що технологічний розвиток людства (передусім в інформаційній сфері та можливостях ведення більш якісних розвідувальних дій) змушує сторони геополітичних конфліктів розглядати як поля можливого конфлікту не стільки «класичні» географічні простори, скільки простори суміжні – економічний, культурний, інформаційний тощо. На цю обставину звертає увагу В. Куткін: «сучасна геополітична теорія <...> має узгоджуватися з новими світовими реаліями, якісними трансформаціями в розвитку суспільства, пов'язаними передусім з науково-технічним прогресом, пануванням інформаційних технологій та новітніми засобами комунікацій, які впливають на всі сфери життя суспільства» [109]. І. Василенко теж підкреслює «комунікативну» трансформацію предмета геополітики, зауважуючи, що «інформаційна революція внесла у сферу геополітики нове – віртуальний вимір простору, змусивши

нас заново переосмислити всі норми та правила геополітичної боротьби» [31, с. 1]. На аналогічні «комунікативні тренди» звертає увагу й В. Дергачов, зазначаючи, що «геополітика – це наука про закономірності розширення та перерозподілу сфер впливу (центрів сили) різних держав та міждержавних об'єднань у багатомірному комунікативному просторі» [54, с. 101].

Відповідно з урахуванням подібних тенденцій новітню геополітику іноді називають інформаційною геополітикою. У межах її категорій під «геополітичним простором слід розуміти «географічну інтерпретацію багатомірного комунікаційного простору (воєнно-політичного, економічного, демографічного, соціокультурного, інформаційного тощо)» [Там само, с. 108].

Кіберпростір у цьому універсально-комунікативному сенсі перетворився на своєрідне «віддзеркалення» суми всіх можливих, традиційних політичних протистоянь. Водночас він постає самостійною ареною протиборства не лише «великих держав», а й країн другого (напівperiферія) і третього (периферія) світів.

Водночас геополітика, залишаючись загальною методологічною рамкою відповідних досліджень щодо кіберпростору, не дає конкретних рекомендацій щодо здійснення зовнішньої (передусім) і внутрішньої політики держав, їх основних кроків, покликаних примножити потенціал держави та її могутність. Цими питаннями займається геостратегування.

Е. Долман, досліджуючи астрополітику, або геополітику космосу, вказує на співвідношення геополітики та геостратегії: «Геополітика розглядає географічні або геоцентричні фізичні та просторові характеристики для пояснення сили. Одиницею аналізу є держава. Важливими є її розташування, розміри, ресурси й населення в контексті політичної ідеології, соціально-культурних цінностей і технології для оцінювання панівних форм війни в даний момент часу. Водночас геостратегія є вмінням використовувати ці знання, визначати ті геопросторові основи, які забезпечать реалізацію планів або стратегій забезпечення військової, економічної, дипломатичної та соціокультурної переваги держави». Різницю понять доповнює й таке твердження дослідника: «Геополітика описує джерела сили держав. Геостратегія пояснює, як їх використати. Розумні керівники держав вивчають географічні особливості, які можуть підвищити силу держави, і намагаються контролювати їх можливості або принаймні не дати контролювати їх опонентам. Вивчення цих можли-

востей, що є складником плану з посилення власної переваги, і є геостратегією» [294, с. 80].

Індійський дослідник К. Міна (*Krishnendra Meena*) так характеризує геостратегію: «Геостратегія є географічним виміром зовнішньої політики держави. Точніше, геостратегія описує, де держава концентрує свої зусилля, передусім воєнні та дипломатичні. Основна ідея геостратегії полягає в тім, що держави мають обмежені ресурси й неспроможні, навіть якщо хочуть, здійснювати тотальну зовнішню політику. Натомість вони мають сконцентруватися на політичній та воєнній компоненті щодо конкретних областей світу. Геостратегія описує зовнішньополітичну спрямованість держави й не має справи з мотиваціями чи процесами прийняття рішень. Відповідно геостратегії держави необов'язково залежать від географічних чи власне геополітичних чинників» [366].

У цілому геостратегію розуміють як субдисципліну геополітики, що є різновидом зовнішньої політики держави, яка керується переважно географічними чинниками, їх впливом, стримуванням (обмеженням) або негативним відображенням на політичному та воєнному плануванні. Як і будь-яка інша стратегія, геостратегія зосереджена на зв'язку цілей і результатів: відповідно – ресурсів країни (незалежно від їх кількості) та геополітичних цілей (локальні, регіональні чи глобальні) [289].

Дж. Паркер (*Geoffrey Parker*) трактує геостратегію ширше – як дослідження просторового розподілу сухопутних, морських та повітряних сил та їх взаємозв'язків з географічним феноменом [156].

Ю. Вознюк зауважує, що «залишаються невідрефлексованими питання, що мали вплив на геополітичне протистояння як прояв конкретної геостратегії: геополітична стратегія – сфера прикладних аспектів геополітичної науки, що адаптуються до динамічних змін у інструментарії міждержавного протиборства з певним запізненням» [35, с. 342].

Геостратегією також часто розуміють як прикладну зовнішню геополітику, застосування на практиці теоретичних положень «фундаментальної» геополітики. На думку В. Цимбурського, геостратегія – це вміння перетворювати фундаментальні геополітичні картини світу на цілі та завдання конкретного гравця, забезпечені ресурсами та сценаріями [220].

Український вчений П. Масляк визначає геостратегію як мету держави на міжнародній арені (виживання, збереження, розвиток тощо) – «боротьбу за місце під сонцем» [125].

Своєю чергою А. Гольцов пропонує розуміти під геостратегією «визначення головних цілей, завдань і принципів зовнішньої політики держави, загальне планування державних дій, розробку засобів і прийомів здійснення політики на міжнародній арені» [45, с. 21], адже «традиційно будь-яка геостратегія зводилася до визначення провідних напрямів зовнішньої політики держави, спрямованих у кінцевому рахунку на здобуття чи/та утримання контролю над певним геопростором» [Там само, с. 22]. Проте дослідник зауважує, що «велике значення [геостратегія – *Авт.*] має також для формулювання концептуальних положень національної безпеки, розробки воєнної доктрини держави. Крім того, вона безпосередньо стосується провідних напрямів економічної, культурної, демографічної, екологічної політики держави на міжнародній арені» [Там само, с. 21].

М. Русанова вважає, що «геостратегія – це вибір напрямів зовнішньополітичної діяльності держави, план її суверенного територіального розвитку, що дозволяє державі досягти своїх теоретичних імперативів – самозбереження і максимальної якості життя своїх співгромадян» [181].

Останнє визначення, на нашу думку, чи не найточніше визначає ключові аспекти геостратегування. Однак зазначимо, що специфіка кіберпростору обумовлює й певні специфічні особливості формування геостратегій держави саме щодо нього. Так, навіть у кіберпросторі можна виділити як «периферійні», так і своєрідні «хартлендові» країни, однак їх статусність та можливості в кіберпросторі майже не залежать від їх реального географічного розташування та обумовлюються іншими чинниками – розвитком *ІТ*-сфери, соціальним капіталом, якістю освіти, продуманістю політики забезпечення кібербезпеки держави, масштабністю та інноваційністю інформаційної інфраструктури тощо. Зважання на це змушує доволі критично поставитися до наявних підходів до геостратегій.

Інша важлива особливість (окреслена вище) – проблема кордонів, а відповідно, й можливість розділити зовнішню та внутрішню політику. Якщо в «класичному» розумінні геостратегії зосереджені саме довкола зовнішньої політики держав, то кіберпростір, маючи подвійну національно-трансграничну природу, майже усуває розбіжності між цими поняттями. Наприклад, політика держави щодо розбудови «національного інформаційного суспільства» де-факто є виміром зовнішньої політики, оскільки буде пов'язана з розбудовою інфраструктури, яка може (і буде) використовуватися також іноземними

структурами. Навіть цілком внутрішні питання освітньої сфери (наприклад, підготовки *IT*-фахівців), з огляду на особливий вплив людського ресурсу на домінування в кіберпросторі, робить це питання частиною зовнішньої політики держави. Аналогічно зовнішні рішення (наприклад, приєднання до тих чи інших міжнародних безпекових ініціатив) справляють вплив на формування внутрішніх механізмів розвитку потенціалу держави в контексті її позиціювання в глобальному кіберпросторі.

Відповідно, вироблення геостратегій держав щодо кіберпростору має ґрунтуватися на суттєво вдосконаленій методології. Використовуючи базові поняття геостратегування (наприклад, жорстку прив'язку до проблеми обмеженості ресурсів і необхідності концентрування своїх воєнних і дипломатичних зусиль на певних напрямах), геостратегії щодо кіберпростору мають бути побудовані принципово цілісніше, пов'язуючи між собою як суто внутрішні політичні процеси, так і зовнішню політику держави, що загалом має спричинити «суверенний територіальний розвиток» і «досягнення теоретичних імперативів самозбереження і максимальної якості життя своїх співгромадян» [313].

За аналогією з «великими стратегіями» США – ізоляціонізму, балансування або відкидання й залучення та взаємозалежності, пов'язані з доктринами Монро, Трумена та Клінтона, – можна зауважити щодо існування «великих кіберстратегій». Причому щодалі увиразнюється вибір країнами цих «великих кіберстратегій». Наприклад, США як єдина у світі наддержава тяжіє до стратегії залучення та взаємозалежності, в той час як країни-члени ЄС та ЄС у цілому обрали стратегію балансування. Ізоляціоністську кіберстратегію щодо власного кіберпростору найяскравіше демонструє КНР. Водночас ця країна знайшла власний до певної міри унікальний «блокадний шлях», за якого частина світових інтернет-ресурсів не просто блокується, а заміщується аналогічними програмними продуктами власного виробництва.

Китайський блогер М. Анті (*Michael Anti*) зазначає: «в Китаї ми маємо «розумну цензуру». Уряд КНР заблокував кожен міжнародний сервіс і всі їх скопіював. Таким чином, китайська політика у сфері інтернет-регулювання надзвичайно проста: блокуй та клонуй. Китайський уряд розуміє необхідність дати людям те, що їм подобається, – соціальні мережі. Однак разом з тим він розуміє необхідність контролювати сервери» [239]. З огляду на те, що в КНР понад 500 млн користувачів інтернету, така політика обмежень поступово формує те, що деякі дослідники називають «національним інтернетом» [143].

Як і будь-які інші узагальнюючі теоретичні конструкції, «великі кіберстратегії» не можуть існувати ізольовано одна від одної, відповідно, значна кількість гравців демонструє їх взаємопроникнення в межах здійснення практичних політик своїх країн. Унаочнює таке взаємопроникнення згадана «моніторингово-обмежувальна» діяльність, характерна для «напівзакритих» країн, яка, проте, дедалі частіше стає звичною практикою і для країн «відкритих».

Власне, політика країн Заходу у сфері внутрішнього інформаційного (кібер) простору дедалі частіше набуває рис політики тих країн, що їх традиційно відносять до авторитарних. Щоправда, у відповідних процесах мають місце суттєві відмінності. Якщо у країнах авторитарного типу реалізується передусім політика прямого обмеження доступу, то країни Заходу збирають дані про користувачів, здійснюють моніторинг національного інтернет-трафіку та створюють можливості цільового відключення окремих елементів мережі або її користувачів.

Такий акцент на «моніторинговій діяльності» обумовлений, зокрема, зростанням кількості телекомунікаційних послуг і мереж, контроль за якими є складним для державних правоохоронних служб. Це стосується, наприклад, контролю за розмовами власників смартфонів та *VoIP*[4]-системи. Зокрема, смартфони *Blackberry* підтримують систему шифрування даних, що передаються, а сервери цієї компанії розташовані у США та Великобританії, що унеможливлює контроль за спілкуванням користувачів *Blackberry* та потенційно робить доступним листування власників смартфонів для американських і британських спецслужб. Саме це спричинило запровадження обмежень (особливо в державному секторі) на використання цих засобів зв'язку у Франції, Німеччині, Індії, Об'єднаних Арабських Еміратах і Російській Федерації. Крім того, співробітникам керівних структур ЄС також заборонено користуватися смартфонами зазначеної фірми.

Стосовно *VoIP*-телефонії, то протягом тривалого часу основні претензії висуваються щодо неможливості контролювати контент, який поширюється програмними засобами, використовуваними механізмами *VoIP*-телефонії. Наприклад, до програмного продукту *Skype*, оскільки тривалий час вважалося, що він забезпечує ефективний криптографічний захист розмов абонентів, який практично

[4] *VoIP* (англ. *voice over IP)* – технологія передачі медіаданих у реальному часі мережею інтернет або іншими *IP*-мережами.

унеможливлює перехоплення їх з боку спецслужб. Це стало однією із причин конфлікту між авторами програми та спецслужбами деяких країн (Італія, Російська Федерація, Індія, Німеччина, Великобританія). Крім того, у 2010 році уряд США додатково виділив ФБР 234 млн дол. США для реалізації спецпроекту з «прослуховування інтернету» (*Advanced Electronic Surveillance – Going Dark*), спрямованого передусім на можливість прослуховування інтернет-комунікаторів (наприклад, *Skype*). Водночас станом на 2014 рік з'являється дедалі більше повідомлень про те, що спецслужби різних країн мають можливість прослуховувати *Skype*.

Найчастіше заходи щодо інтенсивнішого моніторингу контенту мережі та окремих технологічних рішень, що забезпечують доступ до неї, пояснюються однією з таких причин (або їх сукупністю):

• зростання терористичної загрози, використання терористами й міжнародними кримінальними структурами новітніх інформаційних технологій і зростання загрози критичній інфраструктурі держави;

• боротьба з комп'ютерним піратством, протидія порушенню авторських прав на продукти (зокрема аудіо- та відеоконтент);

• протидія поширенню дитячої порнографії.

Активніше застосовуються методи прямого впливу й тиску на власників пошукових інтернет-сервісів, на яких або розміщуються матеріали, що викликають невдоволення з боку державних інститутів, або вони надають доступ до таких матеріалів. Лідером у застосуванні таких методів вважається Китай: конфлікт між урядом Китаю та *IT*-корпорацією *Google* виник через небажання *Google* обмежувати на вимогу уряду пошукові запити китайських користувачів. Незважаючи на те, що безпосередньою причиною виникнення конфліктної ситуації між урядом КНР та *Google* стала спроба китайських хакерів на початку 2010 року «зламати» електронні поштові скриньки, що належать деяким китайським правозахисникам (а на думку керівництва корпорації, ці хакери діяли з відома керівництва КНР), саме «цензурна проблема» стала приводом до відкритого конфлікту.

Конфлікт між Китайською державою та американською *IT*-ТНК уперше призвів до залучення зовнішньополітичних відомств двох країн: Держсекретар США Х. Клінтон (*Hillary Diane Rodham Clinton*) у своїй промові від 21 січня 2010 року (про надзвичайну важливість цієї промови свідчить те, що на той момент це була *єдина* з усіх промов Держсекретаря, перекладена відразу сімома мовами), заявила, що США очікують від КНР «серйозного розслідування випадків, що

змусили *Google* виступити із заявою [щодо перспектив припинення роботи корпорації на китайському ринку]» [270]. Вона також висловила сподівання, «що розслідування та його результати будуть прозорими» [Там само]. У цій промові Х. Клінтон прямо звинуватила керівництво КНР у порушенні інформаційних прав людини, підкресливши, що Держдепартамент намагатиметься здійснювати скоординовану політику у сфері свободи слова з основними американськими компаніями, що надають мережеві послуги.

У відповідь на заяву Х. Клінтон прес-секретар МЗС КНР Ма Чжаосю (*Ma Zhaoxu*) заявив, що КНР рішуче виступає «проти спроб США критикувати політику КНР щодо розвитку мережі інтернет», а будь-які заяви щодо придушення свободи слова «не мають жодних підстав» [304]. Крім того, прес-секретар МЗС КНР зазначив, що регулювання функціонування мережі інтернет на території КНР здійснюється відповідно до міжнародного законодавства [Там само].

Крім того, представник МЗС Китаю Цзян Юй (*Jiang Yu*) заявила, що «китайський сегмент мережі інтернет відкритий, і Китай вітає міжнародні компанії, що ведуть бізнес у Китаї відповідно до закону» [22], тим самим натякаючи, що єдина причина конфлікту полягає в тому, що *Google* не дотримується китайського законодавства.

Непорозуміння у взаємовідносинах між КНР та *Google* щодо проблеми «цензури» мали місце неодноразово. Зокрема, свого часу компанія погодилася на цензуру результатів пошуку, однак надалі між *Google* та китайською владою періодично виникали розбіжності щодо змісту контенту, який має блокуватися. У червні 2009 року Пекін звинуватив *Google* у відсутності цензури порнографічних ресурсів і тимчасово припинив доступ до ресурсів *Google.com* та *Gmail* [309]. Цей конфлікт уперше продемонстрував ступінь інтегрованості американської *IT*-корпорації в систему американської зовнішньої політики.

Активна діяльність *Google* спричинює конфліктні ситуації не лише з Китаєм, а й з європейськими країнами: Францією (щодо оцифрування культурних надбань і книг), Німеччиною, Грецією, Великобританією, Іспанією (через сервіс *Google Street View*[5], що не лише фотографувала вулиці, а й збирала персональні дані громадян через незахищені бездротові канали зв'язку), Італією (через безконтрольне розміщення матеріалів, що порушують право на приватне життя).

[5] *Google Street View* (букв. – *перегляд вулиць*) – функція *Google Maps* та *Google Earth*, що дозволяє переглядати панорамні види вулиць багатьох міст світу з висоти близько 2,5 м.

Спроби держав Західної Європи впливати на контент і результати пошуку, що здійснюється корпорацією *Google*, ілюструє й запущений компанією сервіс *Transparency Report*. Він має висвітлювати частоту звертань держави до корпорації із запитами про вилучення певного контенту або про надання доступу до персональних даних користувачів сервісів корпорації. Згідно з цим звітом лідерами поміж країн, що звертаються до корпорації *Google* з вимогою на вилучення інформації, є інформаційно розвинуті країни або країни БРІК. Наприклад, згідно з даними сервісу лише за червень-грудень 2012 року десятка країн, правоохоронні органи яких найчастіше зверталися до *Google* із запитами (не враховуючи запитів за рішеннями судів), виглядає таким чином: Індія (122 запити), Росія (111), Туреччина (70), Великобританія (67), США (59), Іспанія (59), Бразилія (57), Республіка Корея (56), Німеччина (39), Франція (26) [151].

Систематично виникають складнощі у правоохоронних органів з контентом сайтів, що розміщують аудіо- та відеоматеріали (до найвідоміших належить сервіс *YouTube* – підрозділ *Google*). КНР цензурує аудіо- та відеоконтент подібних сервісів з 2008 року.

Зазначена проблема навіть спричинила розроблення нових регулятивних правил з розміщення відеоконтенту на китайських національних відеосервісах. Вони певною мірою запобігають можливості неконтрольованого розміщення аудіо- та відеоматеріалів у широкодоступних мережах. КНР чітко пов'язала безконтрольність розміщення відео- та аудіоматеріалів із загрозами єдності та суверенітету Китаю, завданням шкоди етнічній солідарності, китайській культурі та традиціям, пропагуванням насильства та порнографії і порушенням прав особи.

Хоча європейські країни намагаються безпосередньо не втручатися в діяльність подібних сервісів, однак свої претензії до деяких елементів контенту порталу *YouTube* висловлювали уряди Німеччини (через оприлюднення роликів, що пропагують нацистську ідеологію та антисемітизм), Великобританії (за надання можливостей для кібербуллінгу[6] школярів), а також Росії – через розміщення екстремістських матеріалів.

[6] Кібербуллінг – хамство, приниження та переслідування в мережі інтернет. Походить від юридичного терміна буллінг (від англ. *bullying*), що позначає певний перелік дій, спроможних викликати переляк, принизити чи іншим чином негативно вплинути на людину.

1.2. Кібермогутність і національна безпека держави

Сучасна школа критичної геополітики та частина американських фахівців дедалі частіше вказують на те, що для кіберпростору мають застосовуватися суттєво модернізовані, проте за суттю ті самі підходи, які були сформульовані класиками геополітики, передусім американцями Х. Маккіндером (*Halford John Mackinder*) і Н. Спайкменом (*Nicholas John Spykman*). Наприклад, дослідники Ф. Крамер (*Franklin D. Kramer*), С. Старр (*Stuart H. Starr*) та Л. Вентц (*Larry Wentz*) зазначають із цього приводу: «так само, як Макіндер та Спайкмен визначили для «земельної могутності» (*land power*), ті, хто розвиватиме теорію кібермогутності, мають визначити ключові ресурси та основні точки для кіберпростору» [285, с. 258].

Водночас надзвичайно важливими є питання інкорпорованості проблеми кіберпростору як нового геополітичного простору в реальну безпекову політику держави та чіткого артикулювання її інтересів («національних інтересів») щодо специфічного середовища кіберпростору.

Я. Волков слушно зазначає, що сама «система національної безпеки нині постає об'єктом теорії геополітики. Такий характер взаємозв'язку теорії геополітики та безпеки обумовлений, з одного боку, усталеним у науці розширеним розумінням безпеки як системи, що забезпечує не тільки захист держави від загроз, а і її стабільний розвиток в економічному, політичному, соціальному та гуманітарному просторах. З іншого боку – змінився погляд на геополітику і передусім на роль фізико-географічного простору в розвитку держав. З'явилися поняття економічного, політичного, інформаційного, цивілізаційного просторів, по-новому розглядається характер протиборства держав та їх союзників на міжнародній арені» [36].

І. Кефелі зазначає, зокрема, що наразі можна констатувати «встановлення міждисциплінарних зв'язків між кібернетикою й теорією інформації (в сучасному їх розумінні) і <...> геополітикою в тій сфері знань, яка отримала назву інформаційна (віртуальна) геополітика. Дослідження останньої в геостратегії набуває форми інформаційно-психологічної війни» [87, с. 8].

Майже на всіх етапах розвитку геополітики як науки її основним постулатом була залежність зовнішньополітичної діяльності держави передусім від її географічного положення, тобто об'єктивного чинни-

ка, який визначає взаємовідносини держав [115]. Органічною частиною цієї тези завжди була залежність від показників економічного, технологічного та військового розвитку держави, які могли істотно вплинути на загальну картину геополітичного стратегування. У загальнішому сенсі «основним категоріальним апаратом геополітики завжди були поняття контролю над простором, балансу сил, політичного простору, інтересу держави або нації, механізмів реалізації інтересів. Ключовою категорією геополітики є геополітичний простір, під яким розуміють оточення визначеного суб'єкта геополітики (держави, блоку держав). Однією зі складових геополітичного простору є силове поле суб'єкта геополітики, тобто простір, що контролюється державою (групою держав) і в межах якого здійснюється вплив суб'єкта з метою забезпечення геополітичних інтересів. Фактично ж йдеться про сферу впливу» [56, с. 4].

Якщо ми розуміємо кіберпростір як один із зазначених просторів, то відповідно, поняття геополітичного простору та його характеристики поширюються і на кібернетичний простір.

Попри всі зроблені спроби «гуманізувати» геополітику, її основою завжди лишається силовий чинник, загальніше – «національна сила», яка є основним системоутворювальним чинником, що визначає поведінку держав на міжнародній арені (їхні геополітичні інтереси як складники інтересів національних). Однак хоча національна сила і є основою геополітики, сучасна наука не виробила єдиного підходу до визначення цього поняття. На думку деяких дослідників, «це узагальнене розуміння цілої сукупності потенціалів держави в різних сферах, що можуть бути задіяні для досягнення поставлених державою цілей» [115]. Більшість інших дефініцій є надто заідеологізованими.

Саме національна сила є першоосновою забезпечення національної безпеки будь-якої країни. Якщо пов'язати це твердження зі спільним для концепції національної безпеки та геополітики поняттям національного інтересу, то можна дійти висновку, що саме національна сила є передумовою реалізації національних інтересів. Причому важливо уточнити, що, власне, мається на увазі під національним інтересом.

О. Воронянський слушно вважає, що «термін «національні інтереси» був запозичений українськими науковцями із західної англомовної політичної літератури, в якій він має значення державного інтересу (*national interest*). У західній науці ототожнення понять «національні інтереси» та «державні інтереси» випливає із традиційного

для неї розуміння категорії «нація» як поєднання мононаціонального суспільства і створеної ним держави. Звідси поняття «національні інтереси» постає як узагальнююча категорія, що знімає суперечності між розумінням інтересів держави і громадянського суспільства» [37, с. 241].

Варто погодитися, що національні інтереси слід тлумачити саме як інтереси державні. Це випливає, зокрема, і з базових концепцій геополітики, яка оперує переважно саме інтересами держави (хоча такі геополітики, як К. Шмітт (*Karl Schmitt*), обстоювали і проблему «прав народу»).

Таким чином, кіберпростір саме через «задіяння» національних інтересів і національної сили не просто може бути одним із предметів, які досліджує геополітика, а є її невід'ємною частиною. А. Маринченко вказує: «у XXI сторіччі на перший план вийшли інформаційні чинники, які зачіпають військові, технологічні, фінансові, культурні та інші проблеми <...> Предметом геополітики дедалі активніше стають інформаційні війни, націлені передусім на психологічну поразку противника, формування суспільної думки. Таким чином, предмет геополітики постійно змінюється, тоді як об'єкт [на думку дослідника, ним є «планетарний простір, геополітичні процеси та явища у світовому співтоваристві як системі» – *Авт.*] лишається більш-менш стабільним» [123, с. 6].

Відповідно, національні інтереси та національна сила безпосередньо пов'язані з політикою держави щодо кіберпростору та її позиціюванням у цьому просторі, вмінням формулювати цілі щодо нього та використовувати його можливості заради збільшення власної могутності.

Г. Раттрей (*Gregory J. Rattray*) на базі порівняння всіх основних просторів за відповідними параметрами доводить, що кіберпростір дійсно є новим простором, на який слід зважати реальній геополітиці, й дуже влучно, на наш погляд, формулює причини важливості оволодіння кіберпростором як джерелом могутності: «Контроль над ключовими аспектами операційного середовища збільшує могутність актора. Нездатність же отримати доступ до таких аспектів чи неможливість управляти ними може призвести до обмеження кола політичних, дипломатичних, економічних, військових та інформаційних аспектів могутності» [285, с. 253].

Проводячи аналогії між кіберпростором та іншими просторами, Г. Раттрей формулює одне з ключових завдань системних геополі-

тичних досліджень, спрямованих на кіберпростір: «Коли основним джерелом суперництва була «земля», життєво важливим був контроль за Малою Азією. Коли долучилося «море», постало питання контролю за Гібралтарською чи Малаккською протокою, оскільки це забезпечувало швидкий транзит військових сил і необхідних економічних можливостей. З підключенням «повітря» постало питання забезпечення повітряних мостів на кшталт Берлінського. З появою «космосу» постали нові ключові елементи й, зокрема, позиції на геостаціонарній орбіті, які є предметом конкуренції між державами та корпораціями, оскільки збільшують можливості зв'язку та проведення розвідувальних операцій. Предмет же досліджень у сфері кіберпростору – це визначення таких «ключових елементів» для нового середовища» [Там само, с. 254]. Водночас важливим нюансом нового простору є його інкорпорованість у забезпечення могутності держави на інших театрах, оскільки більшість сучасної військової техніки чи розвідувальних засобів певною мірою (щороку ця залежність зростає) тісно пов'язані із загальною функціональністю кіберпростору й тих процесів, які в ньому відбуваються.

Інша слушна думка стосується можливості досягнення домінування в кіберпросторі. Відповідно американські дослідники доходять висновку, що таке домінування навряд чи можливе, оскільки «кількість гравців, простота участі та можливості приховування дій робить це вкрай складним» [Там само, с. 12]. На підтвердження цієї думки дослідники наводять цікаве порівняння: «найпотужніший військово-морський флот складається з 300 судів, є лише одна геостаціонарна орбіта з обмеженою можливістю виведення супутників на неї. Один військовий літак може коштувати понад 100 млн дол. США, супутникова система – понад 1 млрд дол. США, а один бойовий корабель понад 3 млрд дол. США. А з іншого боку, є мільярди користувачів інтернету по всьому світу та незліченна кількість з'єднань між сайтами. При цьому вартість доступу до мережі у середньому коштує 40 дол. США на місяць, гарний комп'ютер – близько 600 дол. США, а нескладне програмне забезпечення може бути створене однією особою або взагалі скачане з інтернету» [Там само].

Цікавою особливістю проблеми кіберпростору в контексті використання інструментарію геополітики є проблема кордонів. У класичній геополітиці кордони є однією з головних ознак держави, яка саме цими кордонами окреслюється. Кордони є чинником безпеки держави, відіграючи основну роль у її контактах з іншими гравцями.

Однак кіберпростір доволі складно «розділити» державними кордонами. Панівним медійним дискурсом щодо кіберпростору є надмірно романтично-лібертаріанський, який активно ретранслює сама кіберспільнота (найактивніші користувачі й дописувачі мережі), а в окремих випадках (у своїх власних інтересах) і окремі держави чи міжнародні організації. Напевно, найнаочніше цю тезу підтверджує так звана Декларація незалежності кіберпростору [9], оприлюднена в 1996 році Д. Барлоу (*John Perry Barlow*), одним із керівників Фонду електронних кордонів (*Electronic Frontier Foundation)*. Саме цей текст часто цитується різноманітними кіберактивістами й хактивістами[7], які обстоюють інформаційні свободи людини, особливо щодо їх захисту в мережі інтернет.

Водночас навіть із цього документа можна зрозуміти, наскільки відірваними від реальності є позиції таких активістів: «Уряди Індустріального світу, ви – втомлені гіганти із плоті та сталі; моя ж Батьківщина – Кіберпростір, новий дім Свідомості. Від імені майбутнього я прошу вас, у яких усе в минулому, – залиште нас у спокої. Ви зайві серед нас. Ви не маєте верховної влади там, де ми зібралися <...> Ви не маєте ані морального права володарювати над нами, ані методів примусу, які б дійсно могли нас налякати <...> Кіберпростір лежить поза вашими кордонами. Не думайте, що ви можете побудувати його так, якби він був об'єктом державного будівництва. Ви не здатні на це. Кіберпростір <...> зростає сам завдяки нашим сукупним діям» [Там само].

Відповідно до реалістичнішого підходу (надто саме він є базисом геополітики) кіберпростір на суто фізичному рівні є надзвичайно «національним», оскільки функціонує завдяки телекомунікаційній інфраструктурі. Дослідник Д. Шелдон (*John B. Sheldon*), у минулому британський дипломат, вказуючи на специфічність кіберпростору, привертає увагу до технологічної компоненти: «Кіберпростір задля свого існування життєво потребує штучних об'єктів <...>, інші простори існуватимуть, навіть якщо б людство не змогло встановити супутників на орбіті Землі, море продовжувало б існувати, навіть якщо людина не навчилась би плавати по ньому, повітря також існувало б, навіть якщо людина так ніколи б і не злетіла. Однак кіберпростір не існував би, якби не здатність людини до інновацій та виробництва нових технологій, які здатні використовувати електромагнітний спектр.

[7] Хактивізм – використання інформаційно-комунікативних технологій з метою просування політичних гасел і закликів. Найчастіше реалізується через «злам» титульної сторінки сайту-цілі з подальшим розміщенням на ній політичних закликів.

Усе це робить його унікальним порівняно з іншими просторами» [411, с. 96].

Таку специфіку кіберпростору підтверджують інші американські дослідники, вказуючи, що «[від початку 1990-х років] кіберпростір розглядається як середовище, яке принципово відрізняється від нормального фізичного світу. І тим не менш насправді кіберпростір є надзвичайно фізичним середовищем: він створений абсолютно фізичними мережами та системами, поєднаними між собою та підпорядкованими певним правилам, вираженим через програмне забезпечення та комунікативні протоколи» [285, с. 254]. Понад те, сама основа роботи кіберпростору – це суто фізичні закони електромагнетизму та світла. Саме вони створюють його основну особливість – глобальні комунікації через кіберпростір, які здійснюються майже миттєво, а масштабні обсяги даних передаються на великі відстані, ігноруючи при цьому політичні кордони. Саме ця швидкість і створює проблему та основну перевагу для всіх зацікавлених сторін, оскільки може бути використана майже будь-ким.

При цьому лише повноцінне функціонування вже згаданої інфраструктури може реалізувати такі можливості: «критичні активи в кіберпросторі, що забезпечують фінансові трансакції, координування глобальної логістики та всю множину іншої важливої діяльності, включають фізичну інфраструктуру зв'язку» [Там само, с. 268].

Інфраструктура є одним із ключів до осмислення національного інтересу держав у кіберпросторі. Інфраструктура – це передусім підводні оптоволоконні кабелі та комунікаційні супутники, основні точки взаємопід'єднань, які, власне, і створюють глобальну мережу. Незначна кількість таких «точок» цілком може вважатися кібераналогом гірських проходів чи морських проток, важливих для морських і сухопутних «розумінь» могутності. Контроль за їх працездатністю можна вважати одним з пріоритетів забезпечення національних інтересів у кіберпросторі.

З огляду на зазначене вище, цілком можна стверджувати наявність певних «фізичних» кордонів кіберпростору, хоча і з певними застереженнями. Тоді як частина основних інфраструктурних об'єктів, які забезпечують глобальність та самé повноцінне функціонування кіберпростору, фактично перебуває поза межами національного суверенітету[8], інша їх частина є абсолютно керованою, а контент цього простору

[8] Про особливості такого стану йтиметься в подальших розділах.

(просторів) може бути відстеженим, щоправда, з певними обмеженнями. Зокрема, держави, що входять до Міжнародного союзу електрозв'язку, встановили певні вимоги до протоколів міжміських зв'язків, однак стрімкий розвиток телекомунікацій створив *Voice Over Internet Protocol*, який вже значно складніше модерувати на національному рівні.

Проблема державного контролю «кіберкордонів» часто додатково ускладнюється їх постійним оскарженням іншими гравцями через множинність кіберпростору. Адже «на відміну від інших просторів кіберпросторів можна згенерувати надзвичайно багато. І це відрізняє його від цілком унікального сухопутного, морського, повітряного, космічного просторів. Повітря над США таке саме, як і в Афганістані. Аналогічно щодо моря. Однак кіберпростір багаторівневий, і тут кордони постають доволі умовними та менш очевидними» [411, с. 97].

Усе це робить кіберпростір досить специфічним простором, в якому держави змушені в умовах часткового суверенітету формувати свої позиції та захищати національні інтереси. Цікаво, що на рівні міжнародного права та усталених традицій розуміння поняття *суверенітет*, наявний, хоча й обмежений, суверенітет над телекомунікаційною інфраструктурою є досить неоднозначним. Фактично саме це і створює центральне тло глобального протиборства між державами за майбутнє кіберпростору.

Сучасний кіберпростір нагадує поділ Світового океану: базові кордони (12-мильні зони) подекуди проведено, однак проблеми безпеки змушують держави ставити питання щодо жорсткішої «демаркації» та захисту таких кордонів. Інша аналогія, яка виникає в американських дослідників, – Дикий Захід 70 – 80-х років XIX сторіччя з обмеженими державними функціями та можливістю їх здійснювати [285, с. 257].

На ситуацію подібності підкорення кіберпростору й Дикого Заходу вказують *К. Демчак* (*Chris C. Demchak*) і П. Домбровський (*P. Dombrowski*): «Фронтір не може бути нескінченним. Рано чи пізно добрі сусіди зводять добрі огорожі, які мають бути і в кіберпросторі. Сьогодні ми бачимо початок цього процесу на міжнародному рівні. Кожна країна підходить до цього питання по-своєму, починаючи від спроб Китаю створити власний контрольований внутрішній інтернет і закінчуючи зростанням інтернет-фільтрів та правил доступу в західних демократіях. На нинішній інтернет чекає те саме, що й на американські прерії в 1880-х роках – він зміниться назавжди: раціонально, конфліктно чи манівцями – так, як це вирішать держави» [290, с. 32].

Така багатозначність кіберпростору: з одного боку, його «фізичність», з іншого – «віртуальність»; з одного боку, контрольованість, з іншого – відсутність можливості впливати на частину його інфраструктури, робить його складною компонентою при формуванні позицій держав щодо майбутнього кіберпростору та механізмів взаємодії у ньому.

Ключовим елементом у розумінні забезпечення національних інтересів чи потужності національної сили в кіберпросторі є концепт *могутність*, який традиційно застосовують у контексті визначення морської, повітряної чи космічної могутності.

Сам концепт досі є частково дослідженим та має суттєві відмінності в підходах до його розуміння. Значною мірою неузгодженості пов'язані з тим, що значна кількість дослідників звертається до поняття могутності або як до певного узагальнення, яке вони не пояснюють, або як до синоніму сили чи моці держави. На нашу думку, могутність все-таки відрізняється від зазначених понять.

Так, французький дослідник Р. Арон (*Raymond Aron*) вважає могутність потенцією (можливістю), зазначаючи, що її неможливо точно виміряти, оскільки «дуже часто вона виявляє свою повноту лише через вправляння і це вправляння є зрозумілим лише в певному контексті» [Цит. за: 216]. Він стверджує, що саме тому на міжнародній арені могутність розуміється як здатність політичної одиниці нав'язувати свою волю іншим одиницям [Там само]. На думку Л. Халецької, це, безумовно, можливо при застосуванні потенціалу кіберпростору [Там само].

За Р. Ароном, могутність має три основні параметри, які дозволяють досить приблизно її виміряти:

- простір (територія);
- ресурси:
  - матеріали та знання, що їх можна трансформувати у зброю;
  - кількість людей і мистецтво їх перетворювати на солдат;
- здатність до колективної діяльності:
  - організація армії;
  - якість цивільного та військового командування;
  - дисципліна [Цит. за: 216].

І хоча запропонована структура параметрів могутності створює дещо спрощене уявлення про неї здебільшого у військових термінах, однак таке уявлення може стати однією з основ вироблення адекватнішого розуміння кібермогутності в майбутньому.

Загалом французькі дослідники зробили досить значний внесок у дослідження концепції могутності. Зокрема, П. Боніфас (*Pascal Boniface*), Б. Баді (*Bertrand Badie*) визначили, що сьогодні могутність є здатністю контролювати правила гри в одній чи багатьох ключових сферах міжнародного змагання.

Разом із трансформаціями розвитку людства, передусім пов'язаними з технологічним розвитком, класичні підходи до могутності також зазнали змін. Під впливом досліджень Дж. Най-мол. ці підходи поділилися на «м'які» й «жорсткі», які у французьких дослідників набули значення «могутності впливу» та «могутності сили». У цьому контексті французький міністр закордонних справ у 2002–2004 рр. Д. де Вільпен (*Dominique de Villepin*) зазначив, що справжня могутність – це те, що створює порядок і надає сенс, вона повинна бути тим усвідомленням, яке через силу переконання, прикладу і впливу здатне надати ліки від ускладнення світу [Там само].

П. Боніфас звертає увагу на зміну вагомості традиційних критеріїв могутності. Стосовно військового, історично першого, критерію він робить три головних зауваження: по-перше, військовий критерій залишається таким, який визначається родовими ознаками «могутності»; по-друге, існує можливість трансформації військового впливу в економічний, військова міць залишається чинником впливу, «існування військового впливу достатнє як довід»; по-третє, військовий критерій не є більше єдиним чи переважаючим критерієм впливу, тим більше, що визначення його змінилося: сила армії зводиться не до кількості грудей, які вона може виставити позаду штиків, а до якості її матеріальної частини й управління, складності технологій, які вона використовує [Там само].

Російська дослідниця А. Бутузова, розглядаючи феномен могутності в міжнародних відносинах, зокрема відповідно до реалістського, ліберального та марксистського підходів, звертає увагу на те, що адепти кожного з них по-різному тлумачать це поняття.

Так, реалістська теорія стверджує, що могутність є мірою національних інтересів, їх узагальненим вираженням: «Могутність та національні інтереси – доповнюючі поняття, що переходять одне в одне. Тобто головною основою та метою національних інтересів є збереження чи збільшення могутності. Національні інтереси розраховуються за принципом могутності. Могутність – це інструмент реалізації національних інтересів (які є певними зонами збереження та збільшення могутності). У такий спосіб формується

реалістське замкнуте коло, цей зв'язок отримав назву – політика сили» [16]. Водночас, як зазначає дослідниця, могутність складається не лише з військово-стратегічної могутності. «Вся могутність, необхідна для реалізації національних інтересів, так чи інакше зводиться до військово-промислового комплексу. Захист та напад – це центральна частина понять могутності та національних інтересів» [Там само].

У межах ліберальної теорії спостерігається виразний тренд переміщення могутності зі сфери воєнно-політичної до економічної, відповідно, основним критерієм могутності стає економічний потенціал. Марксистська теорія також акцентує увагу на економічному чиннику могутності, однак вводить в обіг проблему не стільки капіталу як такого, скільки можливості встановлювати контроль над засобами виробництва.

Таким чином, навіть у найзагальнішому розумінні могутності мають місце цілком відмінні підходи до сутності цього поняття. Однак самé поняття стає дедалі затребуванішим, коли йдеться про кіберпростір та його використання в геополітичних смислах. І дедалі частіше з'являється в обігу поняття *кібермогутність*, що робить зрозумілим взаємоузалежнення національних інтересів і могутності держави в кіберпросторі.

Цю тезу розвиває, зокрема, колектив авторів монографічного дослідження «Кібермогутність та національна безпека» зі створеного в межах проекту Центру технологій та політики у сфері національної безпеки Національного університету оборони США. Вони зазначають, що «кібермогутність є фундаментальною основою глобального життя <...>, і США мають створити ефективні національні та міжнародні рамки для використання кіберпростору як частини загальної стратегії національної безпеки. Такі рамки, безумовно, матимуть і геополітичний вимір, <...> геополітичну діяльність буде спрямовано передусім на посилення загального стану національної безпеки та оборонних зусиль. Сюди можна віднести розвиток ідей мережевоцентричних операцій, відповідне комплексне планування можливостей здійснення комп'ютерних атак, поліпшення кіберпланування, створення відповідних доктрин, освітніх програм, а також навчання як військових, так і цивільних елементів» [285, с. 3].

Для подальшого викладу результатів дослідження актуально визначити сутність кібермогутності, сформулювати це поняття й надати його характеристики.

Оскільки кіберпростір є черговим простором для застосування геостратегій, то для нього справедливі ті самі аналогії, що й для землі, води, повітря та космосу. Передусім ідеться про можливість знайти аналог «військово-повітряної» чи «морської» могутності для кіберпростору.

Цікаво, що більшість тих, хто ретельно досліджував можливості військового (чи будь-якого іншого важливого в інтересах держав і націй), використання простору, майже ніколи не давали власного визначення могутності щодо конкретної досліджуваної ними сфери.

Засновник поняття *морська могутность* А. Мехен так і не надав його визначення, описуючи лише чинники, які призводять до військово-морської переваги. У 1920 році поняття орієнтовно визначили В. Стефенс (*William Oliver Stephens*) та А. Весткотт (*Allan Westcott*) як «здатність країни провадити в життя свою волю на морі» [419]. Дж. Дуе *(Giulio Douhet),* який присвятив свої праці дослідженню військово-повітряних сил, також не дав відповідного визначення *військово-повітряна могутність* чи його аналогу. Б. Мітчел (*Billy Mitchell*), який також займався питаннями військово-повітряних сил, доволі широко надав їм визначення як «здатність робити щось у повітрі».

Таким чином, малоймовірно дійсно однозначно сформулювати поняття кібермогутності, хоча певні напрацювання в цій царині існують. Наразі поняття можна визначити через параметри, запропоновані класиками геополітики, – чинники його виникнення.

Американський дослідник С. Старр (*Stuart H. Starr*) під кібермогутністю пропонує розуміти «здатність до використання кіберпростору для створення переваг та впливу в усіх інших операційних просторах через інструменти могутності (*instruments of power*)» [285, с. 38]. При цьому «інструменти могутності» автор розшифровує таким чином: «тоді як кіберпростір як середовище просто існує, кібермогутність завжди є мірою здатності використовувати це середовище. Технології є одним з очевидних чинників, тому що забезпечують базову можливість «увійти до кіберпростору», а отже, можливість його використати» [Там само, с. 39].

Загалом складно не погодитися з тими дослідниками, які кажуть про те, що кібермогутність зобов'язана своїм геополітичним значенням навіть не стільки самому факту свого існування, скільки глибокому проникненню в усі інші ключові сфери могутності держав – політику, військову справу, економіку, дипломатію. Кібермогутність

створює синергії у взаємопоєднанні всіх інших елементів національної могутності, посилюючи їх та надаючи їм додаткових можливостей, яких вони до того часу не мали.

Наразі загальна «теорія кібермогутності» лише розробляється і, як слушно зазначає С. Старр, щонайшвидше, до більш-менш однозначного розуміння буде багато невдач на цьому шляху [Там само]. Він доречно робить аналогії з традиційними науками та їх становленням: «сучасна теорія фізики розвивалася протягом сотень років, починаючи з оригінальних праць Г. Галілея та І. Ньютона. У цій дисципліні є напрацьована загальна база знань, хоча існують значні варіанти для конкретних субнапрямів (наприклад, у квантовій механіці, класичній динаміці чи теорії відносності). Крім того, існують тісні зв'язки з іншими дисциплінами, такими як математика, хімія та біологія. І хоча значення основних термінів і понять, як правило, встановлено, однак слід зазначити, що на цьому шляху було й чимало невдалих спроб, і сто років тому, наприклад, фізикам довелося (неправильно) визнати існування ефіру, через який поширюються електромагнітні хвилі. І навіть у наш час залишаються питання про фундаментальні визначення матерії» [Там само, с. 44].

На цьому тлі *кібермогутність* є ще складнішим явищем, яке для свого пояснення вимагає зусиль військових фахівців, юристів, політологів-міжнародників, фахівців із телекомунікацій та багатьох інших, кожен з яких послуговується власною термінологією та посвоєму розуміє досліджуване поняття.

У нашому дослідженні, кажучи про сутнісне розуміння кібермогутності, ми користуватимемося саме визначенням С. Старра, яке наразі в цілому відповідає як рівню розвитку наукової думки щодо кіберпростору, так і практичним процесам набуття країнами кібермогутності.

Системні дослідження проблеми визначення сутнісних рис кібермогутності здійснюється не лише західними, а й східними вченими. Директор Інституту досліджень інформаційного та соціального розвитку при Китайському інституті сучасних міжнародних відносин Лі Джанг (*Li Zhang*) зазначає, що ще в 2009 році Китай та Японія провели двосторонні перемовини щодо спільних наукових робіт з метою дослідити питання, пов'язані з «гегемонією в добу інтернету» [347]. У результаті досліджень було запропоноване власне спільне бачення кібермогутності, яке безпосередньо пов'язує це поняття зі здатністю держави вести кібервійни. На думку дослідників, термін *кібермогут-*

ність характеризує «можливість країни вживати заходів і впливати на кіберпростір» [Там само], що забезпечується впливом низки важливих чинників.

1. **Можливості інтернету та інформаційних технологій, передусім пов'язані з інноваційним потенціалом країни**, її можливістю здійснювати дослідження та впроваджувати розробки у промисловість.

2. **Можливості *IT*-індустрії**: наявність у країні *IT*-лідерів на зразок *IBM*, *Microsoft*, *Intel*, *Google* чи *Apple*.

3. **Можливості інтернет-ринку**, який залежить від загального розміру країни, розвиненості внутрішньої мережевої інфраструктури, співвідносності ступеня взаємоінтегрованості ключових *IT*-інфраструктур, кількості інтернет-користувачів, кількості комп'ютерів тощо.

4. **Вплив інтернет-культури**: частота використання національної мови в інтернеті, мова веб-сайтів у країні, якість їх ресурсів і контенту, рівень впливу в країні.

5. **Інтернет-дипломатія / зовнішньополітичні можливості**: можливості держави впливати на позицію організацій, які займаються адмініструванням інтернету, таких як *ICANN* (*Internet Corporation for Assigned Names and Numbers*, координування діяльності з розподілу домених імен та *IP*-адрес), Форум з управління Інтернетом (*Internet Governance Forum – IGF*), Міжнародний союз електрозв'язку (МСЕ) тощо.

6. **Кіберскладник військової сили**: можливості країни захистити критичну національну та військову *IT*-інфраструктуру від атак, здійснювати мережеве стримування та проводити наступальні мережеві акції, в тому числі можливість красти таємниці в інших країн і попереджувати таку діяльність щодо власних секретів.

7. **Бажання держави створювати стратегії для участі в боротьбі за кіберпростір**: має існувати теоретично обґрунтована послідовна політика (кіберстратегія), яка відповідно до своїх обґрунтувань обумовлює та встанолює норми поведінки, критерії діяльності та відповідні стратегічні плани [Там само].

Як зазначає Лі Джанг, якщо аналізувати показники кібермогутності за цими параметрами, то ми з необхідністю дійдемо висновку про те, що США є найбільш кібермогутньою країною у світі.

Зважаючи на загальну «аналогічність» просторів, вказану вище, дослідження суті кібермогутності доцільно здійснювати, послуговуючись концептами, аналогічними тим, якими користувався свого часу

А. Мехен. У широкому сенсі для аналізу кібермогутності варто звернутися до напрацювань, забезпечених розвитком теорії воєнних дій у просторі. Так, на думку дослідника Г. Раттрея [285], базовою рамкою дослідження будь-якої могутності (морської, повітряної тощо) є 4 ключових параметри: технічний прогрес, швидкість і масштаби операцій, контроль ключових елементів та національна мобілізація.

Відповідно за *першим параметром* Г. Раттрей визначає, що сама поява кіберпростору та нової якості залежності нашого життя від нього створила нові виклики й небезпеки, які повсякчасно впливають на нашу діяльність. За *другим параметром* можна констатувати, що кіберпростір спричинив суттєве розширення швидкості й масштабів операцій, які проводяться уповноваженими структурами. *Третій параметр* також частково відпрацьований для теорії кібермогутності. Якщо в класичній військово-морській теорії такими ключовими елементами були, наприклад, протоки (або будь-які «вузькі» місця), а для теорії космічної могутності – контроль над геостаціонарною орбітою, то для кібермогутності такими «вузькими» елементами стали певні вузли. До таких вузлів відносяться скупчення та взаємопроникнення інформаційних і телекомунікаційних елементів. У фізичному світі ці елементи можуть зосереджуватися довкола потужних дата-центрів чи важливих для функціонування самого кіберпростору елементів інфраструктури. *Четвертий параметр* набуває особливого значення для набуття країною необхідного показника кібермогутності, оскільки, як зазначалося, сама особливість кіберпростору обумовлена людським ресурсом і тим, як держава може його використати для досягнення поставлених завдань.

Є й інші підходи до феномену кібермогутності та спроби формалізувати його в межах певних, уже напрацьованих, системних підходів. Один з них належить австрійському дослідникові А. Клімбургу (*Alexandr Klimburg*), який для розуміння кібермогутності пропонує використовувати *wholeof*-підходи (*Whole of Government*, *Whole of Systems*, *Whole of Nation*).

Whole of Government-підхід набув популярності під час подій у Косові разом з необхідністю відступити від суто воєнних методів вирішення конфліктів (або відновлення країн після них) на користь ширшого розуміння цього процесу, що передбачає залучення недержавних акторів. Відповідно традиційно *Whole of Government*-підхід базується на 3*D*-підході, де *D* є скороченням від англійських слів *development* (розвиток), *diplomacy* (дипломатія) та *defence* (оборона).

Із приходом Б. Обами на президентський пост у США цей підхід став основою зовнішньої політики, дипломатичною стратегією США на період його президентства (поряд із концепцією, яка багато в чому є наслідком 3*D*-підходу – *Smart Power*[9]) [75].

До поняття кібермогутності А. Клімбург пропонує застосовувати сукупність відповідних підходів, зокрема побудувати Інтегровану модель можливостей кібермогутності (*Integrated Capability Model of Cyberpower*). На його думку, саме ця модель є «найбільш якісною основою для визначення того, які, власне, можливості можуть бути використані для доставки різноманітних інструментів національної кібермогутності» [338]. Сама інтегрована структура (яку він іноді називає «виміром кібермогутності») має три складники (за його термінологією – виміри).

1. Перший вимір – «Інтегровані урядові можливості» (*Integrated Government Capability*). Ідеться передусім про здатність держави ефективно розподіляти свої ресурси в кіберсфері, чітко формулювати свою політику щодо кіберпростору, здійснювати в ньому узгоджені дії, застосовуючи для цього всі можливості держави. На практиці, зокрема, це має вигляд розроблених і узгоджених із приватним сектором планів реагування на надзвичайні події в кіберпросторі, можливість використовувати кіберпростір для захисту чи нападу.

2. Другий вимір – «Інтегровані системні можливості» (*Integrated Systems Capability*). Це здатність держави використовувати формалізовані структури для досягнення своїх цілей. Автор виділяє міжнародні альянси та партнерства (ООН, НАТО), неурядові організації (*FIRST*) чи гібридні структури (*ICANN*). Передусім ідеться про зовнішньополітичні зусилля держав та про місце кібербезпекової проблематики в загальній структурі пріоритетності зовнішньополітичних питань.

3. Третій вимір – «Інтегровані національні можливості» (*Integrated National Capability*). Це здатність держави налагодити дійсно ефективну співпрацю з недержавними акторами, дії яких у подальшому були б спрямовані на ті саме цілі, що їх переслідує держава в кіберпросторі [Там само, с. 174].

Результуючою взаємодії усіх цих вимірів є утворення низки ефектів, які пояснюють сутність кібермогутності держави: скоординованість (*coordiantion* – ефект першого виміру), взаємодія (*collaboration* –

[9] «Смарт-сила» означає, що США збираються об'єднати «тверду» і «м'яку» силу, інтегровано використовувати всі ресурси країни для досягнення стратегічних цілей США [190].

ефект другого виміру), співробітництво (*cooperation* – ефект третього виміру)[10].

Існують і спроби вимірювати показники кібермогутності країн. Зокрема, американська компанія *Booz Allen Hamilton*, яка є підрядником АНБ США з багатьох кібербезпекових питань, запропонувала власну методику визначення та обчислення показників кібермогутності. На думку її фахівців, до таких показників відносяться:

- нормативно-правове регулювання кіберпростору;
- економічний та соціальний контекст;
- технологічна інфраструктура;
- промислове застосування інформаційно-телекомунікаційної інфраструктури в різних сферах [Цит. за: 212, с. 49].

Кожен із показників визначається через сукупність субпоказників (близько 40), з-поміж яких: участь держави в розвитку кіберпростору, розвиненість політик кібербезпеки, ступінь цензури, ступінь проникнення інновацій у бізнес-середовище, відкритість торгівлі, витрати на ІКТ, рівень якості технологій, що використовуються, розвиненість *е*-управління тощо.

Наведені вище теоретичні підходи до розуміння взаємоузгодженості та взаємозв'язку чинників, які обумовлюють кібермогутність держави, хоч і відмінні один від одного, однак мають і багато спільного. На нашу думку, найадекватнішим для окреслення реального стану кібермогутності держави є китайсько-японський підхід. Однак ця схема потребує доопрацювання, оскільки не зважає на низку важливих елементів. Наприклад, на наявність необхідних ресурсів для побудови власного високотехнологічного виробництва чи наявність адекватного національного законодавства, що забезпечує досягнення подібних цілей.

Важливим моментом у визначенні кібермогутності держави (за будь-якою зі схем) є необхідність врахування її принципової двовимірності.

Перший вимір – теоретичний – визначає власне бачення державою своєї могутності через запропоновану систему окремих напрямів та індикаторів. Дійсно, більшість з них можуть бути виміряні, а за окремих обставин і сформовані за допомогою цілеспрямованої державної

[10] Формально в англійській мові слова *collaboration* та *cooperation* схожі за змістом, однак перше вживається зазвичай для співробітництва на базі спільних інтелектуальних інтересів та цілей, в той час як друге спрямоване на отримання взаємного економізованого зиску.

політики. Другий вимір – реальний потенціал кібермогутності, що може бути виявлений лише в умовах надзвичайної ситуації, коли держава (сама або спільно із приватним сектором) муситиме застосувати всі зазначені елементи своєї кібермогутності. Водночас реальні показники можуть суттєво відрізнятися від теоретичних, що пояснюється, з одного боку, досі більш ніж приблизними підходами до розуміння самого концепту кібермогутності, а з іншого – принципово латентним характером протистоянь у кіберпросторі.

Закінчуючи огляд проблем кібермогутності, зазначимо, що важливий вплив на функціонування кіберпростору справляють ще дві компоненти, кожна з яких є складною сукупністю, що потребує додаткового вивчення та концептуалізації, – *геоекономіка* та *геокультура*. Однак у межах даної роботи вбачається неможливим повноцінно звернутися до цих царин, надто, значна частина відповідних напрацювань належить до сфери економічної теорії та проблем гуманітарного розвитку націй.

1.3. Кіберпростір як сфера глобальних конфронтацій

Більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) перебувають нині на етапі створення і трансформації власних військових кібернетичних підрозділів з огляду на можливості використання мережі інтернет проти їх національних інтересів, а також отримання можливості впливати на інші держави.

За даними керівника компанії *McAfee*, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 р. [25], вже у 2009–2010 рр. понад 20 країн планували або здійснювали різноманітні інформаційні операції. Скільки країн стурбовано створенням і модернізацією власних ківбервійськ станом на 2013–2014 рр. невідомо. Однак, зважаючи на випадки (висвітлені пресою) застосування кіберозброєнь, можна припустити, що кількість таких країн істотно зросла.

Якщо в 2010–2011 рр. розвинуті країни лише наблизилися до розв'язання проблеми формування спецпідрозділів, завданням яких є розвідувальна робота в мережі, захист власних мереж, блокування та «обвал» структур противника з використанням можливостей кіберпростору, то в 2012 році кібервійська почали повноцінно функціонувати, і дедалі більше країн розглядали створення таких підрозді-

лів як об'єктивну необхідність. Станом на кінець 2013 року згідно з офіційними заявами військові кіберпідрозділи з виразно захисними функціями створено у США (*U.S. Cyber Command*); Великобританії (урядовий *Cyber Security Operations Centre);* Німеччині (*Internet Crime Unit* та *Federal Office for Information Security*); Австралії (*The Cyber security operations centre*); Індії; Ізраїлі та багатьох інших країнах. Готовність до створення кіберкомандування (інформкомандування) серед сусідів України висловила передусім Російська Федерація. Ще в лютому 2013 року перший заступник голови Комітету Держдуми з оборони В. Заварзін за результатами засідання Комітету за участю глави Генерального штабу В. Герасімова, повідомив, що в Генштабі Збройних сил Росії почав роботу спеціальний підрозділ з кібербезпеки [91]. Також у 2013 році з'явилася інформація про те, що створення кібервійськ починає Білорусь [127]. Активну позицію щодо протидії кіберзагрозам посідають провідні міжнародні безпекові організації й передусім НАТО (*Cooperative Cyber Defence Centre of Excellence*) та ОБСЄ.

Таким чином, провідні держави світу дедалі більше уваги приділяють розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави.

Рівень занепокоєння провідних держав світу щодо сфери кібербезпеки засвідчує бажання врегулювати питання стосовно можливості визнання кібератаки актом війни на міжнародному рівні. Зокрема, вже 30 січня 2010 року під час роботи Всесвітнього економічного форуму в Давосі американський сенатор-республіканець С. Коллінс (*Susan Collins*) зазначила, що США серйозно розглядають питання щодо проголошення кібератак актами війни. А 12 травня 2010 року помічник заступника міністра оборони США з політичних питань Дж. Міллер (*James Miller)* заявляв про готовність США завдати воєнного удару у відповідь на кібератаки на американські комп'ютерні мережі. Трактування кібератак як потенційних кібервоєн отримало продовження в 2010 році, коли група експертів під керівництвом М. Олбрайт (*Madeleine Korbel Albright*) взяла участь у розробці нової Стратегічної концепції НАТО. У 2011 році США оприлюднили Міжнародну стратегію щодо кіберпростору, а у 2013 році з'явилося науково-практичне дослідження групи 20 юристів, які доводили можливість застосування чинного міжнародного законодавства стосовно актів збройної агресії до кібератак.

Усе зазначене спонукає держави світу дедалі активніше позиціюватися з питань внутрішньої та зовнішньої політики в контексті актуальних і потенційних кіберзагроз, розробляти й ухвалювати у цій сфері нормативні документи стратегічного змісту. Станом на кінець 2013 року такі стратегії було напрацьовано більшістю країн ЄС (причому як на національному, так і на загальноєвропейському рівні), США, Канадою, Японією та багатьма іншими країнами. Публічно про розроблення аналогічної стратегії заявила Російська Федерація.

Найпотужнішими та найактивнішими більшість експертів із проблем кібербезпеки вважають військові кіберпідрозділи КНР і США.

Дані про потенціал, чисельність і завдання *китайських* кібервійськ практично відсутні. Однак у доктринальних безпекових документах КНР зростання ролі інформатизації у військовій справі зазначається принаймні від середини 90-х років XX сторіччя. Розширено це питання розглядається в Білій книзі з питань оборони за 2004 рік, де констатується необхідність КНР бути готовою до ведення «локальних війн в умовах інформатизації» [264]. У датованій 2008 роком Білій книзі з питань оборони вказується на бажання досягти до 2020 року значного результату з питань інформатизації армії [265]. Питанню розбудови інформаційного потенціалу збройних сил КНР присвячено також цілий пункт у Білій книзі з питань оборони за 2010 рік.

4 серпня 2010 року очікувалося на оприлюднення даних дослідження компанії *Armorize* стосовно реального потенціалу китайських і тайванських кібервійськ, однак на вимогу керівництва Тайваню доповідь було виключено із програми конференції *Black Hat* [131].

Не містила даних про потенціал кібервійськ Китаю й опублікована усередині серпня 2010 року доповідь Міністерства оборони США про військову міць Китаю [369], однак у цій доповіді робилося припущення, що значна кількість атак проти мереж, що належать уряду США, могла здійснюватися за підтримки або за безпосередньою участю Народно-визвольної армії Китаю чи уряду Китаю.

За даними видання *The Daily Beast* [266, 267], ФБР підготувало секретний звіт, що висвітлював рівень розвитку кібервійськ КНР і вказував на загрози від цих військ для США. Звіт називав армію кібершпигунів КНР «єдиною найбільшою загрозою США щодо кібертероризму» та силою, що наразі володіє потенціалом «знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних». За даними згаданого звіту ФБР, 180 тис. китайських кібершпигунів, які щоденно ата-

кували кібермережі США, лише 2009 року здійснили 90 тис. атак проти комп'ютерів Міністерства оборони США. Зі 180 тис. осіб 30 тис. нібито були військовими, а 150 тис. – комп'ютерними експертами із приватного сектору (працівники приватних компаній, які залучаються до виконання військових чи розвідувальних завдань у кіберпросторі). Їх діяльність мала на меті отримання доступу до військових і комерційних секретів США та внесення розладу в діяльність урядових і фінансових служб.

У 2011 році КНР офіційно визнала існування спеціальних кіберпідрозділів у своїй армії. Спеціальна публікація Женьмінь Жібао[11], присвячена даному питанню, засвідчувала, що «на прес-конференції Міноборони КНР представник відомства Ген Янишен *(Gene Janisch)* підтвердив створення в Китаї «мережевої синьої армії» з метою охорони інтернет-простору» [163]. Формальна чисельність цього підрозділу – близько 30 осіб.

Не менш активною у сфері кібербезпеки є політика *США*. Її найактивніше запровадження розпочалося з часів першої каденції Б. Обами. Лише в 2009 році було здійснено, зокрема, такі кроки:

• оприлюднено «Огляд політики щодо кіберпростору» (*Cyberspace Policy Review)* – комплексний документ, який не лише визначив поточний стан кібербезпекової сфери у США, а й пріоритети нової команди в цій сфері;

• в Адміністрації Президента створено посаду Координатора з кібербезпеки (*Cybersecurity Coordinator*), яку обійняв Г. Шмідт (*Howard Schmidt*);

• створено Кіберкомандування США (*U.S. Cyber Command*) під головуванням генерала К. Александера (*Keith B. Alexander*), який одночасно очолюватиме і згаданий підрозділ, і Агентство національної безпеки. Приблизна чисельність структури – 30 тис. військових;

• оголошено про додаткові заходи з посилення внутрішньої кібербезпеки. Із 1 жовтня 2009 року у США оголошено про додатковий набір 1 тис. співробітників до спеціального кібербезпекового департаменту Міністерства внутрішньої безпеки (*Department of Homeland Security*), які займатимуться виключно безпекою високотехнологічних систем США. Однак навіть ця кількість співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки. У супровідному документі до спеціально організованих урядом США кіберзма-

[11] Офійний друкований орган ЦК КПК.

гань *U.S. Cyber Challenge* наводиться думка одного з експертів про те, що реальна потреба уряду в таких фахівцях становить від 10 тис. до 30 тис. осіб [433];

• збільшено держзамовлення на розроблення нових засобів ведення війни, зокрема кіберозброєнь і нових, більш захищених, військових мереж;

• створено проекти нормативних документів, спрямовані на поліпшення взаємодії у сфері кібербезпеки між союзниками США та убезпечення власного інтернет-простору в разі виникнення ситуацій, що загрожують національній безпеці.

Уперше в загальній структурі загроз США кіберзагрозам відведено окреме місце у вже згадуваній Стратегії національної безпеки 2010 року. Цілісним баченням урядом США найближчого майбутнього в розвитку кіберпростору стала Міжнародна стратегія для кіберпростору (*International Strategy for Cyberspace*)[12]. Протягом 2011–2012 рр. було ухвалено ще цілу низку документів практичного значення, спрямованих на мінімізацію кіберзагроз, зокрема щодо протидії роботі бот-мереж і кібершпигунству. 5 січня 2012 року президент США Б. Обама проголосив зміни в оборонній стратегії США, що було зафіксовано в доповіді «Підтримуючи глобальне лідерство Сполучених Штатів: оборонні пріоритети для XXI сторіччя» (*Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*) [423]. У цьому документі на тлі зменшення видатків на оборону було чітко зазначено, що на кібербезпекову сферу видатки не лише не зменшуватимуться, а навпаки, зростатимуть. Зокрема на інші новітні озброєння (літаки-«безпілотники» тощо), оскільки нова стратегія вбачає в цьому запоруку «критичної спроможності до майбутніх успіхів» США [Там само].

Чітко невідомо, скільки людей забезпечують безпеку США у кіберпросторі. Офіційні особи КНР в 2013 році звинувачували США в тому, що в інтересах США працює понад 100 тис. «кіберсолдатів». Водночас американські дослідники, намагаючись перевірити достовірність такої інформації з відкритих джерел, станом на березень 2013 року отримали такі результати [397].

1. 24-та Авіаційна армія (*24th Air Force*) – 16,4 тис. військових і цивільних.

2. Кіберкомандування військово-морського флоту (*Navy Fleet Cyber Command*) – щонайменше 14 тис. моряків і цивільних.

[12] Докладно про це див. підрозділ 3.3.

3. Морське кіберкомандування (*Marine Cyberspace Command*) – 700–800 моряків.

4. Військове кіберкомандування (*Army Cyber Command*) – близько 21 тис. солдатів і цивільних.

5. Кіберкомандування США (*U.S. Cyber Command*) – 900 осіб з анонсованим зростанням до 4,9 тис. військових і цивільних.

Таким чином, лише у військовій сфері проблемами кіберзахисту й кібернападу наразі опікується близько 53 тис. осіб. І це не враховуючи профільний персонал таких структур, як Агентство національної безпеки США, Федеральне бюро розслідувань, Центральне розвідувальне управління, Міністерство внутрішньої безпеки, Розвідувальне управління Міністерства оборони США та інші. Не враховуються цивільні фахівці, що працюють за контрактом чи на умовах аутсорсингу.

Також складно встановити реальні обсяги фінансових вкладень уряду США в кібербезпекову сферу. У деяких публікаціях [317] називається цифра у 14 млрд дол. США (на 2013 рік). Однак навіть відомості про низку розпочатих тендерів і підписаних контрактів [наприклад, 157, 5, 132], пов'язаних із діяльністю Пентагону, лише за період 2010–2011 рр. дозволяють припустити, що наведена цифра є неточною, оскільки подібні масштабні вкладення (зокрема ті, які заявлені в тендерах) можуть відбуватися з порушеннями фінансової дисципліни[13].

Варто зазначити, що точну оцінку залучення коштів до цієї сфери складно дізнатися не лише через засекречення подібної інформації, а й через особливості бюджетного фінансування у США. Однак один із випадків військового бюджетного планування у США є показовим: у квітні 2013 року Міністерство оборони США подало бюджетний запит на 2014 рік на суму у 4,7 млрд дол. США на поліпшення «операцій у кіберпросторі», в тому числі на спеціальні «атакуючі команди» [26].

На думку військового оглядача *The Foreign Policy* Д. Ріда *(John Reed)* [396], важливість кібербезпекової проблематики для Міноборони США засвідчує таке порівняння: якщо в бюджетному запиті на 2013 рік слова з частиною *кібер* траплялися 47 разів, то в аналогічному запиті на 2014 рік – 153 рази.

---

[13] Наприклад, за результатами перевірки Рахункової палати за останні 12 років Пентагон на 7 млрд дол. США перевищив планові показники лише за програмою впровадження *ERP*-систем [204].

У 2012 році орієнтовні видатки на вдосконалення кіберпотенціалу Збройних сил США становили близько 4 млрд дол. США.

Незважаючи на такі масштаби залучення всіх силових відомств США до питань забезпечення кібербезпеки держави, на Аспенському безпековому форумі влітку 2012 року голова Кіберкомандування США генерал К. Александер оцінив захисний кіберпотенціал держави лише в 3 бали за десятибальною шкалою [240]. 26–29 липня 2012 року він взяв участь у щорічній конференції хакерів *DefCon* у Лас-Вегасі, де звернувся до всіх небайдужих хакерів із закликом допомогти у кібервійні, що набирає обертів [275].

Наймасштабніше, на нашу думку, значущість питань кібербезпеки для США загалом та Адміністрації Б. Обами зокрема ілюструє протистояння щодо прийняття комплексних нормативно-правових документів, спрямованих на повноцінне функціонування системи кібербезпеки США, яке розгорнулося протягом 2009–2013 рр. у Конгресі.

Активне обговорення всеосяжного законопроекту щодо забезпечення кібербезпеки на національному рівні розпочалося в Конгресі США ще у 2009 році. Уже наприкінці квітня 2009 року сенатори О. Сноу (*Olympia Snowe*) та Д. Рокфеллер (*Jay Rockefeller*) запропонували законопроект, покликаний надати президенту США доступ до другої «червоної кнопки», за допомогою якої він зміг би в надзвичайних випадках загроз національній безпеці відключати доступ до мережі інтернет на всій території США. Законопроект отримав неформальну назву *Internet Kill Switch bill*. Невдовзі, 9 липня 2009 року, сенатор К. Джілібренд (*Kirsten Gillibrand*) запропонував законопроект, згідно з яким США зможуть співпрацювати з будь-яким урядом світу в цілях організації глобальної відповіді на кібератаки (*Fostering a Global Response to Cyber Attacks Act*).

Робота в Конгресі щодалі набувала обертів і поширювалася. У 2011 році на розгляд різних палат Конгресу США було представлено щонайменше 13 законодавчих ініціатив, які тією чи іншою мірою стосувалися питань кібербезпеки. Частина з них перейшла до порядку денного наступних років.

У 2012 році найбільш дискусійним і медійно-резонансним був законопроект *Cybersecurity Act of 2012* [232], поданий сенатором Дж. Ліберманом (*Joseph Lieberman*) у співавторстві з головою комерційного Комітету сенатором С. Коллінс, головою Комітету з розвідки сенатором Д. Рокфеллером і сенатором Д. Файнстайн (*Dianne Feinstein*).

«Законопроект Лібермана» лобіював особисто президент Б. Обама. А 16 квітня 2012 року на шпальтах *The Washington Post* із закликом до пришвидшеного прийняття Законопроекту до конгресменів звернувся старший радник президента США з питань контртероризму та внутрішньої безпеки Д. Бреннан (*John O. Brennan*) [245].

Головною «родзинкою» Законопроекту стало передбачене ним державно-приватне партнерство з питань забезпечення тих систем, пошкодження чи знищення яких може призвести до масової загибелі, евакуації, проблем у життєзабезпеченні громадян чи катастрофічним наслідкам для економіки й національної безпеки. Це партнерство мало бути формалізоване у вигляді «кібербезпекового обміну» (*cybersecurity exchanges*). Зокрема, у Законопроекті зазначалося, що існуватиме принаймні один центр «федерального кібербезпекового обміну», що сприятиме обміну відповідною інформацією про кіберзагрози й небезпеки як між приватними структурами, так і між приватними структурами та державними установами.

Важливим моментом також стало законодавче «убезпечення» кібербезпекового обміну від негативного впливу інформаційної відкритості уряду, передбаченої *FOIA* (*Freedom of Information Act*)[14]. Метою такого кроку є підсилення впевненості приватних компаній, які обмінюються відповідною безпековою інформацією з державою, що ці дані не стануть надбанням усього суспільства (а отже, і кримінальних елементів), адже це може негативно вплинути не лише на імідж компаній, а й на їхню безпекову ситуацію в цілому.

Суттєво, що документ покладав функцію оцінювання ризиків та уразливостей критично важливих систем інфраструктури й визначення необхідних стандартів безпеки, яким ці системи мають відповідати, на Міністерство внутрішньої безпеки. З огляду на те, що більшість подібних безпекових систем у США (до 90 %) є у приватній власності, це положення Законопроекту із зрозумілих причин викликало й викликає чимало запитань у приватного сектору. Водночас у Законопроекті закладено й певний компроміс: можливість оскаржувати рішення ДВБ власниками інфраструктурних систем, які вважатимуть, що їхні системи неправильно визначено як об'єкти критичної інфраструктури.

Наразі власники таких систем висловлюють невдоволення і, щонайшвидше, вживатимуть заходів щодо недопущення прийняття За-

[14] Його українським аналогом є Закон України «Про доступ до публічної інформації».

конопроекту (або принаймні пом'якшення відповідного пункту). На їхню думку, уряд має достатньо важелів впливу на забезпечення кібербезпеки приватних організацій, здійснюючи державний контроль над закупівлями. А якщо при цьому необхідно посилити кібербезпеку, то це має здійснюватися передусім через вдосконалену систему реагування на інциденти [321].

Потенційним наслідком упровадження Законопроекту може стати бажання власників систем критичної інфраструктури применшити важливість належних їм безпекових систем, мінімізуючи таким чином державний контроль і відрахування на безпеку, що у стратегічній перспективі знизить рівень захищеності таких систем.

За матеріалами відкритої дискусії можна дійти висновку, що з питань необхідності ухвалення кібербезпекового законодавства досягнуто певного консенсусу, проте відразу після презентації зазначеного «пропрезидентського» Законопроекту до документа виникли запитання навіть з боку представників «пропрезидентської» Демократичної партії. Зокрема, лідер сенатської більшості Г. Рейд (*Harry Reid*) вимагав, щоб не лише «безпековці», а й інші відповідні комітети могли проаналізувати й переглянути Законопроект до того, як він буде проголосований. У цьому контексті доречно зауважити, що Г. Рейд є автором іншого подібного Законопроекту [281], внесеного ще на початку 2011 року, який вимагає оновлення системи безпеки критичної національної інфраструктури з метою попередження катастрофічних кібератак на національні системи водопостачання, електромережі, фінансові системи, а також транспортну інфраструктуру.

Крім політичних опонентів з демократичного табору, претензії та власні пропозиції з питань забезпечення кібербезпеки держави висловлювали також колеги Дж. Либермана з Республіканської партії. Зокрема, сенатор Дж. Маккейн (*John Sidney McCain*) разом із п'ятьма колегами представив альтернативний документ – *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act* (*SECURE IT Act*). Його перевагами деякі «незалежні оглядачі» вважають жорсткіші гарантії недоторка́нності приватного життя й захисту інформації, оскільки Законопроект встановлює додаткову кримінальну відповідальність за порушення роботи комп'ютерів, що входять до критичної інфраструктури [413]. Крім того, документ акцентує увагу на необхідності системних досліджень та освіти (включно з наданням спеціальних стипендій студентам, які спеціалізуються з питань кібербезпеки). Як і автори *Cybersecurity Act*

of 2012, Дж. Маккейн занепокоєний питаннями убезпечення приватних систем, що належать до критичної інфраструктури. При цьому він привертає увагу до необхідності обережного впровадження ідеї державного регулювання приватного сектору і встановлення граничної зони відповідальності закону лише для компаній, що надають послуги електронного зв'язку, дистанційних комп'ютерних послуг чи послуг з кібербезпеки.

Цікавим елементом протистояння («війни») вказаних законопроектів є те, що Законопроект Дж. Маккейна більшою мірою передбачає зростання ролі Агентства національної безпеки та Кіберкомандування США (хоча Дж. Маккейн у своїх численних заявах це спростовує) на противагу ДВБ, представників якого сенатор називає «некомпетентними бюрократами».

У березні 2012 року в Сенаті США відбулися слухання [315] щодо бюджетного запиту Стратегічного командування США та Кіберкомандування США щодо фінансування оборонних програм у 2013 році (обсяг запиту на 2013 рік – 3,4 млрд дол. США, а на довгострокові програми – 17,5 млрд дол. США). Під час слухань між Дж. Маккейном і К. Александером виникла показова суперечка, предметом якої став суб'єкт та обсяг відповідальності за кібербезпеку держави. Керівник АНБ / Кіберкомандування США генерал К. Александер рішуче виступив проти збільшення повноважень підпорядкованої йому структури (зокрема щодо можливості АНБ моніторити внутрішні мережі США та впливати на стан їх безпеки). Він заявив, що найоптимальнішим варіантом розподілу обов'язків вважає стан такий: ДВБ відповідає за внутрішні мережі, об'єкти критичної інфраструктури та обмін інформацією з приватним сектором; АНБ та Кіберкомандування США лише допомагає ДВБ фахівцями чи інформацією.

З-поміж інших обговорюваних у Конгресі США законопроектів є вельми контроверсійний *Cyber Intelligence Sharing and Protection Act* (*CISPA*) [280], запропонований конгресменом М. Роджерсом (*Mike Rogers*), хоча законопроект має понад 100 співавторів. Головним лобістом документа вважається Пентагон. Під час попереднього обговорення Законопроекту наводилися численні приклади гучних порушень приватними компаніями в кіберсфері, у тому числі за участю військових підрядників (*Lockheed Martin Corp*, *Google i Citigroup*) [319].

Водночас у даний законопроект під тиском правозахисних організацій, зокрема Фундації електронних свобод (*Electronic Frontier Foundation*), внесено зміни, які стосуються захисту громадянських

свобод. Борці за права громадян в інформаційній сфері на своїх блогах заявляють, що законопроект аж надто розлого тлумачить термін *кіберзагроза*, щоб надати повну свободу дій уряду стосовно контролю комунікацій, фільтрування контенту сайтів на зразок *WikiLeaks* та контролювання доступу до онлайн-послуг. Розробники Законопроекту подібні звинувачення відкидають, підкреслюючи, що майбутній закон передбачає виключно добровільне надання приватними компаніями інформації щодо загроз Міністерству внутрішньої безпеки. Поступкою авторів Законопроекту правозахисникам вважається вилучення з безпекового процесу Агентства національної безпеки США, оскільки йому захисники громадянських свобод не довіряють через оприлюднені пресою численні факти хакінгу («необґрунтованих» прослуховувань АНБ телефонних розмов) у рамках боротьби з тероризмом.

Лобісти *CISPA* підкреслюють, що метою Законопроекту є лише обмін інформацією про «шкідливі коди програмного забезпечення», а не про зміст повідомлень (важлива форма, а не контент). До речі, в цьому американці вбачають головну відмінність свого кібербезпекового підходу до забезпечення інформаційної безпеки від російського чи китайського.

6 квітня 2012 року з різкою критикою *CISPA* виступила міжнародна організація захисників журналістських прав «Репортери без кордонів» [365]. Разом з тим *CISPA* підтримали деякі представники великого інтернет-бізнесу, які підкреслюють принципову відмінність нового Законопроекту від більш одіозних законопроектів – *SOPA (Stop Online Piracy Act) й PIPA (PROTECT Intellectual Property Act)*.

Зокрема, Д. Каплан (*Joel Kaplan*), віце-президент з питань публічної політики компанії *Facebook*, у відгуку, розміщеному в персональному блозі [233], підкреслював, що Законопроект *CISPA*, по-перше, спрямований на захист прав інтелектуальної власності, а не комп'ютерних мереж від хакерів і, по-друге, не зобов'язує приватні компанії збирати додаткову інформацію про кіберінциденти, а лише пропонує їм своєчасно ділитися такою інформацією з державними правоохоронними органами.

Хоча під тиском громадськості американський політикум свого часу поклав «до шухляди» ідею прийняття *CISPA*, однак уже в березні 2013 року повернувся до його розгляду й, мабуть, неодноразово повертатиметься. Про це свідчить те, що й у червні 2014 року уряд США намагався знов повернутися до його розгляду [432].

Звинувачуючи *CISPA* в порушенні прав людини на приватність інформації, правозахисники протиставляють цей Законопроект, на їхню думку, прогресивнішому *PRECISE Act of 2011* (*Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011*), внесеному на розгляд 9 грудня 2011 року членом нижньої палати Конгресу Д. Лангреном (*Daniel Lungren*) у вигляді поправок і доповнень до Закону «Про Міністерство внутрішньої безпеки» від 2002 року (*The Homeland Security Act of 2002*). Законопроект не передбачає жодних принципових змін, моніторингу кіберпростору на предмет виявлення потенційних та актуальних кіберзагроз, а лише уточнює повноваження Міністерства внутрішньої безпеки у сфері кіберзахисту.

Безумовно, США як одна із країн з найбільшим рівнем інтернет-проникнення в усі сфери життя суспільства чи не найбільше опікується проблемами кібербезпеки, зокрема її військовим аспектом. Хоча країни ЄС і виявляють певну активність у цьому напрямі, але на тлі запеклих протистоянь щодо тих чи інших нормативно-правових документів, що матимуть вплив на забезпечення кібербезпеки США, активність ЄС є набагато скромнішою.

Лише в лютому 2013 року Європейська Комісія спільно з Верховним представником ЄС у закордонних справах та з політики безпеки представили проект Стратегії з кібербезпеки «Відкритість, безпека та надійність» [297]. Стратегія спрямована на поліпшення взаємодії між державним і приватним сектором у подоланні кіберзагроз, створення єдиних баз даних щодо загроз у кіберпросторі тощо.

Аналогічні стратегії створено на рівні окремих країн ЄС, зокрема в Естонії, Фінляндії, Словаччині, Чеській Республіці, Франції, Німеччині, Литві, Люксембургу, Нідерландах, Великобританії, Польщі та Румунії.

Крім упорядкування нормативно-правового поля проблем кібербезпеки, держави ЄС та інші провідні держави готуються до протистоянь у кіберпросторі на суто практичному рівні. Вони беруть участь у навчаннях щодо протидії кібератакам[15]. Кібербезпекові навчання

[15] Із 2006 року США практикують навчання *Cyber Storm* (наразі під егідою Міністерства внутрішньої безпеки США). Станом на 2013 рік такі навчання відбувалися в 2006, 2008, 2010 та 2011–2012 роках. Кількість залучених фахівців та інституцій щороку збільшується. Водночас розширюються масштаби навчань [282]. Крім того, у США щорічно, починаючи з 2001 року [278], функціонує *Cyber Defense Exercise* – турнір між командами чинних захисників кіберпростору США, зокрема Агентством національної безпеки США та курсантами кількох військових навчальних закладів, що спеціалізуються на кібербезпековій тематиці (у навчаннях 2013 року перемогли курсанти) [28].

Cyber Europe вперше відбулися в 2010 році [302]. До наступних навчань 2012 року було залучено 571 особу із 339 організацій з 25 європейських країн включно з інституціями ЄС [279].

У 2011 році проведено спільні американсько-європейські кібернавчання *Cyber Atlantic 2011*, метою яких була перевірка готовності основних безпекових структур до співпраці в протидії кіберзагрозам [274]. Для поліпшення якості таких навчань і моделювання ключових процесів функціонують спеціальні полігони на кшталт *Northrop Grumman* [446], що надають можливість виявляти проблемні зони захисту інфраструктури, моделювати можливі інциденти й виробляти типові схеми реагування, поліпшувати міжвідомчу взаємодію тощо.

Навчання, спрямовані на посилення кібербезпеки учасників, здійснює також НАТО. Із 2009 року Центр кіберзахисту НАТО (*NATO Cooperative Cyber Defence Centre of Excellence*) допомагає в плануванні, розроблені сценаріїв і тренуваннях у межах Навчання НАТО з кіберзахисту (*NATO Cyber Defence Exercises*) – Кіберкоаліція (*Cyber Coalition*) [277]. З-поміж учасників навчань (з 2010 по 2012 роки їх відбулося вже три) є навіть країни, які не є членами НАТО.

Потреба в забезпеченні кібербезпеки та створенні засобів ведення кібервійн наразі спонукає уряди держав переглядати внутрішню політику в кіберсфері, оскільки дедалі частіше трапляються випадки використання розвідувальними службами та спеціалізованими військовими підрозділами можливостей і технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочинності. Звідси і зміни в інформаційній політиці, які, щоправда, стосуються передусім обмежень і цензури як механізмів здійснення внутрішньої політики.

Дедалі активніше застосовується низькотехнологічний (*low-tech*) рівень контролю, до якого відносять бюрократичні, організаційні та обмежувальні методи захисту власного інформаційного та кіберпростору від латентних загроз безпеці даних і заходи, спрямовані на посилення цифрового суверенітету, зокрема на протидію засиллю іноземного програмного продукту.

У контексті посилення цифрового суверенітету використовується кілька ключових підходів, з-поміж яких домінують повноцінне блокування небажаних ресурсів та опосередкований вплив на власників контенту.

На тлі зазначеної цифрової суверенізації дедалі виразнішим є бажання держави більше знати про інтернет-трафік громадян, а за мож-

ливості і про контент їхніх персональних комп'ютерів. Для цього держави намагаються посилити контроль за точками доступу до мережі інтернет (зокрема інтернет-кафе) та інтернет-трафіком громадян.

Зокрема, в КНР для інтернет-кафе діють ті самі правила, що й для барів: розміщення не ближче ніж 200 ярдів (близько 183 м) від школи та обов'язковий віковий ценз для отримання доступу до певних послуг. Загалом, щоб отримати можливість попрацювати з мережею, обов'язково потрібний документ, що посвідчує особу. Однак у деяких містах Китаю, наприклад, у Пекіні, де кількість інтернет-кафе сягає 1500, застосовуються додаткові методи ідентифікації: встановлюються камери спостереження, що фотографують усіх користувачів. За китайським прикладом до подібних кроків вдається й Білорусь.

Контроль за діяльністю інтернет-кафе практикується і в європейських державах. Поліція *Великобританії* також планує налагодити співробітництво із власниками інтернет-кафе з метою контролю за контентом, що переглядається відвідувачами (для запобігання підготовці терактів).

Свою історію контролю за інтернет-трафіком має *Франція*. 13 травня 2010 року Парламент Франції ухвалив Закон з умовною назвою «Про три попередження» (*HADOPI law, Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*), згідно з яким дозволено на цілий рік позбавляти права користування мережею інтернет тих, хто вдруге помічений у скачуванні матеріалів, захищених копірайтом. Для контролю за дотриманням вимог Закону створено спеціальний адміністративний орган – Вища інстанція для захисту копірайту та поширення матеріалів через інтернет (*High authority for copyright protection and dissemination of works on the Internet*). 10 червня 2010 року до Закону внесено зміни з метою посилення його «конституційності». У новій редакції передбачено, що позбавити людину чи організацію права користування інтернетом може лише суд, а провайдер інтернет-послуги зобов'язаний надавати правоохоронним органам дані про користувачів-піратів. Якщо провайдер не надасть даних протягом 8 днів, на нього очікує штраф у 1,5 тис. євро за кожну *IP*-адресу, щодо якої не надано інформацію. Уже в серпні 2010 року на виконання Закону «Про три попередження» французьким користувачам запропоновано (поки на добровільних засадах) встановити на свої комп'ютери спеціальне програмне забезпечення, що відслідковуватиме весь трафік користувача, шукатиме встановлене на комп'ютері нелегальне програмне забезпечення, надаватиме відомос-

ті правоохоронним органам щодо переглянутого користувачем відео в мережі інтернет. У червні 2013 року із Закону вилучено положення про відключення від мережі інтернет користувачів, які систематично порушують закон. Коментуючи цю подію, Ф. Пелерін (*Fleur Pellerin*), міністр Франції з цифрових комунікацій, зазначила: «Це майже те саме, що відключити воду» [187].

На загальноєвропейському рівні діє Директива ЄС щодо охорони прав на інтелектуальну власність (*Directive 2004/48/EC, Intellectual Property Rights Enforcement Directive, IPRED*), що дозволяє правоохоронним органам збирати особисті дані користувачів, підозрюваних у незаконному файлообміні. Водночас варто зазначити, що ця Директива поки імплементована в законодавство лише кількох країн ЄС (Великобританія, Франція, Данія та Швеція).

У червні 2013 року *Washington Post* оприлюднила результати власного журналістського дослідження, яке стосувалося засекреченої програми співробітництва безпекових структур США (зокрема АНБ та ФБР) та провідних приватних компаній, що працюють на світовому інформаційному ринку, – *Microsoft*, *Yahoo*, *Google*, *Facebook*, *PalTalk* та інших. Вартість програми становить 20 млн дол. США щорічно.

Подібна співпраця державного та приватного секторів була налагоджена ще за Адміністрації Дж. Буша-мол. у межах програми *PRISM* і передбачала передачу «компетентним органам» даних, які стосувалися електронної пошти, будь-яких чатів (текстових та відео), завантажених користувачами фото, відео матеріалів та взагалі будь-яких даних (щодо *VoIP*-телефонії, передачі файлів, відеоконференцій, нагадувань щодо будь-яких дій, деталей мережевого соціального життя, запитів тощо) із серверів приватних компаній [381].

Слайди, представлені *Washington Post* [382], надають можливість детально ознайомитися з нюансами роботи такої державно-приватної системи й, зокрема, з'ясувати послідовність приєднання до програми корпоративних учасників: від *Microsoft* та *Yahoo* (в 2007–2008 рр.) до *Apple* (у 2013 році).

Виникли обґрунтовані підозри, що частково можливостями зазначеної системи користувалася одна зі спеціальних служб Великобританії – *GCHQ*.

Пізніше представники АНБ визнали існування згаданої програми, хоча інші її учасники (приватні компанії) досі категорично заперечують свою участь у ній. Проте, навіть визнаючи існування програми, представники спецслужб наголошували, що вони не збирали

персональних даних американців, адже їх метою було стеження за іноземцями.

Однак навіть внутрішні документи свідчать, що оператори системи тотального кібермоніторингу не надто переймалися обставиною громадянства тих, кого вони моніторять.

Зовсім не випадково дані зазначеного журналістського розслідування були оприлюднені 7 червня 2013 року, напередодні зустрічі в Каліфорнії кібернетичних лідерів сучасного світу – США та КНР, для яких питання кібершпигунства та захисту від нього стають дедалі складнішими й актуальнішими.

Особливою увагою правоохоронних органів останнім часом користується контроль за контентом у соціальних мережах, блогах тощо. На цьому тлі інтенсифікації участі державних органів у функціонуванні мережі інтернет та посилення їх моніторингових і контролюючих функцій дещо дивним видається надто скромний спротив такій практиці з боку організацій громадянського суспільства, які опікуються дотриманням демократичних свобод. Зокрема, за результатами опитування стану громадської думки, здійсненими компанією *Sophos*, більшість американців не вважають проблемою те, що уряд використовує технології моніторингу та фільтрування мережевого трафіку, а також має доступ до їхніх поштових серверів. Натомість опитані стверджують, що не проти доступу спецслужб до своєї пошти. Такий стан громадської думки засвідчує повну кризу громадянських свобод і ситуації з правами людини в цілому.

Отже, навіть найдемократичніші країни Заходу, не афішуючи, роблять спроби якомога інтенсивніше та глибше контролювати контент мережі інтернет і здійснюють у цьому напрямі певні кроки, що засвідчує переосмислення ліберального підходу до мережі.

У цьому сенсі вельми показовою була ситуація, яка склалася напередодні саміту *G*8 у французькому м. Довілі 26–27 травня 2011 року. Тодішній президент Франції Н. Саркозі зібрав у м. Парижі «кібернетичний саміт» (*e-G*8) за участю представників провідних *IT*-компаній (голова ради директорів компанії *Google* Е. Шмідт (*Eric Schmidt*), засновник *Facebook* М. Цукерберг (*Mark Zuckerberg*), виконавчий директор *Amazon* Дж. Безо (*Jeff Bezos*), глава *News Corporation* Р. Мердок (*Rupert Murdoch*) та інші)[16]. На саміті Н. Саркозі та міністр економіки Франції К. Лагард (*Christine Lagarde*) запропонували обговорити

[16] Повний список учасників див.: http://www.eg8forum.com/en/speakers/

проблему керованості мережі, її «цивілізованості», дотримання права приватності й авторських прав, відповідність ідеалу «цивілізованого інтернету» (*civilized Internet*). Противники французького президента з-поміж учасників Форуму[17] підтримали ініціативи у сфері забезпечення авторських прав, рішуче відкинувши водночас пропозиції Н. Саркозі щодо фільтрування контенту мережі, кваліфікувавши їх як поширення «китайського підходу».

У 2011 році також активізувалися переговори між ЄС, США, Японією, Канадою, Південною Кореєю, Австралією та кількома іншими країнами щодо митно-торговельної угоди, спрямованої на боротьбу з контрафактною продукцією (Торговельна угода щодо боротьби з контрафакцією – *Anti-Counterfeiting Trade Agreement, ACTA*). Вона передбачала фільтрування контенту мережі з метою протидії піратству, але спричинила масові протести як у США, так і в Європі з боку прихильників «вільного інтернету».

Навіть в умовах досить апатичного ставлення європейського громадянського суспільства до проектів моніторингу всесвітньої мережі правозахисники та громадські активісти досить жорстко зустріли інформацію про бажання ЄС створити європейський аналог китайського «Золотого щита» (*The Golden Shield Project*).

Зокрема, в ухвалі Ради Європи від 11 лютого 2011 року № 7181/11, яка стосується безпеки та митниці [335], йдеться про намір сформувати в рамках ЄС «єдиний безпечний європейський кіберпростір» (*a single secure European cyberspace*) з «віртуальними Шенгенськими кордонами» – *The Great European Firewall*[18] *project*. У цьому просторі існуватимуть своєрідні аналоги митниць – «віртуальні точки доступу», в яких інтернет-провайдери блокуватимуть згідно зі спеціальним «чорним списком» весь нелегальний контент.

Ініціатива вийшла на етап перемовин під егідою Ради ЄС під час президентства Угорщини (перше півріччя 2011 року). Попередня презентація системи «кордонів віртуального Шенгену» (*virtual Schengen border*) відбулася під час Спільного засідання Робочої групи правоохоронних органів та Робочої групи співробітництва митних служб.

Варто зазначити *відсутність у керівних інституціях ЄС єдиного бачення щодо прийнятності або неприйнятності для ЄС подібної програми дій*. Непопулярність ініціативи мала наслідком припису-

[17] Див.: http://www.eg8forum.com

[18] У роботі поняття *firewall* використовується в латинському та кириличному (фаєрвол) написанні – *Прим. ред.*

вання авторства архітектури нової політики щодо інтернет-простору «неназваному «угорському експертові»[19] й запевнення офіційних кіл ЄС, що дана експертна позиція в жодному разі не є офіційною позицією Ради Європейського Союзу, Генерального секретаріату Ради ЄС чи самої Угорщини [291]. Зрештою від цієї ініціативи відсторонилася Н. Кроес (*Neelie Kroes*), Європейський комісар з питань цифрового майбутнього (*European Commissioner for the Digital Agenda*) та віцепрезидент Європейської Комісії, яка написала у *Twitter* [343], що в Єврокомісії немає планів створювати «європейський фаєрвол». Водночас, як слушно зазначають деякі журналісти, таке повідомлення від офіційної особи в Єврокомісії лише засвідчило, що даною проблемою не переймаються саме в Єврокомісії, але цілком можливо, що нею переймаються в інших інституціях ЄС.

Загалом показовим є сам факт обговорень ідеї «віртуального Шенгену» та прогресу в даному напрямі, а не питання про те, чи буде даний проект реалізований вже в найближчому майбутньому. Адже донедавна на загальноєвропейському рівні не розглядалася сама можливість запровадження будь-яких форм централізованої цензури (фільтрування) в інтернеті.

Ідея побудови централізованої системи фільтрування інтернет-контенту з'явилася в ЄС «не на порожньому місці», зважаючи на те, що на законодавчому рівні різноманітні цензурні обмеження контенту мережі практикує більшість країн ЄС.

Зокрема, в Німеччині цензуруються пошукові запити, в яких містяться навіть натяки на заперечення Голокосту. Крім того, у 2010 році прийнято федеральний закон про заборону дитячої порнографії, а в 2011 році на засіданні коаліційного уряду констатовано, що самé лише блокування доступу до мережі не є ефективним і має видалятися безпосередньо незаконний контент[20].

Боротьбою зі шкідливим контентом у Франції з 2010 року займається урядове агентство *HADOPI*. Окремі форми фільтрування кон-

---

[19] У документі наводяться цілком слушні приклади тих випадків, коли цензурування є бажаним та єдино можливим (наприклад, публікація на відеохостингу поза межами ЄС відео, де група дітей фільмує здійснюване ними вбивство людини) [436].

[20] Згідно з непідтвердженими даними видалення такого контенту є дійсно ефективнішим. У статті «Германия: детское порно будут удалять, а не блокировать» (Див.: http://www.webplaneta.de/articles.php?article=2434) наводиться така статистика ефективності видалення дитячого порно в Німеччині: у січні 2011 року в 93 випадках з 143 задокументованих фактів поширення дитячого порно контент був видалений (коефіцієнт видалення – 68 %). У подальшому цей коефіцієнт вдалося збільшити до 99 %.

тенту практикують Італія, Іспанія, Великобританія та інші країни[21]. Туреччина, яка впродовж тривалого часу намагається стати членом ЄС, планувала вже у 2011 році[22] запустити власну систему фільтрування небажаного контенту мережі. Однак станом на 2014 рік не відомо, чи була запущена така система. Водночас у 2014 році в Туреччині було прийнято закон, що надав державним органам можливості для регулювання сфери телекомунікацій.

Наразі важко сказати, чи готовий ЄС дійсно створити подібну систему моніторингу мережі. Однак навіть сам факт того, що подібні переговори та розробки здійснюються, свідчить про відповідні суттєві внутрішні зрушення в певних колах керівництва європейських інституцій.

У 2013 році зазначені ідеї набули нового формату. Внаслідок скандалу зі Е. Сноуденом (*Edward Joseph Snowden*) багато країн значно посилили свою увагу до безпеки даних (передусім персональних даних своїх громадян), і ЄС тут не став винятком. У жовтні 2013 року провідний німецький телекомунікаційний концерн *Deutsche Telekom* виступив з ініціативою «національної маршрутизації» (*National Routing*) інтернету. Офіційний представник концерну Ф. Бланк (*Philipp Blank*) пояснив цю ідею таким чином: «Мета проекту полягає в тому, щоб інтернет-дані, відправлені одним користувачем у Німеччині іншому, не переспрямовувалися через інші країни, як це відбувається сьогодні» [227]. У перспективі цей проект має охопити всі країни Шенгенської зони. І хоча він поки що існує на рівні пропозиції й теми для обговорення, можна припустити, що найближчими роками подібні ініціативи набуватимуть дедалі більшої популярності.

1.4. Спроби категоріально-понятійного осмислення кібербезпекової політики у вимірах наукової теорії

Попри зростаючу небезпеку від кіберзагроз різних рівнів складності, на шляху створення ефективних механізмів протидії кіберзлочинцям досі постають дві важливі проблеми – термінологічна та нормативно-правова.

---

[21] Інтернет-трафік проходить крізь сервіс, що має назву *Cleanfeed*, який ідентифікує сторінки, що містять дитячу порнографію.

[22] Згідно з інформацією, оприлюдненою одним з турецьких доповідачів під час «круглого столу «Україна і Туреччина на шляху до інформаційного суспільства: реалії та перспективи» (м. Київ, 12 травня 2011 року, Комітет з питань свободи слова та інформації Верховної Ради України).

Незважаючи на те, що такі поняття, як *кіберпростір*, *кібервійна*, *кібератака* та *кібертероризм,* широко використовуються в науковій і публіцистичній літературі, дотепер невизначеним є їх зміст, що значно ускладнює наукове осмислення та практичне освоєння проблеми загроз у кіберпросторі.

Безумовно, ключовою проблемою у формуванні тезаурусу сфери кібербезпеки є визначення поняття *кіберпростір*. Американський дослідник Дж. Ліпман (*James M. Liepman*) із цього приводу цитує слова генерал-лейтенанта Р. Елдера (*Robert J. Elder*), одного з керівників ВПС США, відповідальних за забезпечення кібербезпеки США. Він сформулював два основних проблемних напрями при створенні доктрини кіберпростору: «визначення кіберпростору та воєнні дії у кіберпросторі» [Цит. за: 352, с. 74]. Як зазначає сам Дж. Ліпман, важливим є «розуміння того, чим є кіберпростір (і чим він не є), а також того, що означає боротьба у кіберпросторі» [Там само].

Американські дослідники, які працюють у мілітарній площині кібербезпеки [300, 274], вважають, що базовим визначенням поняття *кіберпростір* в американській практиці дослідження проблем кібербезпеки має бути визначення, запропоноване Національною військовою стратегією для операцій у кіберпросторі (2006 рік). У документі *кіберпростір* визначений як «сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язана з ними фізична інфраструктура» [374, с. 9]. Це саме визначення було покладено і в основу розроблення документа Стратегічне бачення Кіберкомандування повітряних сил (2008 рік) [236] та Стратегії національної безпеки США (2010 рік), в якому, зокрема, зазначається, що «військові повинні й надалі мати можливість захищати інтереси США у всіх основних сферах – землі, повітрі, воді, космосі та кіберпросторі» [376, с. 22]. Таким чином, у сучасному офіційному безпековому дискурсі США кіберпростір розглядається саме як «фізичний» простір.

Водночас Дж. Ліпман наполягає [352], що подібний підхід характерний саме для фахівців з Міністерства оборони США (і ВПС зокрема). Останнім часом відбувається часткова зміна цієї точки зору, зокрема з-поміж військових спеціалістів, у бік розуміння кіберпростору як теоретичного (чи, швидше, віртуального) поняття.

Варте уваги також визначення, запропоноване П. Вуллей (*Pamela Woolley*) з Інституту технологій повітряних сил США, яка пропонує

розуміти кіберпростір «як створене людиною цифрове довкілля, що використовується для миттєвого, безкордонного, глобального, без організаційних, культурних, національних чи політичних кордонів збору, зберігання й передачі даних та інформації між електронним обладнанням» [451, с. 8].

«Огляд політики щодо кібепростору» від 2009 року – комплексний документ з оцінки стану кібербезпекового простору США та можливих способів його поліпшення – розуміє кібербезпеку відповідно до визначення, запропонованого в Директиві Президента з національної безпеки 54 / Директиві Президента з внутрішньої безпеки 23 (*National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – NSPD*-54/*HSPD*-23) від 2008 року. Вони визначають кіберпростір як «взаємозалежні мережі, комп'ютерні системи, *IT*-інфраструктури, що включають інтернет, телекомунікаційні мережі, комп'ютерні процесори (*embedded processors*) та контролери у критично важливих сферах» [287, с. 1].

У підготовленій фахівцями Центру стратегічних і міжнародних досліджень (умовно – Інститут Бжезинського) доповіді «Безпека кіберпростору для 44-го Президента» за загальним керівництвом Дж. Льюїса (*A. J. Lewis*) поняття *кіберпростір* широко розуміється як «дещо більше, ніж просто мережа інтернет, і включає всі мережеві форми та цифрову діяльність» [409, с. 11]. Водночас автори документа зазначають, що загрози від кібератак виявилися не зовсім такими, на які очікувалося: «ми вважали, що наслідки від кібератаки будуть переважно фізичними (відкриття шлюзів, авіакатастрофи), натомість вони мають яскраво виражений інформаційний характер» [Там само, с. 12]. На підтвердження цієї думки автори наводять приклади численних проникнень хакерів в інформаційні системи з метою викрадення тієї чи іншої інформації, перехоплення е-листування посадових осіб тощо. Схожого підходу дотримується й американський дослідник М. Лібіцкі (*Martin C. Libicki*), який пропонує розуміти під кіберпростором «сукупність індивідуальних комп'ютерних пристроїв, об'єднаних у мережу» [348, с. 6].

Фахівці з Центру стратегічних і міжнародних досліджень зазначають, що «головні загрози критичній інфраструктурі походять передусім від військових і розвідувальних служб інших держав, оскільки саме вони підготовлені необхідним чином, мають необхідні ресурси та ставлять перед собою чіткі цілі» [409, с. 13]. Цієї самої думки дотримуються й укладачі згаданого «Огляду політики щодо кіберпросто-

ру»: «зростання зв'язків між інформаційними системами, інтернетом, іншими інфраструктурами створює можливості для зловмисників порушити зв'язок, постачання електроенергії, пошкодити трубопроводи, нафтопереробні заводи, завадити діяльності фінансових структур та інших критично важливих об'єктів інфраструктури». Вони також стверджують, спираючись на думку «розвідувальної спільноти», що низка країн вже має технічні можливості для проведення таких атак» [287, с. 2]. При цьому не зазначається можливість доступу до подібних «технічних можливостей» недержавних акторів.

Станом на 2013 рік жодного концептуального розуміння в цьому питанні так і не було сформульовано. Автори спеціального дослідження «Кібермогутність і національна безпека» (*Cyberpower and National Security*) також звертають увагу на те, що зміст концепту *кібер* може бути визначений багатьма способами. Один зі співавторів дослідження Д. Куел (*Daniel T. Kuehl*), який присвятив окремий розділ роботи саме спробі визначення термінології, навів щонайменше 28 визначень кіберпростору. У результаті він запропонував визначити поняття як «операційний домен, обмежений [*framed*] використанням електроніки та електромагнітним спектром для створення, збереження, зміни, обміну та використання інформації у взаємопов'язаних та інтернетизованих [*Internetted*] інформаційних системах та пов'язаній з ними інфраструктурі» [285, с. 4].

Не менш цікавим (з погляду загального розуміння американських наукових підходів до проблеми) є висновок, якого дослідники доходять з багатоманіття визначень поняття *кібербезпека* для практичної діяльності: «найважливіший урок, який ми винесли із цього багатоманіття, це те, що визначення мають допомагати формувати політики чи робити аналіз, а не обмежувати їх» [Там само, с. 4]. На підставі цього вихідного положення дослідники пропонують використовувати базове поняття лише як шаблон, наповнюючи кожен конкретний термін, маючи його на увазі, але одночасно динамічно розширюючи. Наприклад, коли йдеться про *кібервплив*, потрібно включити в обшир поняття і традиційні комунікативні канали, які, однак, «поширюються» за допомогою мережі інтернет, тобто радіо, телебачення, комунікацію за допомогою мобільного зв'язку чи комп'ютерних програм. Аналогічно у *кібервійськову активність* пропонується включити мережевоцентричні операції, комп'ютерні мережеві атаки, операції геополітичного впливу. І нарешті, у власне поняття *кібербезпека* пропонується включити не лише технічні питання, а й людський чинник – ворожі інсай-

дерські дії чи людські помилки, а також проблеми владних відносин на національному та міжнародному рівнях.

Вітчизняні науковці, досліджуючи поняття кіберпростору, працюють переважно або в загальнофілософській, або в юридичній площині. Так, у студіях щодо значення *кіберпростору* О. Манжай наводить таке його визначення: «Це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [122, с. 145]. Своєю чергою А. Погорецький та В. Шеломенцев пропонують розуміти під *кіберпростором* «штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо)» [159, с. 80].

Проблема визначення поняття *кіберпростір* пов'язана також із тим, що принаймні в західних дослідженнях науковці досі не визначилися з тлумаченням його другого складника – *простір*. У той час як у вітчизняній практиці *простір* розуміється переважно як загальне поняття, що описує певну частину буття людини, в західній літературі є три майже синонімічних поняття, які водночас мають різне змістовне навантаження: *domain*, *realm* та *environment*. На нашу думку, перше пов'язане переважно із просторово-географічними характеристиками. Наприклад, саме словом *domain* описується земля, вода, повітря та космос як окремі види просторів. Це поняття використовується тими науковцями й експертами, які апелюють до кіберпростору як до поля можливої боротьби й геополітичного протистояння. Можна сказати навіть інакше: поняття *domain* найчастіше використовується, коли йдеться про державну чи міждержавну політику щодо цієї нової реальності. *Environment* надає кіберпростору характеристик певного «навколишнього середовища», яке можна відчути і на яке можна вплинути повсякденною діяльністю аж до знищення. Як *realm* кіберпростір згадується переважно в навколонауковій літе-

ратурі й у тих роботах, що можуть бути умовно віднесені до робіт прихильників постмодерністських теорій. У запропонованій роботі ми спиратимемося переважно на розуміння кіберпростору як *domain,* узгоджуючи його з поняттям національних інтересів передусім як інтересів держави.

Складнощі з визначенням поняття кіберпростору обумовлюють очевидні проблеми з розумінням понять *кібербезпека* та *війна в кіберпросторі* (*кібервійна*). Дж. Ліпман пропонує таке визначення кібербезпеки для військової сфери США: «забезпечити для США свободу дій, контроль доступу та визначення місцезнаходження противника у кіберпросторі» [352, с. 73]. У вже згаданому документі Стратегічне бачення Кіберкомандування повітряних сил зазначається, що кібербезпеку держави слід розуміти як своєрідну сукупність категорій: «використання кіберпростору» (атаки в кіберпросторі та збільшення власних сил), «контролювання кіберпростору» (оборонні дії в кіберпросторі й атакуючі контрдії в кіберпросторі) та «налаштування кіберпростору» (глобальні спостережні операції в кіберпросторі, операції з управління та контролю за мережами та безпекою, операції з цивільної підтримки в кіберпросторі) [236, с. 11].

Згадувана вище Директива президента США з національної безпеки 54 поділяє сферу кібербезпеки на три ключові компоненти: атаку комп'ютерних мереж, захист комп'ютерних мереж та управління ними. Крім того, саме на Міністерство оборони США (а вже потім на розвідувальні та правоохоронні органи) покладається необхідність забезпечення кібербезпеки.

Американський дослідник С. Бейделман (*Scott Beidleman*) [242, с. 11] зазначає, що поняття *війна в кіберпросторі* є надто широким у його сучасному трактуванні. Кібервійна не є просто синонімом інформаційних операцій, однак цілком може бути їх компонентою. Інформаційні операції включають психологічні операції, військову хитрість, операції із забезпечення безпеки, електронну війну та операції в комп'ютерних мережах [324]. Останні описуються як «використання комп'ютерних мереж» для атаки на «інформацію, що є на комп'ютерах та в комп'ютерних мережах, або самі комп'ютери та мережі [Там само, с. II-5]. Під час кібервійни кіберпростір використовується для атаки на персонал, будівлі або обладнання на додачу до інформації та комп'ютерів [237], і саме це – чіткий зв'язок між комп'ютерним середовищем і фізичною інфраструктурою та довкіллям – є визначальним для виокремлення кібервійни в окрему сферу воєнних дій. Водночас

М. Лібіцкі вважає кібервійну частиною звичайної війни розуміючи її як «дії проти військових цілей під час війни» [348, с. xiv].

Цікаво й те, як деякі з дослідників відокремлюють кібероперації від інформаційних операцій. Д. Куел із цього приводу зазначає: «Інформаційне середовище являє собою три відокремлені, однак пов'язані та синергістичні [*synergistic*] виміри: «під'єднаність» (інфраструктурний вимір, який забезпечує необхідні елементи інфраструктури для функціонування середовища), контент (інформаційний вимір, тобто надзвичайно великий обсяг інформації, яка може бути надіслана будь-кому в цифровому вигляді) та когнітивність (вимір пізнання, тобто здатності сприймати інформацію, який і впливає на прийняття рішень). У той час як інформаційні операції включають усі три виміри інформаційного середовища, кіберпростір працює лише із частиною (щонайбільше з вимірами під'єднаності й контенту) [285, с. 28].

У більшості менш чітких визначень кібербезпеки ключовою ознакою стає можливість захиститися (чи ефективно протидіяти) кібератакам. Водночас це поняття також не визначене в більшості критично важливих офіційних документів.

С. Хілдрет (*Steven A. Hildreth*), один з авторів доповіді Дослідної служби Конгресу США *RL*30735, зазначив, що кібератаки або кіберзагрози – це несанкціоновані спроби проникнення в комп'ютери, керовані комп'ютерними системами або мережами [217]. Розроблений у 2000 році у США Національний план із захисту інформаційних систем під *кібератакою* розуміє «використання вразливостей у програмному забезпеченні управляючих компонентів, що базуються на інформаційних технологіях» [375, с. 148]. С. Бейделман на основі визначення поняття *операція в кіберпросторі*, що наводиться у Словнику військових та пов'язаних термінів Міністерства оборони США [324], пропонує власне визначення поняття *кібератака*: «Кібератака може розглядатися як сукупність кібероперацій з ворожим використанням комп'ютерів та інформаційних технологій з метою досягнення певних ефектів чи цілей через кіберпростір» [242, с. 12].

Водночас жодне визначення кібератаки не пояснює, хто є суб'єктом подібних атак. Крім того, залишається невизначеним, у якому співвідношенні мають розумітися поняття *кібератака* та *кібервійна*: чи є кібератака елементом кібервійни, чи сукупність кібератак призводить до кібервійни, чи кібератаки та кібервійни є цілком незалежними поняттями, що перетинаються лише ситуативно.

З огляду на відсутність подібних пояснень, ми пропонуємо таке визначення кібератаки. *Кібератака може розглядатися як сукупність дій противника або ворожої групи, яка намагається досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, найчастіше – з використанням спеціально розроблених для таких завдань засобів.* Сукупність кібератак, що перевищують за своїм загальним негативним впливом певне порогове значення, можуть розглядатися як початок *кібервійни*. Зазначимо, що проблема визначення «порогового значення» та розгляд кібератак у міжнародному праві як «акту війни» є важливою проблемою для методологічних досліджень у сфері національної та міжнародної безпеки.

Вітчизняні дослідники також активно використовують поняття *кібертероризм*. Причому часто розуміють під ним і кібервійни, і кібератаки тощо, що є неправильним як з методологічної точки зору, так і з погляду відображення сучасних реалій даної безпекової сфери.

Навіть у західній науковій літературі термін *кібертероризм* та опис можливих наслідків актів кібертероризму має переважно ідеологічно-пропагандистську та абстрактно-теоретичну компоненту. Це було обумовлено проголошеною за часів Адміністрації Дж. Буша-мол. глобальною війною з тероризмом. Водночас дотепер більшість реальних загроз критично важливій інфраструктурі інформаційно розвинутих держав (США, Великобританія, Німеччина) надходили не від поодиноких терористичних груп, що просто змінили безпосередню тактику ведення боротьби, а від спеціально підготовлених, інформаційно та матеріально забезпечених спеціалізованих груп, що функціонують в інтересах тих чи інших держав і є фактично продовженням їх «воєнної машини».

У ґрунтовній праці «Кібервійна та Кібертероризм» за редакцією Л. Жанчевскі (*Lech J. Janczewski*) та А. Коларіка (*Andrew M. Colarik*) подано таке визначення кібертероризму: «Кібертероризм – це політично мотивовані атаки, що здійснюються субнаціональними групами чи таємними агентами або окремими індивідами проти інформаційних та комп'ютерних систем, комп'ютерних програм чи даних, результатом яких є насилля проти нонкомбатантів[23]» [328, с. 13]. На нашу думку, це визначення містить дві ключові компоненти, що мають відокрем-

[23] Нонкомбатанти – особи, що входять до складу збройних сил, однак функції яких полягають лише в обслуговуванні та забезпеченні воєнної діяльності збройних сил і які мають право використовувати зброю лише в разі самозахисту. Водночас у даному випадку, швидше, йдеться про цивільне населення в цілому.

лювати кібертероризм від усіх інших форм кіберзлочинів: політична мотивація та насилля проти нонкомбатантів як результат атак.

Словник тероризму (*Dictionary of Terrorism*) описує кібертероризм як «злочин майбутнього, в який буде втягнено злочинців і комп'ютери» з уточненням наявності в кібертерористів «політичної мотивації для їх злочинів» [427, с. 61]. М. Каветлі (*Myriam Cavelty*) пропонує визначити кібертероризм як «незаконні напади з боку недержавних суб'єктів на комп'ютери, мережі та інформацію, що міститься в них, здійснювані з метою залякування уряду (чи населення) чи з метою спричинити певну поведінку залякуваного суб'єкта. Кібератака може розумітися як кібертероризм лише в тому разі, якщо це призводить до фізичного насилля проти осіб чи власності або виникнення значної можливості настання таких наслідків» [255, с. 1].

У вже згаданому дослідженні Л. Жанчевскі та А. Коларіка зазначається, що «дотепер не було серйозних дій кібертерористів, хоча комп'ютерні мережі піддавались атакам у ході конфліктів у Косові та на Близькому Сході» [328, с. 1]. Водночас висловлюється припущення, що «через те, що терористи мають обмежені фінансові можливості, кібератаки стають більш привабливими [ніж класичні воєнні засоби та дії – *Авт.*], оскільки потребують меншої кількості людей та меншої кількості ресурсів» [Там само, с. 2]. На нашу думку, це твердження є дискусійним, оскільки, незважаючи на те, що для кібертерактів теоретично дійсно потрібно менше людських ресурсів, однак до них, їх кваліфікації висуваються підвищені вимоги. Крім того, розроблення (чи навіть придбання) спеціального програмного забезпечення, що може бути використане для відповідних дій, також потребує коштів, а ймовірність бути відстеженим при використанні таких засобів без підтримки (політичної й технічної) певної держави є досить значною.

Зазначимо, що навіть автори наведеного дослідження, наводячи приклади терактів із використанням інформаційних технологій, певною мірою суперечать собі, коли пропонують розглядати як теракт, наприклад, події в Австралії у березні 2000 року[24]. Водночас нескладно побачити, що ця дія не була «політично мотивованою» і не мала на меті «здійснити насилля проти нонкомбатантів».

Як у вітчизняній, так і в західній літературі з проблем кібертероризму до кібертерактів традиційно відносять акцію 1998 року, прове-

[24] Невдоволений працівник, користуючись мережею інтернет (причому це йому вдалося із 45 разу – перші 44 атаки просто ніхто не помітив), випустив 1 млн л стічних вод у річку та на прибережні території Квінсленда.

дену «Тиграми визволення Таміл-Ілама», коли спеціальний підрозділ цієї організації намагався масовою розсилкою електронної пошти на певні адреси призупинити діяльність серверів дипломатичних представництв Шрі-Ланки [116]. Однак, оперуючи наведеним вище двокомпонентним поняттям кібертероризму нескладно помітити, що ця акція не мала на меті завдати фізичну шкоду некомбатантам, а за своїм характером більше нагадувала спам-розсилку, що активно використовується у протиправній діяльності хакерських організацій. Крім того, симптоматично, що ця акція відноситься до 1998 року, однак більш свіжі приклади такої діяльності не наводяться, що також може свідчити про значно перебільшений характер загрози від кібертероризму та про можливість його існування взагалі.

Деякі фахівці пропонують вважати прикладом вдалого реального кібертеракту дію вірусу *Stux.net*, однак у даному випадку доречніше говорити про певну форму диверсії, ніж тероризму.

М. Каветлі наводить власну типологію кіберконфліктів (за ступенем загрози, яку вони несуть), застосування якої може надати більш адекватну відповідь про місце кібертероризму у структурі кібербезпеки та визначитися з категорією більшості згадуваних різними дослідниками прикладів кібертероризму:

• *кібервандалізм* (включає зміни чи знищення змісту, наприклад, веб-сайту, відключення чи перевантаження серверу, є найпоширенішою формою кіберконфлікту, що отримує значний суспільний резонанс, однак наслідки таких інцидентів обмежені в часі та відносно незначні);

• *інтернет-злочини* (діяльність переважно з метою отримання прямого фінансового зиску, може включати як злочини з комп'ютерної техніки, так і суто комп'ютерні злочини);

• *кібершпигунство* (головною жертвою найчастіше стає корпоративний сектор. За окремими підрахунками втрати компаній від такої діяльності становлять до 1 трлн дол. США на рік. Урядові мережі, в яких міститься конфіденційна інформація, стають жертвами атак доволі рідко, хоча останнім часом такі атаки частішають);

• *кібертероризм*[25] (потенційно масштаби збитків від кібертеракту оцінюються надзвичайно високо, однак дотепер не було жодного реального випадку кібертероризму);

• *кібервійна* [255, с. 1-2].

[25] Визначення наведено вище.

З огляду на запропоновану класифікацію, найчастіше акти кібертероризму, що їх так називають дослідники, є, швидше, виявом кібервандалізму («злам» сайтів з метою порушення їх роботи та/чи зміни їх контенту) або належать до інтернет-злочинів. І перша, і друга діяльність є переважно в межах компетенції правоохоронних органів і до справжнього тероризму стосунку не має, якщо, звичайно, не намагатися штучно розширювати межі поняття *тероризм*.

Підбиваючи проміжний підсумок щодо зазначеної термінологічної проблеми, зазначимо, що, незважаючи на значну кількість наукових дискусій з приводу необхідності забезпечення кібербезпеки держав, тезаурус сфери кібербезпеки досі залишається вкрай нечітким, характеризується значними відмінностями в підходах, а подеколи публіцистичним (журналістським) викладом проблеми.

Порівнюючи підходи до понять *кіберпростір*, *кібертероризм*, запропоновані американськими й вітчизняними науковцями та вміщені в офіційних документах, можна констатувати, що американські підходи орієнтовані переважно на можливість використання визначень у суто практичній діяльності (формування ефективних стратегій національної безпеки, створення доктринальних документів у сфері кібербезпеки для тих родів військ або силових відомств, на які покладено обов'язок його захисту). Визначення, що пропонуються вітчизняними дослідниками, багато в чому мають загальнотеоретичний характер, а почасти є перевантаженими різноманітними уточненнями. Крім того, досі у вітчизняній науковій літературі відсутня фахова дискусія з приводу значної кількості термінологічних проблем у сфері кібербезпеки (зокрема відсутності визначень понять *кібератака*, *кібервійна*, *кібербезпека*), що ускладнює методологічний і загалом науковий супровід прийняття державних рішень у досліджуваній сфері.

1.5. Нормативно-правові проблеми розуміння безпеки кібернетичного простору як відображення геостратегічних суперечностей і зіткнень національних інтересів великих держав

Теоретико-методологічні дискусії довкола термінологічної бази стикаються зі значно більш практичною проблемою – застосування чинного нормативно-правового поля (особливо міжнародного) щодо кіберзагроз і з'ясування самої можливості його застосування у відповідному контексті.

Особливо важливо вирішити кілька принципових ускладнень, що унеможливлюють формалізацію безпекової політики в кіберпросторі:

• досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім його «безпековим» похідним;

• не визначено правовий статус кіберпростору;

• на міжнародному рівні відсутній консенсус щодо правил поведінки в кіберпросторі;

• відсутні загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляду як об'єкта міжнародних норм і правил (зокрема щодо визнання кібератаки як акту війни).

При цьому кібератаки (у різноманітних видах) стають повсякденним контекстом діяльності держав, міжнародних організацій та їхніх спеціалізованих установ. Концептуальна невизначеність із формами та методами ідентифікації кібератак відповідно до міжнародного законодавства, різність позицій ключових геополітичних гравців, потенційна ревізія (чи просто порушення) поняття *національний суверенітет* обумовлює особливе значення цього питання при дослідженні безпекових проблем, що стали актуальними з розбудовою інформаційного суспільства.

Незважаючи на широкий інтерес до зазначеного безпекового напряму, наукові дослідження (чи навіть узагальнення з цього питання) досі є поодинокими й часто несистемними.

Стрімке зростання кількості кібератак на державні ресурси й загальне збільшення кіберзлочинів обумовлює необхідність упорядкування проблеми на міжнародному рівні. Так, резолюції чи рішення з даного питання ухвалювали країни «великої вісімки», Організація Об'єднаних Націй, Міжнародний союз електрозв'язку, Рада Європи й інші об'єднання та організації. Водночас досі єдиним дієвим міжнародно-правовим документом є Конвенція про кіберзлочинність[26]. І хоча кількість країн-підписантів постійно збільшується (станом на 2014 рік їх було вже 43 [271, 272]), однак не всі її ратифікували. Однією з причин відмови від ратифікації стало те, що згідно з положенням Конвенції будь-яка зі сторін має право отримувати доступ до комп'ютерних даних (ресурсів), розташованих у мережах загального користування іншої сторони, не повідомляючи її про це. Зазначений

[26] Документ Ради Європи. Назва з офіційного перекладу.

факт, природно, ставить під сумнів дотримання принципу суверенності держав[27].

Низка країн висловлює ідею розроблення універсального документа, що мав би забезпечити збереження класичного розуміння суверенітету в нову цифрову епоху. Зокрема, Росія послідовно підтримує ідею прийняття Конвенції про забезпечення міжнародної інформаційної безпеки (КЗМІБ). Окремі ініціативи в цьому напрямі було висунуто ще 1998 року, а на Другій міжнародній зустрічі високих представників, що відповідають за питання безпеки (м. Єкатеринбург, 20–21 вересня 2011 року), було представлено попередній текст цієї Конвенції [136].

Занепокоєність Російської Федерації, Китаю та деяких інших великих країн питаннями забезпечення суверенітету при попередженні кіберзагроз обумовлена низкою ініціатив з боку провідних країн і міжнародних безпекових організацій Заходу, пов'язаних із можливістю визнати кібератаки актами агресії, отже, розглядати їх як оголошення (чи початок) війни й відповідно реагувати. Як уже зазначалося, ця ідея була висловлена в рекомендаціях групи експертів з розроблення нової Стратегічної концепції НАТО [135]. У рекомендаціях неодноразово наголошувалося, що через зростання залежності країн-членів від телекомунікаційних технологій і збільшення кількості атак на інформаційну інфраструктуру НАТО має дуже відповідально підійти до питання класифікації кібервійни як дії, що підпадає під статтю 5 Вашингтонського договору. Причому реагування може бути не лише симетричне (кібернетичне), а й воєнне (кінетичне).

Незважаючи на те, що до остаточного варіанту Стратегічної концепції оборони та безпеки членів Організації Північноатлантичного договору від 19 листопада 2010 року [420] такі радикальні пропозиції так і не увійшли, документ зафіксував важливість кібербезпекової проблематики для НАТО у стратегічній перспективі. Так, у статті 12 Стратегічної концепції зазначено, що «кібератаки стають дедалі частішими, організованішими та збитковішими для державних установ, підприємств, економіки і, можливо, також транспортної й електричної мереж та інших об'єктів критичної інфраструктури; вони можуть сягнути критичного рівня, який загрожує національному і євроатлантичному процвітанню, безпеці та стабільності. Джерелом таких атак можуть бути іноземні військові й розвідувальні служби, організовані

[27] Докладніше див. підрозділ 3.3.

злочинні угруповання, терористичні та/або екстремістські групи». У статті 19 (підпункт 8) перелічуються орієнтовні засоби, за допомогою яких має реалізовуватися кібербезпека членів Альянсу: «розвивати й надалі наші можливості щодо запобігання, виявлення, захисту й відновлення від кібератак, зокрема у спосіб використання процесу планування НАТО для поліпшення та координації національних можливостей кіберзахисту, охоплюючи всі органи НАТО централізованим кіберзахистом, а також ліпше інтегруючи кіберобізнаність, попередження й реагування з державами – членами Альянсу».

На виконання зазначених пунктів Стратегічної концепції в липні 2011 року міністри оборони країн-членів Альянсу ухвалили Нову політику кібербезпеки [378]. Також було анонсовано подальше розроблення Плану дій з упровадження Нової політики на практиці. Таким чином, можна констатувати, що НАТО поступово посилює свою політику у сфері кібербезпеки та готується до виконання проголошених групою експертів рекомендацій.

Незважаючи на те, що подібні ідеї досі не мають суттєвої підтримки світового товариства, безпекознавці, зокрема юристи-міжнародники, дедалі наполегливіше працюють над такими ініціативами. Наприклад, у 2013 році за загальною редакцією американського юриста-міжнародника М. Шмітта (*Michael N. Schmitt*) вийшов друком «Талліннський підручник з міжнародного законодавства щодо кібервійни» [407], в якому пропонуються конкретні підходи до використання положень чинного міжнародного права для визнання кібератак «актами агресії». І хоча на даний момент це, швидше, загальнотеоретична побудова, яку навряд чи дійсно зможуть використати на практиці навіть зацікавлені сторони, однак як науково відпрацьоване питання загальної стратегічної концепції реформування міжнародного законодавства цей документ може справити певний вплив. Видання було різко розкритиковане російськими фахівцями з інформаційної безпеки під час Сьомого міжнародного форуму «Партнерство держави, бізнесу та громадянського суспільства при забезпеченні міжнародної інформаційної безпеки» та Сьомої наукової конференції Міжнародного дослідного консорціуму з інформаційної безпеки. На цій конференції з критикою виступив представник Міністерства оборони РФ, який зазначив, що саме факт обговорення правил ведення війни в кіберпросторі й легітимізує ці кібервійни. Російська сторона дотримується думки, що необхідно не допускати виникнення кібервійн, а для цього працювати над за-

ходами, спрямованими на підвищення довіри та ухвалити правила поведінки держав у кіберпросторі [48].

Подібною до політики Альянсу у сфері забезпечення кібербезпеки є також офіційна політика США. Її логічним наслідком стала запропонована 16 травня 2011 року вже згадувана Міжнародна стратегія для кіберпростору [325], яка стверджує, що США залишають за собою право на самозахист відповідно до положень установчих документів ООН та у відповідь на загрозу своїй інформаційній інфраструктурі готові застосовувати «дипломатичні, інформаційні, воєнні та економічні» засоби реагування на інциденти. Керівництво США запропонувало цей документ як глобальну ініціативу й фактично закликає усіх своїх партнерів приєднуватися до такого бачення майбутнього кіберпростору. Документ також акцентує увагу на діяльності США щодо вироблення міжнародних норм поведінки в кіберпросторі: «Цифровий світ більше не є територією беззаконня, сферою інтересів невеликої групи еліти. Довгострокові міжнародні норми поведінки держав – у періоди миру та конфліктів – застосовувані й у кіберпросторі <...> Ми продовжимо працювати на міжнародній арені з метою вироблення консенсусу щодо норм поведінки в кіберпросторі» [Там само].

Усі дискусії щодо застосування норм міжнародного права до подій у кіберпросторі та потреби вироблення відповідної поведінки відбуваються на тлі концептуальної термінологічної невизначеності й відсутності загальновизнаних юридично значущих критеріїв віднесення кібератак до таких, що можуть бути кваліфіковані як «акт війни» або «застосування сили».

Як зазначалося вище, в науковій літературі досі не визначеним є зміст понять *кіберпростір*, *кібербезпека*, *кібератака* тощо. Активне використання цих понять у політичних колах також не вирішує проблеми, адже жодних офіційних трактувань даної термінології не існує, а це змушує кожну країну самостійно виробляти підходи в цій сфері [65].

Незважаючи на те, що проблемі ідентифікації кібератак приділяється менше уваги (принаймні публічної), насправді вона є навіть важливішою, ніж перша. Основна дискусія точиться довкола питань можливості прирівнювання актів кіберагресії[28] (*cyberattacks*) до тих актів «застосування сили» (*use of force*), що підпадають під дію стат-

[28] Поняття так само не визначене.

ті 2 (пункт 4) Статуту ООН [206], та можливості ототожнення кібератак зі «збройними нападами», що підпадають під дію статті 51 Статуту ООН.

Досі незрозуміло, чи припустимо поширювати на кібервійни традиційне міжнародне «право війни», покликане, з одного боку, попереджати виникнення війн як крайнього способу розв'язання міжнародних конфліктів із застосуванням збройного насильства («право розв'язати війну» – *jus ad bellum*), а з іншого – відрегулювати «правила війни» (*jus belli*), мінімізувати втрати поміж цивільного населення, руйнування цивільної інфраструктури тощо.

Відповідно до Резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 року [146] «агресією є застосування збройних сил державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави, або будь-яким іншим способом, несумісним зі Статутом Організації Об'єднаних Націй, як це встановлено в цьому визначенні» (стаття 1). У Резолюції також подано список дій, що в будь-якому випадку будуть кваліфіковані як «акти війни» (стаття 3):

• вторгнення чи напад збройних сил держави на територію іншої держави чи будь-яка військова окупація, який би тимчасовий характер вона не мала, яка є результатом такого вторгнення чи нападу, або інша анексія з використанням сили території іншої держави чи її частини;

• бомбардування збройними силами держави території іншої держави чи використання будь-якої зброї державою проти території іншої держави;

• блокада портів чи берегів держави збройними силами іншої держави;

• напад збройними силами держави на сухопутні, морські або повітряні сили чи морські та повітряні флоти іншої держави;

• використання збройних сил однієї держави, що перебувають на території іншої держави за її згодою, в порушення умов, передбачених угодою, чи будь-яке продовження перебування на такій території після припинення дії угоди;

• дія держави, яка дозволяє, щоб її територія, яку вона надала в розпорядження іншій державі, використовувалася для здійснення акту агресії проти третьої держави;

• засилання державою чи від її імені озброєних банд, груп, іррегулярних сил чи найманців, які здійснюють акти застосування збройної

сили проти іншої держави та мають настільки серйозний характер, що це рівнозначно перерахованим вище актам, чи значна участь у них.

Як бачимо, більшість цих визначень так чи інакше передбачає фізичний контакт двох держав, найчастіше – із застосуванням кінетичної зброї. Кібератаки (вже через саму невизначеність національного кіберпростору) є розпорошеними, встановити суб'єкта їх здійснення (державні органи, збройні силам держави) часто неможливо. Крім того, виконавці кібератак найчастіше вміло маскують свої дії, створюючи складні ланцюги виконавців, що дозволяє видавати за авторів атак інших осіб (або держави). Це може призвести до того, що автором атаки буде визнано іншу державу й відповідно саме до неї буде застосовано всі потенційно можливі санкції [71].

Одним зі способів вирішення проблеми є визнання кіберзброї формою традиційної зброї. Це дозволило б вирішити політичну частину проблеми (можливість застосовувати до кібернападів визначення *агресії* та *акту війни*), перевівши її в суто технічну площину – гарантованого визначення джерела атаки та надання міжнародному товариству однозначних доказів її здійснення.

Водночас існує й інший варіант – розроблення методологічних підходів, які дозволили б уже зараз співвіднести кібернапади з поняттям *застосування сили*. Зокрема, такі підходи розробляє і професор М. Шмітт [405]. Він звертає увагу на один з основних предметів дискусії при ідентифікації кібератак[29]: коли саме кібератака може розглядатися з позиції міжнародного права, зокрема Статуту ООН, як використання сили? Для поєднання «комп'ютерних мережевих атак» з об'єктами чинного міжнародного права дослідник пропонує використовувати шість критеріїв, що порівнюють наслідки звичайної та мережевої атак [Там само, с. 18-19]:

• **небезпека *(severity)***. Збройні напади призводять до фізичних травмувань чи псування майна набагато частіше, ніж інші форми примусу. Фізичне благополуччя зазвичай посідає верхівку в ієрархії людських потреб;

• **миттєвість *(immediacy)***. Негативні наслідки збройного нападу чи загрози, як правило, настають раптово на відміну від інших форм насилля, для яких притаманна поступовість. Тому ймовірність для держави-об'єкта чи світового товариства досягти мирного компромісу зазнає перешкод;

[29] У роботах дослідника йдеться про «комп'ютерні мережеві атаки».

• **очевидність (*directness*).** Наслідки збройного нападу набагато очевидніше пов'язані із вчиненням протиправних дій, ніж інші види примусу, що часто залежать від інших супутніх обставин. Таким чином, заборона використання сили з більшою ймовірністю відвертає негативні наслідки;

• **інвазивність (*invasiveness*).** Під час збройної атаки шкода зазвичай заподіюється на території держави-об'єкта, тоді як в економічній війні основні дії відбуваються поза межами даної держави. У результаті, хоча військові й економічні дії можуть мати приблизно однакові негативні наслідки, у разі збройної атаки спостерігається більше втручання в права і, як наслідок, справляється більший негативний вплив на міжнародну стабільність;

• **вимірність (*measurability*).** Тоді як обсяг наслідків збройного нападу, як правило, можна легко визначити (наприклад, з'ясувати обсяг руйнувань), фактичні негативні наслідки інших видів насилля виміряти складніше. Факт збройного нападу викликає загальний суспільний осуд і невдоволення. Він менше піддається сумніву, ніж у разі застосування збройних сил;

• **презумпція законності (*presumptive legitimacy*).** Здебільшого відповідно до внутрішньодержавного чи міжнародного права застосування насилля вважається незаконним, крім випадків самооборони. Це когнітивний підхід заборони.

На практиці дана структура застосовується в такий спосіб: при визначенні відповідності кібератаки рівню, який може потрапляти під дію міжнародних нормативних документів (Статуту ООН), варто порівнювати її наслідки з можливими наслідками збройного насильства (за допомогою усереднених коефіцієнтів збитку). Якщо наслідки від кібератаки є аналогічними тим, що можуть настати від використання зброї, то будь-яка відповідь у межах міжнародного законодавства, в тому числі воєнна, може бути законною. Якщо ні – мають застосовуватися інші механізми реагування. М. Шмітт наводить кілька прикладів застосування методології [405, с. 19–20].

1. Під час складних погодних умов у результаті кібератаки було вимкнено систему управління повітряним рухом, що призвело до катастрофи авіалайнера та загибелі пасажирів. Кінетична сила не була використана для знищення літака, однак саме кібератака була безпосередньою причиною трагедії. Тому ця дія має розглядатися як застосування сили, оскільки тяжкість наслідків, висока смертність і фізичне знищення прирівнюють дану ситуацію до збройного насилля. І хоча

об'єктом атаки став не безпосередньо літак, однак саме виведення з ладу системи управління спричинило його знищення. Наслідки атаки легко вимірювані (з погляду людських і майнових втрат).

2. Здійснено кібернапад на університетську комп'ютерну мережу з метою зірвати дослідження, що здійснюються на замовлення військових. Рівень загроз атаки, якщо її розглядати з погляду загальних цінностей, значно нижчий, ніж у разі збройного примусу. Жодного вимірюваного майнового збитку не завдано, відсутні фізичні страждання (втрати), принаймні в короткостроковій перспективі. Орієнтовний бажаний результат зловмисників – зниження можливостей противника на полі бою, однак визначення наслідків пов'язане з низкою невизначених чинників, з-поміж яких можливість відновити втрачені дані, існування інших дослідних груп, що займаються тією самою науковою проблемою, ймовірність подальшого фінансування проекту тощо. І хоча сама атака, безумовно, є злочином, однак підрахувати наслідки дуже складно. Отже, подібна атака не підпадає під визначення використання сили і поширення на неї відповідного міжнародного правового інструментарію є недоречним.

Водночас дослідник наголошує, що ця методологія є лише проміжним етапом у розбудові принципово нової архітектури міжнародних правових документів, які б суттєво розширили поняття *застосування сили* відповідно до нових викликів у сфері безпеки. Характерно, що вперше методологію було запропоновано ще в 1999 році, однак відтоді суттєвих удосконалень міжнародного законодавства, крім зазначених вище, не відбулося.

Запропонована М. Шміттом методологія має один суттєвий недолік: вона спрямована передусім на встановлення еквіваленту фізичних втрат (знищення об'єктів, загибель людей), однак мало застосовувана до інших (наприклад, економічних) наслідків. 2003 року група дослідників використала методологію М. Шмітта для моделювання можливого кібернападу терористів на систему управління метрополітеном м. Вашингтона (зіткнення поїздів, загибель 30 людей) [Там само]. У цьому випадку методологічну рамку було застосовано цілком вдало: порівнюючи потенційні наслідки фізичної атаки терористів та аналогічної кібератаки, дослідники дійшли висновку про їх практичну ідентичність. Натомість для кібератак, яких зазнали свого часу Естонія та Грузія (саме ці приклади найчастіше згадуються в безпекових документах країн Заходу), такий підхід практично не можливо застосувати.

Незважаючи на описану вище невизначеність щодо кібератак і потенційних кібервійн, сучасні дослідники розглядають останні як частину безпекової реальності, на яку доведеться зважати найближчим часом. Розробляються окремі механізми структурування кіберконфліктів і пропонуються відповідні правила поведінки. Так, на Мюнхенській конференції з питань безпеки 21 лютого 2011 року [288] відбулася презентація спільного американсько-російського дослідження у сфері протидії наслідкам протистояння в кіберпросторі [452].

У доповіді йдеться про необхідність юридичного визначення «правил бою» в кіберпросторі. Рекомендується внесення відповідних змін до Женевських і Гаазьких конвенцій з урахуванням реалій кібервійн, оскільки відсутність юридично прийнятного визначення змісту поняття *кібервійна*, її компонентів та принципової відмінності від традиційних війн, уповільнює створення погодженої міжнародної політики боротьби із цими війнами, що отримали умовну назву «цифрового бліцкригу», або «цифрового Перл-Харбору», та їх імовірно катастрофічними наслідками.

Доповідь *East West Institute* закликає до встановлення різного правового статусу для військових і цивільних об'єктів у кіберпросторі й забезпечення більшої безпеки «певних ключових доменів». Також у ній ідеться про поширення на кібервійни Женевських конвенцій[30] нового покоління, в яких розвиваються нинішні міжнародно-правові норми щодо захисту жертв війни.

Призначенням конвенцій нового покоління передусім є:

• відокремлення мирних об'єктів кіберпростору воюючих сторін від немирних за допомогою спеціальних маркерів на зразок червоного хреста (півмісяця, кристала);

• виокремлення «заборонених прийомів» кібервійни у спосіб прирівняння їх до міжнародно-правових заборон деяких особливо негуманних видів зброї на зразок хімічної чи бактеріологічної;

• визначення особливого правового статусу держав, що перебувають у стані кібервійни.

Головне питання, до якого привертає увагу зазначений документ, – можливість законодавчого й технологічного виокремлення захищених об'єктів гуманітарної інфраструктури кіберпростору від незахи-

[30] Відповідні норми закріплені в Гаазькій конвенції 1899 року та 1907 року і конвенціях, підписаних у Женеві в 1864, 1906, 1929 й 1949 роках.

щених. Саме так, як цивільні об'єкти користуються захистом міжнародних домовленостей під час війни.

Автори документа пропонують встановлення спеціальних кібермаркерів для позначення захищених зон кіберпростору, подібних до маркера червоного хреста (півмісяця, кристала), яким під час воєнних дій традиційного типу маркуються захищені міжнародним правом цивільні об'єкти (транспортні засоби, шпиталі тощо).

Крім того, міжнародним органам належить вирішити, яку кібернетичну зброю (віруси, «трояни» тощо) слід вважати аналогом зброї, забороненої Женевським протоколом (наприклад, отруйних газів).

Таким чином, можна дійти висновку, що формування кібербезпекового сектору (і особливо в нормативно-правовій частині) як на національному, так і міжнародному рівні триває. Цей процес стикається з низкою проблем, обумовлених інноваційним характером кібербезпекової проблематики. Сутнісними проблемами стають термінологічна невизначеність і неготовність чинної міжнародно-правової бази дати відповідь на нові загрози. Окремі зусилля (на кшталт прийняття Конвенції про кіберзлочинність) залишаються лише обмежено успішними через неготовність усіх країн повноцінно приєднатися до них. Додатковою проблемою стає концептуальна розбіжність поглядів основних геополітичних гравців на природу та правила поведінки в кіберпросторі.

Має місце брак методологічних підходів для адаптації кібернападів до чинної нормативно-правової бази. Запропоновані окремими науковцями методологічні межі становлять значний інтерес, однак досі є фрагментарними.

Зростаюча активність прихильників «радикального» підходу до кібератак – розуміння кібератак як «акту війни» з відповідними наслідками – дозволяє припустити, що тема кібератак і кібервійни в подальшому становитиме значущу частину дискусій світових геополітичних гравців.

Висновки до розділу

У цілому можна констатувати, що кібербезпекова проблематика дедалі активніше стає не лише проблемою суто національного рівня, а й частиною великих геополітичних протистоянь.

Держави ініціюють щодалі активнішу політику щодо посилення своєї кібербезпеки й шукають механізми використання вразливостей

у кібернетичному просторі інших країн для посилення свого глобального домінування. Кібермогутність як основа реалізації національних інтересів держави у глобальному кіберпросторі набуває значущості, а її теоретичні обґрунтування стають дедалі цілеспрямованішими. З наявних на сьогодні підходів до розуміння кібермогутності найбільш адекватним і цілісним є, на нашу думку, китайсько-японський підхід. У його межах пропонується масштабний перелік дій, які не лише сприяють збільшенню кібермогутності держави, а і спричинюють її економічне зростання.

Маємо констатувати, що протиборство держав у глобальному кіберпросторі є надзвичайно активним, про що свідчать, зокрема, факти створення спеціальних кіберпідрозділів у різних країнах та збільшення коштів, що вкладаються в забезпечення кібербезпеки.

Водночас кібербезпекова сфера має низку принципових невирішених питань, зокрема термінологічних та нормативно-правових.

Незважаючи на активне використання різноманітних понять із частиною *кібер* дотепер відсутнє цілісне розуміння навіть базового поняття *кіберпростір*, не кажучи про більш серйозні й масштабні, зокрема *кібервійна*, *кібератака*, *кібердиверсія*, *кібертероризм* тощо.

Це спричинює формування нормативно-правової проблеми, невирішеність якої не дозволяє ані на національному, ані на міжнародному рівні виробити загальноприйняту модель протидії кіберзагрозам і мінімізації можливостей мілітаризації кіберпростору. Хоча при цьому мають місце спроби окремих держав прирівняти кібератаки до дій, що підпадають під дію Статуту ООН у частині визначення «актів війни». Подібна діяльність поширюватиметься надалі і, швидше за все, матиме далекосяжні наслідки для всієї світової спільноти.

Розділ 2.

СУЧАСНІ КОНФЛІКТИ В КІБЕРПРОСТОРІ. У ПЕРЕДЧУТТІ «ХОЛОДНОЇ ВІЙНИ *V*2.0.»

2.1. Відносини США – КНР як ключовий геополітичний наратив початку XXI сторіччя: співробітництво, суперництво, протистояння?

Сучасні геополітичні умови характеризуються, з одного боку, очевидною постбіполярною невизначеністю, а з іншого – виразним глобальним трендом зміщення фокусу геополітичного впливу з Європейського до Азіатсько-Тихоокеанського регіону. Як цілком справедливо зазначає Юй Сяотун[31], «на початку XXI сторіччя у Східній Азії сформувався новий розподіл сил, за якого визначилися лідируючі ролі двох великих держав – Китаю та США, а також другорядні ролі Японії, Південної Кореї та Росії» [199]. Водночас, на нашу думку, майже аналогічне співвідношення ролей характерне й на більш глобальному рівні, з додаванням до групи країн «другорядних ролей» Німеччини, Великобританії, Франції та Індії.

Розглядаючи кібербезпекову тематику в більш широкому контексті глобальних політичних процесів, виходимо з того, що світ лише формує нову геополітичну модель, перебуваючи в постбіполярній невизначеності. Доволі короткий період американського унілатералізму, що постав на руїнах біполярної моделі, був суттєво скорегований кількома ключовими чинниками, зокрема:

• відсутністю дійсно сформованої та узгодженої політики Європейського Союзу щодо його майбутнього за одночасного бажання відігравати більш значну роль на міжнародній арені;

[31] Російський дослідник.

• частковим відновленням Росії на початку 2000-х років як щонайменше регіонального лідера з амбіціями світового гравця;

• загальним зростанням економік країн, що входять до БРІКС;

• якісним та кількісним зростанням економіки КНР, що поступово перетворює цю країну не просто на світового лідера, а й на реальну противагу США як єдиної надсили;

• низкою зовнішньополітичних помилок США, передусім на Близькому Сході та в Північній Африці.

У таких умовах можливості (а з огляду на певні національні інтереси – змушеності) США підтримувати статус «світового жандарма» обмежуються, а здійснення ними зовнішньополітичних акцій доводиться узгоджувати з дедалі більшою кількістю зацікавлених сторін. За президентства Б. Обами спостерігається послідовна політика відмови від активної ролі на зовнішній арені з переорієнтуванням на внутрішні проблеми країни. Це цілком природно, зважаючи на глобальну фінансово-економічну кризу 2008–2009 років, наслідки якої досі змушують США переглядати свою бюджетну політику в напрямі економії та зменшення дефіциту бюджету.

На цьому тлі КНР демонструє не просто стабільне зростання економіки, а й побудову дійсно розвинутої держави (зокрема у сфері високих технологій та високотехнологічних виробництв), яка вже зараз вдало конвертує ці здобутки у військову могутність. Протягом останніх двадцяти років Китай подолав неабиякий шлях від країни, що розвивається, до другої світової економічної сили та другими після США видатками на армію. Іншою цікавою особливістю, яка сприяла посиленню Китаю, стало, на думку деяких дослідників, зокрема О. Ломанова [113], те, що політична система КНР, незважаючи на всі апокаліптичні прогнози прибічників теорій демократичного розвитку, залишається стабільною і, що більш важливо, передбачуваною. Дослідник визначає як причину цього набагато більшу, ніж у режимах Близького Сходу, гнучкість колективного керівництва Політбюро ЦК КПК та обмеження терміну перебування на китайському політичному Олімпі 10 роками. При цьому передача влади новій владній команді відбувається спокійно та мирно. Саме ця модель самим фактом свого існуванням створює ідеологічну конкуренцію розвинутим демократичним суспільствам.

Водночас дискусійним, однак від цього не менш важливим, є питання стосовно реальних планів КНР щодо трансформацій глобального геополітичного простору, свого місця в цих трансформаціях і дійсного напряму актуальних геостратегій Китаю.

Міркуючи про основи нинішньої зовнішньої й безпекової політики КНР більшість дослідників одностайні в думці, що багато в чому ця політика детермінована культурною спадщиною Китаю [211]. Саме цей «культурологічний» елемент становив підмурівок того, що називають концепцією «м'якого піднесення» – концепції, сформульованої у 2003 році під час виступу Чжен Біцзяня (*Zheng Bitszyan*), який у 90-х роках XX сторіччя очолював відділ пропаганди ЦК КПК та довгий час є проректором Центральної партшколи КПК [108]. Концепція стала провідною ідеєю для всього часу керівництва Ху Цзіньтао і мала на меті м'яко трансформувати ідеї Ден Сяопіна щодо необхідності «ховати в темряві свої можливості», адаптувавши їх до нових геополітичних реалій. У такий спосіб Китай хотів пояснити світу, що його зростання не є небезпечним для сусідів. Уповні цю концепцію було викладено в книзі Ся Ліпіна (*Xia Lipin*) та Цзянь Сіюаня (*Jian Siyuanya*) «Мирне піднесення Китаю» [Там само], в якій КНР описується як «відповідальна велика держава», зацікавлена в мирних зовнішніх умовах для свого розвитку і здатна своєю чергою сприяти миру та стабільності в Азіатсько-Тихоокеанському регіоні. Досягнення зазначених цілей ґрунтується на таких ключових положеннях «мирного піднесення»: опора на власні сили, на внутрішній ринок, на трудові та фінансові ресурси, взаємовигідна співпраця із зовнішнім світом. Ключовим у «мирному піднесенні» є питання розбудови, з одного боку, ефективних двохсторонніх відносин із США із широкого кола питань (у тому числі щодо Тайваню), а з іншого – багатосторонніх відносин як у регіональному (КНР – Японія – США), так і в міжнародному вимірі (КНР – Європа – США та КНР – *G*8 – НАТО).

У цілому концепція виконувала важливу роль за кількома напрямами. Передусім вона принаймні на 10 років зафіксувала саморепрезентативний статус КНР як регіонального лідера, «відповідальної великої держави», яка будує відносини заради мирного зростання, намагаючись уникати складних питань на кшталт Тайваню. До певної міри це збігається і з певними зовнішньополітичними орієнтирами щодо КНР. На думку російського дослідника І. Зевельова, керівництво США здійснює курс, спрямований на те, щоб стимулювати залучення Китаю до світових процесів як відповідального гравця й одночасно стримувати його військову міць. Цей підхід політики Б. Обами базується на концепції, яка склалася за Дж. Буша-мол.: зробити КНР «відповідальним утримувачем акцій» ліберального світо-

порядку в поєднанні з хеджуванням ризиків, пов'язаних зі зростаючою міццю Пекіна [80].

Водночас зміна керівництва КНР у 2013 році – обрання на посаду Голови КНР Сі Цзиньпіна – може спричинити певне корегування концепції.

У цьому сенсі цікавою була зустріч між Сі Цзіньпіном та Б. Обамою в межах американсько-китайського саміту в Каліфорнії 7-9 червня 2013 року. Американські оглядачі вже напередодні цієї події акцентували увагу на незвичності подібного формату для американсько-китайських відносин, оскільки зазвичай лідери цих країн зустрічаються для обговорення широкого кола питань, які мають бути вирішені у вкрай короткі терміни. Каліфорнійський саміт, навпаки, надав можливість максимально глибоко проговорити найскладніші двосторонні питання.

Пошук нового формату співробітництва між двома державами відображає їх новий статус: США, які дотепер багато в чому залишаються єдиною наддержавою, розуміють необхідність пошуку унікального формату спілкування та взаємодії із сучасним Китаєм, який, вочевидь, відтепер не є суто регіональним лідером, однак не хоче набувати і статусу наддержави.

Відповідно цей стан і сформулював ключове питання саміту – майбутнє двосторонніх відносин Китай – США. Напередодні саміту сторони в цілому озвучили свої позиції як щодо ключових тем, так і щодо формату їх обговорення. Зокрема, офіційну позицію США щодо нової КНР було сформульовано як встановлення «тісних стратегічних зв'язків між військовими обох країн, базованих, швидше, на спільних, аніж на суперницьких зусиллях у вирішенні регіональних проблем Азії» [Цит. за: 138].

І хоча складно було однозначно говорити про ключовий меседж цього обговорення заздалегідь, однак професор-міжнародник Народного університету Ши Янхун (*Jian Siyuanya*) (його часто залучають до консультування уряду Китаю) зазначив, що з боку керівника КНР ключовим повідомленням буде «донести до американського президента думку, що Вашингтону слід визнати драматичне зростання Китаю, як в економічній, так і у військовій сфері, визнати активність Пекіна у світовій дипломатії» [Там само].

На нашу думку, показовим є те, що чи не вперше тематика кібербезпеки і передусім взаємної кіберактивності США та КНР стала предметом спілкування керівництва двох держав. Це питання при-

родно постало на порядку денному, зокрема, тому, що безпосередньо напередодні саміту (6 червня) розгорнулася ініційована Е. Сноуденом викривальна кампанія довкола масового несанкціонованого збору даних АНБ та ФБР США.

Уже після першого дня зустрічі під час коротких відповідей Б. Обами та Сі Цзіньпіна на запитання принаймні три перші з них стосувалися саме теми кібербезпеки. У своїй відповіді Б. Обама згадав, що вони з очільником КНР вже зачепили питання кіберпростору [398]. Крім того, як зазначив Б. Обама, США розуміють необхідність вирішити проблему убезпечення кіберпростору на міжнародному рівні, і саме із цього питання двосторонні та багатосторонні домовленості відіграватимуть ключову роль. На нашу думку, особливий сенс цих слів полягає в тому, що коментуючи скандал, який виник довкола масового збору персональних даних АНБ та ФБР, Б. Обама зазначив, що урядові структури й надалі співпрацюватимуть із приватними компаніями заради забезпечення безпеки американців. І це на тлі таких стратегічних питань, як співвідношення китайської та американської валюти, територіальних суперечок КНР та Японії тощо.

На думку деяких американських експертів, це цілком може спричинити більш серйозну двосторонню дискусію, принаймні щодо «правил у сфері кібершпигунства» [196]. Водночас навіть ці експерти (наприклад, К. Лібертал (*Kenneth G. Lieberthal*) із Інституту Брукінгс (*Brookings Institution*) погоджуються, що, незважаючи на існування певних зон взаємних інтересів обох держав у кіберпросторі, із цілої низки проблем жодних домовленостей ніколи не буде досягнуто [439].

Незважаючи на це, по закінченні саміту саме тема кібербезпеки стала, на думку обох лідерів, ключовою для подальшого співробітництва. Т. Донілон (*Thomas E. Donilon*), радник президента США з питань національної безпеки, за результатами саміту навіть заявив, що вирішення проблем у сфері кібербезпеки є «ключем до майбутнього» американсько-китайських двохсторонніх відносин [443].

Зазначені вище дискусії відбуваються на тлі критичного переосмислення самими США своїх зовнішньополітичних стратегій. Зокрема, на думку американського дослідника Р. Беттса (*Richard K. Betts*), Вашингтон має визначитися, чи вважати Пекін загрозою, яку слід стримувати, чи державою, з якою потрібно уживатися, оскільки на сьогодні «малозрозумілий компроміс – це поширена та іноді розумна дипломатична стратегія. Однак в Азії це означає недооцінювання

ризиків вагання та нерішучості, коли міць Китаю зростає, а його стриманість зменшується» [11].

Саме дискусії щодо бажання (питання можливості постають значно рідше) КНР стати новою наддержавою становлять чи не основне ядро наукових гіпотез стосовно оцінок китайських перспектив розвитку.

На думку багатьох експертів і науковців, геостратегічна концепція КНР спрямована на отримання статусу наддержави та реального закріплення біполярного світу (наприклад, [47]).

Водночас інші дослідники ([76]) з посиланням на внутрішні політичні й медійні дискусії в самій КНР пропонують цілком інше уявлення про прагнення Китаю на міжнародній арені. Зокрема, вказується, що «тотальний виклик США не відповідає планам Китаю. Часто підкреслюється, що не потрібно боротися з Америкою за світову гегемонію. Довгостроковим державним курсом є те, що КНР не стане наддержавою. Одночасно не варто і погоджуватися з американською гегемонією, підлаштовуватися під неї» [Там само].

На особливу увагу заслуговує позиція відомого українського китаєзнавця П. Ленського [112], що звертає увагу на позицію тих китайських аналітиків, які ключовими рисами китайської традиційної стратегічної культури визначають її оборонний характер, прагнення одержати перемогу без війни.

Говорячи про довготермінові геостратегії США щодо КНР, частина дослідників [226] звертається до концепції «стримування через залучення» – розширення участі КНР у різнорівневих політичних та економічних регіональних проектах, що зробить поведінку Пекіна більш прогнозованою та контрольованою завдяки підвищенню його статусу як відповідального члена міжнародного товариства. При цьому О. В. Шевчук цілком слушно зазначає, що американська зовнішньополітична стратегія щодо КНР має суперечливий характер і є, швидше, реакцією на конкретні обставини, ніж складником загальної стратегії, спрямованої на просування інтересів США. Можна припустити, що це цілком може бути обумовлено стрімкістю процесів геополітичних змін, особливо протягом останніх 10–15 років.

На нашу думку, найбільш раціональним поясненням сьогоднішніх геостратегічних відносин США та КНР є позиція, артикульована китайськими експертами: «хоча між Пекіном та Вашингтоном існують серйозні протиріччя, ми не перетворилися на супротивників, можемо та повинні нарощувати співробітництво. Розширення західних вій-

ськових союзів не означає їх націленість на розв'язування агресивних війн. Разом з тим складно не визнати, що до процесів, які відбуваються, не варто ставитися надто поблажливо, розраховуючи на нестабільність НАТО й американсько-японського союзу, на те, що вони самі собою стануть слабкішими» [Цит. за: 76]. Схожу думку висловлюють й інші експерти, акцентуючи увагу на тому, що «відносини КНР та США багато хто в Китаї вважає пріоритетними в усій китайській зовнішній політиці та найважливішими з усіх двосторонніх відносин у сучасному світі» [77]. Вони зазначають, що «у своїй стратегії Пекін намагається всебічно уникнути лобового протистояння зі США. Тут він використовує методи класичної китайської дипломатії – поступатися стратегічною ініціативою в обмін на привабливе проміжне положення, що передбачає балансування між основними носіями протиріч» [Там само].

Таким чином, на відміну від «старого» геополітичного протистояння США та СРСР з домінантною концепцією «жорсткого протистояння» в новій геополітичній реальності такою концепцією стає «суперництво», причому в усіх площинах – економічній, політичній, культурній та військовій [60]. Очевидне переважання стратегій суперництва в американсько-китайських двосторонніх відносинах засвідчують і китайські дослідники. Зокрема, дослідник Чжань Веньму (*Zhan Venmu*) зазначає, що «конфронтація США та КНР не має системного, глобального характеру. Сьогодні китайсько-американський конфлікт – це зіткнення національних поточних інтересів, а не довгострокові протиріччя» [Цит. за: 110, с. 123]. Хоча в іншому місці він зазначає, що це *протистояння*, хоча й не базоване на реальному конфлікті ідеологій чи відмінностях політичних систем, проте має в основі геополітичні суперечності. Про «тривале стратегічне суперництво» між двома державами зазначає і американський науковець Е. Голдштейн (*Avery Goldstein*), зазначаючи, що «загострення такого суперництва хоч і можливе, але не обов'язкове» [43, с. 77].

На таку стратегію «суперництва» (причому навіть радикальнішу) звертає увагу і Н. О. Жданова [77], коли стверджує, що протягом 1990-х–2000-х років уся стратегія Китаю у сфері міжнародних відносин була спрямована на зміщення центру геополітичного суперництва в бік невійськових методів утвердження власної сили та авторитету – культурних, економічних, інформаційних, психологічних. Отже, «м'яка сила» використовується як основний механізм реалізації власних інтересів.

Ще в 2006 році на цю особливість нових американсько-китайських відносин звертали увагу й дослідники із Центру стратегічних та міжнародних досліджень: «Багато хто [з китайських лідерів – *Авт.*] підозрює, що США намагаються спрямувати КНР шляхом СРСР, який і Китайську державу призведе до колапсу та розпаду. Китай постійно виявляє обережність, аби не повторювати помилок СРСР. Свідченням цього є відмова від гонки озброєнь із США, небажання вступати з ними в ідеологічні протиборства, а також концентрування зусиль на економічному розвитку з відкладанням драматичних політичних реформ на майбутнє» [10, с. 173].

Коли йдеться про відмінності між «суперництвом» та «протистоянням», мається на увазі принципова відмінність між цими базовими поняттями. Словники таким чином тлумачать «протистояння»: «бути протиставленим, відрізнятись по суті, за сутністю». Тобто *протистояння* визначає принципово відмінні позиції, що характеризуються повною протилежністю сторін у певній сфері. І са́ме *протистояння* характеризувало відносини між США та СРСР періоду «холодної війни» – протистояння ідеологічне, економічних моделей тощо. Натомість «суперництво» за тим самим словником – це «намагання перевершити когось у чомусь», причому «суперники» є рівними у своїх правах та можливостях. І це вже значно більше схоже на нинішню ситуацію, в якій обидві сторони не стільки жорстко протистоять одна одній, скільки змагаються за досягнення зрозумілих цілей у глобальному масштабі.

Своєрідне резюме наведеним вище підходам до американсько-китайських відносин зводиться до того, що в умовах зростання потенціалу КНР, здійснення його політики, спрямованої на поступове утвердження в сучасній геополітичній ситуації, двосторонні відносини двох великих держав можуть розвиватися лише в контексті суперництва, однак не протистояння. Такої самої думки дотримується й Г. Кіссинджер (*Henry Kissinger*): «Обидві сторони [США та КНР – *Авт.*] мають бути готові сприймати діяльність один одного як природну частину міжнародного життя, а не привід до занепокоєння. Невідворотна тенденція до зіткнення не повинна прирівнюватися до усвідомленого прагнення стримувати чи домінувати, поки сторони здатні розрізняти ці поняття та відповідно порівнювати свої дії. Китаю та США необов'язково вдасться вийти поза межі звичного процесу суперництва великих держав. Однак заради самих себе та миру вони повинні принаймні спробувати це зробити» [94].

Спробу пояснити наявний стан американсько-китайських відносин з погляду класичної геополітики зробив Е. Долман: «На перший погляд здається, що геополітичні сили є в динамічній рівновазі. США – це ключова морська та повітряна сила, орієнтована на напад, швидкий маневр і точний удар, що надасть перевагу у війні. На противагу їм КНР – це потенційно найбільша сухопутна держава, оборона якої залежить переважно від сухопутних сил. Жодна з них не має визначної переваги щодо іншої. Відповідно, немає жодного правдоподібного короткострокового сценарію, в якому США може вторгнутися в КНР і підтримувати окупацію її материкової частини. Аналогічно США убезпечені від вторгнення та окупації китайськими силами» [294, с. 82]. При цьому дослідник додатково зазначає, що «США та КНР пов'язані надзвичайно тісно. Китайські ринки відкриваються і, власне, саме продуктивність виробництва в КНР дозволила США перейти до постіндустріальної економіки. Істотно зростає торгівля. І саме Китаю найбільше заборгували США. Усе це вже зараз обумовлює уникнення конфліктів між державами, що можуть розірвати чи послабити ці зв'язки. Незважаючи на політичні розбіжності між китайським комунізмом і західним ліберальним демократичним капіталізмом, обидві сторони явно цінують людські зв'язки та міждержавні відносини. У цих двосторонніх відносинах цікавим чином поєднано американські технологічні новації та китайська праця, базована на специфічній духовній етиці» [Там само].

Такі особливі відносини між двома потужними країнами яскраво ілюструють дві, хоч і периферійні, однак показові події. Причому обидві так чи інакше стосуються кібербезпекових питань.

Перша з них мала місце наприкінці травня 2013 року, коли під час саміту *Shangri-La Dialogue* в Сінгапурі відбулося своєрідне зіткнення між представниками Пентагону та китайськими військовими. Під час свого виступу на саміті міністр оборони США Ч. Хейгел (*Chuck Hagel*) неодноразово висловлював занепокоєння США щодо зростання кількості кібератак, частина з яких так чи інакше стосується китайських урядових і військових структур. На це директор Центру китайсько-американських відносин у сфері оборони при Академії воєнних наук генерал-майор Яо Юньчжу (*Yao Yunzhu*) запитала, як, на думку Вашингтона, збільшення військової присутності США в Азіатсько-Тихоокеанському регіоні сприятиме зміцненню довірливості в американсько-китайських відносинах [93]. Таким чином, сторони вже

на високому рівні визнають співвідносність кібербезпекових і класичних воєнних питань.

Водночас на тлі цього взаємного обміну незручними запитаннями цікавою є поведінка офіційного керівництва КНР щодо ситуації довкола Е. Сноудена.

Хоча свої офіційні заяви Е. Сноуден зробив на території Гонконгу, офіційний Пекін максимально відсторонився від його діяльності і зробив усе можливе, аби Е. Сноуден якомога швидше залишив територію Китаю. Водночас було очевидно, що КНР не видала б Е. Сноудена американській стороні на запит останньої. Це підтверджує й суто формальна поведінка, яку обрав Китай щодо ситуації. Незважаючи на те, що США надали Китаю документи, в яких Е. Сноудена офіційно звинувачено у шпигунстві, уповноважені структури КНР поставили ці документи в чергу на плановий розгляд подібних запитів, очікуючи додаткових роз'яснень. Звичайно, поки вони надійшли, Е. Сноуден залишив Китай [191].

Понад те, Китай демонстративно закрив очі на саму суть викривальних заяв щодо актів кібершпигунства з боку розвідувальних структур США проти китайських громадян та електронних ресурсів. А між тим факти були доволі показовими: за версією Е. Сноудена, Агентство національної безпеки США проникало на сервери китайських мобільних телефонних компаній і переглядало мільйони текстових повідомлень. Крім того, АНБ «зламувало» десятки комп'ютерів в університеті Ціньхуа (*Tsinghua University*) в Пекіні та комп'ютери *Pacnet* – найбільшої телекомунікаційної компанії зі штаб-квартирою в Гонконзі та Сінгапурі [128].

У цих умовах деякі аналітики зазначають невпинне формування передумов переходу суперництва в протистояння у форматі хоч і доволі умовного, але все ж біполярного світу, де роль СРСР виконує КНР. Наприклад, саме такої думки дотримується російський дослідник Л. Івашов. У своїй роботі «Росія та світ у новому тисячолітті» він зазначає, що «майбутнє світової системи полягає в поверненні до більш стабільної біполярності. При цьому місце другого полюсу дедалі переконливіше посідає Китай» [Цит. за: 126]. Е. Голдштейн із цього приводу зазначає: «Китай та США сьогодні не є супротивниками – принаймні в тому сенсі, як СРСР та США в період холодної війни. Однак ризик кризи насправді значно вищий, ніж якби Пекін та Вашингтон вели безкомпромісну боротьбу» [43, с. 78].

Якщо тренди розвитку принципово не зміняться (а оновлені стратегічні воєнні пріоритети США свідчать при низьку ймовірність подібного розвитку подій), уже в найближчій перспективі світ зіткнеться з оновленою «холодною війною» у вигляді протистояння двох світових сил. Схожість ситуації з «холодною війною» між СРСР та США засвідчує і Я. Бремор (*Ian Bremmer*), президент *Eurasia Group* [447].

Принциповою відмінністю нового протистояння стане існування інформаційного суспільства, процеси розвитку інформаційних технологій та формування «п'ятого» простору протистояння.

«Холодна війна» між СРСР та США характеризувалася високим рівнем латентних загострень на міжнародній арені, непрямими методами боротьби (передусім активізацією розвідувальної діяльності з обох сторін), винесенням конфліктів на територію третіх країн (наприклад, у формі протистоянь за сфери впливу) та гонкою озброєнь.

Кіберпростір суттєво впливає на таку логіку протистояння, не зачіпаючи її основні елементи, однак дозволяючи реалізовувати їх в інший спосіб. Зростання кількості систем, що оперують дедалі більшою кількістю інформації про особу (особливо такої, яка або збирається автоматично, або «добудовується» автоматизованими системами самостійно на базі певних параметрів), украй ускладнює непомітну діяльність сучасних розвідників. Про це свідчить зростання у світі кількості виявлених розвідувальних груп і мереж у різних країнах. Кібершпигунство в таких умовах є чи не найоптимальнішою альтернативою, яка дозволяє обом сторонам підтримувати статус-кво у принципово новому просторі протистояння.

Іншою важливою перевагою кіберпростору стає можливість впливати через нього на цілком реальні об'єкти на території іншої країни, включно із проведенням диверсій на об'єктах критичної інфраструктури. І хоча заклики до підвищення убезпеченості таких об'єктів (у тому числі і їх відключення від мереж загального користування) дедалі голосніші, однак реальність демонструє неготовність їх власників (переважно приватних осіб) відмовитися від зручних, ефективних і сучасних систем управління ними, що базуються, зокрема, на використанні інтернету. Та навіть не підключені до мереж загального користування системи не є у цілковитій безпеці, що наочно продемонструвала ситуація довкола вірусу *Stuxnet*. Додатковою перевагою (або проблемою) для сторін є те, що кіберпростір дотепер практично позбавлений міжнародного правового регулювання, особливо в частині застосування кіберозброєнь. І така ситуація спостерігатиметься

принаймні найближчими роками, попри всі намагання США змінити ситуацію.

Маємо розуміти, що механізми захисту власного кіберпростору, які базуються на суттєвих обмеженнях доступу чи контролі за контентом, хоч і можуть мати ситуативні позитивні ефекти (як це сталося в КНР), проте не вирішують проблему в цілому. Про це свідчить зростання кількості атак на урядові мережі Китаю. Однак і цілковита відкритість, про яку багато говорять прихильники ліберальних парадигм і подібних ідеологічних конструкцій (на кшталт «каліфорнійської ідеології») так само далекі від реального бачення майбутнього, передбаченого для кіберпростору та діяльності в ньому. Тотальна відкритість, незважаючи на її теоретичну обґрунтованість і доцільність для інноваційного розвитку, більше не виправдовує ризики, які вона несе для суспільства в цілому. Відповідно, слід очікувати поступового взаємопроникнення суто рестриктивних (обмежувальних) і «вільних» підходів до відкритості та їх поєднання, можливо, з поширенням саме рестриктивних заходів.

Таким чином, нова «холодна війна», яка фактично вже триває, буде не менш запеклою та жорсткою, ніж попередня, однак матиме і принципово інші риси, які дозволять ідентифікувати її як «холодну війну *v*2.0.».

Схожі думки в контексті зростання ваги кіберпростору висловлюють й інші дослідники у сфері міжнародних відносин. Так, Д. Роткопф (*David J. Rothkopf*), головний редактор видання *The Foreign Policy,* називає [402] новий тип протистояння між США та КНР не «холодною війною» (*cold war*), а «прохолодною війною» (*cool war*) і передусім саме через технології, що застосовуються: «Технології «холодної війни» зробили її неможливою. Технології «прохолодної війни» роблять її непереборною (*irresistible*)» або інакше: «метою «холодної війни» було отримання переваги, яка стане в нагоді при переході на рівень «гарячої» війни або повністю її попередить. Мета «прохолодної війни» – мати можливість завдавати удару, не розв'язуючи «гарячої» війни» [Там само].

Зазначимо, що Д. Роткопф не випадково використовує са́ме слово *cool* на позначення нової війни, оскільки в англійській мові воно має подвійне навантаження: може позначати як «прохолоду», так і бути синонімом слова «крутий». Пояснюючи таку подвійну природу нового типу війни, він вказує на дві ключові причини. З одного боку, вона дійсно «прохолодна», оскільки очевидно є «теплішою»,

ніж «холодна війна», через те, що сторони мало не весь час залучені до наступальних дій, і хоча вони далекі він того, що можна назвати війною, однак намагаються завдати шкоди чи ослабити конкурента, порушуючи його суверенітет. З іншого боку, ця війна дійсно «крута», оскільки в ній задіяно найпередовіші технології, що змінюють саму парадигму конфлікту сильніше, ніж будь-хто з тих, хто брав участь у «холодній війні» [402]. Понад те, особливістю нової війни є те, що, незважаючи на принципово схожі методи протистояння (передусім розвідувальна й контррозвідувальна діяльність), малоймовірним є розірвання сторонами двосторонніх відносин навіть у разі виявлення конкретних кібершпигунів, що було однією з постійних загроз під час класичної «холодної війни». При цьому, на думку Д. Роткопфа, всі «останні попередження» з обох сторін мають користь здебільшого для таких компаній і структур, як *Mandiant* (приватна компанія, що займається дослідженнями у сфері кібербезпеки) та кіберпідрозділам Міністерства оборони США, які отримують додаткові бюджетні кошти.

Особливу небезпеку кіберпротистояння становить в умовах подальшого становлення «інтернету речей» (*Internet of Things*) і ширшого використання «розумних речей», керування якими здійснюється через кіберпростір. Це дозволяє завдавати ударів по найнеочікуванішим цілям з мінімальним ризиком бути впійманим. Як зазначає Д. Роткопф, «це лише початок. Це нова гра. Безумовно, вона включатиме дедалі нові неочікувані повороти, які вже змусили гравців із КНР та США переосмислити рівень небезпеки нової гри порівняно зі старими підходами. Однак маємо розуміти, що ми знаходимося на середині дороги переосмислення природи сили націй» [Там само].

Про кіберпротистояння як про новий тип «холодної війни» говорить і професор Університету штату Нью Йорк у Буффало Р. Діперт (*Randall R. Dipert*), який вважає, що «вже сьогодні ми перед обличчям довгої «холодної кібервійни» (*Cyber Cold War*), яка характеризується хоч і обмеженими, однак частими пошкодженнями інформаційних систем» [275]. Так само «холодною кібервійною» називає зростаючу кількість кіберінцидентів і дослідник Д. Редкліф (*Deb Radcliff*) [275]. Саме в термінах «холодної війни *v*2.0.», однак у ширшому колі учасників, описує нове протистояння і Є. Черненко: США – РФ – КНР або США+НАТО проти ОДКБ+Китай [222]. Щоправда, на нашу думку, Росія в цьому протистоянні наразі відіграє все-таки другорядну роль, значно поступаючись кіберпотенціалом США та КНР.

На проблему «нової «холодної війни» звертає свою увагу й редакційний матеріал видання *The Observer* [428], вказуючи, що цьому об'єктивно сприяє зростання напруженості між ключовими світовими гравцями, яке ускладнюється не лише кібервійною, а й гонкою кіберозброєнь. Так само автори статті вказують на те, що запропонований Д. Роткопфом термін «прохолодна війна» об'єктивно знаходить своїх прихильників у найвищих кабінетах, оскільки реалія, позначувана ним, видається дешевою, не призводить до загибелі військовослужбовців, а також є політично вигіднішою.

Очевидною проблемою стає й те, що до досліджуваного протистояння в кіберпросторі дедалі частіше застосовують поняття, нерозривно пов'язане із класичною «холодною війною» – гонка озброєнь. Думку про гонку кіберозброєнь підтримує ізраїльський фахівець із кібербезпеки А. Рафф (*Aviv Raff*): «Ми є свідками справжньої гонки кіберозброєнь, однак використовувати цю зброю можуть не лише держави, а й будь-які люди та компанії, що мають для цього достатню кількість ресурсів» [92]. Водночас, на думку військового експерта й головного редактора журналу «Національна оборона» І. Коротченка, «дослідницькі компанії та хакерські групи ще не вийшли на той рівень, на який може вийти держава, спроможна забезпечити всю необхідну структуру для створення кіберзброї» [Там само]. Можливість нарощування гонки кіберозброєнь також засвідчують фахівці відомих антивірусних компаній. Так, начальник дослідного відділу компанії *F-Secure* М. Хіппонен (*Mikko Hyppönen*) зазначає, що віруси, які з'явилися останнім часом, суттєво «змінюють гру» на полі розвитку небезпечних програм: «Мені здається, що ми спостерігаємо перші кроки гонки озброєнь» [207]. Водночас до подібних заяв представників комерційних компаній варто ставитися з певною часткою скепсису. Нагнітаючи ситуацію довкола даної проблеми, вони створюють ринок для своєї діяльності.

Гонка озброєнь пов'язана також з уже згадуваною «дилемою безпеки», суть якої полягає в тому, що держава, відчуваючи брак власної небезпеки, нарощує свій військовий потенціал, який з необхідністю викликає абсолютно аналогічну реакцію з боку іншої (інших) держав і зациклює цей процес, виснажуючи всі сторони. У цікавому дослідженні Е. Джелленка (*Eli Jellenc*) [334], присвяченому проблемі гонки кіберозброєнь (а також прямим аналогіям із гонкою кіберозброєнь і гонкою озброєнь під час «холодної війни»), зазначається: якщо в 2005 році лише п'ять країн могли вважатися такими, що мають

стратегічні інтереси в кіберпросторі та здатні їх обстоювати (зокрема завдяки кіберзброї), то в 2012 році таких держав стало принаймні двадцять п'ять. На її думку, початкове розгортання гонки кіберозброєнь відбувалося за такою логікою: спочатку США, КНР і Росія, рано зрозумівши потенціал кібершпигунства, розробили свої кіберарсенали, а слідом за ними ті суб'єкти політичних відносин країни, які уважно спостерігають за їх розвитком і кроками (Франція, Великобританія, Австралія щодо США, Тайвань, Південна та Північна Кореї щодо КНР) також долучилися до цієї гонки. Якщо у 2007 році загальні видатки на сферу кіберозброєнь становили 10 млрд дол. США, то в 2012 році ця цифра перевищила 50 млрд дол. США.

Е. Джелленк вважає, що станом на початок 2012 р., геополітична конкуренція між основними геополітичними гравцями зосередилася на двох масштабних протистояннях:

• США проти Росії, КНР, Ірану та Північної Кореї;

• КНР проти Південної Кореї, Росії, Японії та Індії.

А також низці менших (локальних): Південна Корея проти Північної Кореї; Індія проти Пакистану; Росія проти Грузії; Іран проти Ізраїлю; Сирія проти Ізраїлю.

Логіка нарощування кіберозброєнь і збільшення можливостей їх застосування додатково зростає, оскільки наступальна доктрина саме в сенсі кіберпростору вважається більшістю експертів і фахівців найбільш адекватною. У. Лінн (*William J. Lynn*), 30-й заступник міністра оборони США, зазначає: «оскільки ви не знаєте, як побудувати надійний захист, ви не зможете відвернути масштабний наступ. І ви не можете забезпечити потрібну відповідь, оскільки ефективне стримування надзвичайно складне. Таким чином, якщо ви хочете скористатися кіберпростором, ви робитимете ставку на наступальні операції заради власної оборони» [357]. При цьому зважатимемо, що стосовно наступальних і захисних технік у сфері кібербезпеки зазвичай ідеться про дуже схожі елементи, які потребують сумісного обладнання, однакових навичок персоналу тощо.

Додаткову складність у сфері кібербезпеки становить той факт, що державам доводиться вживати наступальних і захисних заходів не лише проти формально ворожих країн, а й проти тих, які вважаються союзниками. Так у 2009 році в одному зі звітів Збройних сил Великобританії зазначалося, що поміж 20 країн, які «зламали» закриті урядові системи, були і країни-союзники. У тому самому 2009 році схожий матеріал оприлюднила служба зовнішньої розвідки Німеччи-

ни через видання *Der Speigel*, відзначивши недружню кіберактивність формальних союзників [Дані подано за: 334].

Е. Джелленк доходить висновку, що сучасна гонка кіберозброєнь, судячи з її динаміки має дедалі більші шанси закінчитися значущим конфліктом, що, відповідно, актуалізує на міжнародному рівні роботу щодо нейтралізації такої ескалації напруження.

Безумовно, кіберозброєння дотепер доволі неточно описані, передусім через уже згадані на початку роботи термінологічні проблеми. Крім того, кіберозброєння виробляються переважно в умовах максимальної конфіденційності, оскільки значно уразливіші для нейтралізації з боку захисних систем супротивника, ніж класичні види озброєнь. Маємо розуміти, що більшість кіберозброєнь у тій чи іншій формі експлуатують уразливості програмного забезпечення, а відповідно, відомості про такі уразливості стають важливою інформацією при створенні ефективних засобів протидії кіберзброї. Деякі держави офіційно визнають, що розробляють кіберозброєння. Наприклад, США через заяву екс-директора АНБ визнало, що має досвід застосування новітніх технологій, які порушують роботу комп'ютерних систем потенційного противника [198]. Інший приклад – Великобританія, яка розпочала програму розроблення наступальної кіберзброї [13].

У контексті проблеми гонки кіберозброєнь та загострення протиріч між великими державами зростає й вірогідність стрімкої ескалації кіберконфлітів. Американський фахівець із питань кіберконфліктів Х. Лін (*Herbert Lin*) звертає увагу на три обставини, які досі є недостатньо вивченими, однак у разі реального загострення можуть стати суттєвою проблемою [353]:

• принцип ескалації конфліктів у кіберпросторі та дії щодо її стримування;

• спосіб деескалації поточних кіберконфліктів та потрібні для цього заходи;

• умови перетворення кіберконфлікту на кінетичний конфлікт.

Зазначимо при цьому, що теорії динаміки конфліктів спершу розроблялися щодо ядерного протистояння, тобто одного із центральних «змістів» «холодної війни».

У своєму дослідженні Х. Лін наводить цікавий умовний приклад кіберпротистояння між двома умовними державами («сині» та «червоні»), в якому одна зі сторін («сині») начебто зазнає кіберудару від іншої сторони («червоних»), хоча цей удар завдавався зловмисниками, які з цієї метою спеціально «зламали» інформаційні системи

держав «червоних». «Сині», зважаючи на загальну політичну ситуацію і стан двосторонніх відносин між ними та «червоними», а також не маючи надійних механізмів визначити ініціатора й автора атаки, вживають контрзаходів щодо «червоних», що спричинює ескалацію конфлікту між двома державами.

При цьому автор справедливо зауважує, що ескалація – процес інтерактивний і передбачає часто неочікуване сторонами зростання рівня напруження між ними внаслідок взаємних дій. Проте, зважаючи на описані вище взаємовідносини між США та КНР, подібний сценарій виглядає загрозливо.

Складність визначення джерела атаки, наприклад, через відсутність доказів останньої, неможливість використати спеціальних агентів під прикриттям, відсутність відомих мотивацій потенційних зловмисників тощо, обумовлює одну з основних проблем дослідження зазначених питань.

2.2. Суперництво США та КНР у кіберпросторі як основа «холодної війни v2.0.»

Із 2010 року на міжнародній арені спочатку повільно, а потім з наростаючою швидкістю починає зароджуватися напівлатентний кіберконфлікт між США та КНР, який цілком може стати потенційною «холодною війною» постбіполярного світу. Безумовно, нині навряд чи можна з абсолютною упевненістю говорити про суто біполярне протистояння за лінією США – КНР, що випливає з теоретичних розвідок, наведених у першому розділі. Дійсно, сучасне «холодне» протистояння характеризується, по-перше, більшою кількістю ключових учасників (зокрема Російська Федерація, Північна та Південна Корея, Індія, Іран, низка європейських країн), однак саме лінія конфлікту (досі доволі умовного) США – КНР починає створювати «геополітичний наратив» XXI сторіччя. Саме це протистояння додатково посилює «дилему безпеки», а невпорядкованість кіберпростору на рівні міжнародного законодавства робить цей наратив особливо гострим і медійно виграшним.

Умовною точкою розгортання активної фази протистояння можна вважати дату 13 січня 2010 року, коли, нагадуємо, корпорація *Google* заявила, що може повністю піти з китайського ринку через спроби китайських хакерів «зламати» електронні поштові скриньки деяких китайських правозахисників. Як уже зазначалося, на захист

інтересів бізнес-компанії постав Держдепартамент США. Натомість китайська влада наполягала, що всі погрози з боку *Google* не матимуть жодного продовження, і компанія в жодному разі не піде з китайського ринку.

Водночас, на думку фахівців, конфлікт довкола *Google* є лише видимою частиною протистояння США та Китаю, що певною мірою відволікає увагу громадськості від реального рівня загрози інформаційній інфраструктурі США з боку Китаю. Як зазначалося вище, у 2010 році було начебто підготовлено звіт ФБР, в якому описувалися масштаби китайських хакерських угруповань, контрольованих урядом КНР [266]. Принагідно слід зауважити, що дані цього «таємного звіту» (про який достеменно невідомо, чи існував він взагалі), хоча частково і підтверджуються, однак багато в чому залишають враження надмірного нагнітання напруження.

Базою ж для вербування нових хакерів до військових кіберпідрозділів армії КНР[32] стають хакерські клуби, за якими керівництво Китаю уважно спостерігає. Щоправда, схожим шляхом прямують також і США, і ЄС. Зростання хакерського потенціалу КНР може бути пов'язане не лише з безпосередньою підтримкою такої діяльності з боку керівництва держави, а й з економічною привабливістю такої діяльності для молоді. За даними, оприлюдненими президентом китайської «Компанії комп'ютерної безпеки 360» Ці Сяндуном (*Tsi Xiangdong*), рівень доходу китайських хакерів у 2009 році сягнув 1,5 млрд дол. США [29].

Як зазначається у згадуваному звіті ФБР, головною метою КНР є створення до 2020 року найбільш «інформатизованої» армії у світі. Основним способом діяльності китайських хакерів ФБР називає використання «шкідливих» (*malicious*) комп'ютерних кодів. Уже в 2009 році компанії, що здійснюють свою діяльність в енергетичній (нафта і газ), банківській, аерокосмічній і телекомунікаційній сферах, мали суттєві проблеми з китайським «шкідливим» комп'ютерним кодом.

Незважаючи на те, що назви компаній у звіті не подаються, існують повідомлення про окремі випадки, що підтверджують ефективність китайських (на думку американських експертів) кібервійськ та їх успішної діяльності проти приватних компаній зазначених секторів економіки та військових мереж уряду США.

---

[32] Докладніше щодо механізмів залучення молодих китайських *IT*-спеціалістів до кіберпідрозділів армії КНР див.: [433].

25 січня 2010 року *Christian Science Monitor* повідомив [442], що принаймні три нафтові американські компанії (*Marathon Oil, ExxonMobil, ConocoPhillips*) постраждали внаслідок діяльності китайських хакерів[33]. Причому персонал компаній не зміг повністю зрозуміти масштаби й загрозу атак, що розпочалися ще у 2008 році, і повідомив ФБР лише на початку 2009 року. За цей час китайські хакери отримали доступ до найбільш важливої комерційної інформації (включно з результатами розвідок територій, електронним листуванням топ-менеджерів компаній тощо). На думку фахівців ФБР, які розслідували цю справу, було використано принципово нові типи вірусів, що не визначалися жодним спеціальним антивірусним програмним забезпеченням [Там само].

29 березня 2009 року канадська компанія *Information Warfare Monitor* звинуватила владу Китаю в побудові та використанні шпигунської комп'ютерної мережі [437], призначеної для отримання закритих урядових даних. За даними цієї компанії, мережа складається мінімум із 1295 вузлів, з яких частина є спеціально створеними для кібератак комп'ютерами, однак більшість – «зламані» ПК, розташовані в державних установах 17 країн світу. Влада Китаю 30 березня офіційно спростувала можливість існування подібної мережі [95], однак це вже не перше звинувачення на адресу Китаю щодо застосування шпигунського програмного забезпечення з метою збору закритої урядової інформації [184; 105].

Ефективною є діяльність китайських хакерів проти баз даних військового відомства США. Так, у червні 2007 року китайським хакерам вдалося отримати доступ до комп'ютерної мережі Пентагону та, відповідно, до внутрішнього електронного листування співробітників і порушити роботу близько 1500 комп'ютерів військового відомства [104]. На початку 2009 року американські військові підтвердили [213] факт «зламу» інформаційної бази Пентагону, звідки хакерам вдалося зняти кілька терабайт інформації щодо новітніх розробок Військово-повітряних сил США, зокрема розробки винищувачів нового покоління, бюджет яких становить близько 300 млрд дол. США. Також ефективною атакою хакерів (за версією Міністерства оборони США, здійсненою спецпідрозділами Північної Кореї за безпосередньої підтримки хакерів з КНР) є викрадення з комп'ютерів Міністер-

[33] Видання наводить докладні дані щодо процесу зараження комп'ютерної мережі нафтової компанії *Marathon Oil.* Наведена схема може свідчити про відпрацьованість схеми та чітке визначення цілей подібних хакерських атак.

ства оборони Південної Кореї оперативних планів розгортання американських військ на території півострова в разі конфлікту з КНДР.

Останньою на часі (січень 2013 року) «успішною» атакою, яку американські фахівці приписують також китайським кібершпигунам, став «злам» Національного реєстру гребель. Цей реєстр є базою даних, яку веде Інженерний корпус армії США , та містить інформацію про 79 тис. гребель на території США. У ній вказуються слабкі місця гребель, оцінка можливої кількості загиблих у разі прориву та інші дані [33]. Більшість інформації є закритою, однак хакери отримали доступ саме до уразливої інформації. Атаку вдалося виявити лише 3 місяці потому – у квітні 2013 року.

Схожі повідомлення є і стосовно інших компаній на території США – космічної галузі, основних військових підрядників оборонних відомств США тощо. Але це лише відкрита інформація щодо здійснених кібератак.

У відповідь на таке посилення Китаю в кіберпросторі Пентагон збільшує зусилля із протидії такій діяльності й розроблення новітніх засобів кібервійн. Агентство перспективних розробок Пентагону *DARPA* (*Defense Advanced Research Projects Agency)* уклало контракт з одним з найпотужніших виробників військової техніки у світі – компанією *Lockheed Martin* (орієнтовна сума контракту становить 31 млн дол. США) – на створення нової версії інтернету для військових цілей. Новий протокол із кодовою назвою *MNP* (*Military Network Protocol*) передусім має забезпечувати підвищену безпеку й динамічний перерозподіл пропускної можливості каналів. За словами головного спеціаліста *Lockheed* з кіберзброї Дж. Менгучі (*John S. Mengucci*), «нові мережеві загрози й атаки потребують революційних підходів до забезпечення безпеки» [355]. Інструменти, створювані за новим проектом, мають забезпечити боєготовність армії США навіть в умовах масованих кібератак.

У відповідь на численні звинувачення у використання кібершпіонів та кіберзброї китайське керівництво все спростовує та звинувачує США в посиленні гонки озброєнь у кіберпросторі. В англомовній версії веб-сайту *Peope's Daily* один із редакторів у своїй статті заявив, що саме «США є першою країною у світі, що представила концепцію кібервійни; вона мала на меті створення нового типу армії, кіберармії, та залучення хакерських груп. Американська розвідка може за допомогою спеціальних технічних засобів здійснювати суцільний моніторинг, спостерігати і знищувати он-лайнову інформацію, що

зашкоджує національним інтересам США. За такої політики було б цілковитим безглуздям вимагати від інших країн забезпечення вільних потоків інформації в мережі» [Цит. за: 259]. Звинувачення з боку китайської сторони отримують додаткову фонову підтримку через активне небажання керівництва США долучатися до переговорного процесу під егідою ООН щодо впорядкування на міжнародному рівні використання кіберозброєнь та протидії мілітаризації кіберпростору. Хоча за деякими повідомленнями, певні позитивні зрушення в цьому плані вже є [179].

Не можна сказати, що китайсько-американські відносини щодо кіберпростору супроводжували лише конфліктні ситуації. Протягом останніх років мали місце також спроби сторін домовитися про спільні заходи щодо протидії кіберзлочинцям чи принаймні встановлення певних «правил гри». Ще в 2010 році заступник директора департаменту мережевої безпеки Міністерства суспільної безпеки КНР Гу Цзянь (*Gu Jian*) повідомив, що оскільки саме Китай є однією з головних жертв комп'ютерних хакерів, він має об'єднатися зі США для розв'язання цієї проблеми. За його даними, станом на 2009 рік понад 200 китайських урядових сайтів щоденно зазнавали кібератак, 8 із 10 комп'ютерів ставали жертвою ботнетів[34] [98]. У 2011 році ситуація ще більше погіршилася: за даними китайського Національного центру комп'ютерної безпеки (*National Computer Network Emergency Response Technical Team/Coordination Center of China*), кількість хакерських атак на китайські урядові сайти в 2010 році зросла порівняно з 2009 роком на 68 % [103].

У 2012 році відбувалося певне пожвавлення китайсько-американських двосторонніх відносин щодо посилення кібербезпеки та налагодження співробітництва. Так, за даними британського видання *The Guardian*, КНР і США таємно проводили кібернавчання, організовані Центром стратегічних та міжнародних досліджень (*Centre for Strategic and International Studies, CSIS*) і Китайським інститутом сучасних міжнародних відносин (*China Institute of Contemporary International Relations*) [97]. Також у квітні 2012 року стало відомо про роботу китайських, американських і російських експертів, спрямовану на створення «гарячої» лінії зв'язку на випадок суттєвих кіберінцидентів. Ця система має діяти аналогічно створеному між СРСР та США

[34] У роботі використовуються паралельні назви*: ботнет* та *бот-мережа*. – *Прим. ред.*

у 1988 році Центру зі зменшення ядерної небезпеки, який мав попереджувати ядерні загрози. Тоді між двома країнами було налаштовано комунікаційний канал, більш відомий як «червоний телефон» [180].

У травні 2012 року, під час зустрічі міністра оборони США Л. Панетти (*Leon Edward Panetta*) та його китайського колеги Лян Гуанлє (*Liang Guanglie*), було озвучено домовленість сторін співпрацювати у сфері розроблення механізмів кіберзахисту. Голова американського військового відомства зазначив, що співробітництво в цій сфері є вкрай важливим, оскільки обидві сторони далеко просунулися в розробленні технологічних рішень [96].

Усі зазначені проблеми протягом 2011–2013 років не лише не зникли, а й набирають обертів.

У червні 2011 року тодішній міністр оборони США Р. Гейтс (*Robert Michael Gates*) заявив, що Вашингтон серйозно занепокоєний кібератаками з боку КНР і готовий застосувати силу, розцінивши їх як воєнні дії проти США [438]. На це заступник очільника МЗС КНР Цуй Тянькай (*Cui Tyanikai*) заявив, що між КНР і США не ведеться жодних кібервійн на рівні офіційних установ і що до хакерських атак, від яких постраждали обидві країни, урядові структури Китаю не мають жодного стосунку [99].

Звинувачення КНР з боку США значно почастішали у 2012 році. Уже на початку року Д. Макконнелл (*John Michael McConnell*), екс-голова Агентства національної безпеки США, заявив, що згідно з даними АНБ за 2011 рік Росія та Китай найчастіше використовують кібершпигунство для отримання торгових і технологічних секретів [17]. Аналогічну заяву в листопаді 2012 року зробив і головнокомандувач американської розвідки адмірал С. Кокс (*Samuel J. Cox*), який звинуватив КНР у постійних спробах «зламати» комп'ютерні системи не лише Пентагону та отримати доступ до секретної інформації, а й до комерційних таємниць американських корпорацій і секретів підприємств оборонного комплексу [3].

У травні 2012 року з'явилася доповідь компанії *Northrop Grumman* [386], підготовлена для Комісії у справах американсько-китайських відносин у сфері економіки та безпеки. Ключовими висновками документа стали такі [34]:

- КНР дійсно має цілісну стратегію інформаційного протиборства;
- КНР використовує кіберзасоби проти США;
- потенціал КНР достатньо значущий, аби становити загрозу для воєнних операцій США, здійснюваних у разі конфлікту;

• комерційні фірми КНР з іноземним капіталом мають доступ до сучасних технологій і надають такий доступ військам КНР;

• КНР свідомо й активно розповсюджує свої пристрої та комплектуючі поміж американських військових, у державних і приватних організаціях, які можуть мати доступ до критичної інфраструктури.

Доповідь з'явилася в результаті багатомісячного дослідження, ініційованого Комітетом з розвідки Палати представників США та спрямованого на виявлення фактів спеціального вбудовування китайськими компаніями *Huawei* та *ZTE* так званих бекдорів (*backdoor*)[35] у їхнє телекомунікаційне обладнання. Після понад 18-місячного дослідження проблеми, використавши можливості розвідувальних служб, застосувавши опитування клієнтів компанії, так і не вдалося однозначно довести робочу гіпотезу [449]. Незважаючи на це, американські політики продовжують наполягати на наявній загрозі, що походить від обладнання цих компаній, для кібербезпеки США.

Дедалі частіше такі побоювання, що не підтверджуються наявністю однозначних фактів, виглядають як намагання штучно «демонізувати» КНР, а разом і їхні компанії. Це призводить до цілком конкретних збитків та зірваних домовленостей. Наприклад, компанія *Huawei* так і не змогла взяти участь в австралійському багатомільярдному проекті розбудови широкосмугового доступу через побоювання уряду Австралії, що створена інфраструктура може стати об'єктом кібератак з боку КНР [1]. При цьому Конгрес США продовжує обґрунтовувати необхідність подальших перевірок цих компаній перед їх допуском на американський телекомунікаційний ринок.

Початок 2013 року характеризується загальним зростанням напруженості між США та КНР у сфері проблем кібербезпеки. На початку лютого 2013 року у звіті компанії *Mandiant* [298], по-перше, названо конкретний підрозділ армії КНР, відповідальний за наступальні дії в кіберпросторі («Підрозділ 61398»), по-друге, компанія звинуватила КНР у тривалій (з 2006 року) кібершпигунській атаці на 141 установу (з них американських – 115) з метою викрадення чутливих даних та інтелектуальної власності[36], зокрема креслень, схем процесів виробництва, бізнес-планів, партнерських угод і контактних листів компаній. Експерти *Mandiant* зазначили, що компанії, які були цілями атак, здійснюють свою діяльність у тих сферах еко-

[35] Програми, які встановлюються на обладнанні з метою отримання доступу до даних системи.

[36] Найбільший обсяг вкраденої інформації з однієї установи становив 6,5 Тбайт.

номіки чи за напрямами розвитку, які описуються принаймні чотирма із семи стратегічних напрямів розвитку КНР, визначених 12-ою П'ятирічкою (*12th Five Year Plan*) Китаю.

Унаслідок цих заяв та низки інших повідомлень про акти кібершпигунства з боку КНР наприкінці березня 2013 року з'явилося спеціальне розпорядження Б. Обами стосовно процедур державних закупівель щодо високотехнологічних рішень. Згідно з новими правилами США припиняє співробітництво з КНР у сфері поставок *IT*-обладнання для організацій державного сектору (зокрема Міністерства торгівлі та юстиції США, НАСА та Національного наукового фонду) [2]. Норма мала діяти до 30 вересня 2013 року, однак згідно з даними системи *THOMAS*[37] вона «працювала» і в 2014 році. Водночас згідно із зазначеним документом згаданим вище організаціям дозволяється купувати окремі технології, однак лише після консультацій із фахівцями ФБР щодо безпечності їх використання [307].

КНР в особі міністра закордонних справ висловила протест проти подібних дій керівництва США, зазначаючи, що жодних достовірних даних, що підтверджують підозри, немає, а відповідно, така політика, швидше, нагадує неринкові методи протекціонізму.

Водночас постають питання щодо практичної реалізації розпорядження (забезпечення контролю з боку уряду США), оскільки це може поставити під удар цілу низку компаній, що сприймаються як суто американські – *Apple*, *Dell*, *HP*, але мають життєво важливі для них зв'язки з китайськими виробниками. Наприклад, найвідоміший продукт фірми *Apple iPhone* виробляється саме в КНР на заводах компанії *Foxconn* (крім *Apple*, *Foxconn Technology* співпрацює з такими компаніями, як *Amazon*, *Dell*, *Hewlett-Packard*, *Motorola*, *Nintendo*, *Nokia*, *Samsung* та *Sony*)[38].

У травні 2013 року Міністерство оборони США оприлюднило доповідь для Конгресу США «Військовий та безпековий розвиток КНР 2013» [368, 369], у якій прямо звинувачує уряд КНР і Народно-визвольну армію Китаю у ворожих кіберакціях проти Міноборони США та інших американських установ: «Китай використовує можли-

---

[37] База законодавства США. Схожим аналогом вітчизняної бази є база Верховної Ради України «Законодавство».

[38] У лютому 2011 року на спеціально організованому ланчі між Президентом США Б. Обамою та ключовими гравцями Силіконової долини на запитання Президента «що потрібно для того, щоб виробляти *iPhone* у США?» тодішній голова *Apple* С. Джобс (*Steven Paul Jobs*) відповів, що ці робочі місця назавжди втрачені («не повернуться») для Америки [295].

вості комп'ютерних мереж для підтримки розвідувальної діяльності, спрямованої проти дипломатичних установ США, економіки та індустріальної бази сектору оборони, в тому числі проти тих структур, які підтримують національні оборонні програми США» [368, с. 36]. Крім того, в доповіді КНР звинувачується у продовженні докладання зусиль, спрямованих на посилення контролю за інтернет-простором, а також у руйнівній (*disruptive*) ролі, яку він виконує разом із Російською Федерацією, стосовно багатосторонніх зусиль із забезпечення прозорості та зміцнення довіри в міжнародних форумах, таких як Організація з безпеки і співробітництва в Європі (ОБСЄ), Регіональний форум АСЕАН та Група урядових експертів ООН [368, с. 37].

У результаті американська сторона заявила про готовність запроваджувати цілком конкретні (передусім економічні) санкції проти КНР у разі, якщо вона не перегляне свою політику щодо кібершпигунства. У квітні 2013 року заступник Державного секретаря США з питань економіки, енергетики та екології Р. Хорматс (*Robert Hormats*) зазначив, що кібератаки з боку КНР підривають довіру американських інвесторів, що може позначитися на обсязі інвестицій до КНР [336]. 8 травня 2013 року в Судовому комітеті Сенату США відбулися слухання «Кіберзагрози: правозастосування та відповідальність приватного сектору» [283], в яких порушувалися не просто питання кібершпигунської діяльності з боку КНР, а й методів асиметричної протидії їй. Поміж запропонованих заходів зазначалися: надання постійного місця проживання у США тим китайським фахівцям з кібершпигунства, які цього забажають, точкове переслідування (в тому числі через аналоги «акта Магнітського») хакерів і відповідальних осіб, які продовжують займатися підривною діяльністю проти США, тощо.

Окремі американські експерти пропонують своє бачення заходів, яких має бути вжито для убезпечення США від кіберрозвідувальної діяльності з боку КНР. Цікаво, що частково ці заходи є оновленими «старими методами», що підтверджує ідею загального оновлення протистояння в режимі *v*2.0. Так, Д. Блюменталь (*Dan Blumenthal*) [244], посилаючись на інших дослідників (Д. Рабкіна (*Jeremy Rabkin*) та професора *А. Рабкіна* (*Ariel S. Rabkin*), взагалі пропонує повернутися до практик XIX сторіччя та реанімувати для цифрового сторіччя «каперські свідоцтва». Оновлений дозвіл для «кіберкаперів» має надати можливість приватним компаніям атакувати ворожі об'єкти від імені держави, що дозволить уряду США ефективно реалізувати стратегію

відплати й оптимізує використання потенціалу власних «кіберсил». Крім того, американській дипломатії пропонується бути жорсткішою, встановити чітку та зрозумілу градацію в системі «виклик – відповідь» і пояснити китайському керівництву, що відповідь на атаки на критичну інфраструктуру буде більш жорсткою та масштабною ніж, припустімо, на сайт *The New York Times.*

На тлі взаємних звинувачень США та КНР у кібератаках стосовно одне одного в 2013 році Китай офіційно заявив, що розроблятиме й запроваджуватиме нові правила боротьби з міжнародним кібершпигунством [100].

2.3. Механізми реалізації кіберконфліктів у міжнародній політиці XXI сторіччя: хактивізм, кібершпигунство та кібердиверсії

Усі міркування щодо кіберзагроз, про які йшлося в попередніх розділах, будуть, вочевидь, неповними без наведення конкретних випадків або застосування кіберозброєнь (того, що під ним розуміється), або значущих кіберінцидентів, які суттєво вплинули на світову громадську думку щодо кібербезпекової проблематики загалом.

Зауважимо, що в цьому підрозділі йтиметься про певну умовну сукупність кіберконфліктів, які можна поділити на три великі категорії:

- хактивізм, або політично вмотивовані хакерські атаки;
- кібершпигунські акції;
- кібердиверсії.

Хактивізм за останні 2-3 роки став одним з мейнстрімів поміж форм політичних та ідеологічних протестів. Не в останню чергу це пояснюється тим, що в більшості випадків для нього використовується нескладний арсенал технологічних рішень, цілком доступних і не фахівцям.

Розглядаючи суть хактивізму, більшість дослідників виходять з того, що він є сучасною формою громадянської непокори. Один із дослідників цього явища П. Тейлор (*Paul Taylor*) визначає термін як «поєднання методів «зламу» з політичною активністю» [425]. Майже аналогічно про це висловлюється й інший дослідник Д. Томас (*Daniel Tomás*): політика хакінгу, чи створення технологій для досягнення політичних або соціальних цілей [434].

Наприклад, найпоширенішою формою здійснення атак хактивістів є *DDoS*-атаки (атака на зразок «відмова в обслуговуванні» – від англ. *Distributed Denial of Service*) – атаки на обчислювальну систему

з метою доведення її до відмови виконувати завдання, тобто створення умов, за яких легальні користувачі системи не можуть отримати доступ до системних ресурсів (сервісів) або цей доступ є ускладненим. У найпростішому вигляді це створення надзвичайно великої кількості запитів (які генеруються, зокрема, через спеціальні системи) до сайту або іншого ресурсу мережі інтернет. Змоделювати атаку можна на прикладі служби відповіді на запити громадян за допомогою пошти. Є певне приміщення, де працюють люди, які відповідають на запити громадян, що надходять поштою. Нормою навантаження є 1500–2000 листів. Це штатна робота системи. Під час атаки замість 2000 листів у приміщення починають безконтрольно надходити не тисячі, а десятки та сотні тисяч листів, які заповнюють собою все приміщення. Причому більшість цих листів взагалі не містить жодної корисної інформації – просто лист з адресою. Будь-які спроби відкрити двері в приміщення призводять лише до збільшення кількості листів. Зрозуміло, що в таких умовах ані відповідати, ані працювати служба не може, і їй потрібен час, аби впоратися з тим, що вже є, та усунути причину такого збільшення листів у конкретний момент часу.

DDoS-атаки стали звичною практикою в суто конкурентній боротьбі. Піддаватися атакам на замовлення можуть офіційні сайти компаній конкурентів. Іноді хакери займаються прямим шантажем приватних компаній, вимагаючи гроші за те, щоб не атакувати їх сайти.

Однак з появою на міжнародній арені групи *Anonymous DDoS*-атаки дедалі частіше асоціюють саме з політично, або, швидше, ідеологічно мотивованою протестною діяльністю. Так, у 2010 році *Anonymous* здійснили серію *DDoS*- та інших атак на сайти організацій, які сприяли прийняттю законів про авторське право, обмеження свободи в мережі інтернет, здійснювали пошук «піратів». У межах операції «Відплата» із застосуванням *DDoS*-атак було заблоковано сайти (а в деяких випадках і порушено роботи платіжних систем) *PayPal*, *Mastercard*, *Visa*, банку *PostFinance*, сайт шведського уряду, шведської прокуратури, портал інтернет-магазину *Amazon.com*. У 2011 році аналогічні атаки було здійснено проти Міністерства інформації Єгипту і правлячої Національної демократичної партії Єгипту. 2012 року через закриття сайту *MegaUpload.com* було заблоковано роботу Федерального бюро розслідувань, Білого Дому, Міністерства юстиції США, холдингу звукозапису *Universal Music Group*, Американської асоціації компаній звукозапису, Американської асоціації кінокомпаній, Американського управління авторського права. Загалом у 2012 році

DDoS-атак з боку *Anonymous* зазнали сайти Європарламенту, Інтерполу, Американсько-ізраїльського комітету у справах громадськості (*AIPAC*), Ватикану та деякі інші.

Незважаючи на таку масштабну діяльність *Anonymous,* визначними для міжнародного товариства *DDoS*-атаками, про які завжди згадують у контексті можливості використання кіберпростору для досягнення політичних і воєнних цілей (або підтримки інших дій держави), є події естонсько-російського (2007 р.) та грузинсько-російського (2008 р.) конфліктів.

Події 2007 року пов'язані з бажанням влади Таллінна перенести пам'ятник радянським солдатам («Бронзовий солдат») із центрального району міста на околицю. Конфлікт, який виник довкола цієї ініціативи, супроводжувався масштабною *DDoS*-атакою на урядові естонські сайти з 27 квітня по 18 травня. Досліджуючи цей інцидент, який багато хто із фахівців у сфері кібербезпеки називав «першою кібервійною», естонський фахівець Р. Оттіс (*Rain Ottis*) зазначав, що більшість атак відбувалися з-за кордону, переважно з Російської Федерації (яка посідала активну позицію з питання). Понад те, у своєму дослідженні він наводить макет листівки (російською), в якій подано поетапну інструкцію для тих громадян, які хочуть взяти участь у кібератаці на естонські сайти [388]. Загалом за менше ніж 30 днів кіберконфлікту на естонські ресурси було здійснено 128 унікальних *DDoS*-атак, переважна більшість з яких тривала до однієї години [379]. Л. Алманн (*Lauri Almann*), який на час атак був незмінним помічником міністра оборони Естонії, у своєму інтерв'ю зазначив, що під час протидії цим атакам естонські фахівці виділили дві фази [337]. Перша була пов'язана з діяльністю звичайних користувачів, зокрема тих, хто скористався порадами з листівок. Ця атака, хоч і неочікувана, однак у цілому з нею могли впоратися. Під час другої фази до атак приєдналися організовані групи, які використовували ресурси ботмереж, що збільшило кількість комп'ютерів, які брали участь в атаці, до понад мільйона.

За результатами розслідувань цих подій естонська прокуратура притягнула до відповідальності лише одну людину – естонського 20-річного студента Д. Галушкевича, якому було присуджено штраф у 1000 євро [229].

Під час кіберконфлікту на тлі грузинсько-російського протистояння в серпні 2008 року масованих *DDoS*-атак зазнала значна кількість грузинських інформаційних ресурсів. Атаки не просто збіглися

з розгортанням активної фази воєнних дій, а супроводжували їх майже весь час. На сьогодні існує кілька версій того, хто перший розпочав атаки та у відповідь на які дії (поміж озвучених версій – це була відповідь на дії грузинських хакерів [250]), однак це не є предметом нашого дослідження і, власне, не суттєво для ситуації, яку потрібно проілюструвати.

На думку західних експертів, у зазначеному конфлікті можна виділити дві фази кібератак. Перша фаза характеризувалася саме масштабною *DDoS*-атакою, здійснювана за допомогою ботнетів (до 6 одиниць, як відомих на той час, так і нових). Жертвами атаки стали урядові ресурси та грузинські онлайн-медіа. При цьому деякі дослідники, порівнюючи якість комунікаційних систем Грузії та Естонії, доходять висновку, що атака була більш вдалою через недосконаліть і застарілість грузинських інформаційних систем. Варто зазначити, що на відміну від естонських подій кількість атак була значно меншою, однак їх інтенсивність та якість зросли. Першим було виведено з ладу новинний сайт *Civil.ge* – він повернувся до роботи завдяки діям естонських фахівців з кібербезпеки та корпорації *Google*. Друга фаза кібератаки стала не лише продовженням атаки на вже атаковані ресурси, а й характеризувалася розширенням списку атакованих та зміною характеру атаки. Так, до новинних та урядових сайтів (сайт Президента Грузії припинив працювати 20 серпня) додалися фінансові установи, підприємства, навчальні заклади, деякі із західних ЗМІ (*BBC* і *CNN*), а також сайт грузинських хакерів [Там само]. А крім, власне, *DDoS*-атак почали застосовуватися дефейси (*deface*) – атаки, за яких головна сторінка сайту замінюється на іншу, зазвичай провокаційну.

На цьому ж етапі спостерігалася ситуація, схожа з естонською, коли на частині сайтів російського сегмента мережі інтернет поширювалися листівки з інструкціями щодо того, як можна брати участь у *DDoS*-атаках на грузинські сайти. Експерти зазначають, що на тлі грамотно організованої атаки дуже професійно працювали системні адміністратори російських хакерських сайтів, які ефективно захищали їх від спроб контратак [254]. Натомість дії грузинських фахівців з кібербезпеки були значно менш гнучкими, що дозволяло атакувати навіть ті сайти, які тимчасово було переведено на зарубіжні хостинги.

На думку західних експертів, основною метою такої масованої кібератаки було, з одного боку, зниження можливості Грузії подавати світові свою версію подій, а з іншого – справляння певного психоло-

гічного тиску як на урядовців, так і на звичайних громадян [435]. Крім того, через провокації щодо грузинських банків атаки завдали певного економічного збитку. При цьому важливим, на думку західних аналітиків, є той факт, що російські хакери, маючи реальну можливість атакувати системи *SCADA*[39], не робили цього, уникаючи завдавати реальних пошкоджень грузинським об'єктам критичної інфраструктури. Важливим наслідком цього кіберпротистояння став висновок про те, що військовим, які беруть участь як у звичайних, так і у кіберконфліктах, варто прискіпливіше підходити до безпеки цивільного сектору й цивільних мереж, оскільки атака на них завдає опосередкованого удару і по самим військовим, зокрема через психологічний вплив на населення [410].

Незважаючи на те, що всі ці акції набули міжнародного розголосу та були по-своєму доволі ефективними, за своєю суттю *DDoS*-атака лише умовно може вважатися елементом кіберозброєнь. Понад те, суто з технічної точки зору *DDoS*-атака, якщо вона не здійснюється за допомогою бот-мережі, навряд чи взагалі може бути названа протизаконною дією. У деяких країнах було навіть запропоновано ініціативи щодо легалізації *DDoS*-атаки як форми протесту поряд з пікетом, демонстрацією чи забастовкою. Із такою ініціативою виступили, наприклад, представники голландської ліво-ліберальної політичної партії «Демократи 66». Вони вважають, що легалізація є цілком можливою, якщо протестуючі узгоджуватимуть час і термін проведення онлайн-акцій завчасно (як це відбувається зі звичайними протестними акціями) [21].

Хоча *DDoS*-атаки дійсно можуть становити загрозу державним і недержавним інституціям, однак завдати принципової шкоди системі вони неспроможні, особливо якщо адміністратори системи, яка атакується, мають відповідну кваліфікацію й технічні ресурси. Хоча, за спостереженнями експертів з кібербезпеки, останнім часом потужність *DDoS*-атак зростає: у першому кварталі 2013 року середня потужність атак зросла в 7 разів порівняно з попереднім кварталом, і, швидше за все, цей процес триватиме [241].

---

[39] *SCADA* – програмний пакет (програмно-апаратний комплекс), призначений для розроблення або забезпечення роботи в реальному часі систем збору, оброблення, відображення та архівування інформації про об'єкт контролю або управління. *SCADA*-системи використовуються в усіх галузях господарства, де потрібно забезпечувати операторський контроль за технологічними процесами в реальному часі. *SCADA*-системи уразливі для хакерських атак: у 2010 році з використанням вірусу *Stuxnet* (детальніше див. далі) було атаковано центрифуги для збагачення урану в Ірані.

Принципово інший рівень небезпек, які, як випливає з попередніх розділів, наразі чи не найбільше турбує керівництво розвинутих держав світу, створює **кібершпигунство**. Під ним розуміємо заходи в кіберпросторі, спрямовані на отримання конфіденційної, секретної або просто чутливої для об'єкта атаки інформації. На сьогодні день можна стверджувати, що кібершпигунство стає очевидною домінантною ознакою «холодної війни *v*2.0.», а за своєю суттю реалізується у вигляді «точкових» акцій проти конкретних компаній і масованих довгострокових вторгнень.

«Точкові» акції проти конкретних компаній (організації) мають на меті отримання інформації про конкретні заходи компанії (організації) та/або використання цих компаній (організацій) задля подальших атак. Масовані довгострокові вторгнення здійснюються не лише з метою отримання конкретних відомостей, а й потокового збору деталізованих даних про життя компанії (організації) та її персоналу. Можуть бути як спрямованими, так і мати вигляд «сліпого пошуку».

Деякі приклади «точкових» акцій наводилися вище (наприклад, атака на американські нафтові компанії). А одним з найнаочніших прикладів може бути атака на компанію *Mitsubishi Heavy Industries.*

У серпні (за непідтвердженими даними, в червні) 2012 року *Mitsubishi Heavy Industries, Ltd.*[40] виявила у своїх системах віруси, що дозволяли зловмисникам отримувати доступ до внутрішньої інформації та здійснювати масштабне промислове шпигунство. Проте корпорація повідомила про це свого замовника – Міністерство оборони Японії – тільки в другій половині вересня, що викликало різке невдоволення військового відомства [32], адже відповідно до умов контакту всі сторони зобов'язуються терміново повідомляти про будь-які випадки несанкціонованого доступу до особливо важливої чи таємної інформації. У зв'язку із ситуацією міністр оборони країни наказав провести повне розслідування інциденту [329]. Майже одночасно з атакою на *Mitsubishi Heavy Industries* була спроба атакувати

[40] Японська компанія, що входить до *Mitsubishi Group*. Штаб-квартира розташована в м. Токіо. Компанія посідає 327 місце в *Fortune Global 500* за 2013 рік. Крім виробництва об'єктів цивільного призначення (нафтові танкери, круїзні лайнери, кондиціонери тощо), широко задіяна в оборонній сфері. Зокрема, корпорація виробляє ракети й елементи космічних кораблів, військові кораблі (субмарини, міноносці). У 2013 році *Mitsubishi Heavy Industries* уклала 215 угод загальною вартістю 260 млрд єн (3,4 млрд дол. США) з Міністерством оборони Японії, що становить майже чверть усіх витрат Міністерства оборони за рік.

іншу японську корпорацію, пов'язану з військовими замовленнями, – *Kawasaki Heavy Industries Ltd*.[41]

Згідно з оприлюдненими даними кібератаці було піддано 83 сервери та персональні комп'ютери корпорації *Mitsubishi Heavy Industries*. Для атаки було використано 50 вірусів, частина з яких була написана спеціально для атаки. Деякі віруси спеціально стирали сліди «зламу», що ускладнює оцінювання масштабів збитку. Використані хакерами віруси дозволяють віддалено керувати комп'ютерами, переміщати наявну на них інформацію, а також активізувати вбудовані в комп'ютери мікрофони та камери. Це дозволяло зловмисникам на відстані стежити за подіями в робочих і дослідних приміщеннях, фотографувати осіб, які працюють на комп'ютерах. Загалом, починаючи із середини серпня, хакери близько 300 тис. разів заходили на сервери *Mitsubishi Heavy Industries*, одного разу отримавши значний обсяг даних. Інформація з узятих під контроль комп'ютерів перекачувалася на 20 серверів за кордоном, зокрема на материковій території КНР, в Гонконгу, США, Індії [331]. Представник компанії *Mitsubishi Heavy Industries* повідомив, що віруси, застосовувані під час атаки, є схожими на ті, від яких постраждала компанія *Sony Corp*. у квітні, внаслідок чого відбувся витік особистої інформації близько 77 млн користувачів онлайн-сервісів компанії *Sony* [183].

Департамент поліції Токіо Метрополітен розпочав розслідування щодо незаконного доступу й інших правопорушень (Японія є одним з учасників Конвенції про кіберзлочинність, а в червні 2011 року верхня палата парламенту Японії ухвалила зміни до Кримінального кодексу, що запроваджують додаткову відповідальність за створення, поширення та зберігання комп'ютерних вірусів [363]).

Однозначні дані щодо характеру вкраденої інформації так і не було повідомлено. За твердженнями представників корпорації та Міністерства оборони Японії, наразі не виявлено суттєвих втрат важливих (секретних, конфіденційних) даних. Припускається, що об'єктом атаки мали стати саме дані про військову компоненту діяльності корпорації. Існує ймовірність викрадення частини доповіді про характеристики ракет (зокрема авіаційну протикорабельну ракету типу 80 (*Type 80 ASM-1*), що використовується для берегової оборони по-

[41] Японська корпорація зі штаб-квартирами в містах Кобо й Токіо. Крім цивільної продукції (мотоциклів і мотовсюдиходів), займається поставками апаратури для літальних і космічних апаратів, гелікоптерів, авіасимуляторів для потреб оборонного сектору, розробляє повітряно-реактивні двигуни та ракетну зброю.

вітряного базування проти надводних цілей. Незважаючи на те, що доповідь класифікується як конфіденційна, дані, до яких, можливо, отримали доступ хакери, не розглядаються Міністерством оборони як секретні [370].

На думку головного антивірусного експерта «Лабораторії Касперського» О. Гостєва, успіху операції сприяла її ретельна підготовка. За його словами, програма, за допомогою якої хакери атакували *Mitsubishi Heavy Industries*, протягом тривалого часу залишалася недетектованою більшістю антивірусів: «На підготовку такої програми потрібні місяці тестування і налагодження» [140]. На ретельну підготовку атаки вказує також той факт, що всередині програми містилися точні адреси внутрішніх серверів *Mitsubishi Heavy Industries*, а також логіни й паролі для доступу до них. Таку інформацію можна було здобути лише після попередніх досліджень. За оцінкою О. Гостєва [88], замовникам, якщо такі були, атака коштувала кілька десятків тисяч доларів.

Поки що достовірно невідомо про всі особливості кібератак на японські корпорації, однак з відкритих джерел можна встановити таку послідовність діяльності зловмисників.

1. Хакери вкрали поштові електронні адреси у *Товариства Японських компаній Аерокосмічної промисловості* (*Society of Japanese Aerospace Companies, SJAC),* яке має списки керівників підрядників з оборонної сфери, його директорів, а потім вилучили вміст електронних листів від *Mitsubishi Heavy Industries Ltd.* За таким саме алгоритмом було отримано адреси працівників *Kawasaki Heavy Industries Ltd., адже* обидві компанії є членами *SJAC.*

2. Атака за допомогою *e-mail* на *Kawasaki Heavy Industries Ltd.* розпочалася ввечері 26 серпня, було використано назву одного із членів *SJAC*, який є одним з основних виробників електронної апаратури. У червні й липні відбувалися аналогічні спроби: в обох випадках хакери відрекомендовувалися представниками компанії у префектурі Канагава, що займається виробництвом деталей літаків. Електронні листи з назвою «Попереднє розсилання документів» містила прикріплений файл «Коментарі щодо отримання разової суми». Тексти повідомлень переважно було скопійовано з електронних листів учасника *SJAC*, що надсилалися іншим учасникам за 10 годин до фальшивої пошти. Таким чином, на попередньому етапі використовувалися практично класичні фішингові техніки[42].

[42] За даними експертів, від 40 до 60 % усіх успішних кібератак здійснюються з використанням елементів соціальної інженерії, в тому числі фішингу.

3. Фальшиві *e-mail* надсилалися через міжнародну телефонну компанію у *Chuo Ward*, м. Токіо. Поліція виявила, що комп'ютер компанії був заражений вірусом та використовувався хакером для фальшивої ідентифікації. Крім того, виявилося, що комп'ютери *SJAC* також були давно інфіковані.

4. Безпосередньо атака на *Mitsubishi Heavy Industries Ltd.* була багато в чому схожою на атаки проти *Kawasaki Heavy Industries Ltd.*, однак із важливим доповненням. Об'єктом атаки був один чітко визначений комп'ютер і його користувач. Хакери надіслали йому листа, в якому містився шкідливий *pdf*-файл. Зміст листа було сформовано таким чином, щоб «жертва» відкрила прикріплений файл. Вибір конкретного співробітника обумовлювався тим, що на його робочому комп'ютері стояла застаріла версія програми *Adobe Reader* – давно відома уразливість програмного забезпечення *Adobe* дозволила хакерам завантажили свою «троянську» програму. При цьому представники корпорації не виключають і саботаж з боку власних працівників, оскільки деякі системи можна було атакувати тільки зсередини компанії [150].

5. Потрапивши на комп'ютер, «троян» встановив зашифроване з'єднання із сервером зловмисників і надав останньому можливість діяти далі. На думку О. Гостєва [88] та за наявними даними, «злам» і викрадення потрібної хакерам інформації здійснювалися вручну – зловмисники уникали завантаження додаткових модулів, щоб знизити ймовірність виявлення. Такий метод дозволив їм залишатися непоміченими службою безпеки протягом місяця.

У медіа (передусім японських) тиражувалася думка, що потенційним замовником та виконавцем атаки була КНР. Подібне припущення було зроблено з низки причин:

• в одному з вірусів, що використовувався в кібератаці проти *Mitsubishi Heavy Industries*, виявлено застосування китайської мови[43]. Управління поліції Токіо Метрополітен підозрює залучення до кібератаки особи чи осіб, що добре володіють китайською мовою[44], та розглядає цей інцидент як міжнародне шпигунство [308];

• більшість серверів, на які надходили вкрадені дані, розташовувалися на території КНР. Крім того, останнім часом КНР активно

[43] «Китайськими ієрогліфами замінялися слова «автоматичний», «захоплення» та «зображення».

[44] Водночас деякі японські експерти з кібербезпеки зазначили, що злочинці могли навмисно використовувати китайські ієрогліфи, щоб замаскувати атаку під китайську.

займається космічними програмами, у планах держави створення власної багатомодульної пілотованої орбітальної станції, а в майбутньому – багаторазові транспортні космічні системи. Обидві атаковані японські корпорації були активно задіяні саме у сфері аерокосмічних розробок;

• загальна активізація діяльності КНР у кіберпросторі. Згідно з даними сайту *Wikileaks* ще в лютому 2010 року під час зустрічі представників японської та американської сторін із питань безпеки КНР згадувалася саме в контексті збільшення зусиль із двостороннього американсько-японського співробітництва у сфері кібербезпеки. З-поміж іншого на зустрічі було прийнято рішення про розширення досі секретної Двосторонньої робочої групи з питань інформаційної безпеки (*Bilateral Information Security Task Force – BISTF*) до державної (відкритої) робочої групи з інформаційної безпеки, що буде заснована на базі *BISTF* [440];

• можливості саме китайських хакерів вдало здійснити подібну атаку, її масштабність і продуманість. Підбір індивідуального підходу до об'єкта атаки, складна система фальшивих ідентифікаторів, багатоступеневість при створенні системи заражених комп'ютерів, особливості отриманої інформації, орієнтовний час підготовки нападу свідчать про те, що за атакою стояла не звичайна група хакерів, а професіонали у сфері економічного шпигунства, що шукали цілком конкретну інформацію. Офіційний Пекін прокоментував ситуацію неоднозначно. 20 вересня 2011 року під час традиційної прес-конференції речник МЗС КНР Хун Лей (*Hong Lei)*на запитання щодо причетності КНР до атаки звернув увагу присутніх на те, що КНР активно бореться із хакерами і сама є однією з головних жертв хакерів [303].

Після виявлення масштабної кібератаки японські урядові структури розпочали низку заходів щодо визначення готовності ключових підприємств, задіяних у військовому секторі та системі державного управління, реагувати на можливі кібератаки. Міністерство оборони провело опитування близько 100 оборонних фірм і не виявило інших витоків конфіденційної інформації.

Міністерство оборони запропонувало компаніям, які здійснюють оброблення секретних оборонних даних, розробляти внутрішні правила для застосування такої інформації та використовувати окрему комп'ютерну мережу для конфіденційної інформації після укладання договорів. Воно також вимагає, щоб підрядники негайно повідомляти про підозрілі витоки даних.

Остання вимога є особливо актуальною, оскільки приватні компанії намагаються до останнього не розкривати відомості про подібні інциденти. Після виявлення факту кібератаки на *Mitsubishi Heavy Industries, Ltd.* кілька великих компаній визнали, що вони теж у минулому були об'єктами атак. Дослідження, проведене *The Yomiuri Shimbun*, виявило занепокоєння деяких компаній через негативні наслідки від розкриття подібної інформації. Опитування щодо кібератак було проведено поміж 20 компаній і груп, які уклали найбільш вартісні контракти із Забезпечувально-будівничим центром Міністерства оборони Японії на 2010 рік. *П'ять респондентів визнали факт атак у минулому, сім – заперечили, а ще п'ять відмовилися відповідати*. Зокрема, провідна машинобудівна компанія повідомила, що опублікування такої інформації може спричинити *copycat*-злочини[45] з боку кібертерористів.

Водночас самé Міністерство оборони також було мішенню для хакерів, а його чиновники останніми роками отримували підроблені електронні повідомлення від імені реальних колег. У вересні 2010 року сайт Міністерства зазнав *DDoS*-атаки, спрямованої на збільшення трафіку на серверах та уповільнення швидкості обміну даними [284].

Рада з політики інформаційної безпеки Японії (*Information Security Policy Council*), створена в 2005 році після атакування урядового сайту (в перші роки існування проводила близько шести засідань на рік, однак у 2011 році відбулося лише два), 7 жовтня 2011 року прийняла рішення про проведення тренувань, у межах якого розсилалися фальшиві електронні повідомлення для 50 тис. співробітників міністерств і відомств з метою підвищення їх обізнаності з питання кібербезпеки. Повідомлення мали містити прикріплений файл із підробленим вірусом і розсилатися в період між жовтнем і груднем. Ті, хто відкрив прикріплений файл, мали бути поінформовані про способи уникнення зараження вірусом.

Рада також прийняла рішення щодо співпраці між державним і приватним сектором у сфері протидії кібератакам.

У цьому контексті цікавим є експеримент, який проводили двоє дослідників з компанії *Godai Group*. Метою дослідження було з'ясування потенційних масштабів тайпсквотингу (*typo* – помилка друку + *cybersquatting*) – реєстрації доменних імен, близьких за написанням до адрес популярних сайтів, з розрахунком на випадкову по-

[45] Злочин, що копіює прецедент, висвітлений у ЗМІ.

милку частини користувачів при написанні доменного імені. Дослідники зареєстрували 500 доменів-двійників, які за написанням дуже схожі на домени компаній зі списку *Fortune* 500. Піврічна робота цих доменів і поштових серверів дозволила зібрати 20 Гбайт електронних листів, що прийшли не на потрібну адресу. У перехоплених повідомленнях виявилися закриті корпоративні дані, логіни та паролі для корпоративних систем, дані про конфігурацію корпоративних мереж, різноманітні ділові документи та інші відомості [228].

Крім того, з метою захисту державних секретних даних Японії в серпні 2011 року Національне агентство поліції розпочало комплекс дій поміж близько 4000 компаній. Метою цих дій було визначено інформування поліцейських сил про цільові кібератаки.

Не виключено, що саме атаки на японські корпорації стали причиною прийняття в жовтні 2011 року Директиви Федеральної Комісії США з контролю над операціями із цінними паперами, яка зобов'язує ділові структури повідомляти про всі кібератаки, яких зазнають їх інтернет-сайти та комп'ютерні мережі, особливо якщо було втрачено інформацію [4].

Випадок з *Mitsubishi Heavy Industries, Ltd.* до певної міри можна вважати класичним прикладом здійснення сучасної кібершпигунської діяльності. Це не разові спроби отримати доступ до серверів напряму, а складні, багатоходові схеми з активним використанням технік соціальної інженерії[46], спеціально написаних для атаки вірусів тощо. Масштабність, високий рівень спланованості, якість реалізації та залученість ресурсів свідчать про те, що за подібними атаками, найшвидше, стоїть професійна розвідувальна структура, а не приватний капітал, хоча й це не можна повністю виключати. Майстерність, із якою хакери знищують всі сліди своєї присутності й діяльності свідчать про їх високий професіоналізм, який вимагає від компаній, що бажають захиститися від подібних атак, неабияких витрат на безпеку.

Крім подібних «точкових» акцій, для реалізації яких провадиться максимально прискіплива попередня розвідка (в тому числі «розробляються» конкретні люди), дедалі масштабнішим стає інший вид кібершпигунської діяльності. Він є значно масовішим, однак при цьому лише частина атак здійснюється методом «сліпого пошуку», натомість більшість із них є продуманими та орієнтованими на конкретні

[46] У роботі розуміється як використання маніпулятивних заходів з метою злочинного вивідування даних.

об'єкти. Ідеться про ціле сімейство вірусів, виявлене безпековими компаніями в 2012 році.

Справжній розквіт масштабного кібершпигунства припадає на 2011–2012 роки і триває дотепер.

У вересні 2011 року угорські антивірусні компанії заявили про виявлення вірусу, який у подальшому отримав назву *Duqu*. З огляду на те, що це сталося майже відразу після скандалу з вірусом *Stuxnet*, до нього була прикута особлива увага дослідників. Понад те, як вдалося згодом встановити дослідникам, код вірусу *Duqu* використовував оригінальні вихідні коди вірусу *Stuxnet*. Однак на відміну від *Stuxnet* вірус *Duqu* був суто шпигунською програмою, яка не мала на меті атакувати системи *SCADA*. Вірус потрапляв на комп'ютери через спеціальний файл формату *Microsoft Word*, а для закріплення в системі використав *zeroday*-уразливість. Суттю так званих *zeroday*-(0-*day*) уразливостей є те, що це цілком нові уразливості програмного продукту, які до цього часу не були виявлені дослідниками безпеки. Сам термін («нульовий вік» уразливості) пов'язаний з тим, що уразливість стає публічно відомою лише після атаки. Пошук і подальша передача відповідним компаніям за винагороду *zeroday*-уразливостей є своєрідним форматом безпекового бізнесу та вважається цілком нормальною практикою поряд з, наприклад, етичним хакінгом. Водночас є дослідні групи, які принципово не передають інформацію про такі уразливості власникам продуктів, сподіваючись отримати більшу вигоду в конкурентів.

Повертаючись до *Duqu*, маємо констатувати, що вірус був надзвичайно складною програмою (її дослідники навіть не відразу змогли зрозуміти, яка саме мова програмування використовувалася для його написання) та включав 3 основні шпигунські модулі [51].

1. *Infostealer*. Він збирав інформацію про список запущених процесів; перелік логічних дисків (включно з мережевими); скриншоти користувача; адреси мережевих інтерфейсів і таблиць маршрутизації; «логи», або лог-файли (*log file*) натискання клавіш клавіатури; імена відкритих вікон і програм; перелік доступних ресурсів мережі; повний список файлів на всіх дисках, зокрема портативних; список комп'ютерів у мережі.

2. *Reconnaissance*. Збирав інформацію про те, чи є комп'ютер частиною домену; шляхи до системних каталогів *Windows*; версію операційної системи; ім'я поточного користувача; список мережевих адаптерів; системний, а також місцевий час.

3. *Lifespan extender*. Реалізовував функцію підвищення значення кількості днів, які залишилися до завершення роботи. За замовчуванням це значення було рівним 30 або 36 дням.

Робота вірусу та збирання інформації від нього координувалися через низку серверів, розташованих по всьому світу (В'єтнам, Індія, Німеччина, Сінгапур, Швейцарія, Великобританія, Нідерланди та Південна Корея), причому всі вони були попередньо «зламані». Уже за три дні після оприлюднення інформації про виявлення вірусу всі командні центри були знищені самими хакерами.

Найбільше вірус вразив організації, що знаходилися на території Франції, Нідерландів, Швейцарії, України, Індії, Ірану, Судану та В'єтнаму, меншою мірою – Австрії, Угорщини, Індонезії та Великобританії [445]. Автори вірусу надзвичайно якісно попрацювали для забезпечення своєї програми можливостями з'єднання з командними серверами: як мінімум одна організація, атакована вірусом, надала докази того, що *Duqu* був здатний поширюватися через *SMB*-з'єднання[47], які використовуються для передачі файлів між різними комп'ютерами. Відповідно, коли деякі із заражених комп'ютерів були відключені від мережі інтернет, вірус використовував *SMB*-з'єднання для отримання доступу до комп'ютерів, підключених до мережі [52].

На думку фахівців компаній «Лабораторія Касперського» (*далі* – ЛК) та *Symantec*, вірус від самого початку не був розрахований на стихійне самопоширення, маючи на меті більш-менш конкретні цілі. Вважається, що основна мета вірусу полягала в збиранні інформації про промислові системи контролю та проектну документацію [203].

У травні 2012 року ЛК виявила новий вірус-шпигун, який уразив близько 400 комп'ютерів у 10 країнах світу – *Flame*. За даними ЛК, вірус функціонував щонайменше з 2010 року, а його код мав чи не рекордні 20 МБайт, що було само по собі дивно, адже зазвичай створювачі вірусів намагаються зробити їх якомога меншими[48]. Цей вірус мав низку відмінностей від *Duqu,* з-поміж яких – вбудовані можливості самовідтворення в разі надходження відповідної команди від командного центру. Крім того, він був бекдором, закріплюючи на

[47] Даний протокол характерний для продуктів корпорації *Microsoft* і використовується, наприклад, для спільного використання файлів і принтерів.

[48] Водночас деякі експерти із цього приводу зазначають, що подібні великі віруси стають можливими через зростання швидкостей мережі інтернет і підвищення якості широкосмугового доступу.

«зламаному» комп'ютері можливість повторного доступу зловмисника до системи. Як і *Duqu*, *Flame* пересилав отримані дані на командні сервери, а оператори цих серверів могли обирати з можливих 20 (!) додаткових шпигунських модулів, які завантажували на заражений комп'ютер. Незважаючи на таку його продуманість, він належить до вірусів, мішенню яких, схоже, не є якісь конкретні компанії і які працюють, швидше, в режимі «сліпого пошуку» [429].

Вірус міг збирати файли даних, віддалено змінювати параметри комп'ютера, записувати звук, скриншоти і підключатися до чатів. Додатковим нюансом діяльності *Flame* було те, що він працював і з тими пристроями, на яких був увімкнений *Bluetooth* – він збирав інформацію про такі пристрої. Поміж файлів, що їх цілеспрямовано шукав вірус на заражених комп'ютерах, – файли у форматі *.pdf* (документи) та *.dwg* (формат програми *AutoCAD*, у якому роблять і зберігають креслення) [224].

З огляду на це, складно не погодитися з думкою експерта ЛК О. Гостєва: «*Flame* можна легко назвати однією з найбільш комплексних загроз, які коли-небудь були виявлені. Він великий і надзвичайно складний. Одним своїм існуванням він може сприяти перегляду понять *кібервійна* та *кібершпигунство*» [448]. Також експерти звертали увагу на те, що, зважаючи на географію поширення вірусу, він, вочевидь, був створений для цілком конкретного середовища. Загалом вірусом було уражено 189 комп'ютерів у Ірані, 98 – у Ізраїлі та Палестині, 32 – у Судані, 30 – у Сирії, 18 – у Лівії, 10 – у Саудівській Аравії та 5 – у Єгипті.

Дослідникам так і не вдалося знайти надійних доказів того, що *Flame* був пов'язаний з *Duqu* чи *Stuxnet*, хоча певні спільні риси в них були (наприклад, метод зараження). Більш-менш однозначно стверджують те, що всі проекти реалізовувалися паралельно групами, які могли мати доступ до розробок партнерів. Про ґрунтовну підготовку тих, хто створив вірус, і тих, хто здійснював керівництво його роботою, свідчить і той факт, що зловмисники витратили багато сил на створення цілої низки фальшивих персон, на яких було зареєстровано домени командних серверів.

Як і у випадку з *Duqu*, протягом тижня автори вірусу дали йому команду на самознищення – повне самовидалення *Flame* з комп'ютера, а на його місці розмістити беззмістовну інформацію. Вона ускладнила роботу комп'ютерних спеціалістів, що займаються дослідженням вірусу [86].

Майже відразу після виявлення вірусу *Flame* антивірусні компанії знайшли ще один складний шпигунський вірус – *Gauss*. І знову його основною метою стали комп'ютери на Близькому Сході (Ліван, Ізраїль, Палестина). Масштаби зараження більші, ніж у *Flame*, – понад 2500 комп'ютерів. Основною відмінністю цього вірусу від попередніх став об'єкт інтересу його авторів. Якщо попередні віруси намагалися максимально зібрати інформацію про самі автоматизовані системи чи про можливі розробки, то *Gauss* «цікавився» передусім фінансовими даними. Вірус збирав інформацію з уражених комп'ютерів з вересня 2011 року і до моменту свого виявлення у червні 2012 року.

Gauss інфікував комп'ютери на базі *Windows* і крав історію перегляду *web*-сторінок користувачів, а також фінансові дані клієнтів платіжної системи *PayPal*, а також таких установ, як *Bank of Beirut BlomBank*, *ByblosBank*, *FransaBank* і *Credit Libanais* (всі розташовані в Лівані) та *Citibank* [41].

На думку фахівців ЛК, *Gauss* поширювався через *USB*-накопичувачі. Вірус встановлював до восьми окремих модулів на атаковану машину, кожен з яких був націлений на виконання свого завдання, зокрема збирання паролів, банківських реквізитів, даних про комп'ютер і даних доступу до аккаунтів у соціальних мережах [306]. Усі командні сервери було відключено авторами вірусу в липні 2012 року.

Усі фахівці одностайні в тому, що це розробка, здійснена за участю якоїсь держави, оскільки масштабність робіт над подібним вірусом вимірюється мільйонами доларів США.

У лютому 2013 року було виявлено черговий шпигунський вірус – *MiniDuke*. Він суттєво відрізнявся від попередніх вірусів низкою характеристик, на які звернув увагу керівник ЛК Є. Касперський: «Я в шоці. Чому? Зазвичай я не дивлюся код нових троянів-шпигунів, але цього разу подивився. Я цей код бачив останній раз років 10 тому. Цей троян-шпигун написаний не просто «у стилі старої школи». Щось мені підказує, що він зроблений «старими руками», зокрема фахівцями, які наприкінці 90-х років XX сторіччя входили до хакерської групи 29A. Саме вони були засновниками майже всіх сучасних вірус-технологій. Вони вигадали поштових хробаків (1999), флеш-хробаків (2003), а також віруси для смартфонів (2004) і багато чого іншого» [18]. На думку фахівця, «це елітні автори вірусних програм старого гарту, які мають досвід у створенні складних вірусів, зараз суміщають свої навички з новими методами оминання захисних технологій для того, щоб атакувати державні установи й наукові ор-

ганізації у різних країнах. Поєднання досвіду «олдскульних» авторів вірусів з новітніми вразливостями та хитрими навичками соціальної інженерії – надзвичайно загрозлива суміш» [118].

Новий вірус мав надзвичайно малий розмір – лише 20 Кбайт (тобто приблизно в 1000 разів менший, ніж вірус *Flame*). Загалом ним було заражено не так багато комп'ютерів (дослідники виявили 59 жертв у 23 країнах), однак у діяльності вірусу чітко проглядалася зацікавленість його авторів у збиранні зовнішньополітичної інформації. Це дозволяє дійти висновку, що за вірусом, щонайшвидше, стояла певна країна. Надто для кожної зі «зламаних» систем бекдор був модифікований, тобто про «сліпий пошук» не йдеться.

Жертвами кібершпигунської програми стали, зокрема, державні установи України, Бельгії (можливо, посольство), Португалії, Румунії, Чехії та Ірландії. Крім того, від дій кібершпигунів постраждали дослідний інститут, два науково-дослідних центри та медицинська установа у США, а також дослідний фонд в Угорщині [Там само].

Для проникнення у системи жертв кібершпигуни використовували прийоми соціальної інженерії: було створено спеціальні *pdf*-документи, які являли собою актуальні та якісно зроблені набори фальшивого контенту. Зокрема, вони містили інформацію про семінари з прав людини, дані про зовнішню політику України (наприклад, для атаки на бельгійські ресурси використовували фальшивий «План дій Україна-НАТО з набуття членства» [430, с. 3], а для атаки на Люксембург – «Українські дослідження регіональної політики. Рік після помаранчевої революції» [Там само, с. 4]), а також плани країн – участниць НАТО. Всі ці документи містили уразливості, які атакували комп'ютер через програму *Adobe Reader* (через нову *zeroday*-уразливість). Зараження системи відбувалося через невелику програму, унікальну для кожної із заражених систем, яка до того ж «вміла» ховатися від інструментів антивірусного аналізу. У разі виявлення деякими антивірусними засобами вірус тимчасово призупиняв свою діяльність. Відповідно, дійшли висновку про те, що автори вірусу добре обізнані з методами роботи антивірусних компаній.

Новацією роботи вірусу була і система управління ним. На відміну від попередніх, яким для цього потрібні були спеціальні командні сервери, новий вірус взаємодіяв із системою мікроблогів *Twitter*, де шукав спеціальні твіти на заздалегідь визначених аккаунтах. Твіти на цих аккаунтах мали специфічні теги, які маркували зашифровані адреси для бекдору. І вже саме через таку систему вірус взаємодіяв

із серверами управління. Якщо ж на зараженому комп'ютері *Twitter* не працював, вірус міг використовувати *Google Search* для пошуку зашифрованих посилань на серверах управління. Після свого повноцінного завантаження на заражений комп'ютер вірус міг починати роботу: переміщувати чи видаляти файли, створювати каталоги, зупиняти процеси та завантажувати нові шкідливі програми. Командні сервери розташовувалися у Панамі та в Туреччині.

Трохи відокремлений від наведеної вище групи вірус, виявлений одним з останніх (і, напевно, один з найуспішніших) – «Червоний жовтень» (*Red October*). Цей вірус до певної міри унікальний вже самим часом свого існування: за попередніми оцінками він почав свою діяльність ще у 2007 році, а вперше був виявлений лише наприкінці 2012 року (офіційно повідомлено про його викриття у січні 2013 року). Основна його діяльність – шпигунство за дипломатичними, урядовими та науковими організаціями різних країн світу, приватними компаніями, які діють у сферах енергетики, зокрема ядерної, нафтової та газової, космосу й торгівлі. Зловмисники намагалися передусім отримати доступ до конфіденційної інформації, даних, що відкривають доступ до комп'ютерних систем, персональних мобільних пристроїв і корпоративних мереж, а також збирати геополітичні дані.

Найбільше постраждали країни колишнього СРСР, країни Східної Європи, а також низка держав у Центральній Азії [145]. Загалом зареєстровано сотні заражень, найбільша кількість з яких припадає на Російську Федерацію, Казахстан, Азербайджан, Бельгію, Індію, Афганістан, Вірменію, Іран, Тукменистан й Україну.

Для роботи вірусу його автори створили цілком нове програмне забезпечення з унікальною архітектурою – мультифункціональною платформу для здійснення атак, яка містила кілька десятків розширень (модулів) і шкідливих файлів, здатних швидко адаптуватися до різних конфігурацій техніки. Поміж таких модулів:

• модуль відновлення, який дозволяв зловмисникам отримувати повторний доступ до зараженого комп'ютера навіть у разі виявлення основного вірусу;

• удосконалені криптографічні шпигунські модулі, призначені для викрадення інформації з різноманітних криптографічних систем, зокрема використовуваних у організаціях НАТО та ЄС (Європарламент та Єврокомісія);

• модуль, що уможливлював інфікування мобільних пристроїв, зокрема смартфонів.

Крім того, вірус виконував понад десяток одноразових і багаторазових завдань, спрямованих на викрадення інформації із системи.

Як і *MiniDuke*, *Red October* не був вірусом «сліпого пошуку». Для зараження систем зловмисники розсилали фішингові листи, адресовані конкретним отримувачам з тієї чи іншої організації (наприклад, пропозиції для дипломатичних представництв купити машини за прийнятною ціною). Саме в цих листах містилася шкідлива програма, яка для свого встановлення використовувала уразливості *Microsoft Office*. Ця уразливість і раніше використовувалася для різноманітних кібератак, зокрема на тибетських активістів, військову та енергетичну сфери низки держав Азіатсько-Тихоокеанського регіону [145].

Проміжні командні сервери вірусу розташовувалися на території Німеччини та Росії, однак реальний центр командування так і не вдалося відстежити. Водночас, на думку дослідників, є достатні підстави вважати, що автори вірусу мають російське коріння (в коді вірусу транслітеровано використовувалися російські слова – напевно, в безпосередніх авторів вірусу не завжди вистачало англомовного словарного запасу, хоча можна припустити, що подібні «помилки» були зроблені навмисно). Експерти так і не змогли надати однозначну відповідь щодо можливих замовників і виконавців атаки. Як і щодо інших вірусів, відповідальність за написання *Red October* покладається на китайських і російських фахівців. З огляду на специфічність здобутої вірусом інформації, можна припустити також участь однієї з потужних світових держав. За підрахунками експертів, за 5 років своєї роботи *Red October* зміг передати своїм авторам сотні терабайт чутливої інформації, яка цілком могла бути використана проти тих чи інших держав.

Наведений загальний і досить побіжний огляд кібершпигунської активності водночас дозволяє дійти висновку про масштабність явища. Внаслідок діяльності лише виявлених вірусних мереж державні структури втратили терабайти чутливої інформації. Скільки таких вірусів ще продовжує функціонувати, а надто розробляється нових, – невідомо. Водночас складно не помітити, що найменше страждають від дії цих вірусів КНР і США. І хоча це може свідчити про надзвичайну ефективність їхніх захисних систем, однак так само дозволяє зробити припущення про участь деяких з цих держав у створенні подібних вірусів. Маємо розуміти, що подібна кібершпигунська діяльність не лише не припиниться найближчим часом, а навпаки, розвиватиметься разом з подальшим проникненням ІКТ у всі сфери життя

суспільства, передусім у державне управління. Це порушує питання про забезпечення необхідного рівня безпеки державних установ, а також організацій, які володіють чутливою інформацією.

Проте навіть кібершпигунські системи не становлять такої небезпеки, як віруси, призначенням яких є не збирання інформації, а її знищення або цілеспрямоване атакування певних вузлів управління, що може не просто зупинити їх роботу, а й призвести до людських жертв. Йдеться про потенціал **кібердиверсій**, які здійснюються на об'єктах критичної інфраструктури або об'єктах, важливих для життєдіяльності держави.

На сьогодні прикладів застосування таких вірусів небагато, зробимо загальний огляд двох з них – *Wiper* та *Stuxnet*.

Пошук вірусу *Wiper* був чи не першим випадком, коли міжнародна організація офіційно запросила кібербезпекову компанію дослідити сукупність чуток щодо нового вірусу, який діяв передусім на території Ірану.

У 2012 році Міжнародний союз електрозв'язку звернувся до ЛК з проханням дослідити серію інцидентів, які призвели до знищення інформації на комп'ютерах у країнах Західної Азії. Власне, саме під час цього дослідження і були виявлені згадані *Flame* та *Gauss*, однак не вони були безпосередньою метою дослідників. Ішлося про вірус, який назвали *Wiper* (існують обгунтовані припущення, що вірус розпочав свою «роботу» ще в 2011 році). Проблема полягала в тім, що неможливо було знайти жодних слідів цього вірусу, адже він не лише знищував інформацію на комп'ютерах, а й майстерно прибирав будь-які свої сліди у комп'ютерній системі. Фахівцям компанії так і не вдалося відшукати безпосередньо код вірусу, однак, працюючи з опосередкованими доказами, вдалося отримати підтвердження його існування.

Основним завданням вірусу було знищення інформації, те, що вдавалося знищити, перезаписувалося «сміттєвими файлами». Судячи з відновленого експертами списку розширень файлів, які підлягали знищенню вірусом, передбачалося, що він знищить всю більш-менш важливу інформацію в системі. По суті, експертам вдалося лише частково відновити саму інформацію про вірус: «Шкідлива програма була написана так професійно, що після активації вона не залишала жодних даних. Тому, незважаючи на те, що ми бачили сліди зараження, сама програма залишається невідомою: ми не знаємо про інші інциденти з перезаписом вмісту диску, які мали таку саму схему, не заре-

єстровано також виявлення цього шкідливого програмного забезпечення механізмами наших захисних рішень» [223]. Опосередковано було встановлено зв'язок з вірусом *Flame*.

Уся шкода, завдана вірусами, про які йшлося вище, не завжди є вимірюваною. Проте найвідоміший на сьогодні вірус, який з повним правом може називатися кіберзброєю і який був застосований для кібердиверсії, має цілком конкретне «втілення»: 1368 з 5000 центрифуг на заводі із збагачення урану в Натанзі, а також зірвані терміни запуску ядерної АЕС у Бушері. І це все одна шкідлива програма, яка містить у ядрі лише 500 Кбайт коду, – вірус *Stuxnet*.

Перші повідомлення про те, що іранські ядерні об'єкти зазнали кібердару з'явилися в липні 2010 року. 10 липня білоруська компанія *VirusBlokAda* (*VBA*) повідомила про появу нового вірусу *Stuxnet*. І хоча увага преси зосередилася передусім на Ірані, від вірусу постраждало набагато більше країн. Поміж тих, які зазнали основного удару, Індія та Індонезія. Також вірус було знайдено на комп'ютерах у КНР, Росії, США, більшості країн ЄС та інших.

В Ірані відбулося концентроване зараження персональних комп'ютерів і великих автоматизованих комплексів. Понад те, впевнено можна стверджувати, що саме ядерна програма Ірану була основною ціллю вірусу. Про ефективність атаки свідчить той факт, що президент Ірану М. Ахмедініжад фактично публічно визнав, що вірус істотно вплинув на ядерну програму держави [422].

Сама структура та особливості поширення вірусу передбачали, що його метою є захищені системи без підключення до мережі інтернет (системи з підвищеним рівнем безпеки). За версією газети *The New York Times*, таке зараження відбулося в кілька етапів [247].

1. На зовнішньому носії (найшвидше, карті пам'яті) вірус був занесений у певну локальну мережу, що мала доступ до глобальної мережі.

2. Автоматично оновившись через спеціальній сервер у мережі інтернет, вірус поширювався в межах локальної мережі доти, доки не потрапив на комп'ютер людини, що має можливість користуватися переносними запам'ятовуючими засобами у внутрішній мережі індустріальних об'єктів (до яких належить і АЕС у Бушері).

3. Після потрапляння в потрібну внутрішню мережу вірус розпочав виконувати свою основну функцію – атакувати керуючі контролери компанії *Siemens*.

4. Подальша недбалість (невиконання протоколів безпеки) «звільнила» вірус, і він почав поширюватися планетою.

Кажучи про цей вірус, керівник ЛК Є. Касперський зазначав: «*Stuxnet* не краде гроші, не відсилає спам і не займається крадіжкою конфіденційних даних. Він створений для контролю за виробничими процесами, в буквальному сенсі – управляти масштабними виробничими потужностями <...> настає час кібертероризму, кіберзброї і кібервійни» [134].

Основною метою атаки вірусу були системи *SCADA*, що використовуються у системах моніторингу та управління промисловими, інфраструктурними та сервісними процесами на нафтопроводах, електростанціях, у потужних системах зв'язку, в аеропортах, на судах і навіть на військових об'єктах. Причому вірус *Stuxnet* «працює» не просто з будь-якими системами *SCADA*, а саме з тими, які мають конкретне програмне забезпечення – *SIMATIC WinCC* (система, що розробляється і підтримується корпорацією *Siemens*).

За два роки з моменту виявлення вірусу з'явилося чимало докладних звітів як про структуру вірусу, так і про механізми його «роботи» (наприклад, серія звітів фірми *Symantec* [221]). Загальними моментами, висвітленими в цих звітах і принциповими для дослідження, є такі: вірус однозначно не був витвором хакерів-одинаків і був спрямований на чітко визначену ціль. Підтвердженням цих висновків є такі факти.

1. У програмному коді вірусу використано чотири *zeroday*-уразливості та справжні цифрові сертифікати фірм *Realtek* та *JMicron*, що дозволило класифікувати атаку як унікальну. Загальна вартість лише схожих уразливостей на «чорному ринку» без розроблення програмного коду становить близько 60–70 тис. дол. США [78].

2. Вірус був розроблений для поширення передусім за допомогою флеш-накопичувачів, що у сучасному світі вкрай рідко використовується через незначні потенційні обсяги зараження.

3. Вірус не мав на меті жодної з класичних для вірусів цілей: знищення інформації, розсилка спаму, формування ботнета тощо. *Єдина мета – виводити з ладу певні вузькопрофільні системи.* Крім того, вірус, крім видимої частини, містить іншу, приховану, яка прописує себе на чіпи, що є нетиповим для класичних вірусів.

4. Вірус був доволі складним за своєю структурою, що повністю виключає самостійну роботу «ентузіастів». Технічний директор компанії *GSMK* Ф. Рігер (*Frank Rieger*), оцінюючи вартість створення такого вірусу, назвав цифру у 3 млн дол., США щодо кількості авторів і часу, потрібного для створення вірусу, він вказав близько 10 досвідчених програмістів і до півроку роботи [Цит. за: 186].

Додатково фахівці компанії *Symantec* розглянули інші можливі варіанти авторства вірусу (наприклад, хакер-одинак, незадоволений працівник, конкуренти) і дійшли висновку, що це малоймовірно і найбільш вірогідним варіантом залишається або спрямоване шпигунство, або пряма диверсія, за якою стоїть одна з розвинутих держав.

Хоча на сьогодні абсолютно точно відомо, що вірус міг уразити системи тільки через *USB*-накопичувач (який на режимному підприємстві міг використати тільки хтось з вузького кола осіб), досі однозначних даних про те, хто був цією особою, немає. У медіа є лише певні згадки про те, що цією людиною був один з працівників фірми *Siemens*[49].

Дискусійним залишається і питання конкретного авторства цього вірусу. У книзі «Протистояти та приховувати: таємні війни Обами та несподіване використання американської сили» (*Confront and conceal: Obama's Secret Wars and Surprising Use of American Power*) американський журналіст Д. Сенгер (*David E. Sanger*) з посиланням на «свої» джерела однозначно характеризує операцію з використання вірусу як спільну дію США та Ізраїлю [185]. Аналогічна інформація згадувалася й у публікації *The Washington Post* у липні 2012 року [372].

На нашу думку, з огляду на особливу зацікавленість у припиненні ядерної програми Ірану, спільна участь США та Ізраїлю дійсно має високий ступінь вірогідності. Надто навіть сам код вірусу містить деякі натяки на участь ізраїльської сторони:

• вірус позначається в реєстрі системи *Windows* як «19790509», що дуже схоже на дату. Фірма *F-Secure*, яка здійснила докладний аналіз вірусу зазначає, що 9 травня 1979 року в Тегерані був розстріляний бізнесмен Хабіб Ельганян (*Habib Elghanian*). Це був перший єврей, страчений революційним ісламським комітетом за шпигунство на користь Ізраїлю [421];

• у коді самого вірусу було знайдено слово *myrtus*, що може означати як гілку мірти, так й ім'я Есфірь (по-єврейські *Hadassah*). Ця іудейка була однією з дружин перського царя Ксерокса і змогла попередити євреїв про змову персів проти них. У результаті євреям вдалося врятуватися й помститися персам, а на честь цієї події святкується Пурим[50];

---

[49] Інформацію не було підтверджено, в інтернет-публікаціях її пов'язують з газетою *Sueddeutsche Zeitung*. У роботі наведено дані за публікацією [182].

[50] Водночас зазначимо, що подібне буквосполучення у комп'ютерній сфері може мати й принципово інше тлумачення, наприклад є скороченням від *My RTUs*, де *RTU* є абревіатурою від *Remote Terminal Units*, що використовується у системах на великих промислових підприємствах.

• у 2011 році в публікації газети *The New York Times* [247] з посиланням на експертів було висунуто версію, що вірус створений в ізраїльському ядерному центрі в Дімоні спільними зусиллями ізраїльських та американських фахівців протягом 2009–2010 рр. Дімон міг стати полігоном для випробувань, оскільки центрифуги, що там встановлені, майже ідентичні центрифугам у Бушері. Опосередковано цю версію підтверджує те, що окремі елементи вірусу було виявлено саме в 2009 році, однак тоді на них не звернули увагу.

Водночас фахівці вже в 2011 році звертали увагу на те, що з'явилося надто багато «прямих доказів» причетності Ізраїлю до цієї атаки. Що свідчить, швидше, про бажання реальних авторів вірусу відвести від себе підозру. Адже «недбалість» авторів вірусу дисонує з якістю самого вірусу: здається малоймовірним, що фахівці такого рівня могли залишити так багато «хвостів», за якими їх можна ідентифікувати.

Були також спроби «розділити» відповідальність за використання вірусу з європейськими країнами. 18 січня 2011 року британська газета *The Guardian* оприлюднила один з матеріалів сайту *Wikilieaks* [312], згідно з яким ідея проведення саботажів (до яких увійшли «нез'ясовні» вибухи, нещасні випадки та хакерські атаки) була озвучена ще наприкінці січня 2010 року одним з німецьких експертів у бесіді з послом США у Німеччині [441]. Однак з огляду на те, що вірус розроблявся принаймні з 2009 року, пропозиція німецького експерта не може розглядатися як прямий заклик до дії, що спричинив використання вірусу. Надто, за іншими повідомленнями у ЗМІ, Державний департамент США рішуче відмовився від подібних рекомендацій [30].

Прихильники різноманітних конспірологічних теорій звертали увагу також на неоднозначну роль двох комерційних фірм, що мали безпосередній стосунок до платформи, на якій здійснено атаку, – *Microsoft* і *Siemens*. Зокрема, викликало певні сумніви те, що фахівці однієї з найпотужніших *IT*-корпорацій у світі (*Microsoft*), програмні продукти якої використовуються, зокрема, у секторі безпеки, понад два роки не здогадувалися про наявність чотирьох (!) критично важливих уразливостей у власному програмному забезпеченні. Особливо зважаючи на зв'язки корпорації *Microsoft* з Агентством національної безпеки США, фахівці якого є надзвичайно кваліфікованими саме з питань *IT*-безпеки.

У геополітичному сенсі *Stuxnet*, завдав значно страшніший і небезпечніший удар, ніж виведення з ладу низки центрифуг. Він пере-

творив предмет напівтеоретичної дискусії про можливість використання кіберпростору у воєнних цілях на реалію і тим самим практично визначив майбутню невідворотну мілітаризацію кіберпростору. Це змінило баланс уваги провідних держав світу, змушуючи їх зважати і на цей рівень небезпек, нарощувати відповідний потенціал та стимулювати гонку кіберозброєнь. Вірус *Stuxnet* самим фактом свого існування назавжди підірвав позитивістське сприйняття кіберпростору суто як простору можливостей і зростання.

З упевненістю можна твердити, що саме *Stuxnet* став переламним моментом у загальному розумінні державами своєї уразливості перед кіберзагрозами. Як зазначають К. Демчак і П. Домбровський, «до *Stuxnet* держави не зовсім розуміли, як саме вірусні загрози можуть вплинути на них на стратегічному рівні. Однак *Stuxnet* змінив все. Якщо такі віруси можуть вплинути на загальнодержавні енергетичні системи, то держави просто не мають іншого виходу, ніж реагувати на цю загрозу, якщо вони хочуть захистити свої урядові та військові дії, а також своїх громадян від нових загроз. Держави зрозуміли, що в новому інтернетизованому суспільстві поняття вразливості для тих самих об'єктів критичної інфраструктури якісно змінилося. Понад те, механізм роботи *Stuxnet* продемонстрував, що навіть, здавалося б, найнадійніший спосіб боротьби з кіберзагрозами – вимкнення інтернету – не є панацеєю, оскільки кіберпростір не є абсолютною єдністю, а існує і на рівні окремих самодостатніх об'єктів» [290, с. 33].

Висновки до розділу

Очевидним є те, що суперництво між США та КНР зростає. Обидві сторони активно шукають новий формат взаємовідносин, однак поки що ці спроби є лише обмежено вдалими. Водночас на цьому тлі відбувається відчутне загострення двосторонніх відносин у кіберпросторі, де сторони звинувачують одна одну в діях, що завдають шкоди іншій стороні.

Якщо не буде винайдений реальний формат взаємовідносин між країнами, існує суттєвий ризик переростання їх суперництва в нове «холодне» протистояння, полем якого стане саме кіберпростір. Уже зараз експерти кажуть про зародження «холодної війни *v*2.0.», основними інструментами якої стануть вже звичні методи класичної «холодної війни» – непрямі методи боротьби, шпигунство, гонка озброєнь – з перенесенням їх до кіберпростору.

Обриси протистояння стають дедалі чіткішими, про що свідчить, зокрема, зростання кількості повідомлень у світових ЗМІ про вдалі чи невдалі спроби сторін здійснити взаємноспрямовані негативні дії. Усталеним інструментарієм такого суперництва/протистояння є хактивізм, кібершпигунство та кібердиверсії. Понад те, в окремих випадках можна говорити про розроблення програмних комплексів, що можуть бути кваліфіковані як кіберзброя.

Відсутність ефективних міжнародних інструментів протидії цим процесам може спричинити цифровий аналог Карибської кризи.

ГЕОСТРАТЕГІЧНІ АЛЬТЕРНАТИВИ КІБЕРНЕТИЧНОГО ПРОСТОРУ: ЗБРОЙНІ КОНФРОНТАЦІЇ *VS* КОМПРОМІСИ ТА СПІВРОБІТНИЦТВО

3.1. Альтернативні тренди кіберпростору: мілітаризація vs демілітаризація

Існують переконливі аналогії між трендами мілітаризації космосу й кіберпростору, на що звернув увагу, зокрема, Ф. Макдоналд: «Незважаючи на те, що ще в 1967 році було прийнято Договір ООН щодо космосу, в якому прямо заборонялося його мілітаризувати, провідні світові гравці і тоді, і зараз, міркуючи про подальші дослідження космосу, розглядають передусім його мілітарний потенціал <...> це справедливо і для кіберпростору» [359, с. 600].

Ціла низка специфічних ознак кіберпростору перетворюють його на поле воєнного протистояння, на що вказує Дж. Най-мол.: «Кібердомен включає не лише комп'ютери, під'єднані до мережі інтернет, а й інтранет, стільникові технології, оптоволоконні кабелі та розташовані в космосі комунікації. Кіберпростір має фізичний рівень інфраструктури, підпорядкований економічним законам суперництва за ресурси та політичним законам суверенної юрисдикції і контролю. Цей аспект інтернету не є «спільним» у традиційному розумінні. Водночас він має віртуальний, або інформаційний, рівень, що забезпечує масштабне економічне зростання й політичні практики. Він робить складним юридичний контроль за інтернетом. Атаки з інформаційної реальності коштують надзвичайно мало, однак можуть бути спрямовані проти фізичного домену, ресурси якого обмежені та недешеві. З іншого боку, фізичний рівень може мати на інформаційному рівні територіальний

й екстериторіальний ефекти. Кіберсила може продукувати результати (*outcomes*) як у кіберпросторі, так і поза його межами. За аналогією морська сила спрямована на використання ресурсів у морському просторі задля перемоги в морських битвах, однак океани так само можуть бути використані, аби впливати на битви, торгівлю, точки зору на суші. Таку аналогію можна застосувати й для повітряного простору» [383, с. 19].

Ще виразніше на зацікавленість військових структур у кіберпросторі вказує Д. Шелдон: «Основною стратегічною ознакою кіберсили, яка і робить її настільки унікальною у сучасному світі, є її можливість за воєнних і мирних часів маніпулювати стратегічною обстановкою, не даючи водночас противнику зорієнтуватися в цій обстановці. Стратегічна обстановка – це те, що вже сьогодні сприймається крізь призму кібертехнологій [мається на увазі, що більшість даних нині надходить з джерел, «під'єднаних» до кіберпростору, – *Авт.*] і, відповідно, залежить від них. Отже, здатність кіберсили впливати на сприйняття противником стратегічної обстановки з часом лише зростатиме, так само як і маніпулятивні можливості кіберпростору <...>. Відповідно, метою кіберстратега є максимізація зусиль, спрямованих на використання відповідних інструментів (кіберзброї), яка дозволить вирішувати диверсійні завдання проти кіберзалежного противника, знешкоджувати його системи зв'язку, моніторингу та шпигунства в кіберпросторі та, що найголовніше, впливати на прийняття ним тих чи інших рішень на користь того, хто маніпулює ресурсом» [411, с. 104].

«Безпековий дискомфорт», який відчувають сучасні держави, коли мають справу з кіберпростором та мережею інтернет, спричинений передусім неврегульованістю цих відносин. Адже якщо вияви агресії на фізичному рівні більш-менш формалізовані та унормовані як на національному, так і міжнародному правовому рівні, то кіберпростір з його можливістю впливати на фізичний простір викликає у сучасних держав «правове непорозуміння» [61].

Додатковим ускладнювальним чинником є сама історія створення нового домену міждержавного протиборства і, зокрема, його найбільш відомої компоненти – інтернету. Як слушно зауважує Дж. Най-мол., «проблема в тім, що інтернет був розроблений для легкого використання, а не для безпеки» [383, с. 21].

Незважаючи на військове призначення *ARPANETy,* з 80-х років XX сторіччя він дедалі більше комерціалізується, перетворюючись на структуру, де «всі один одного знають». Своєрідна іронія подальшого

розвитку кіберпростору полягає в тім, що в міру зростання рівня інформатизованості країни її можливості в різних сферах пропорційно зростають, але водночас така країна стає дедалі уразливішою до зовнішніх і внутрішніх викликів і загроз, що спричинює зрештою новий виток гонки кіберозброєнь.

Оцінюючи потенціал кіберпростору як джерела небезпек і руйнувань, доречно порівняти ці небезпеки та руйнування з потенційними наслідками ядерної війни. Таке порівняння наводить М. Лібіцкі, на думку якого, «знищення або від'єднання кіберсистем здатне повернути економіку в 1990-ті роки через значне зниження ВВП, водночас маємо пам'ятати, що ядерний удар цілком може повернути нас у кам'яний вік» [349, с. 136]. Водночас М. Лібіцкі як головний науковий співробітник *RAND Corp.*, який спеціалізується на питаннях кібербезпеки, постійно скептично висловлюється щодо «алармістського» переоцінювання кіберзагроз, зазначаючи, зокрема, що більшість організацій (незалежно від форми власності) залежні від кіберпростору лише настільки, наскільки вони хочуть бути залежними [348, с. xiv]. Крім того, на його думку, «операції, що можуть визначені як «кібервійна», завдають шкоди передусім індивідуальності, не знищуючи при цьому обладнання (з певними винятками). У гіршому разі ці операції можуть збентежити та дезорієнтувати операторів військових систем, і справді лише тимчасово. Тому кібервійна може підтримувати інші елементи воєнних дій, зокрема обеззброювати противників» [Там само, с. xiv-xv].

Така скептично-раціональна позиція в оцінюванні руйнівних наслідків воєнних дій у кіберпросторі характерна в цілому для американських науковців, наближених до військового сектору. Потенційні наслідки тлумачаться переважно в контексті заходів підтримання основних сил, оскільки самостійні «змушуючі» можливості кіберпростору вважаються доволі обмеженими. Причому для ілюстрації цих обмежень американські дослідники використовують, у дусі традицій «холодної війни», приклади російських кібератак на кіберсистеми Естонії й Грузії (2007–2008 рр.) Хоча, як зазначалося у розділі 2, зазначені події є майже хрестоматійними прикладами демонстрації саме небезпеки кібервійн.

Обстоюючи зазначену скептичну позицію на цих прикладах, Д. Шелдон зауважує, що Естонія реагувала в першу чергу на більш традиційні погрози з боку російської сторони, передусім дипломатичні, тоді як кіберкомпонента стала лише додатковим «неприємним»

чинником. Аналогічно в Грузії. Так, російські кібератаки порушили процес надання інтернет-послуг, однак складно уявити, що російська воєнна кампанія була б скільки-небудь менш вирішальною, якби кібератак не було або вони закінчилися б невдало [411, с. 99].

Зазначимо певну невідповідність позиції тих, хто вважає можливості кіберозброєнь недостатніми для впливу на реальну обстановку. Так, у термінах традиційного військового розуміння «примусу» кіберозброєння дійсно можна визнати такими, що мають обмежений потенціал. Однак оцінюючи можливості впливу кіберозброєнь на формування позицій осіб, які вповноважені приймати рішення (зокрема високопосадовців), потенціал кіберозброєнь переоцінити важко.

Водночас ідеї стрімкої мілітаризації кіберпростору підживлює об'єктивна неспроможність більшості держав виробити міжнародні правила гри, які гарантували б їм базову безпеку. Г. Раттрей з цього приводу зазначає: «Кіберпростір перетворюється на основне середовище політичного та військового суперництва. Нові загрози виходять від акторів, які не є суперниками в інших реальностях (*realms*). Інтелектуальна власність може бути втрачена; противники можуть здійснювати руйнівні операції <...> Нові воєнні можливості та інтереси приватного сектору потребують збалансування можливостей і ризиків; це вимагає прискіпливого аналізу, досі не зробленого. США мають вивчити, як захистити свою присутність у кіберпросторі економічно доцільним способом. Це може спричинити створення масштабних атакуючих сил для захисту комерційних інтересів у мережі; управління міжнародними зусиллями та нормами, спрямованими на обмеження руйнівної активності одних держав проти інших, та покарання недержавних авторів; можливо, новий кібер-Манхеттенський проект може встановити безпечнішу технологічну основу кіберпростору.» [285, с. 265].

Г. Раттрей пояснює і саму важливість кіберпростору для військового сектору: «розвиток військово-повітряних сил у першій половині XX сторіччя означав, що атака проти стратегічних центрів може бути здійснена впродовж години. Поява балістичних ракет з ядерними боєголовками скоротила цей термін до кількох хвилин. Актуалізація кіберпростору скоротила його до секунд.» [Там само, с. 267].

Водночас спроби розв'язання проблем правової протидії мілітаризації кіберпростору наражаються на обмежену готовність міжнародного законодавства відповісти на цей загрозливий тренд. Ключове питання більш-менш точно сформулював американський фахівець

з кіберправа Д. Аддікотт (*Jeffrey F. Addicott*), який зазначив, що міжнародне законодавство, пов'язане з використанням сили, є не зовсім адекватним проблемі протидії кібервійнам [235]. Інші дослідники (наприклад Дж. Чарлз (*J. Charles*) [258]) вказують на «кібернетизацію законів воєнного конфлікта (*Law of armed conflict – LOAC*[51])». Зокрема, кіберексперт Б. Шнаєр (*Bruce Schneier*) звертає увагу на те, що час, відведений для створення адекватної кіберугоди, спливає, і це означає, що використання кіберзброї й досі залишається юридично неврегульованим питанням, хоча вірогідність кіберконфліктів зростає [408].

Однак навіть налаштовані оптимістично міжнародні правники сумніваються в можливості прийняття у найближчому майбутньому міжнародного документа, спроможного впорядкувати зазначені питання. Причиною є передусім його доволі умовна ефективність. Відомий американський політичний коментатор Ч. Краутхаммер (*Charles Krauthammer*) формулює, зокрема, цю проблему так: «Починаючи з морської угоди 1920 року і дотепер контроль над озброєннями завжди балансував між двома полюсами, одним з яких (і це в ліпшому разі) був істотний символізм режиму контролю, а другим (у гіршому разі) цілковита беззмістовність, спроможна завдати збитків світовій безпеці в цілому. Проблемою ніколи не була зброя як така; проблемою був режим контролю озброєнь» [340].

Дійсно, режим контролю вкрай рідко був ефективним і неадекватно сприймався великими країнами, які часто вважали його лише елементом стримування. Зокрема, цей підхід є офіційною позицією чинного керівництва США. Заступник міністра оборони У. Лінн зазначив, що традиційні угоди з контролю озброєнь, щонайшвидше, нездатні стримувати кібератаки передусім тому, що провести відповідну перевірку практично неможливо [357]. Незважаючи на це, США в цілому висловлюють готовність брати участь у розробці нових норм поведінки в кіберпросторі, хоча й не на базі ідей, які пропонують Росія та КНР [258].

Ключовим питанням, тісно пов'язаним з проблемою мілітаризації кіберпростору, є проблема визначення акту війни в кіберпросторі (які дії в кіберпросторі можна вважати актом війни), про яку йшлося вище. Без адекватної відповіді на це запитання держави очевидно безпорадні в тім, які конкретно інструменти можуть бути використані

[51] Також відомі як «закони (право) війни» – *Law of War, LOW.*

проти них у кіберпросторі зі шкодою для їхніх національних інтересів. Водночас, розуміючи невирішеність даного питання, вони не можуть встояти перед непереборним бажанням скористатися такими інструментами, поки впевнені у відсутності зворотної відповіді потенційної жертви.

Розуміння кібератаки як акту війни переводить її в поле правозастосування *LOAC*, а отже, і всього комплексу економічних, дипломатичних і воєнних заходів. Якщо ж йдеться не про акт війни, то питання потрапляє в поле кримінального правозастосування, тобто є сферою відповідальності не військових, а правоохоронних органів. Нинішня модель міжнародної поведінки держав за мовчазної згоди зводиться саме до розуміння кібератак у кримінальному сенсі.

Саме поняття *акт війни* досить умовне і є, швидше, політичною, ніж юридичною конструкцією. Як зазначає Дж. Чарлз [258], насправді Статут ООН зробив все можливе, аби викинути з міжнародного юридичного лексикону слово *війна*. В його ключових статтях які, власне, і відносять до «військових» (ст.ст. 2(4) та 51) геть не йдеться про *війну* – натомість згадується значна кількість евфімізмів на кшталт *загроза силою; застосування сили проти територіальної цілісності; збройний напад; право на самооборону*. Все це створює значні проблеми для стратегування в кіберпросторі, оскільки існують суттєві нюанси в режимах застосування сили, коли всі учасники застосовують силу, однак не всі види застосування сили класифікуються як *збройні напади*.

Водночас деякі юристи-міжнародники все ж бачать можливості застосування чинного законодавства для кібернападів. Наприклад, для цього використовуються окремі положення Протоколу 1 Женевських конвенцій. Хоча це є, швидше, паліативом, сумнівним з погляду політичного обґрунтування.

Зауважимо, що описане є складником більш масштабної проблемної ситуації, пов'язаної з вельми невизначеним юридичним тлумаченням поняття *акт війни* та розумінням того, які саме події підпадають під дію ст. 51 Статуту ООН. Саме тому подеколи Міжнародний суд ООН визнавав випадки надання військової допомоги повстанцям недостатньою умовою для застосування сили у відповідь.

Для кіберпростору ця невизначеність ускладнюється тією обставиною, що ст. 51 Статуту ООН, яка регулює відносини між державами, побудована на реаліях вестфальського світоустрою, тоді як кіберпростові проблеми вочевидь пов'язані з поствестфальською

моделлю міжнародних відносин. У контексті тлумачення поняття *акт війни* це є особливо актуальним. Адже атаку на державні структури може здійснювати недержавний актор з території певної держави, а тому виникає закономірна колізія щодо відповідальності цієї держави за подібну кібератаку. На це звертає увагу вже згадуваний юрист-міжнародник М. Шмітт: «Кібернасильство будь-якого рівня інтенсивності, якщо воно здійснюється окремими особами чи навіть неорганізованими злочинцями, навіть якщо воно здійснюється проти уряду, не створює *збройного конфлікту* в тому сенсі, як його розуміє Женевська конвенція» [406].

Отже, через можливість зловмисників вдало маскувати свою діяльність і навіть представляти свої агресивні дії такими, що були здійснені з території іншої держави, питання постає особливо гостро. Одним з можливих шляхів його вирішення є процедура звернення до урядів (чи уповноважених національних безпекових структур) відповідних країн з вимогою припинити діяльність зловмисників. Лише тоді, коли ці державні структури не захочуть чи не зможуть вплинути на ситуацію, юридично справедливими можна вважати заходи активної самооборони, тобто відсічі кіберагресорові з усіма негативними наслідками для країни його місцезнаходження. Однак такий сценарій дій є доволі умовним через особливості ведення агресивних дій у кіберпросторі, адже реагування має здійснюватися у режимі реального часу, мало не паралельно із самою кібератакою, отже, на переговори просто не вистачить часу.

Інше непросте питання полягає в тім, як юридично тлумачити статус *учасників кібервійн*. Адже згідно з чинним міжнародним законодавством повноважні учасники збройних конфліктів – це солдати, або комбатанти, які мають особливий юридичний статус повноважних брати участь у збройних конфліктах. Комбатанти не переслідуються у судовому порядку за здійснені ними під час війни вбивства, бо мають «маркери», які відносять їх до збройних сил тієї чи іншої держави та інші супутні ідентифікуючі елементи. Якщо таку юридичну практику поширити на учасників кібервійн, то їх також слід визнати комбатантами, тобто «військовослужбовцями, які тиснуть на клавіші задля виведення з ладу ворожих систем» [269, с. 233].

У контексті дискусії про статус учасників кібервійн цікаво зауважити, що, незважаючи на жорстку позицію керівництва США щодо розрізнення кіберпитань й інформаційно-психологічних впливів, безпекові структури США (передусім Міністерство оборони США

та ЦРУ) активно здійснюють інформаційно-психологічні операції у блогосфері (соціальних мережах тощо), створюючи вигідну для себе громадську думку з актуальних воєнних і безпекових питань (наприклад довкола компаній в Іраку та Афганістані) [258, с. 96].

Мілітаризацію кіберпростору також обумовлює латентний характер загроз, які з нього виходять. З цього приводу Д. Шелдон зазначає: «кіберсила[52] може бути надзвичайно прихованою. Одна з привабливих рис кіберсили – можливість її застосування в глобальному масштабі без виявлення. Шкідливе програмне забезпечення може ховатися у ворожих мережах, поки не буде активоване і не завдасть шкоди. Бази даних можуть бути «зламані» заради закритої чи пропрієтарної інформації, а її власники можуть навіть не помітити, що в них вкрали терабайти даних. Так само пересічні громадяни можуть відчути вплив кіберзлочинців на своє життя лише тоді, коли їм вже буде заподіяно шкоду – зруйновано їхній кредитний рейтинг або спустошено їхні кредитні карти. Ця здатність кіберсили бути абсолютно непомітною робить її надзвичайно привабливою для урядів та інших акторів» [411, с. 101].

Ще однією особливістю кіберпростору, яка змушує військові структури більшості світових держав надавати йому особливої уваги, пов'язана з тотальною цифровізацією озброєнь. Ця реалія має як суто технологічну компоненту, так і компоненту людську: персональні комп'ютери військовослужбовців; обладнання для операторів, які керують різноманітними безпілотниками, наприклад БПЛА; використання технологій *SCADA*; застосування ІКТ у всіх основних видах озброєнь – танках, літаках, кораблях, ракетах й навіть у ручній зброї. Щороку залежність військової техніки від ІКТ зростає, а отже, взаємообмін даними між військовими ІКТ-пристроями є елементом загального кіберпростору.

Відповідно, й система командування, яка, на думку ізраїльського військового аналітика М. ван Кревельда (*Martin van Creveld*), є «функцією, яка має існувати більш-менш безперервно задля того, щоб армія могла існувати та працювати», перетворюється на заручницю ІКТ [273, с. 5].

---

[52] Щороку в роботах американських дослідників поняття *кіберсила* з'являється дедалі частіше, однак при цьому його визначення є ще більш неоднозначними ніж, припустимо, визначення *кіберпростору* чи *кібервійни*. На нашу думку, це перспективнй напрям наукових міркувань, оскільки дозволяє в осяжній перспективі формалізувати кіберкомпоненту та її значення для забезпечення національних інтересів.

Таке узалежнення елементів військової системи, критично важливих для обороноздатності держави та захисту її національних інтересів, від ІКТ є об'єктом пильної уваги потенційних «опонентів» держави, які розробляють плани деструктивного впливу на подібні системи в разі збройного конфлікту. До того ж дедалі частіше поширення ІКТ у військових системах опосередковано викликає в командирів нижчої ланки спокусу використати доступну їм надзвичайно детальну тактичну інформацію для самостійного прийняття рішень та ігнорування вищого командування, яке володіє стратегічною обстановкою в цілому.

Саме такі сценарії перехоплення управління «цифровізованими» військовими системами зазвичай створюють образ «цифрового Перл Харбору» як прецеденту тотальної поразки та неготовності збройних сил держави відповісти на миттєвий неочікуваний удар. Левова частка наукових досліджень й науково-публіцистичних робіт, присвячених проблемі протистояння в кіберпросторі, апелює саме до цього образу. Цікаво, що більшість подібних робіт належить відставним генералам ВПС США, які, вочевидь, бажають подібним «алармічним» способом впливати на формування пріоритетів розвитку Збройних сил США.

На нашу думку, надзвичайні масштаби кіберкатастрофи, як, проте, і надмірно заспокійливі сценарії кібернетичного майбутнього, автори яких наполягають на «периферійності» кіберпростору та загроз, з ним пов'язаних, слід визнати такими, що не відповідають сучасним реаліям.

Дж. Бреннер *(Joel Brenner),* який майже 20 років присвятив розвідці (передусім Агентству національної безпеки США) і, зокрема, кібербезпеці, в книзі «Америка вразлива: усередині матриці нової загрози цифрового шпигунства, злочинів і війни» (*America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*) цілу главу присвятив гіпотетичній дипломатичній кризі у відносинах США – КНР, яка, не переростаючи в жорстке воєнне протистояння, відбувається в кіберпросторі. Згідно з гіпотетичним сценарієм Дж. Бреннера внаслідок дій китайських хакерів не відбуваються вибухи на хімічних підприємствах, не падають авіалайнери та не сходять із рейок потяги. Стирається значний масив даних у військових мережах, вносяться інформаційні шуми у системи керування ракетами та навігаційне обладнання літаків і здійснюється низка інших подібних актів з метою змусити керівництво держави та її розвідувальні органи зрозуміти, що вони не володіють ситуацією і не мо-

жуть з упевненістю передбачити, де буде завдано наступний удар та чи не станеться так, що він буде більш жорстким [Цит. за: 246].

Незважаючи на очевидність надзвичайно деструктивного потенціалу кіберозброєнь, багато експертів не бачать необхідності в розробленні міжнародних договорів щодо кіберозброєнь. Наприклад, Л. Мюїр (*L. Lawrence Muir, Jr.*), ад'юнкт-професор права в Університеті Вашингтона та Лі, зазначає що,такий договір буде абсолютно недоцільним через правовову невизначеність більшості понять з частиною *кібер,* передусім поняття *кібервійна.* Крім того, зважаючи на можливості злочинців приховувати свою діяльність, малоймовірним є віднайдення форми доказовості щодо таких злочинів (а надто застосування кіберозброєнь), які була б прийнятною для міжнародного товариства [344].

Ш. Лоусон (*Sean Lawson*) з Університету Юти також вважає подібну угоду недоцільною [Там само], звертаючи увагу на те, що практично всі технології, пов'язані з кіберпростором, є технологіями «подвійного призначення», а те, що наразі називають кіберзброєю, не є зброєю в традиційному розумінні. Подібної думки дотримується і Д. Ліндсей (*Jon Lindsay*) [354].

Показово, що ідею опрацювання міжнародних договорів щодо кіберозброєнь заперечують також два знаних американських фахівці у сфері кібербезпеки – М. Лібіцкі та Дж. Льюїс. М. Лібіцкі, обґрунтовуючи свою позицію, зазначає, що такий договір буде неефективним через складність контролю того, заради чого його буде укладено: «при виробництві кіберозброєнь не виробляється, власне, нічого, що можна було б контролювати та відслідковувати. Такі озброєння тестуються у відокремлених від мережі системах, які лише її імітують. Якщо до цього додати можливості хакерів приховувати свої дії та не залишати «відбитків пальців», то шансів їх упіймати надзвичайно мало» [350]. Директор Програм з технологій та державної політики Центру стратегічних і міжнародних досліджень Дж. Льюїс також зазначає неможливість реалізувати положення таких договорів на практиці [346]. Він звертає увагу на те, що ідеї подібних договорів належать початку 90-х років XX сторіччя, і їх продовженням є останні неактуальні ініціативи Росії щодо Конвенції про забезпечення міжнародної інформаційної безпеки (КЗМІБ).

Усупереч подібним скептичним зауваженням певні наукові розробки щодо міжнародно-правового впорядкування проблеми застосування кіберозброєнь здійснюються. Так, екс-працівник Агент-

ства США із захисту інформаційних систем Д. Браун (*Davis Brown*) у 2006 році виклав своє бачення важливості міжнародного врегулювання кібервійн [248], запропонувавши структуру можливої міжнародної конвенції, що регулює використання інформаційних систем у збройних конфліктах. Звернувши увагу на те, що більшість війн і конфліктів так чи інакше призводили до ухвалення міжнародних конвенцій, що забороняли або певні дії, або певні види озброєнь (наприклад Женевський протокол 1925 року, Конвенція про біологічну зброю 1972 року чи Конвенція про хімічну зброю 1992 року), Д. Браун слушно зазначає, що зростання можливостей сучасних інформаційних технологій під час воєнних дій змушує розглянути доцільність прийняття подібної конвенції і в цій сфері.

Крім того, Д. Браун, посилаючись на професора М. Шмітта, зауважує, що сучасні конфлікти з використанням кіберзброї характеризує значний рівень «зростання залежності військових від громадян (*civilians*), громадських об'єктів (*civilian objects*) та громадської активності». Це створює важливий зв'язок між сучасними воєнними діями та громадським, що є феноменом, хоча і не принципово новим, але виняткова важливим. Вказуючи на можливість визначення поняття *інформаційна зброя* (Д. Браун уникає поняття *кіберзброя,* однак, судячи з тексту, має на увазі саме це, більш широке, поняття) автор проводить аналогію з вогнепальною зброєю. Сама по собі така зброя (пістолет, рушниця чи інший її різновид) не є, власне, зброєю (хіба що її буде використано в ролі кийка) й сама по собі куля не може вбити людину (хіба що вибухне випадково). Таким чином, власне зброєю можна вважати лише заряджений пристрій, з якого зроблено постріл кулею, яка, вилітаючи з певною швидкістю, дозволяє поціліти – заподіяти шкоду. Щодо інформаційної зброї, то, на думку Д. Брауна, йдеться про певний комплекс інструментів, які не просто співіснують, але з певною метою поєднані: «Таким чином, кажучи про ідентифікацію *інформаційної зброї,* маємо на увазі три компоненти: код, комп'ютерну систему та оператора. Кожен з цих компонентів має підпадати під міжнародне законодавство, яке регулює збройні конфлікти. Відповідно, застосування цієї зброї має стримуватися принципами воєнної необхідності, пропорційності, гуманності, лицарства, а цілі для неї мають бути легітимними» [248, с. 185].

Слід зазначити, що за такого розуміння кіберзброї поле застосування міжнародного законодавства буде доволі непевним, на що, зрештою, вказує сам Д. Браун. Він зазначає, що інформаційною зброєю є

лише комп'ютер, на якому генерується шкідливий код, тоді як решта комп'ютерів, природно, не є такою зброєю.

Отже, на даному етапі міжнародні ініціативи, спрямовані на заборону розроблення та застосування кіберозброєнь чи ведення кібервійн, мають сумнівні шанси на прийняття, і поготів – на реалізацію. І хоча варто погодитися з ініціативами на кшталт ідеї фахівців Східно-Західного інституту (*EastWest Institute*[53]) щодо спеціального «цифрового маркування» суто цивільних об'єктів, проти яких не має застосовуватися кіберзброя, але потрібно розуміти обмеженість дії подібних договорів. Вони радше, роблять ставку на моральність учасників кібервійн, а не на «вразливість» технологій до застосування контрольних механізмів детекції.

Загалом дискусія довкола проблем мілітаризації/демілітаризації кіберпростору дедалі активніше повертається до сюжетів часів «холодної війни»: політики «стримування», ідей «гарантованого знищення» тощо. Проблеми, пов'язані з кіберзброєю, порівнюються з проблемами, пов'язаними з ядерною зброєю, із загальносвітовим розумінням необхідності створення механізмів, які дозволили б уникнути самознищення людства. Китайський дослідник кібербезпекових проблем Л. Тенг (*Lan Tang*) вказує в даному порівняльному контексті: «кіберпростір сьогодні такий саме небезпечний, як і світ 1950-х років, коли склався жахливий баланс ядерного терору» [424, с. 44].

Проте, наприклад Дж. Най-мол., який звертається до цієї проблеми докладніше у статті «Ядерні уроки для кібербезпеки?» [383], вказує, що запозичення досвіду подій 70-річної давнини для опису сьогоднішньої ситуації є недоцільним через значну відмінність у технології. Якщо ядерний вибух є цілковито однозначною подією, яка відбувається тут і зараз, завдає очевидної кінетичної шкоди, то кібератака може бути не виявленою впродовж тривалого часу й навіть тоді, коли вона виявлена, далеко не завжди є зрозумілим, проти чого, власне, її було застосовано.

З'являються також порівняння впливу кіберзагроз із загрозами, пов'язаними з хімічною або біологічною зброєю. Однак кібербезпекову та ядерну проблематику зближують питання історії й динаміки вирішення.

---

[53] *East-West Institute (EWI),* відомий як Східно-Західний інститут досліджень у сфері безпеки, є міжнародною неприбутковою, недержавною «фабрикою думки та дії», що фокусується на вирішенні міжнародних конфліктів за допомогою різних засобів.

Аналогії політики ядерного стримування з політикою стримування загроз, які виходять з кіберпростору й невпинно зростають на тлі його подальшого розвитку та узалежнення від нього життєдіяльності людей, мають екзистенційний характер. Неприпустимість масованих ядерних атак обумовлювалася відсутністю переможців і переможених у разі їх здійснення, отже, йшлося про виживання людства. Особливо гостро було усвідомлено подібну безальтернативність після винайдення водневої бомби. Саме так виник «парадокс використання»: ядерна зброя може попередити агресію тільки якщо існуватиме можливість її використання, однак потрібно не робити її настільки зручною, щоб виникла така спокуса[54] [253, с. 34].

Неможливість реального використання ядерної зброї і перетворення у певний момент «методології досліджень наслідків ядерного нападу на катехізис» [Цит. за: 383, с. 24] спричинили виникнення апологетики апокаліптичних ядерних сценаріїв і цілої плеяди «залякувачів», яких Дж. Най-мол. кваліфікував як «ядерних богословів». У їхньому розпорядженні опинилися чималі ресурси для створення гіпотетичних сценаріїв ядерного апокаліпсису.

Наразі чимало дослідників кібербезпеки висловлюють подібні підозри щодо перебільшення загроз, пов'язаних з мілітаризацією кіберпростору. Д. Жирар (*John Girard*), віце-президент та аналітик *Gartner*, компанії, яка розробляє прогнози розвитку *IT*-сфери, порівняв у «алармічному» контексті сучасну індустрію кібербезпеки з фінансовою пірамідою: «усе починається із законних інвестицій [у кібербезпекову сферу – *Авт.*], а потім настає новий виток [у розвитку кібербезпекової сфери – *Авт.*]. Вам обіцяють певний дохід і просять залишитися. Коли ви з цим себе пов'язуєте, то не можете піти, оскільки такий крок створюватиме певні проблеми.» [20].

Зауважимо, що кібербезпекова проблематика має беззаперечну перевагу в плані залякування. Масштабні регулярні атаки хакерів і кіберзлочинців усіх рівнів створюють необхідну «базу залякування» політиків, якої не існувало за часів політики ядерного стримування.

Попри різність підходів до визначення різних кібервиявів і ставлення до мілітаризації кіберпростору та незважаючи на взаємну недовіру між ключовими геополітичними суб'єктами, вони усвідомлюють необхідність співпраці заради забезпечення глобальної кібербезпеки.

---

[54] Англ.: *Nuclear weapon can prevent argession only if there is a possibility that they will be used, but we do not want to make them so usable that anyone is tempted to use one.*

І, хоча деякі країни наразі намагаються уникнути відповідальності за забезпечення кібербезпеки у спосіб непідписання наявних безпекових документів (в тому числі регіональних на зразок Конвенції про кіберзлочинність), однак вони дедалі більше розуміють, що намагання самотужки вирішувати проблеми кібербезпеки є обмежено ефективними. Міжнародна співпраця має реалізовуватися передусім у напрямі генерування й реалізації ідей стратегічної демілітаризації кіберпростору й створення механізмів взаємного стримування гонки кіберозброєнь.

Однак для закріплення подібного розуміння стратегічної демілітаризації кіберпростору недостатньо просто раціонального мислення. Можливо, розуміння сягне повноти лише на тлі цифрового аналогу Карибської кризи.

Дж. Най-мол. вважає, що, виходячи з історії взаємовідносин великих країн протягом останніх 70-ти років, складно уявити, що вони дійсно можуть створити міжнародні правила гри, які реально обмежуватимуть забезпечення ними їхніх національних інтересів. Водночас цілком ймовірно, що на частину дій, які нині зашкоджують усім ключовим гравцям (наприклад, кібершпигунство), буде накладено неформальні обмеження, взяті на себе країнами добровільно. Це знову нагадує реалії «холодної війни» та формування «кодексу правил взаємної поведінки, спрямованих на мінімізацію небезпеки», бо будь-яка інша політика може виявитися самогубством [249, с. 244]. Саме ці правила викликали взаємну «повагу» в питаннях розподілу сфер впливу та вирішенні Карибської кризи, що в подальшому стало підґрунтям ядерного роззброєння.

Щодо кіберпростору ситуація, щонайшвидше, складатиметься аналогічно – поступово оформлюватиметься спільне розуміння всіма зацікавленими сторонами необхідності напрацювання спільних підходів.

Водночас вирішення питання демілітаризації кіберпростору ускладнюється низкою особливостей, пов'язаних, зокрема, з формально-юридичною диференціацією *воєнних дій (того, що можна вважати воєнними діями) і хуліганства* (*злочинної діяльності)* в кіберпросторі.

Уже згадуваний фахівець з кіберконфліктів Х. Лін зауважує на відсутності необхідного історичного досвіду, який дозволив би диференціювати *воєнний кіберконфлікт* уже на початковій стадії. Він слушно підкреслює, що таке розрізнення є проблемою навіть для традиційних кінетичних війн і ще більше ускладнюється для кібервійн [353].

Іншим аспектом невизначеності у зусиллях мінімізації глобальних кіберконфліктів є *зміцнення довіри* та *прозорість підготовчих (попереджувальних) дій*. Якщо для звичайних озброєнь існує цілий комплекс загальновизнаних заходів контролю та прозорості дій (наприклад, узгоджений порядок проходження військово-морських суден, попередження сусідніх країн про переміщення великих груп військ, звітування перед міжнародними структурами щодо масштабів закупівлі військової техніки тощо), то для кіберпростору з його невизначеними кордонами та зонами відповідальності це є досі доволі умовним. Особливо зважаючи на те, що генерування сил, необхідних для кібератаки, може відбуватися абсолютно таємно. Понад те, сам успіх кібератаки багато в чому залежить від прихованості дій.

Далеко не остання за значущістю проблема попередження кіберконфліктів полягає у відсутності чітких механізмів їх припинення чи зменшення ризиків ескалації. Сама природа кіберпростору перетворює гіпотетичні механізми взаємних гарантій і зобов'язань на умовні й ненадійні.

Розглядаючи можливість створення дієвих міжнародних угод щодо обмеження кіберозброєнь, Дж. Най-мол. слушно зауважує: «Деякі люди закликають до переговорів щодо контролю кіберозброєнь і підписання формалізованих договорів, однак відмінності в культурних нормах і неможливість підтвердження [дієвості механізмів] робить подібні договори складними для обговорення чи імплементації. Такі спроби могли б насправді знизити [рівень] національної безпеки, якщо асиметрична імплементація поставить США з їх специфічною юридичною культурою в невигідне становище стосовно суспільств з більш високим рівнем урядової корупції. Водночас зовсім «не зарано» ставити питання щодо міжнародних переговорів і налагодження співпраці» [383, с. 36]. Загалом позиція Дж. Ная-мол. зводиться до такого.

Звертаючись до можливих ідей, на базі яких великі країни могли б розпочати переговори щодо демілітаризації кіберпростору, доцільно ще раз звернути увагу на досвід часів «холодної війни» та ядерного стримування. Перші угоди на цьому шляху стосувалися не стільки взаємного роззброєння чи обмежень, скільки третіх сторін (наприклад, непроліферації, тобто ненадання третім сторонам, ядерних технологій). Потенційну демілітаризацію кіберпростору також доцільно розпочати з питань, непов'язаних з антагоністичними суперечностями. Предметом відповідних договорів може бути протидія терорис-

тичним кібератакам, здійснюваним третіми сторонами. Знайдені на цьому шляху спільні позиції згодом можуть перетворитися на першооснову більш масштабних договірних порозумінь (на зразок Заключного Акту Гельсінкської угоди 1975 року).

Вказуючи на перепони на шляху до підписання можливої угоди з питань демілітаризації кіберпростору, М. Лібіцкі зазначає неможливість прямих аналогій між ядерним стримуванням й кіберстримуванням. У першому випадку чітко зрозумілим був предмет загроз та їх наслідки, проте вони досі не усвідомлені щодо кіберзагроз [333]. Крім того, М. Лібіцкі зауважує на чіткій різниці ядерного стримування від кіберстримування: «Під час ядерної реальності часів «холодної війни» визначення атаки не було проблемою, перспективи бойового ураження були зрозумілими, тисячі бомб були могутніми, як кулак, протидія була можливою, непотрібно було непокоїтися через треті сторони, приватні компанії не очікували, що мають захищати самі себе, не існувало будь-яких вищих рівнів війни, сторонам [конфлікту] було що втрачати» [348, с. xvi]. Однак, як зауважує дослідник, все це є неактуальним у разі кіберпротистояння [Там само]. Не впевнений він і в правомірності аналогій між кіберстримуванням та ядерним стримуванням щодо попередження масштабного конфлікту. Ядерний удар обов'язково обернеться ударом у відповідь (при цьому вважається, що удар у відповідь не зачепить «невинуватих», оскільки точно відомо, хто першим завдав удару). Зовсім іншою є ситуація складається для застосування стратегії кіберстримування:

• далеко не завжди можна визначити, хто, власне, атакує;

• навіть якщо вдасться відповісти на масштабну кібератаку, зовсім не факт, що вдасться це зробити вдруге;

• навіть у разі можливості завдати удару у відповідь немає жодних гарантій, що об'єкт цілі дійсно буде виведений з ладу;

• немає жодних гарантій, що у протистояння не будуть втягнені треті сторони, передусім недержавні актори;

• кіберстримування може стати неправильним сигналом для внутрішніх гравців: якщо держава заявить про потенційну можливість кібератак як ударів у відповідь, спрямованих на об'єкти критичної інфраструктури, що належать приватному сектору, то це неодмінно спричинить небажання власників інфраструктурних об'єктів вкладати кошти в їх безпеку (зокрема кібербезпеку);

• державам буде вкрай складно встановити порогові значення, понад які буде завдано удар у відповідь. Це може спонукати до подібних

ударів навіть на незначні кібератаки на тлі недооцінювання інших, більш значних;

• кіберпротистояння, щонайшвидше, не обмежиться кіберпростором і в разі загострення обов'язково перетвориться на конфронтацію «у реальному світі»[55].

Водночас екс-керівник національної розвідки США М. Макконнелл вважає, що кіберстримування може прислужитися цілям розбудови безпечного кіберпростору. Наявність могутніх кібернаступальних потенціалів може виконувати роль стримувального чинника щодо можливості застосування масштабних кібератак проти США [364].

Загалом можна припустити, що кіберстримування є виключним привілеєм «кібермогутніх» держав. Державам, які мають надто скромні показники кібермогутності[56], кіберстримування не дозволить уникнути небезпеки кібератак і мілітаризації кіберпростору в цілому. М. Лібіцкі в цьому контексті зауважує, що «кібератаки є потенційно небезпечними проти непідготовлених або безталанних супротивників, які мають достатньо досвіду, щоб отримати інформаційні технології і потрапити від них у залежність, однак не є достатньо розумними, аби захиститись від атак» [349, с. 134].

Тезу М. Лібіцкі щодо узалежнення від високих технологій й неможливості захиститися від загроз, з ними пов'язаних, слід сприймати критично. Адже кібератаки уможливлюються, зокрема, критичними уразливостями в програмному забезпеченні або помилками програмного коду, а отже, в разі невикористання таких технологій можна надійно застрахуватися від кіберзброї. Однак весь досвід розвитку сфери програмного забезпечення демонструє нереальність подібних ситуацій, оскільки що більше ускладнюються технологічні системи, то більше вони є вразливішими, більше в них виявляється помилок, виправляючи які, фахівці з безпеки автоматично роблять нові.

Інша теза М. Лібіцкі стосується від'єднання критично важливих об'єктів від мережі інтернет, тобто переведення їх у режим *off-line*. Проте досвід зараження комп'ютерів, які керували іранськими ядерними об'єктами, вірусом *Stuxnet* демонструє, що навіть від'єднаність від інтернету не гарантує захищеності від кібератак.

---

[55] Цю думку висловлює також Х. Лін, який у своїх працях зазначає високу ймовірність ескалації кіберконфліктів поза межі кіберпростору із застосуванням кінетичних озброєнь.

[56] *The Cyberpower Index*.

Власне, всі публічні міркування фахівців з кібербезпеки слід сприймати зі здоровим скепсисом. Часто вони є медійним лобіюванням інтересів військово-кібернетичного комплексу, який вкладає нині мільярдні кошти в кіберозброєння як наступального, так і оборонного (безпекового) характеру.

Підсумовуючи, підкреслимо, що концепція кіберстримування не є, вочевидь, найоптимальнішою відповіддю на зростання кіберзагроз. Взаємопов'язаність (інтерконективність) сегментів мережі й численність державних і недержавних акторів спричинюють потенційний зворотно-негативний ефект «кіберударів у відповідь» [424]. Наприклад, дестабілізація роботи банківської системи опонента може призвести до втрат національної економіки та фінансів. Адекватною відповіддю на зростання кіберзагроз може бути лише посилення міжнародної співпраці включно з виробленням взаємопогоджених міжнародних договорів щодо основних принципів функціонування кіберпростору, вдосконаленням міжнародної правової бази та інтенсифікацією міждержавного діалогу [Там само].

3.2. Проблематика міжнародної кібербезпеки: пріоритет співробітництва та демілітаризації

Проблеми кібербезпеки є предметним полем діяльності кількох міжнародних інституцій, передусім спеціалізованих організацій ООН, зокрема ЮНЕСКО й МСЕ. Проте ООН через свою невідповідність реаліям нового тисячоріччя (структура Ради Безпеки ООН «застрягла» на етапі закінчення Другої світової війни) так і не змогла повноцінно відповісти на нові виклики, які постали перед світом, зокрема у сфері кібербезпеки. Відповідно немає нічого дивного в тім, що ООН поступово втрачає функції головного міжнародного інституту у сфері міжнародної безпеки, поступаючись цими функціями таким міждержавним форумам, як *G*8,[57] *G*20, ОЕСР, ШОС, АТЕС тощо.

Саме тому всупереч реальним і гіпотетичним економічним і географічним обмеженням зазначені та подібні до них організації дедалі активніше перебирають на себе роль не лише регіональних, а й міжнародних, поширюючи сфери своїх безпекових інтересів і впливів на все світове товариство. Разом з тим парадоксальним є той факт,

[57] З березня 2014 року *G*8 фактично перестала існувати, однак з червня 2014 року збирається *G*7. Водночас, найшвидше, *G*7 і надалі виконуватиме зобов'язання, взяті країнами в межах *G*8.

що в низки регіональних безпекових та оборонних структур, зокрема НАТО, Ради Європи, ОБСЄ, поки що відсутні відповідні амбіції міжнародного рівня, й вони досі є регіональними структурами. Навіть неодноразово згадувана Конвенція про кіберзлочинність, яка фактично вийшла поза межі не тільки географічної, а й політичної Європи, а поміж її підписантів є країни, географічно вельми віддалені від Європи (наприклад Японія), не може, по суті, вважатися документом міжнародного значення. Наразі це істотно ускладнює приєднання до цього документа ключових країн.

Активною є нормотворча й інституційно-організаційна кібербезпекова діяльність на національних рівнях. Масштабність кібербезпекової проблематики і ступінь залученості до її розв'язання найбільших світових гравців спонукають до пошуку рішень попри традиційну термінологічну та іншу невизначеність, яка так або інакше відображає принципові розходження з питань осмислення не лише кібербезпекової проблематики, а й проблематики міжнародної безпеки в цілому. Навіть на рівні ООН досі не існує загальновизнаного підходу до визначення того, що вважати основним предметом міждержавних домовленостей у відповідній сфері безпекової діяльності: убезпечення світового кіберпростору чи забезпечення режиму міжнародної інформаційної безпеки.

При цьому термінологічне питання є принциповим, оскільки відображає несумісні погляди найбільших гравців.

Концептуальна ключова відмінність полягає в тім, що США та значна частина європейських держав дотримуються погляду щодо необхідності розглядати на міжнародному рівні лише проблеми кібербезпеки, залишаючи осторонь проблеми інформаційно-психологічних впливів. Натомість РФ, КНР та інші держави «напівзакритого» типу послідовно обстоюють позицію, відповідно до якої кібербезпеку не можна розглядати як окремий техніко-технологічний напрям, тобто відособлено від соціальних, політичних, економічних і воєнних наслідків застосування сучасних інформаційних технологій.

Зауважимо, що за техніко-технологічного підходу до кібербезпекової проблематики, якого дотримується західний блок, у міжнародному контексті недоречною виглядає навіть улюблена теза американців щодо «вільних потоків інформації». Адже інформаційно-безпекова тематика обов'язково мусить охоплювати питання *наслідків* впливу «вільних потоків інформації» на державу та її громадян. Отже, не слід упереджено відмовляти в рації РФ, КНР та іншим державам із зазна-

ченого питання. Підтримуючи погляд щодо первинності змістовної сторони інформації (контенту) над техніко-технологічними способами її руху, вони вважають застосування *кібербезпекового* понятійно-термінологічного поля в контексті міжнародних домовленостей не зовсім доречним і надають перевагу понятійно-термінологічному полю *інформаційної безпеки* чи *міжнародної інформаційної безпеки.*

Як зазначалося, в ООН ситуація довкола зазначеної понятійно-термінологічної плутанини склалася доволі неоднозначна. З одного боку, експерти й чиновники ООН протидіють спробам розширити поняття *міжнародна інформаційна безпека* (задля віднесення до цієї сфери суто політичних питань) і намагаються попередити використання поняття й відповідної термінології з метою досягнення «дискримінаційних» внутрішньополітичних цілей, боротьби з «вільними потоками інформації», тобто впровадження різноманітних форм цензури. З іншого – «прооонівське» експертно-бюрократичне товариство не зовсім погоджується з використанням кібербезпекової тематики у її виключно техніко-технологічному, «проамериканському», значенні. Відповідно, більшість документів ООН оперує поняттям *міжнародна інформаційна безпека* (МІБ), з максимальною обережністю наповнюючи його змістовно. У результаті поняття, що його використовує ООН, виглядає якщо не як компроміс між двома альтернативними концепціями, то принаймні як таке, що може вести до зазначеного компромісу.

Перші спроби ООН знайти цілісний підхід до розгляду проблем МІБ було зроблено наприкінці 90-х років XX сторіччя. Зокрема, 4 грудня 1998 року було прийнято Резолюцію Генеральної Асамблеї *A/RES/*53/70, в якій зазначено, що поширення та використання інформаційних технологій і засобів зачіпає інтереси всієї міжнародної спільноти, а також висловлене занепокоєння, що ці технології потенційно можуть бути використані в цілях, несумісних із завданнями міжнародної стабільності та безпеки [57]. Зважаючи на зазначене, Генеральна Асамблея:

• закликає держави-члени сприяти розгляду на багатосторонньому рівні наявних і потенційних загроз у сфері інформаційної безпеки;

• просить усі держави-члени інформувати Генерального секретаря про їхній погляд з питань:

– загальної оцінки проблем інформаційної безпеки;

– визначення основних понять інформаційної безпеки включно з несанкціонованим втручанням або неправомірним викорис-

танням інформаційних і телекомунікаційних систем та інформаційних ресурсів;

– доцільності розроблення міжнародних принципів, які спрямовувалися б на посилення безпеки глобальних інформаційних і телекомунікаційних систем та сприяли б боротьбі з інформаційним тероризмом і криміналом.

Результати цієї Резолюції згодом трансформувалися в Доповідь Генерального Секретаря «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (*Developments in the field of information and telecommunications in the context of international security*) [58], яка представила у стислому викладі позиції деяких країн із зазначених питань.

Австралія зазначила, що вже здійснює на національному рівні захист телекомунікаційних систем. При цьому держава зауважила, що визначення конкретних понять міжнародної інформаційної безпеки є недоцільним через «швидкий прогрес технологій»: існує ризик тісно пов'язати питання міжнародної інформаційної безпеки з конкретними технологіями. Австралія в даному разі (як і в багатьох інших) виступала в ролі проамериканського рупору, оскільки з 1948 року входить до своєрідного оборонного альянсу інформаційної безпеки *UKUSA* (союз п'яти англомовних країн: США, Великобританії, Канади, Австралії і Нової Зеландії).

У пропозиціях **Білорусі**, чия позиція відповідала переважно російському погляду на проблему, чітко зазначено потребу щонайшвидшого «розроблення та узгодження концепції міжнародної інформаційної безпеки та міжнародно-правові принципи, спрямовані на посилення безпеки глобальних інформаційних та телекомунікаційних систем, а також попередження інформаційного тероризму та злочинності» [58].

У зауваженнях, висловлених делегатом **Куби**, містилися звинувачення на адресу США щодо техніко-технологічного домінування. Пізніше, наприкінці 10-х років XXI сторіччя, вони актуалізувалися в дискусіях довкола майбутнього кіберпростру: «США як одна з найпотужніших держав, особливо у сфері інформатизації та телекомунікацій, посідають панівне становище, що дозволяє їм нав'язувати технологічні стандарти, які полегшують [для них – *Авт.*] використання інформаційних і телекомунікаційних систем як засобу агресії» [Там само].

На особливу увагу в доповіді заслуговують ґрунтовні матеріали, представлені РФ та США, які вже на тому етапі заклали базу діамет-

рально протилежних підходів до осмислення тематики міжнародної інформаційної безпеки, не погоджені дотепер.

У матеріалі, представленому **РФ**, увага привертається до того, що розвиток інформаційних технологій і пришвидшення процесів інформатизації «призводять до зміни глобального та регіонального балансу сил, виникнення напруження між традиційними та новими центрами сили та впливу. Формується принципово нова сфера протиборства на міжнародній арені, створюється ризик нового витка гонки озброєнь на базі науково-технологічних досягнень у сфері інформатизації та зв'язку» [58].

Саме в доповіді РФ чи не вперше цілісно сформулювала свою позицію щодо розуміння загроз у сфері МІБ, до яких, зокрема, було віднесено:

• інформаційний вплив з метою підриву політичної і соціальної систем держави;

• психологічна обробка населення з метою дестабілізації суспільства;

• дії держав, що призводять до домінування та контролю в інформаційному просторі;

• маніпулювання інформаційними потоками, дезінформація та приховування інформації з метою викривлення духовного середовища суспільства, ерозії традиційних культурних, моральних, етнічних та естетичних цінностей [Там само].

Більшість представлених формулювань майже дослівно були використані в іншому документі, датованому 2012 роком. Цей документ РФ запропонувала для обговорення з метою поліпшення забезпечення МІБ.

Хоча й не безпосередньо, але в доповіді було також артикульовано позицію **США**, яка зводилася фактично до пропозицій розглядати інформаційну безпеку передусім як сукупність проблем застосування технологій, і переважно не самостійно, а на додаток до інших дій (йдеться, наприклад, про радіоелектронне протиборство під час воєнних дій). Ключова теза США зводилася до необхідності вирішення проблем інформаційної безпеки передусім на національному рівні. США давали зрозуміти, що не сприймають всерйоз міжнародне регулювання проблеми й вказували, що «зважаючи на широке коло аспектів проблеми інформаційної безпеки та неоднозначність їх взаємодії, передчасно розпочинати розроблення загальних принципів, які стосуються інформаційної безпеки в усіх її аспектах» [Там само].

Після цього ґрунтовного матеріалу ООН у своїх резолюціях ще кілька разів зверталася до питань міжнародної інформаційної безпеки. Йдеться, зокрема, про Резолюцію *A/RES*/54/49 (1 грудня 1999 року), Резолюцію *A/RES*/55/28 (20 листопада 2000 року), однак всі вони принципово не відрізнялися від Резолюції *A/RES*/53/70. Зазвичай усе зводилося до констатацій необхідності подальшого контролю за даною тематикою.

На особливий інтерес заслуговує Резолюція *A/RES*/55/63 від 4 грудня 2000 року «Боротьба із злочинним використанням інформаційних технологій» (*Combating the criminal misuse of information technologies*). Її ухваленню сприяло завершення обговорення Конвенції про кіберзлочинність (на завершальному етапі вона стосувалася саме інформаційної злочинності), а також підбиття підсумків кількох міжнародних конгресів і конференцій з проблематики кіберзлочинності. Як наслідок суттєвого коригування зазнала резолютивна частина *A/RES*/55/63, в якій зокрема, вказано на необхідність реалізації таких напрямів діяльності:

• вжиття на державно-національному рівні більш активних заходів, спрямованих на протидію кіберзлочинцям;

• посилення співробітництва між правоохоронними органами;

• оптимізація системи захисту персональних даних, інформаційних систем електронних даних;

• підвищення обізнаності населення щодо нових викликів інформаційного суспільства.

Резолюція *A/RES*/56/19 «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» (*Developments in the field of information and telecommunications in the context of international security*) від 29 листопада 2001 року на тлі стандартної риторики містила важливе уточнення. Вона закликала Генерального секретаря ООН «провести дослідження концепцій, що згадуються у п. 2 [йдеться про міжнародні концепції, спрямовані на посилення безпеки глобальних телекомунікаційних систем – *Авт.*], за допомогою групи призначених ним на основі справедливого географічного розподілення урядових експертів, яка має бути створена в 2004 році» [59].

Своєрідним підсумком попередніх резолюцій стало прийняття 20 грудня 2002 року Резолюції *A/RES*/57/239 «Створення глобальної культури кібербезпеки» (*Creation of a global culture of cybersecurity*), в якій вперше чітко використовувалося поняття *кібербезпека* й зазна-

чалося: «Ефективна кібербезпека залежить не лише від дій державних чи правоохоронних органів; вона має досягатися завдяки превентивним заходам та користуватися підтримкою всього суспільства» [192]. Важливою частиною цієї Резолюції став Додаток «Елементи для створення глобальної культури кібербезпеки», в якому було зафіксовано ключові положення такої культури:

- обізнаність;
- відповідальність;
- реагування;
- етика;
- демократія;
- оцінка ризику;
- проектування та впровадження засобів забезпечення безпеки;
- управління забезпеченням безпеки;
- переоцінка (повторне оцінювання цінностей безпеки).

Подальше обговорення питань кібербезпеки відбувалося під час першої (Женева, 2003 р.) та другої (Туніс, 2005 р.) фаз Всесвітнього саміту з інформаційного суспільства (*World Summit on the Information Society, – WSIS*) під егідою ООН та МСЕ.

За результатами «женевської фази» було прийнято два ключових документи:

- Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячоріччя» (*Geneva Declaration of Principles. Building the Information society: a global challenge in the new millenium)* [53];
- План дій *Geneva Plan Action.*

Цікаво, що в Декларації питанням загроз і викликів міжнародній інформаційній безпеці приділено мінімальну увагу. На дев'яти сторінках тексту, де згадуються мало не всі можливі аспекти розбудови інформаційного суспільства, безпекові питання висвітлено лише в кількох пунктах. Зокрема, Декларація містить принцип 5 «Зміцнення довіри та безпеки при використанні ІКТ», який, однак, сформульований надзвичайно обережно. Зокрема, у п. 35 вказано «необхідність формувати, розвивати та впроваджувати глобальну культуру кібербезпеки» [Там само], а також потребу активізації співробітництва між зацікавленими країнами та підвищення рівня захисту даних і недоторканності приватного життя. У п. 36 наголошується на тім, що «діяльність ООН має бути спрямована на попередження використання ІКТ з метою, несумісною із завданнями забезпечення міжнародної

стабільності та безпеки та здатною справити негативний вплив на цілісність державних інфраструктур» [Там само]. У цьому самому контексті наголошувалося на потребі «попередження використання інформаційних ресурсів і технологій із злочинною й терористичною метою» [Там само].

Таким чином, результати дискусій з тематики міжнародної інформаційної безпеки, які тривали протягом майже 5 років (від моменту ухвалення першої Резолюції Генасамблеї ООН у 1998 році й до проведення першої фази *WSIS* у 2003 році), були фактично винесені «за дужки» обговорення в рамках *WSIS* на користь нібито більш актуальних питань кібербезпеки.

Аналогічно в тексті ухваленого Плану дій [158] положення міжнародної інформаційної безпеки теж принципово не актуалізовано. Єдиний загальний акцент зроблено на важливості міждержавного співробітництва в межах ООН, оскільки, як вказувалося в документі, саме державні органи у співпраці з приватним сектором мають попереджати, виявляти і реагувати на вияви кіберзлочинності та зловживання високими технологіями. Наголошувалося також на необхідності посилення інституційної підтримки діяльності держав щодо запобігання інформаційним загрозам на міжнародному рівні. Останнє сприятиме розробленню керівних принципів міжнародного законодавства в інформаційній сфері.

Своєрідним політичним підсумком обговорення проблеми міжнародної інформаційної безпеки у форматі *WSIS* стало визнання принципів загального недискримінаційного доступу до високих технологій для всіх націй, підтримка діяльності ООН, спрямована на забезпечення міжнародного миру й стабільності, запобігання потенційному застосуванню інформаційних озброєнь, здатних негативно вплинути на територіальну цілісність, інфраструктуру та масову свідомість населення будь-якої держави [177].

Подальше обговорення питання інформаційної безпеки продовжилося під час «туніської фази» *WSIS*. При цьому проблему власне безпеки в контексті становлення інформаційного суспільства доповідачі під час пленарних засідань практично не порушували вона згадувалася лише в окремих доповідях.

Наприклад, тодішній голова МСЕ Й. Уцумі (*Yoshio Utsumi*) зазначив, що, на його думку, кіберпростір кидає виклик поняттю *державний суверенітет*, оскільки «традиційні принципи національного суверенітету «не працюють», коли йдеться про інтернет» [416]. У цьому

зв'язку він зауважив, що необхідно напрацювати нову концепцію «комунікаційного суверенітету», яка включатиме питання управління мережею на основі багатостороннього підходу. Під багатостороннім підходом голова Міжнародного союзу електрозв'язку, вочевидь, розумів передачу управління інтернетом очолюваній ним міжнародній структурі ООН.

У контексті проблеми зміни системи управління інтернетом проблему безпеки розглядав також представник Німеччини: «Забезпечення стабільності та безпеки інтернету є ключовим питанням для життя глобального інформаційного суспільства. Ми переконані, що тривала стабільність можлива лише в умовах широкої міжнародної участі в управлінні інтернетом» [414].

Однією з найґрунтовніших була доповідь представника **КНР**, яка містила ключові положення подальшої політики КНР щодо розбудови міжнародного інформаційного суспільства. Передусім КНР звертала увагу на те, що розвинуті країни мають більш інтенсивно допомогти технологіями, фінансами та іншими ресурсами країнам, що розвиваються. При цьому, проте, у своєму розвитку країни мають покладатися передусім на власні сили.

Великий фрагмент доповіді китайського представника на *WSIS* був присвячений темі, яка в подальшому стала мало не головною в дискусіях КНР – РФ, з одного боку, та США – з іншого. Ідеться про повагу відмінностей у соціальних системах і культурі: «Зважаючи на багатоманітні відмінності між країнами в їхній історії, культурі та різницю ситуацій, надзвичайно важливо <...> щоб ці відмінності повністю сприймалися іншими учасниками <...>. Безумовно, мають бути надані гарантії свободи слова, однак, з іншого боку, має бути і соціальна відповідальність заради створення гармонійного та впорядкованого суспільства» [418].

Питання суто інформаційної безпеки у виступі китайського представника на *WSIS* також згадувалося в контексті необхідності трансформування системи управління Всесвітньої мережею.

За результатами роботи саміту було прийнято низку документів, які фактично визначили характер дискусій на тему інформаційного суспільства (зокрема її безпекового аспекту) у більш віддаленій перспективі. Зокрема, у Туніських зобов'язаних вказувалося, що учасники саміту «визнають необхідність ефективної протидії загрозам, які виникають при використанні ІКТ у цілях, несумісних із завданнями підтримки міжнародної стабільності та безпеки, та які також можуть

негативно вплинути на цілісність інфраструктури в межах окремих держав» [152].

Більше уваги безпековим аспектам відведено в Туніській програмі для інформаційного суспільства, яка, зокрема, вказує на необхідність посилення уваги до протидії кіберзлочинності (в тому числі відповідно до Конвенції про кіберзлочинність).

Дискусії з проблем управління інтернетом згодом продовжилися в межах Форуму з питань управління Інтернетом. Форум запроваджений *WSIS* і проводиться щорічно на світовому та національному рівнях (в Україні з 2010 року).

Цікавим доповненням до офіційних документів Туніського саміту стали офіційно зафіксовані трактування окремих пунктів Туніських зобов'язань деякими країнами. Документи містять пояснення розуміння цими країнами тих чи інших положень.

Так, США, коментуючи тезу про «належне державне управління інформаційним суспільством», зауважили, що розуміють під цим виключно «розумну економічну політику (включно із політикою, що заохочує конкуренцію), наявність надійних демократичних інститутів, які відгукуються на потреби людей та які є прозорими для людей, а також дотримання прав людини та принципу верховенства права» [153]. Прозорою є ідеологічна ангажованість такого застереження, витриманого в дусі неоліберальної парадигми з її надмірно підкресленою мінімальною роллю держави в будь-яких процесах, зокрема інформаційних.

Загалом документи обох «фаз» *WSIS* засвідчують реакція великих міжнародних акторів на еволюцію загроз у кіберпросторі та проблеми, пов'язані з його регулюванням. У значній частині документів, ухвалених *WSIS*, ключовими загрозами в інформаційному суспільстві визначено:

- невирішеність питань міжнародного регулювання мережі інтернет;
- спам;
- кіберзлочинність.

Варто зауважити, що протягом майже 10 років, які минули після другого етапу *WSIS*, проблему міжнародного регулювання інтернету так і не було розв'язано. Проблема спаму, хоча і не зникла, однак суттєво трансформувалася в проблему протидії функціонуванню ботмереж. Щодо проблеми протидії кіберзлочинності, яка перетворилася на практично повсюдне явище, то вона на міжнародному рівні на-

буває рис військової проблематики, оскільки сама кіберзлочинність дедалі більше мілітаризується.

Важливою особливістю дискусій щодо майбутнього кіберпростору (зокрема безпекового питання) є те, що вони так або інакше пов'язані з проблемою міжнародного регулювання мережі інтернет. Нині реальний контроль за технічною частиною функціонування мережі здійснюється корпорацією *ICANN* та *організацією IANA* (*Internet Assigned Numbers Authority*), надзвичайно тісно пов'язаними з державними структурами США. Значний вплив *ICANN* зберігає, зокрема, у сфері контролю за діяльністю кореневих серверів *DNS* (*Domain Name System* – система доменних імен), через які переважно здійснюється маршрутизація інтернету. Технічні стандарти встановлюються двома іншими організаціями, розташованими у США: *Internet Engineering Task Force* (*IETF*) та *Internet Architecture Board* (*IAB*). Вони інтегровані в *Internet Society,* штаб-квартира якої розміщена також у США.

Хоча 30 вересня 2009 року корпорація *ICANN* підписала новий договір з Міністерством торгівлі США, згідно з яким вона набула статусу «незалежної міжнародної некомерційної» організації, на думку більшості експертів, це не звільнило її від пильного контролю з боку США. Намагання корпорації позірно дистанціюватися від урядових структур Сполучених Штатів[58] не може ввести в оману ключових геополітичних гравців (зокрема ЄС, Китай та Російську Федерацію), які дедалі активніше вимагають, щоб контроль за мережею інтернет здійснювався міжнародними організаціями (наприклад ООН) з метою його деполітизації, демілітаризації та диверсифікації ризиків.

У 2005 році ООН провела Конференцію з торгівлі та розвитку, за результатами якої опубліковано звіт «Інформаційна економіка 2005» (*Information economy report 2005*). У Звіті окрему главу було присвячено темі захисту інформаційного суспільства та боротьбі з виявами кіберзлочинності [393], основними поняттями якої стали *кіберзлочини* та *кібербезпека*.

У звіті також чітко зазначені напрями, за якими, на думку ООН, має бути посилена кібербезпека в усьому світі та реформоване кримінальне законодавство; подано визначення кіберзлочинів, механізмів їх локалізації тощо.

---

[58] Напередодні конференції *ICANN* у Сан-Франциско представники Консультативної ради корпорації відмовилися від пропозиції Управління торгівлі США щодо надання права вето згаданому відомству на рішення про прийняття тих чи інших нових кореневих доменних імен.

Активно до теми безпеки кіберпростору звертається МСЕ, особливо після завершення «женевського» й «туніського» форумів *WSIS* та Повноважної конференції МСЕ 2006 року. Ключова роль МСЕ, на думку керівників цієї організації, полягає в зміцненні довіри та безпеки при використанні інформаційно-комунікаційних технологій. Таку позицію підтримують глави держав та урядів та інші світові лідери, що брали участь у зустрічах під егідою МСЕ. Вони делегували цій організації повноваження розробляти конкретні заходи щодо обмеження кіберзагроз і незахищеності, пов'язаних з інформаційним суспільством [90].

МСЕ ухвалив низку резолюцій і рекомендацій, які безпосередньо стосуються проблеми кібербезпеки. На особливу увагу заслуговує Рекомендація МСЕ-Т[59] X.1205 від 2008 року [327], яка надає визначення *кібербезпеки*, представляє у систематизованій формі загрози кібербезпеці та уразливості (включно з переліком найпоширеніших інструментів хакерських атак). Крім того, в Рекомендації МСЕ від 2008 року зроблено огляд різноманітних технологій кібербезпеки включно з антивірусним захистом, системами виявлення вторгнень, моніторингу систем тощо, подано принципи захисту мереж, технологій і стратегій управління ризиками тощо.

Зауважимо, що наразі МСЕ є чи не єдиною міжнародною організацією, яка «наважилася» визначити поняття *кібербезпека*: «Кібербезпека – це набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, керівні принципи, підходи до управління ризиками, діями, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Ресурси організації та користувача включають під'єднані комп'ютерні пристрої, персонал, інфраструктуру, програми, послуги, системи електрозв'язку та всю сукупність переданої та/чи збереженої інформації у кіберсередовищі. Кібербезпека полягає в намаганнях досягти та зберегти властивості безпеки у ресурсів організації чи користувача, спрямованих проти відповідних загроз безпеці в кіберсередовищі» [147].

У 2008 році в Йоханнесбурзі асамблея МСЕ-Т прийняла Резолюцію – 50 «Кібербезпека» [176], яка привернула увагу до необхідності більш інтенсивної співпраці членів МСЕ задля вироблення узгоджених стандартів у боротьбі з кіберзлочинами, а також збільшення

[59] МСЕ-Т – сектор стандартизації електрозв'язку МСЕ, постійний орган МСЕ, який відповідає за дослідження технічних, експлуатаційних і тарифних питань і за випуск Рекомендацій щодо них з метою стандартизації електрозв'язку на світовій основі.

масштабів інформування про такі злочини та відповідні механізми протидії. У розвиток Резолюції було прийнято низку інших, поміж яких, зокрема:

• Резолюція 174, у якій акцентовано увагу на необхідності більш активного використання механізмів МСЕ щодо узагальнення досвіду протидії протиправному використанню ІКТ на міжнародному та національному рівнях;

• Резолюція 179 про захист дітей у онлайн-середовищі;

• Резолюція 130, присвячена проблемі розвитку проекту «Глобальна програма кібербезпеки» й ускладненням, які виникають через відсутність точного визначення кордонів національних юрисдикцій щодо кіберпростору.

Поміж важливих кроків МСЕ, спрямованих на подальше убезпечення кіберпростору, варто виокремити створення фахівцями цієї структури такого важливого документа, як «Розуміння кіберзлочинності: Керівництво для країн, що розвиваються» (*Understanding Cybercraime: A Guaide for Developing Counries*) [161]. У Керівництві викладено ключові погляди МСЕ на ситуацію у сфері кібербезпеки, запропоновано ключові визначення та універсальна модель взаємодії основних суб'єктів забезпечення кібербезпеки на національному рівні. Досі цей документ залишається достатньо актуальним і виваженим.

Факт надзвичайної важливості проблематики кібербезпеки для МСЕ засвідчило те, що саме це питання було центральним на порядку денному П'ятого Всесвітнього форуму з політики у сфері електрозв'язку, який відбувся в червні 2013 року в Женеві [89].

Крім ООН та пов'язаних з нею спеціалізованих організацій, проблемами кібербезпеки, як зазначалося, опікуються інші міжнародні структури, зокрема *G*8, яка вперше звернулася до проблем протидії «високотехнологічним злочинам» ще у 1997 році. Тоді, під час зустрічі міністрів внутрішніх справ та юстиції було ухвалено спільне комюніке, додатком до якого стали «Принципи та План дій щодо боротьби з високотехнологічними злочинами» (*Principles and Action Plan to Combat High-tech Crime*). Частина додатку «Принципи» містить формулювання 10 ключових принципів боротьби з високотехнологічними злочинами.

1. Не повинно бути безпечних місць для тих, хто зловживає інформаційними технологіями.

2. Розслідування та карне переслідування міжнародних високотехнологічних злочинів має бути погоджене всіма зацікавленими державами незалежно від того, де такі злочини було скоєно.

3. Співробітники правоохоронних органів повинні бути відповідно підготовленими й мати ресурси для боротьби з такими злочинами.

4. Правові системи повинні захищати конфіденційність, цілісність і доступність даних і систем від несанкціонованого втручання і забезпечити покарання за серйозні порушення.

5. Правові системи мають забезпечувати збереження та швидкий доступ до електронних даних, які часто є вирішальними для успішного розкриття злочинів.

6. Режими взаємної допомоги мають забезпечувати своєчасне збирання та обмін доказами у справах, пов'язаних з міжнародними високотехнологічними злочинами.

7. Транскордонний доступ правоохоронних органів до загальнодоступних (відкритих) джерел не має потребувати дозволів від держав, які зберігають потрібні дані.

8. Мають бути розроблені судові стандарти отримання та перевірки достовірності даних, які максимально сприяють виявленню злочинців.

9. У міру можливостей інформаційні та телекомунікаційні системи повинні бути розроблені в такий спосіб, щоб допомогти запобігти та виявити зловживання в мережі, а також сприяти відстеженню злочинців і збиранню доказів.

10. Робота у цій сфері має бути скоординована з діяльністю відповідних міжнародних форумів [392].

У Плані дій щодо боротьби з високотехнологічними злочинами [234] було більш-менш докладно відображені ці саме принципи з незначними уточненнями. Наприклад, вказувалося на необхідність більш активної співпраці з промисловістю, потребу розроблення міжнародних стандартів кібербезпеки, взаємного вивчення правових систем з метою використання найліпших практик тощо.

Прийняті *G*8 документи цікаві тим, що в них закладено потенціал інформаційної «десуверенізації» у вигляді безпосередньо сформульованої тези (положення 7 «Принципів») про надання правоохоронним органам певної країни можливості здійснювати частину своєї діяльності без отримання дозволу від іншої країни. Хоча на той час з цим положенням погодилися всі члени *G*8, однак вже за 5 років, коли постало питання про підписання Конвенції про кіберзлочинність, відповідний пункт став причиною, через яку РФ відмовилася підписувати цей документ.

У тому ж 1997 році *G*8 створила Підкомітет з високотехнологічних злочинів (Група Рим–Ліон), який працює й досі.

Докладніше ознайомитися із зусиллями *G*8 щодо протидії кіберзагрозам можна із згаданого документа МСЕ «Розуміння кіберзлочинності: Керівництво для країн, що розвиваються». У ньому подано огляд діяльності *G*8 до 2007 року [177].

Водночас *G*8 постійно концептуально переосмислює проблеми протидії кіберзагрозам. Це, зокрема, унаочнює такий факт: якщо у 1997 році проблеми кіберзлочинності обговорювалися у форматі міністрів юстиції та внутрішніх справ, то у квітні 2013 року в межах *G*8 *у* Лондоні вже відбулася зустріч міністрів закордонних справ, на якій чимало часу було відведено дискусіям з проблем кібербезпеки. Зокрема, під час зазначеної дискусії було зафіксоване положення про те, що інтернет є необхідним інструментом, який сприяє економічному розвитку, забезпеченню свободи, демократії та прав людини [305]. «Вісімка» також позитивно оцінила роботу Групи урядових експертів ООН з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки й підтвердила на рівні міністрів, що міжнародне право стосується як цифрового середовища, так і до середовища, з ним не пов'язаного. Було констатовано, що в боротьбі з кіберзлочинністю більш активними мають бути спільні зусилля держав, бізнесу та громадянського суспільства.

Підхід *G*8 до проблем міжнародної кібербезпеки характеризується передусім намаганнями «вмонтувати» ці питання в якомога ширший контекст економічного зростання та соціальних вигод.

3.3. Кібербезпекова політика Сполучених Штатів Америки: від внутрішніх дискусій до міжнародних стратегічних ініціатив

Сполучені Штати Америки є найбільшою країною світу, яка зуміла вибудувати сучасний інформаційний і кібернетичний простір й одноосібно задає в ньому правила гри. Її інформаційне середовище характеризується надзвичайно високим рівнем проникнення інформаційно-комп'ютерних технологій у життя суспільства і є в цьому аспекті зразком для інших країн світу.

Зокрема, у США зосереджено до 40 % обчислювальних ресурсів планети й близько 60 % ресурсів інтернету. Якщо російський пошуковий ресурс *Yandex* (один з найбільш потужних зі створених на пострадянському просторі) використовує до 5000 серверів, то американський *Google* – до 2 млн серверів (офіційні дані відсутні, оскільки є комерційною таємницею цієї компанії).

Володіючи потужною кібернетичною інфраструктурою, США відповідно вразливі до різноманітних кібератак. Актуальність кібербезпекової проблеми була усвідомлена керівництвом США ще наприкінці 80-х років XX сторіччя. Однак перші системні документи в цій царині з'явилися фактично лише під час другої каденції Б. Клінтона та актуалізувалися за двох адміністрацій Дж. Буша-мол. Зокрема, у 2003 році було прийнято Національну стратегію захисту кіберпростору [282].

Упродовж тривалого часу основне навантаження із захисту кіберпростору було покладено у США на ФБР, Міністерство внутрішньої безпеки та Секретну Службу. Активну підтримку цій «трійці» надавали інші силові відомства та служби.

Зокрема, у 1996 році у складі ФБР на правах окремого управління створено Кіберпідрозділ (*Cyber Division FBI*), на який було покладено функцію надання допомоги іншим підрозділам ФБР у розслідуванні злочинів, скоєних з використанням комп'ютерних і телекомунікаційних технологій.

Секретна Служба, що входить до складу Міністерства фінансів США, займається переважно розслідуванням фінансових злочинів [15].

Політика Б. Обами у сфері кібербезпеки є, як зазначалося, значно активнішою, ніж політика його попередника Дж. Буша-мол. Не останньою чергою це пов'язано з особистою позицією 44-го президента США як активного користувача новітніх інформаційних технологій. Його перша передвиборча кампанія, на думку багатьох політологів [24], була виграна саме завдяки широкому використанню можливостей мережі інтернет.

Відповідно, нова Адміністрація із самого початку визначила питання кібербезпеки ключовими, а віце-президент США Дж. Байден (*Joseph Robinette Biden*) під час церемонії представлення нового керівника ЦРУ Л. Панетти навіть назвав політику нової Адміністрації у сфері кібербезпеки «однією з трьох основних» (поряд з політикою США в Афганістані та Іраку) [400].

Пильна увага керівництва США до проблематики кібербезпеки обумовлена, по-перше, курсом на збільшення інвестицій в інфраструктурні проекти (зокрема комп'ютерну інфраструктуру), що згодом створить можливість забезпечити американську *IT*-індустрію новими держзамовленнями; по-друге, США дедалі більше стикаються зі зростаючою активністю хакерів.

За даними центрального порталу американського електронного урядування *america.gov* [193], у 2006 році лише сайт Міністерства оборони США піддавався кібератакам 6 млн разів, а у 2008 році кількість таких спроб зросла до 360 млн. На думку генерал-лейтенанта К. Александера, голови АНБ та Кіберкомандування США, найбільшу небезпеку для США становлять Росія і Китай, які «активно готують спеціалістів для війни у кіберпросторі» [Там само].

Одразу ж після перших призначень до апарату нової Адміністрації, 9 лютого 2009 року, Б. Обама видав розпорядження про підготовку в 60-денний строк вже згадуваний «Огляд політики щодо кіберпростору» для «розроблення стратегічної основи кіберініціатив уряду США» [390]. Цим документом до ключових завдань керівництва США у сфері кібербезпеки віднесено:

• забезпечення центральної ролі Білого Дому у формуванні кібербезпекової політики, що має на меті продемонструвати аудиторії як усередині США, так і міжнародним партнерам серйозність намірів американського керівництва у сфері кібербезпеки;

• перегляд законодавства та політики у сфері кібербезпеки;

• посилення федерального лідерства та відповідальності у сфері кібербезпеки;

• просування лідерських проектів державного, регіонального та локального рівня [287].

Крім того, в документі окреслено ключові завдання, що мають на меті посилити кібербезпеку США:

• підвищити готовність суспільства до кіберзагроз;

• посилити кібербезпекову освіту;

• збільшити кількість федеральних працівників, що розуміються на інформаційних технологіях;

• просувати кібербезпеку як важливий елемент відповідальності урядів всіх рівнів.

Особливу увагу Адміністрація Б. Обами приділяє проблемі організаційного-кадрового забезпечення кібербезпекової політики. 5 березня 2009 року було призначено Федерального Директора з інформаційних технологій, до посадових обов'язків якого належали питання інформаційної безпеки та координування дій оргструктур, задіяних у системі кібербезпеки держави [391].

«Огляд політики щодо кіберпростору» став початком доволі динамічних змін американського безпекового сектору щодо його посилення на кібернапрямі.

9 лютого 2009 року було запроваджено посаду Керівника кібербезпеки Ради національної та внутрішньої безпеки, до серпня 2009 року обов'язки на цій посаді виконувала М. Хатавей (*Melissa Hathaway*), яку одночасно було призначено відповідальною за підготовку «Огляду». Одразу ж після інавгурації Б. Обами було призначено також помічника президента з питань внутрішньої безпеки та контртероризму Д. Бреннана, який також безпосередньо займається питаннями кібербезпеки.

26 травня 2009 року у своєму зверненні Б. Обама назвав проблему кібербезпеки однією з основних у XXI сторіччі поряд з проблемами протидії тероризму й розповсюдженню ядерної зброї [417]. Погляди на проблему кібербезпеки Б. Обама проголосив 29 травня 2009 року в Зауваженнях щодо забезпечення національної кіберінфраструктури (*Remarks by the President on securing our nation's cyber infrastructure*), зазначивши, що «кіберпростір – це світ, від якого ми залежимо щодня <...> Кіберпростір реальний, а отже, і загрози в ньому цілком реальні» [399].

На думку Б. Обами, рівень кіберзлочинності сягнув такого рівня, що загрожує добробуту американців, бо лише впродовж 2007–2009 років діяльність кіберзлочинців коштувала американцям 8 млрд дол. США Наводячи приклади кібервтручань терористів у федеральні мережі США (у сфері воєнної безпеки, енергетики, водопостачання тощо), Б. Обама висновує, що «кіберзагрози є одним з найбільш серйозних викликів економічній і національній безпеці, з яким зіткнулася нація» [Там само]. У такий спосіб американський президент проголосив цифрову інфраструктуру США «стратегічною національною цінністю» [Там само], а її захист – національним пріоритетом.

Крім того, у зазначеній промові Б. Обама окреслив п'ять основних напрямів розв'язання кібербезпекових проблем:

• розроблення всеохватної стратегії забезпечення безпеки інформаційних і комунікаційних мереж;

• розроблення систем попередження та реагування на кібератаки;

• посилення партнерства між державою та приватним сектором;

• продовження інвестування в передові дослідження та інновації інформаційної інфраструктури;

• ініціювання широкої національної кампанії щодо посилення готовності суспільства до реагування на кіберзагрози.

У тій самій промові Б. Обама проголосив створення в Білому Домі відділу з кібербезпеки, до обов'язків якого було віднесено, зокрема,

організацію та інтегрування кібербезпекових політик для представлення уряду та координування відповіді в разі кіберінциденту або атаки. Керівник нового відділу мав звітувати перед Радою національної безпеки та Економічною радою, а також мати регулярні зустрічі з питань кібербезпеки з президентом.

29 травня 2009 року був плідним для кібербезпекової тематики днем ще й тому, що цього дня в *The New York Times* з'явилося повідомлення про наміри керівництва Пентагону створити спеціальне командування для ведення війн у кіберпросторі [403]. Згодом, 24 червня 2009 року, тодішній міністр оборони США Р. Гейтс заявив [367], що вже найближчим часом у структурі Міноборони буде створено Кіберкомандування США, підпорядковане безпосередньо Стратегічному командуванню США (*United States Strategic Command*), що і було, як зазначалося, здійснено наступного 2010 року.

Президент Б. Обама істотно посилив традиційні безпекові інституції, що наразі також займаються проблемами кібербезпеки. Зокрема, у лютому 2009 року з метою запобігання можливості «зламу» урядових комп'ютерних мереж було частково розширені повноваження Агентства з національної безпеки США щодо контролю над кіберпростором США (включно з можливістю втручатися в мережеві підсистеми федеральних і місцевих адміністрацій) [6]. Нагадаємо, що проти такого розширення повноважень виступив керівник АНБ генерал К. Александер. Посилення державного втручання виявилося також у фінансуванні згадуваного проекту *Advanced Electronic Surveillance – Going Dark* [208] та кадровому посиленні кібербезпекового департаменту Управління національної безпеки.

Активна внутрішня політика у сфері інформаційної безпеки і кібербезпеки та постійні звинувачення на адресу Росії та Китаю у тім, що саме вони є основними джерелами кіберзагроз національній кібербезпеці США, очікувано викликали реакцію з боку представників зазначених країн.

Так, голова Міжвідомчої комісії з інформаційної безпеки Ради Безпеки РФ В. Шерстюк виступив з обвинуваченням на адресу США щодо їх активного небажання реально співпрацювати у сфері кібербезпеки. Ішлося, зокрема, про співпрацю в межах ООН. США та їхніх союзників обвинувачено в активній протидії спробам прийняття на міжнародному рівні універсального міжнародно-правового документа з констатаціями загроз міжнародній інформаційній безпеці та сценаріями спільних дій з мінімізації негативних наслідків кібератак для забез-

печення національних інтересів окремих країн та інтересів міжнародного співтовариства в цілому, демілітаризації ІКТ тощо. В. Шерстюк зазначив, що мілітаризація кіберпростору «підкріплюється практикою розбудови збройних сил деяких держав, які створюють спеціальні підрозділи, кіберкомандування, призначені для здійснення воєнного протиборства в глобальній інформаційній інфраструктурі» [178].

Наразі посилення кібербезпеки США на тлі зусиль з мілітаризації кіберпростору в цілому засвідчує перехід від «жорсткого» підходу, характерного для адміністрації Дж. Буша, до політики застосування «м'якої сили». Як зазначалося, головним ідеологом цієї політики є Дж. Най-мол., який нерозривно пов'язує «м'яку силу» з поняттям *інфолідерства*. Згодом з'явилося синтетичне (об'єднавче) поняття *розумної сили* (*smart power*), яке активно використовувала у своїй риториці екс-Держсекретар США Х. Клінтон.

Попри офіційно проголошену політику забезпечення безпеки кіберпростору, політика Б. Обами дедалі більше зводиться до створення нового фронту глобальної гонки озброєнь та розбудови військово-кібернетичного комплексу США. З необхідністю це посилює напруження між ключовими гравцями кіберпростору. Декларована Адміністрацією Б. Обами політика «убезпечення» має тенденцію еволюціонувати в напрямі політики забезпечення «тотальної безпеки» і розроблення цілісної концепції кібервійни.

Надмірна увага Адміністрації Б. Обами до кібербезпекової проблематики спричинила не лише трансформації безпекових підходів у США, а й зрушення в загальнополітичному дискурсі, що яскраво виявилося під час президентської виборчої кампанії 2012 року.

Своєрідний початок відповідним дискусіям поклала оприлюднена 5 січня 2012 року та згадувана в роботі у зв'язку зі зростанням видатків США на кібербезпеку та інші види новітніх озброєнь доповідь «Підтримуючи глобальне лідерство Сполучених Штатів: оборонні пріоритети для 21 сторіччя» [423]. Принципово важливим пунктом нової оборонної стратегії була переорієнтація стратегічних інтересів США з Євроатлантичного регіону до регіону Азіатсько-Тихоокеанського. Водночас США відмовилися від чинної концепції одночасного ведення війн у двох віддалених регіонах, або «війн на два фронти», яка отримала назву Стратегії 2*MRC*[60], та фінансово надзвичайно витратних поствоєнних «демократичних реконструкцій».

[60] 2*MRC* – абревіатура від *the two major regional conflict*.

Цей стратегічний документ містить виразні ознаки «кризовості», оскільки, як зазначалося, спрямований на скорочення оборонних витрат США. Проте скорочення стосувалося переважно сухопутних сил (Армія США) і морської піхоти (корпус морської піхоти США)[61]. Але пропоновані скорочення важко назвати істотними, бо вони становили лише десяту частину масштабних скорочень державних витрат, спрямованих на зменшення бюджетного дефіциту США (впродовж десяти років – 3 трлн дол. США). Несуттєвість запропонованих скорочень засвідчує й той факт, що впродовж «нульових років» XXI сторіччя військові видатки США подвоїлися й вийшли на рівень сумарних військових видатків решти країн світу [317].

Чимало ідеологічних супротивників Б. Обами (документ з'явився в розпал президентських передвиборчих перегонів) негайно скористалися цією оборонною стратегією як слушним моментом для звинувачень чинного президента в нехтуванні глобальними зобов'язаннями Америки з підтримання світового порядку, у провокуванні «світового хаосу» тощо. Зокрема, святкуючи свою перемогу на праймеріз у штаті Нью-Гемпшір, конкурент Б. Обами, республіканський кандидат М. Ромні (*Willard Mitt Romney*) 10 січня 2012 року заявив, що «Обама хоче покінчити з військовою могутністю США» та «застосувати в міжнародному масштабі стратегію заспокоєння», оскільки «гадає, що роль Америки як світового лідера залишилася в минулому» [401]. На противагу «капітулянтській» позиції конкурента М. Ромні закликав «будувати збройні сили, настільки смертоносні, щоб жодній державі у світі не спадало на думку кидати виклик США» [Там само].

Американські оглядачі не були одностайними в думці про значущість кібербезпеки як важливої позиції у передвиборчій кампанії [257]. Подальший розвиток подій засвідчив, однак, що питання кібербезпеки, якщо й не стали визначальними у порядку денному суперників, але принаймні були достатньо чутливими пунктами дебатів.

Одного разу тематика кібербезпеки була предметом спеціальної дискусії між кандидатами в президенти від Республіканської партії. Ідеться про дебати у Південній Каролині наприкінці листопада 2011 року. Спільним для всіх кандидатів-республіканців була позиція визнання КНР основним джерелом кіберзагроз [252].

---

[61] Упродовж 10 років витрати на ці види військ мали бути скорочені, за даними Пентагону, на 489 млрд дол. США.

Прикметно, що саме М. Ромні максимально ігнорував кібербезпекову тематику, акцентуючи на більш традиційних загрозах, зокрема на проникненні терористичних організацій у країни Латинської Америки [256]. Поміж причин неуваги суперника Б. Обами до кібербезпекового питання основною, напевно, була низька емоційність цього питання, що унеможливила його використання для мобілізації електорату. Відіграв свою роль й традиційно низький рівень уваги американських виборців до проблем зовнішньополітичного характеру та національної безпеки (окрім питань, пов'язаних з воєнними діями)[62].

Але всупереч більше ніж стриманому ставленню до питань кібербезпеки М. Ромні у своїй передвиборчій програмі та виступах з цього приводу [426] чітко артикулював кібербезпекову проблематику, акцентувавши на необхідності пошуку шляхів вдосконалення кібербезпеки США. У розділі «Контртерористична політика та заходи щодо органів внутрішньої безпеки»[63] зазначалося, що Адміністрація Б. Обами здійснила певну роботу з поліпшення кібербезпеки США, але водночас цілком справедливо стверджувалося, що вона не спромоглася оновити Національну стратегію забезпечення безпеки кіберпростору [431], підписану 2003 року Дж. Бушем-мол. Це не дозволило реально забезпечити цілісність трансформацій безпекового сектору відповідно до нових викликів. У програмному документі кандидата від республіканців зазначалося, що в разі його перемоги на виборах уже в перші 100 днів його адміністрація замовить повний міжвідомчий огляд, який стане основою вироблення цілісної національної стратегії стримування та захисту від воєнних кібератак, кібертероризму, кібершпигунства, а також крадіжок інтелектуальної власності. Крім того, в короткому огляді передвиборчої програми М. Ромні питання кібербезпеки було зазначено поміж перших восьми кроків, які мала здійснити його адміністрація в разі перемоги [299].

Загалом увага М. Ромні до питання кібербезпеки певною мірою пояснювалася наявністю в його команді радників з питань національної безпеки та міжнародної політики – М. Хайдена (*Michael Vincent Hayden*), колишнього керівника ЦРУ (2006–2009 рр.), та колишнього

---

[62] За влучним висловлюванням Дж. Люїса (Центр стратегічних і міжнародних досліджень США), «як тільки хакерської атаки зазнає один з ресурсів, що беруть участь у передвиборчих перегонах, вони [кандидати] заговорять про кібербезпеку» [257].

[63] З текстом передвиборчої програми можна ознайомитися на сайті www.mittromney.com.

директора Агентства національної безпеки (1999–2005 рр.), а також М. Чертоффа (*Michael Chertoff*), колишнього міністра внутрішньої безпеки США[64].

В американському розвідувальному товаристві М. Хайден відомий як фахівець, який з 1996 року працював на різних посадах у розвідувальних органах й найдовше був керівником Агентства національної безпеки. Очоливши відомство в період кризи і налагодивши ефективну систему менеджменту, він також збільшив публічну відкритість АНБ. При цьому М. Хайдена зазвичай відносили до ліберально налаштованих керівників й, зокрема, тому, що він негативно поставився до можливостей посилення контролю за внутрішніми (на території США) комунікаціями. Однак його погляди на покликання й методи роботи спецслужб радикально змінилися після терактів 2001 року. Репутацію М. Хайдена як ефективного керівника АНБ зіпсував скандал, пов'язаний із проектом *Trailblazer,* що мав забезпечити додаткові можливості аналізу даних з різноманітних комунікаційних систем (мобільного зв'язку, електронної пошти тощо). Витрати в 1 млрд дол. США бюджетних коштів не виправдали очікувань, проект так і не був доведений до завершення (закритий у 2006 році)[65]. Саме негатив, пов'язаний з цією історією, спричинив перехід М. Хайдена на посаду керівника ЦРУ, з якої його було звільнено у 2009 році, практично водночас з початком роботи Адміністрації Б. Обами.

М. Хайден як радник М. Ромні висловлював думку про необхідність всебічного посилення ролі АНБ у забезпеченні кібербезпеки США, наголошуючи, що лише це спецвідомство має у своєму розпорядженні всі необхідні засоби для підтримання необхідного рівня кібербезпеки. Крім того, він однозначно висловлювався за посилення на федеральному рівні координування діяльності відомств, відповідальних за забезпечення кібербезпеки США. М. Хайден наголошував, що таке координування неможливо здійснити, лише запровадивши в Білому Домі посаду «кіберцаря», тобто посадовця, відповідального

---

[64] Крім того, що вони обидва є консультантами М. Ромні, вони є бізнес-партнерами: в 2009 році їх зусиллями було створено приватне консалтингове агентство у сфері безпеки *Chertoff Group.*

[65] Цьому «посприяв» публічний розголос проблеми: у 2005 році видання *Baltimore Sun* (базуючись на інформації одного з працівників АНБ Т. Дрейка (*T. Drake*) опублікувало критичну статтю з даного питання, що спричинило згодом розслідування ФБР щодо джерел витоку інформації та низку обшуків у експрацівників АНБ. Водночас є повідомлення, що схожа програма (з назвою «Ідеальний громадянин» – *Perfect Citizen*) була знов розпочата в 2010 році [311].

за кібербезпекову політику США та координування діяльності відповідних силових відомств [380]. Певною мірою цю тезу М. Хайдена можна було сприймати як віддзеркалення низького рівня довіри американських військових, задіяних у сфері кібербезпеки, до компетентності й повноважень тодішнього «кіберцаря» Г. Шмідта [316].

У вересні 2011 року на Симпозіумі з питань розвідки та національної безпеки М. Хайден висловив також своє неприйняття ідеї управління АНБ і Кіберкомандуванням США однією людиною. Він зазначив, що є прихильником розділення цих структур, кожну з яких має очолювати окремий керівник. Фактично М. Хайден запропонував генералу К. Александеру піти з посади глави АНБ і зосередитися виключно на роботі у Кіберкомандуванні США [238], що кореспондувало з пропозиціями щодо призначення главою АНБ цивільної особи[66].

М. Чертофф[67] більшу частину життя пропрацював у різноманітних юридичних фірмах, а також на прокурорських посадах. Міністерство внутрішньої безпеки він очолив у 2005 році, залишивши цю посаду лише на початку 2009 року одночасно з інавгурацією Б. Обами. За час керівництва М. Чертоффом Міністерство внутрішньої безпеки значно посилило заходи щодо обмеження незаконної міграції. Саме М. Чертофф був одним зі співавторів Патріотичного Акту (*USA PATRIOT Act*), який після терактів 11 вересня 2001 року значно розширив можливості правоохоронних органів у відстеженні інформаційних потоків усередині держави та зборі персональної інформації про громадян, що проживають на території США.

Незважаючи на передвиборчу взаємообвинувачувальну критику кандидатів на посаду президента США, істотних розходжень у тлумаченні ними конкретно партіями демократів і республіканців загалом, інтереси яких вони репрезентували, в питаннях кібербезпеки та кібервійн не існувало. А якщо вони й існували, то лише на рівні експертних дискусій, які точилися між наближеними до партій «фабриками думок» (*think tank*).

---

[66] Одна з чернеток матеріалів виступу має виправлення, які стосувалися передусім того моменту, де М. Хайден говорить про те, що К. Александер має (може) стати «останнім офіцером *військової* розвідки, що очолює АНБ». У виправленому варіанті цей текст прибрано.

[67] М. Чертофф має певний зв'язок з пострадянським простором: його дідусь емігрував з території царської Росії. М. Чертофф походить з релігійної іудаїстської сім'ї: його дідусь був рабином, а батько очолював єврейську конгрегацію в місті Нью-Джерсі (США).

У більшості офіційних безпекових документів США останніх років кібербезпекове питання представлене доволі широко, хоча принципово нові положення в них відсутні. Зокрема, в усіх документах містяться твердження, що загрози кібербезпеці США можуть створювати як державні, так і недержавні актори, а поміж основних суб'єктів загроз у сфері кібербезпеки (в сенсі асиметричних нападів) зазвичай фігурують КНР, Росія, Іран та Північна Корея.

Усі внутрішні дискусії щодо важливості кібербезпекових питань для національної безпеки США сприяли напрацюванню Адміністрацією Б. Обами цілісного стратегічного бачення поточного стану і перспективи розвитку кіберпростору, а також потенційних напрямів його регулювання, формування зовнішньої політики з цього питання тощо.

Зовнішньополітичну кібербезпекову ініціативу було проголошено Адміністрацією Б. Обами 16 травня 2011 року, вона отримала назву Міжнародна стратегія для кіберпростору (*далі* – Стратегія кіберпростору) [325]. Документ не лише визначив принципові положення, якими керуватимуться США в процесі формування власної політики щодо кіберпростору, а й окреслив бажане для США майбутнє кіберпростору.

Базовими принципами, що мають бути забезпечені при формуванні політики щодо кіберпростору, було визначено такі.

1. «Фундаментальні свободи» (можливість шукати, отримувати й передавати інформацію та ідеї будь-якими засобами зв'язку та незважаючи на кордони).

2. «Прайвесі» (усвідомлення користувачами кіберпростору загроз їх персональній інформації та можливості вчинення проти них кіберзлочинів).

3. «Вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, оскільки вони лише створюють видимість безпеки. Натомість кіберпростір має бути місцем інновацій та співпраці держави й бізнесу задля забезпечення вищого рівня безпеки).

«Бажане майбутнє» кіберпростору для США окреслюється уникненням його міжнародного регулювання. Документ визначає три стратегічні цілі, що мають бути досягнуті для реалізації цього «майбутнього» [Там само].

1. *Відкритість і сумісність.* Розвиток цифрових систем має невпинно здешевлювати доступ до кіберпростору для дедалі більшої

кількості людей. Для поширення цих процесів впроваджувані інновації мають бути взаємосумісними, а їх впровадження здійснюватися на тлі дедалі активнішого використання програмного забезпечення з відкритим кодом, що дозволить створювати системи з єдиною логікою використання для всіх регіонів світу. Альтернатива цьому процесу, яка передбачатиме фрагментування мережі інтернет з метою заборони доступу до сучасного контенту великим групам людей через особливі політичні інтереси держав, є неприйнятною. Отже, пріоритетом має бути розроблення нових інформаційних технологій, заснованих на міжнародних стандартах, що забезпечить зростання цифрової економіки та рух суспільства вперед.

2. *Безпека та надійність.* Користувачі мають бути впевнені в безпеці своїх даних. Виконання цього завдання є поліаспектним і таким, що потребує відповідальності на всіх рівнях, починаючи від пересічних користувачів і закінчуючи державними органами та ефективною міждержавною співпрацею. Ключовим є питання розроблення міжнародних технічних стандартів щодо програмного та апаратного забезпечення та систем управління інцидентами, а також узгоджених міжнародних норм поведінки держав. Це потребуватиме розширення співпраці з питань обміну технічною інформацією між державним й приватним секторами, окремими державами й міжнародною спільнотою. Оскільки основним елементом надійності є безпека мереж, США готові інвестувати в цю безпеку не лише на національному рівні, а й сприяти посиленню надійності мереж за кордоном.

3. *Стабільність через норми.* Принцип, покладений в основу визначення цієї цілі, артикулює американське бачення чинного міжнародного правового поля щодо кіберпростору та орієнтирів його трансформації. Єдині правила поведінки в кіберпросторі – ключове завдання, оскільки їх «вироблення <...> сприятиме передбачуваності поведінки держав, що дозволить попереджувати конфліктні ситуації чи непорозуміння» [325], і США готові працювати над виробленням консенсусної точки зору щодо критеріїв «прийнятної поведінки», а також партнерства у кіберпросторі [Там само]. При цьому США не бачать необхідності додатково ухвалювати принципово нові міжнародні документи, оскільки чинне міжнародне законодавство не є застарілим щодо реалій кіберпростору: «розроблення правил поведінки держави в кіберпросторі не потребує оновлення існуючого міжнародного законодавства та не робить існуючі міжнародні норми застарілими. Багаторічні міжнародні норми, що визначають дії держави під час

миру та війни, також стосуються кіберсередовища». Але необхідним є певне доопрацювання зазначених норм, оскільки «унікальні характеристики мережевих технологій потребують додаткового опрацювання, що має на меті з'ясувати, яким чином ці норми слід використовувати та які додаткові тлумачення є необхідними. Ми продовжимо працювати на міжнародному рівні задля досягнення консенсусу щодо використання норм поведінки в кіберпросторі, усвідомлюючи важливість першого кроку в цьому напрямі та в очікуванні мирного та справедливого поводження в кіберпросторі» [325].

Пріоритетною для США в міжнародних кібериніціативах 2011 року визнана Конвенція про кіберзлочинність, бо саме цей документ, на думку авторів Стратегії кіберпростору, «є моделлю для розроблення та оновлення чинних законів» [Там само] у кіберсфері, а отже, має стати базовим для всіх подальших напрацювань у виробленні норм поведінки в кіберпросторі. Відповідно, розділ Стратегії кіберпростору «Розширення співробітництва та верховенство права» значною мірою дублює Конвенцію про кіберзлочинність і коментує її. Зокрема, вказується, що США розглядають подальші дискусії щодо міжнародних норм протидії кіберзлочинності передусім як «поширення чинних зусиль, таких як Будапештська конвенція[68]» [Там само] на всіх учасників. Крім того, підкреслюється, що США докладатимуть зусиль для налагодження двосторонньої співпраці між державами. Другий пункт зазначеного розділу безпосередньо вказує на необхідність узгодження національних нормативно-правових документів у сфері протидії кіберзлочинності з Конвенцією про кіберзлочинність. США, зі свого боку, зобов'язуються стимулювати інші країни приєднуватися до Конвенції.

Неважко спрогнозувати, що довготривалий інтерес США до просування Конвенції про кіберзлочинність як основного документа для двостороннього та багатостороннього співробітництва спонукатиме США докладати зусиль для перетворення цього документа на повноцінний міжнародний договір.

Формально Конвенція про кіберзлочинність має характер регіонального безпекового документа, підписаного в рамках Ради Європи. Крім того, в нинішній її редакції Конвенція не зможе охопити всі країни, що відіграють ключову роль у питаннях кібербезпеки. Так, Російська Федерація не підписала Конвенцію [271]. Можна перед-

[68] Конвенція про кіберзлочинність.

бачити, що вона не зробить цього, доки з документа не буде прибрано низку положень, які, на думку російської сторони, ущемлюють її цифровий суверенітет. До таких передусім, як зазначалося, належать положення Конвенції про доступ до ресурсів, розташованих у мережах загального користування іншої держави[69]. Малоймовірно, що це положення коли-небудь влаштує також КНР і низку інших країн, які реально турбуються про свій цифровий суверенітет.

Окрім іншого, Стратегія кіберпростору визначає орієнтовну модель поведінки держав у Всесвітній мережі та щодо окремих аспектів її роботи на засадах:

• *дотримання основних свобод*. Держави мають поважати свободу слова та зібрань, що так само актуальні для онлайну, як і для офлайну;

• *поваги до власності*. Держави у своїх ініціативах мають поважати право на інтелектуальну власність включно з патентами, торговельними таємницями, товарними знаками та авторськими правами;

• *поваги до цінності приватного життя*. Користувачі інтернету мають бути захищені від довільного/незаконного втручання у їхнє приватне життя;

• *захисту від злочинців*. Держави мають виявляти та переслідувати кіберзлочинців, створюючи для цього законодавство та практики, що не дозволять зловмисникам переховуватися на їхній території, а також сприяти співробітництву з міжнародними структурами, що переслідують таких злочинців;

• *права на самозахист*. Відповідно до Статуту ООН держави мають право на самозахист, що може бути застосований у відповідь на агресивні дії в кіберпросторі;

• *глобальної сумісності*. Держави мають вживати заходів, що сприятимуть максимальній сумісності та зручності використання мережі інтернет, а також її доступності якомога більшій кількості громадян;

• *мережевої стабільності*. Держави мають поважати свободу потоків інформації в національних мережах та не втручатися в роботу інфраструктури, віднесену до тісно пов'язаних з міжнародною функціональністю мережі;

---

[69] Ідеться про статтю 32 Конвенції «Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними»: будь-яка Сторона може, не отримуючи дозвіл іншої Сторони, здійснювати доступ до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно» [271].

• *надійного доступу*. Держави не мають штучно заважати доступу громадян до мережі інтернет чи мережевих технологій;

• *багатостороннього управління* інтернетом, яке не має обмежуватися виключно урядами, а повинне здійснюватися й іншими стейкхолдерами;

• *особливої уваги до кібербезпеки*. Держави мають визнавати свою відповідальність за безпечність і надійність роботи власних сегментів мережі інтернет та відповідної інфраструктури.

На особливу увагу в цьому переліку заслуговують два контроверсійних щодо перспектив забезпечення національно-державного цифрового суверенітету пункти про «право на самозахист» і «надійний доступ», з яким тісно пов'язаний пункт про «дотримання основних свобод».

Хоча кібератаки неможливо юридично кваліфікувати крізь призму чинного міжнародного законодавства, у Стратегії кіберпростору безпосередньо йдеться про те, що США готові застосовувати «дипломатичні, інформаційні, військові та економічні» засоби для реагування на кіберінциденти [325]. Досі незрозуміло, яким чином подібне положення може бути реалізоване на практиці без внесення кардинальних змін до Резолюції 3314 (XXIX) ООН, що надає визначення агресії. Адже, як зазначалося, поки існують лише окремі наукові напрацювання у сфері міжнародного права, що пропонують або визнати кіберзброю зброєю масового ураження, або (що виглядає реалістичніше) виробити механізм оцінювання наслідків від здійснення кібератак і порівнювати їх з можливими наслідками від застосування традиційних озброєнь.

Проблемам «надійного доступу» та «дотримання основних свобод» у Стратегії присвячено розділ «Інтернет-свобода: підтримуючи фундаментальні свободи та прайвесі», в якому вказано чотири основних напрями докладання відповідних зусиль з боку США.

1. Підтримка громадянського суспільства з питань отримання надійних і безпечних платформ для забезпечення свободи слова та зібрань. США закликають усіх до максимально активного використання цифрових засобів зв'язку з метою обміну думками, інформацією, моніторингу виборів, боротьби з корупцією, організації суспільних і політичних рухів і засудження тих, хто переслідує людей, які користуються такими цифровими засобами, арештовує їх чи погрожує їм. США готові всебічно сприяти розширенню прав і можливостей громадянського суспільства, правозахисників і журналістів використо-

вувати такі цифрові засоби, а також сприяти тим урядам, які «протидіють реальним загрозам у кіберпросторі, а не нав'язують компаніям обов'язки щодо обмежень свободи слова чи вільних потоків інформації» [325].

2. Співробітництво з громадянським суспільством і неурядовими організаціями щодо підвищення рівня їх кібербезпеки (зокрема з питань безпеки їхніх електронних поштових адрес, веб-сайтів, мобільних телефонів, інших засобів).

3. Сприяння міжнародному співробітництву в напрямі якомога ефективнішого захисту конфіденційності комерційних даних.

4. Забезпечення наскрізної сумісності систем, використовуваних для передачі інформації в мережі інтернет.

Тематиці «основних свобод» в інтернеті було присвячено ґрунтовний виступ Держсекретаря США Х. Клінтон під час конференції про свободу в інтернеті 8 грудня 2011 року в Гаазі [174], де вона особливо гостро критикувала практику затримання в РФ громадських активістів-блогерів (О. Навальний) та дії китайського уряду, пов'язані з укладанням спеціальних угод з компаніями, що надають телекомунікаційні послуги[70].

Заяви Х. Клінтон із зазначеного питання цілковито співзвучні запропонованому Стратегією кіберпростору формату забезпечення положень про «фундаментальні права»*:* «Виконання належного у стосунку інтернет-свободи вимагає спільних дій, і ми повинні зав'язати глобальну розмову на основі загальних принципів <...> Ця справа не є питанням погодження на переговорах єдиного документа і оголошення, що роботу зроблено. Вона вимагає постійних зусиль, щоб враховувати нову реальність, в якій ми живемо у цифровому світі, і робити це таким чином, щоб максимальними були переваги, який він обіцяє» [Там само][71].

Водночас у промові Х. Клінтон було порушено три додаткові тези, що дозволяють дійти висновків про довгострокові плани США щодо кіберпростору.

---

[70] «У Китаї кілька десятків компаній у жовтні підписали зобов'язання, за яким вони повинні зміцнити свої – цитую – "внутрішнє управління, стриманість і сувору самодисципліну" Так, якби йшлося про фінансову відповідальність, ми усі могли б погодитися. Але йшлося про пропоновані китайському народу інтернет-послуги, і це було кодове формулювання про відповідність жорсткому урядовому контролю над інтернетом» [174].

[71] Тут і далі всі цитати з промови Х. Клінтон дослівно подано в перекладі, розміщеному на офіційному сайті Посольства Сполучених Штатів.

1. *Приватний сектор має виконати свою роль у захисті інтернет-свободи*. На думку Х. Клінтон, приватні компанії, що торгують технологіями, які можуть бути використані для придушення свободи слова (системи спостереження, моніторингу інтернет-трафіку тощо) мають фактично *вдаватися до самоцензури при обранні клієнтів для своєї продукції* та не очікувати на відповідні рішення Держдепартаменту: «Коли компанії продають обладнання для стеження агентствам безпеки Сирії або Ірану, або, в колишні часи, Каддафі, не може бути жодного сумніву, що воно буде використане для порушення прав людини. Дехто може сказати, що для того, щоб змусити до гарної поведінки в бізнесі, відповідальні уряди мають просто накласти широкі санкції, і це закриє проблему <...> санкції є частиною рішення, але вони не все рішення <...> Подвійні технології і продажі третіми сторонами не дозволяють режиму санкцій ідеально запобігати використанню технологій поганими дієвими особами із поганими намірами. Часом компанії кажуть нам, Державному департаменту: «Просто скажіть нам, що робити, і ми будемо це робити». Але насправді, не слід чекати розпоряджень. У XXI-му сторіччі розумні компанії повинні вживати заходів до того, як вони потраплять [у] суперечливе становище» [174]. Подібна позиція США концептуально не збігається з панівною (в публічному дискурсі) неоліберальною концепцією «вільного ринку», відповідно до якої роль держави полягає саме у встановленні граничних меж ринку, а не в саморегулюванні бізнесу на основі встановлення «розумності» або «нерозумності» бізнесових процесів.

2. *Неможливо допустити використання урядами тематики «управління інтернетом» з метою посилення «контролю за інтернетом»*. «Прямо зараз на різних міжнародних форумах деякі країни працюють над тим, аби змінити регулювання інтернету. Існуючий багатосторонній підхід, де в єдину глобальну мережу включені уряди, приватний сектор і громадян[и], і забезпечується вільний обмін інформацією, вони хочуть замінити. Натомість вони прагнуть нав'язати систему, закріплену глобальним кодом, який розширює контроль над інтернет-ресурсами, установами і змістом, і централізує таке управління в руках урядів» [Там само]. Особливе занепокоєння США викликає можливість створення національних правил гри для окремих сегментів мережі, що порушить принцип її сумісності. *В більш широкому сенсі США виступають категорично проти будь-яких бар'єрів у кіберпросторі, що можуть трактуватися як своєрідні «кордони держави в кіберпросторі»*. Причому Х. Клінтон рішуче відкидає зв'язок

цієї проблеми з питаннями безпеки (протидією кіберзлочинності, запобіганням поширенню дитячої порнографії, боротьбою з кібертероризмом), наголошуючи, що ці проблеми мають вирішуватися інакше, не порушуючи «динамізм інтернету».

3. *Потрібно створити коаліцію за «відкритий інтернет»*. Ця теза Х. Клінтон фактично є продовженням другої тези, однак з практичною рекомендацією об'єднуватися (під егідою США) у коаліцію держав, щоб не допустити обмежень мережі в окремих країнах.

Наразі важко сказати, наскільки успішно реалізується Стратегія кіберпростору і чи користується вона загальносвітовою підтримкою поза межами європейських країн та частини країн Східної півкулі (Японія, Австралія, Нова Зеландія та інші), які традиційно рухаються в кільватері американської зовнішньої політики.

У вересні 2011 року Австралія та США включили співробітництво з протидії кіберзагрозам до Договору про взаємну оборону [276].

У жовтні 2011 року, під час спільної прес-конференції міністрів оборони США та Японії, очільник японського військового відомства Я. Ітікава (*Yasuo Ichikawa*) зазначив, що сторони активно обговорюють питання поглиблення співробітництва у сфері кібербезпеки [332].

Особливу зацікавленість у американської сторони викликають перспективи співпраці з країнами БРІКС, деякі з яких розпочали інтенсивнішу двосторонню співпрацю із США. Так, у липні 2011 року Індія та США досягли домовленостей щодо посилення співпраці у сфері протидії кіберзагрозам: відповідний Меморандум про взаєморозуміння було укладено між департаментом електроніки та інформаційних технологій Міністерства комунікацій та інформаційних технологій Індії та Департаментом державної безпеки США [323].

Деякі проблеми співпраці США із країнами-партнерами у сфері технологій і методів протидії кіберзагрозам висвітлив начальник розвідки кіберкомандування контр-адмірал С. Кокс. Виступаючи в Джорджтаунському університеті на семінарі, присвяченому кібербезпеці, він зазначив передусім слабку захищеність комп'ютерних систем союзників США по НАТО, що «забезпечує» легкий доступ противника до інформації, якою США діляться із союзниками. Щоправда, С. Кокс публічно [200] не називав країни з вразливими комп'ютерними мережами, хоча зазначив, що поміж них немає Канади, Великобританії, Австралії й Нової Зеландії, з якими США тісно співробітничають у військовій і безпековій сферах відповідно до угоди про *UKUSA* від 1948 року.

Співпрацю воєнних відомств країн НАТО з партнерськими країнами гальмує також надмірна засекреченість військових технологій і технологій подвійного призначення, а також надто жорсткі американські закони щодо експортного контролю трансферу таких технологій. Відповідно до цих законів Пентагон часто не має права продавати чи надавати ці технології іншим країнам.

Хоча на думку деяких експертів [197], співробітництво з питань кібербезпеки в трикутнику США – КНР – РФ налагоджується (зокрема з питань визначення термінології та пожвавлення діалогу), є кілька позицій, які, переконання фахівців Національного інституту стратегічних досліджень [72], ці держави не зможуть погодити, принаймні в найближчій перспективі.

По-перше, ключовий, на думку США, документ щодо поліпшення глобальної кібербезпеки – Конвенція про кіберзлочинність – як зазначалося, найшвидше не буде підписаний РФ без внесення до нього істотних змін. Таким чином, зважаючи на акцент США щодо пріоритету просування Конвенції, можна припустити, що результативної дискусії у найближчій перспективі очікувати не варто.

По-друге, традиційна американська теза про «вільні потоки інформації», що не можуть бути за жодних умов обмежені чи контрольовані національними урядами, принципово розходиться з позиціями не тільки РФ і КНР, а й багатьох інших країн. Особливо зважаючи на те, в яких і чиїх інтересах реально використовуються ці «потоки» (йдеться зазвичай про зусилля в напрямі дестабілізації політичної, економічної й соціальної ситуації у певній «революційній» країні). Офіційні пояснення уряду США щодо потреби у «вільних потоках» для створення глобального громадянського суспільства зайвий раз переконують уряди неприхильних до цієї ідеї країн (переважно з-поміж країн перехідних або приналежних до «третього світу»), що йдеться фактично про обмеження реального державного суверенітету.

По-третє, малоймовірно, що США та їх союзники з одного боку та доволі широка коаліція держав (до якої входять не лише РФ і КНР, а й значна кількість європейських, латиноамериканських та африканських країн) з другого боку зможуть знайти дійсно єдину (консолідовану) точку зору щодо проблеми управління інтернетом. США однозначно захищають гегемоністську позицію щодо продовження контролю за мережею за допомогою корпорації *ICANN*. Хоча, як зазначалося, 2009 року ця корпорація офіційно перестала контролюватися американським урядом, більшість країн світу (передусім КНР)

наполягають на передачі її повноважень і функцій спеціально створеному органу під егідою ООН (можливо, МСЕ).

По-четверте, КНР і РФ принципово не згодні з позицією США щодо відокремлення (а фактично підміни) проблем кібербезпеки від проблем інформаційної безпеки. Натомість позиція цих країн небезпідставно ґрунтується на твердженні, що кібербезпека має розглядатися виключно як частина інформаційної безпеки, охоплюючи при цьому низку гуманітарних питань, які регулюються державою відповідно до принципів забезпечення національної безпеки.

3.4. Кібербезпекова політика Китайської Народної Республіки: національно-державний і міжнародний аспекти

Внутрішня інформаційна політика керівництва КНР щодо свободи доступу до інтернету та анонімності поведінки в мережі й відкритості її ресурсів принципово відрізняється від політики країн Заходу. Якщо ЄС та США принаймні проголошують ліберальний і неоліберальний підходи до розуміння основ функціонування інтернету та відповідних наслідків для користувачів у сфері доступу до інформації, то КНР цілком однозначно обстоює більш жорсткий контроль не лише за внутрішнім інформаційним полем, а й за ресурсами, до яких можуть отримати доступ громадяни КНР.

На думку американських оглядачів, політика КНР у сфері контролю над ІКТ пов'язана передусім з «побоюваннями уряду, що ліберальні організації, внутрішні чи зовнішні, використають інформаційні технології аби підірвати довіру громадян до режиму» [371, с. 116].

Відповідно КНР упродовж останнього десятиріччя вдалася до низки послідовних кроків, спрямованих на зміцнення національно-державного цифрового суверенітету. Внаслідок цього США та їх союзники неодноразово звинувачували цю державу в намірах зруйнувати цілісність мережі інтернет. Частина цих обвинувачень стосується активної моніторингової діяльності спеціальних державних структур КНР, спрямованої на пошук певного специфічного контенту та його цензурування.

Політика КНР щодо функціонування мережі інтернет у її внутрішньому інформаційному просторі та пов'язане з нею порушення прав громадян на свободу інформації є, на думку Заходу, поганим прикладом для інших країн з авторитарним режимом правління. Тому ця тематика стосується не лише правоохоронців і фахівців

з міжнародного права, а й зачіпає сферу великої міжнародної політики і є однією з центральних тем взаємовідносин у трикутнику КНР – США – ЄС.

Оскільки антиліберальні підходи й практики КНР з питань регулювання інтернету є предметом запеклої ідеологічної боротьби, то тут вистачає нашарувань різноманітних міфів (наприклад довкола згадуваного проекту «Золотий щит»). Це вкрай ускладнює оцінювання дійсного стану регулювання інформаційного (кібер) простору в КНР з боку незалежних спостерігачів.

Передусім слід зважати на той факт, що КНР є країною з найбільшою кількістю інтернет-користувачів у світі. За даними системи *Internet World Stats* [326], станом на середину жовтня 2013 року кількість користувачів мережі інтернет у КНР сягнула 538 млн осіб (аналогічний показник на кінець 2009 року – 339 млн осіб). Для порівняння: у всьому Європейському Союзі налічується 368 млн інтернет-користувачів, у США – 245 млн. Причому щороку зростає не лише кількість користувачів китайського сегменту інтернету, а й якість з'єднань. КНР впроваджує амбітні плани розвитку широкосмугового доступу (ШСД) на всій території країни, передбачивши вкласти в цей проект протягом наступних 5 років 60 млрд дол. США. Для порівняння: аналогічний проект у США коштуватиме близько 15 млрд дол. США, а в ЄС – 9 млрд євро. Наразі значна кількість користувачів КНР вже користуються ШСД-підключенням [260].

Керівництво КНР не сумнівається, що розвиток ІКТ і мережі інтернет є одним з основних джерел економічного зростання держави. 9 липня 2012 року Постанова Державної Ради (уряду) КНР визначила в межах дванадцятої п'ятирічки 25 «національних проектів», завданням яких є «закладення основи для розвитку з метою підвищення конкурентоспроможності в критичний момент» розвитку держави [455]. До першої трійки цих проектів входить «Нове покоління індустрії інформаційних технологій», що передбачає створення національної інформаційної інфраструктури, координування ШСД і створення нового покоління мобільного зв'язку. Загалом у межах проекту передбачено три напрями.

1. «Наступне покоління інформаційних мереж для промислового розвитку».

2. «План розвитку електронної основи інфраструктури».

3. «Високоякісне програмне забезпечення та нові інформаційні послуги».

Другий напрям стосується переважно необхідності нарощування власних потужностей у виробництві сучасної електроніки, третій – сприяння власному виробництву програмного продукту, захисту інтелектуальної власності на нього, створення цілісної бази розроблення програмного забезпечення з метою широкого виходу на міжнародну арену.

Виконання основних завдань, визначених керівництвом КНР у сфері національної безпеки, ускладнює необхідність пошуку певного розумного балансу між розвитком ІКТ і забезпеченням внутрішньої стабільності. Розв'язання цієї проблеми, з одного боку, стимулює розширення мережі інтернет у Китаї, а з іншого – збільшує контроль за його використанням.

Умовно можна виділити два основних напрями такого контролю: «низького рівня» (*low-tech*) та «високого рівня» (*high-tech*) [68]. Під контролем «низького рівня» в КНР розуміють не технологічні, а переважно організаційні та регуляторні (бюрократичні) методи, пов'язані з широким застосуванням цензури. На думку американського дослідника Д. Мульвенона (*James Mulvenon*), саме бюрократична регулятивна компонента є найбільш ефективним інструментом «лінії захисту» в безпековій політиці КНР щодо інтернету [371]. Зокрема, китайське законодавство покладає відповідальність за зміст розміщеного користувачами контенту не лише на них, а й на провайдера інтернет-послуги, що змушує провайдерів турбуватися про дотримання китайського законодавства щодо оприлюднення бажаної/небажаної інформації у власному сегменті мережі.

Крім того, цензурна політика є основою взаємовідносин між урядом КНР та потужними *IT*-ТНК (*IT*-корпораціями, що за своїм впливом і масштабами діяльності можуть розглядатися як своєрідні транснаціональні компанії – *Google*, *Yahoo!* та інші). Хоча такі відносини часто зазнають суттєвих загострень, як, наприклад, між урядом КНР і корпорацією *Google*[72]. Із 2007–2008 рр. КНР, як зазначалося, блокує *YouTube* через систематичне розміщення в цій мережі відеороликів, що, на думку керівництва КНР, можуть справляти негативний вплив на суспільну думку та міжнародний імідж Китаю. Один з випадків блокування відеоконтенту *YouTube* був пов'язаний з розміщенням відеоролика, що фіксував побиття солдатами монахів та інших мешканців Тибету [101].

[72] Докладніше див. підрозділ 1.1.

Ситуація із сайтом *YouTube* та необхідність здійснювати цензурний контроль за аудіо- та відеоконтентом у мережі інтернет у цілому змусили Державну адміністрацію з радіо, фільмів та телебачення КНР спільно з Міністерством промисловості та інформаційних технологій у січні 2008 року розробити нові регулятивні правила розміщення відеоконтенту на національних відеосервісах. Це дещо обмежило неконтрольоване розміщення аудіо- та відеоматеріалів у широкодоступних мережах. Крім того, під заборону розміщення потрапляє відео, що може зашкодити єдності та суверенітету Китаю, завдати шкоди етнічній солідарності, сприяє поширенню забобонів, пропагує насильство, порнографію, азартні ігри чи тероризм, порушують права особи, завдають шкоди китайській культурі чи традиціям або шкодить чинному законодавству Китаю [404]. Ці цензурні правила не є оригінальними та збігаються з тими обмеженнями щодо інформаційного обміну, які існували в китайському сегменті мережі інтернет від початку 2000-х років.

Упродовж останнього десятиріччя цензурна політика КНР не зазнає принципових змін, принаймні щодо прискіпливого контролю. На думку Г. Вакера (*Gudrun Wacker*) [268, с. 62], обмеження на вільне поширення можуть стосуватися інформації, яка:

- суперечить принципам, визначеним Конституцією;
- створює загрозу національній безпеці;
- розкриває державну таємницю;
- підриває довіру до уряду;
- руйнує єдність держави;
- завдає шкоди честі та інтересам держави;
- збурює етнічну ненависть чи пропагує дискримінацію, руйнує єдність китайської нації;
- може мати негативні наслідки для державної політики у сфері релігії;
- поширює культи насильства або феодальних релігій;
- поширює чутки;
- порушує громадський порядок;
- підриває соціальну стабільність;
- пропагує розпусту, порнографію, азартні ігри, насильство, вбивства, терор або підбурює до злочину;
- ображає або ганьбить інших, ущемлює закріплені Конституцією права і наміри інших;
- містить інший зміст, заборонений законом або адміністративним регулюванням.

Американський аналітик у сфері свободи слова в мережі інтернет Р. Маккінон *(Rebecca MacKinnon*), аналізуючи цензурний документ 2008 року, доходить висновку, що політика КНР здійснюється за трьома основними напрямами регулювання [360].

1. Всі види потокових відео-сайтів (деяких – у режимі реального часу), що можуть містити контент, який ніколи не був би продемонстрований на державному ТБ.

2. Поширення відео у пірінгових (торент) мережах, що стосується передусім порнографічних матеріалів.

3. Сайти, що функціонують у межах філософії *Web* 2.0. – «контент, створений самими користувачами» (йдеться передусім про китайські *YouTube*-клони: *www.tudou.com*; *www.youku.com*; *www*.56.*com*; *www.ouou.com*).

Особливі правила встановлені в КНР для роботи в інтернет-кафе, які зовні є такими самими, як для барів та інших подібних закладів розваг: розміщення не ближче ніж за 200 ярдів від шкіл, обов'язковий віковий ценз для отримання доступу до певних послуг (отже, обов'язково потрібен документ, що посвідчує особу) тощо. Однак у деяких містах Китаю (наприклад у Пекіні, де інтернет-кафе близько 1500) застосовуються додаткові методи ідентифікації: встановлюються камери спостереження, а будь-який користувач має бути сфотографований [251]. І навіть незважаючи на такі жорсткі умови доступу до мережі, китайська влада надає перевагу примітивному блокуванню іноземних соціальних мереж, наприклад *Facebook* чи *Twitter* [263].

Окрім регулятивно-бюрократичних методів контролю «низького рівня», китайська влада вдається й до більш «вишуканих» методів придушення дисидентської активності в медіа (кібер) просторі. Китайські медіа час від часу оприлюднюють інформацію про арешти деяких блогерів-дисидентів, не акцентуючи при цьому увагу на тім, що до цих арештів спричинив моніторинг, здійснюваний інтернет-поліцією. На неї покладено обов'язки відстежування публіцистичної діяльності в інтернет-медіа з метою спонукати користувачів інтернету в КНР утримуватися від будь-якої політично мотивованої діяльності в мережі, щоб уникнути карного переслідування [Цит. за: 371].

«Високий рівень» контролю, а отже, протидії поширенню небажаної інформації в КНР пов'язаний передусім з використанням ІКТ для поліпшення процедур державного контролю за внутрішнім інформа-

ційним простором і забезпечення подальшого домінування в цьому просторі держави. Ідеться передусім про проекти «Золотий щит» та «Зелена дамба» (*Green Dam*)[73].

Проект китайського уряду «Золотий щит» покликаний відстежувати поведінку громадян у мережі інтернет і контролювати розміщений там контент. Проте розроблявся він як система інформатизації всіх сфер життя суспільства, особливо сфери громадської безпеки. Першопочатком «Золотого щита» був цивільний проект кінця 1980-х років «Автоматизований офіс», що мав на меті запровадження на всіх рівнях китайського державного апарату комп'ютерів і комп'ютерних мереж. «Золотий щит», що спеціалізується з питань безпеки, власне, є лише одним з 20-ти «золотих проектів», що охопили всі сфери *e*-урядування: фінансовий сектор, соціальну безпеку, сільське господарство, оподаткування, митні послуги, водне господарство, виробничі стандарти, державний контроль тощо [358].

Кіберконтроль у межах проекту «Золотий щит» є лише одним з елементів кібербезпекової політики КНР, яка включає, крім того, запровадження особистих електронних карток. Такі картки є різновидом електронного паспорта з можливістю використання електронно-цифрового підпису, що створює потужну можливість відслідковування «протиправної» діяльності. Проте першопричиною впровадження таких *e*-паспортів стала не тільки і не стільки проблема безпеки та адміністративного контролю, скільки нереформованість упродовж останніх 50 років системи ідентифікації громадян.

Донедавна значна частина китайців використовувала як ідентифікатор особистості «сертифікат внутрішньої реєстрації» (*household registration certificate*), що не був паспортом у звичному розумінні, але надавав можливість громадянину отримувати доступ до послуг у сферах зайнятості, освіти, охорони здоров'я та інші. Така практика була пов'язана з особливостями законодавства щодо міграційних процесів (внутрішньої мобільності) усередині країни. Однак із початком лібералізації цього законодавства за часів Ден Сяопіна така адміністративна практика втратила ефективність, оскільки практично унеможливила відслідковування поліцією переміщення громадян усередині країни. Таким чином, впровадження ідентифікаційних карток (*ID*

[73] Цікаве дослідження (хоча і трохи однобічне) з проблем технічного цензурування та методик, які для цього використовуються, належить Е. Додсон (*Elizabeth Kathleen Dodson*) – «Зламуючи «Золотий щит»: проблеми зростання технологій цензури в КНР» [293].

card) стало майже єдиною реальною можливістю упорядкування міграційної сфери.

У межах проекту «Золотий щит» реалізується також процес масштабного встановлення на вулицях великих китайських міст камер спостереження (що вже віддавна є традиційною практикою для країн Заходу). Так, за свідченням адміністрації міста Гуанчжоу, саме встановлена система відеоспостереження (близько 3000 камер) допомогла здійснити понад половину арештів під час проведення кампанії щодо боротьби з вуличною злочинністю *Sword Lily*.

Кіберкомпонента «Золотого щита» пов'язана з діяльністю сил «громадського контролю безпеки мережі» та кіберполіції. Важко наразі сказати, скільки «кіберкопів» працює в КНР, однак як приклад наводять оприлюднені дані щодо розвитку такого підрозділу в одній з китайських провінцій – Гуандун (найбільш густонаселена провінція). Підрозділ кіберполіції розпочав там роботу в 1994 році зі штатом у 2 особи й після численних трансформацій і змін пріоритетів у 2008 році складався вже з 1000 осіб.

Попри такий «значний штат», говорити про реальну можливість здійснювати дійсно жорсткий контроль за мережевим контентом не доводиться, адже, за офіційними даними МЗС КНР, у Китаї зареєстровано лише персональних блогів понад 180 млн, веб-сайтів – 3,86 млн [304]. До того ж завданням «кіберкопів» є не лише інтернет-моніторинг, а й протидія комп'ютерним злочинам, таким як поширення вірусів, шкідливого програмного забезпечення, хакерські атаки, онлайн-шахрайство тощо. Водночас деякі оглядачі припускають, що система «Золотого щита» є важливим елементом у цензурній системі КНР і відповідає за блокування сайтів за *IP*-адресою та ключовими словами [320].

Не менше запитань у правозахисників до системи «Зелена дамба». Уряд КНР та Міністерство промисловості та інформаційних технологій позиціювали цю систему як цензурне програмне забезпечення, що має вберегти китайських користувачів (передусім школярів і студентів) від «шкідливих матеріалів», передусім порнографічних.

У основі системи – блокування картинок, тексту та веб-адрес за певними значеннями. Основні претензії правозахисників викликає саме добір ключових фраз для блокування, що свідчить не стільки про анти порнографічне, скільки про політичне спрямування програми. Так, за даними аналітичного дослідження американських фахівців у сфері *IT* з Мічиганського університету [450], поміж фраз, за якими

відбувається блокування, є, наприклад, слово *фалунь*, яке пов'язане із забороненою в Китаї сектою Фалуньгун.

Від початку реалізації програми передбачалося, що ця цензурна система має бути встановлена на всіх комп'ютерах, які виробляються та продаються/ввозяться на територію материкового Китаю. Однак з огляду на реакцію громадськості (переважно світової), Міністерство промисловості та інформаційних технологій вирішило зменшити зону дії нового програмного забезпечення. Обов'язково воно встановлюватиметься та функціонуватиме лише на комп'ютерах, розміщених у школах, інтернет-кафе й інших місцях публічного доступу. Станом на червень 2009 року систему було встановлено на понад 500 тис. комп'ютерів у КНР [361].

Далеко не всі дослідники проблем цензурної (і рестриктивної) політики в інтернеті засуджують політику уряду КНР. Чимало з них зазначають продуманість подібної «розумної цензури» й вказують на її національно-культурну специфіку [318]. Адже проблема цензурування та взагалі втручання держави в інформаційний контент має в Китаї тривалу історію і не стосується суто мережі інтернет. Китайська політична традиція завжди надавала контролю більшого значення, ніж західна [111].

Китайська система цензури є багаторівневою, що і забезпечує її успішність в умовах розвитку сучасних технологій [454]. Одним з таких рівнів є «пасивна цензура» – дії, спрямовані на часткове ізолювання загалу громадян від інформування з певної тематики та її обговорення. При цьому «елітарні» групи таким обмеженням не підлягають.

Джек Лінчуан Цю (*Jack Linchuan Qiu*), аналізуючи структуру користувачів мережі інтернет у КНР, доходить висновку про їх поділ на штучно створені «вищі» (елітарні) та «нижчі» класи користувачів. Він вказує при цьому на те, що «нижчі» класи впродовж тривалого часу були позбавлені широкого доступу до мережі інтернет [394]. На думку дослідника, одна з важливих стратегій КНР полягає в недопущенні інформаційного перетину «вищих» і «нижчих» класів із приводу обговорюваних тем за одночасного забезпечення своєрідної свободи спілкування та обговорення тем для «вищих» класів.

Загалом китайський уряд намагається децентралізувати методи контролю медіа для досягнення якомога ефективніших механізмів цензурування та зменшення політичних ризиків, пов'язаних з їх застосуванням. Отже, здійснюється «ефективне домінування» у сфері

комунікацій, але не ставиться завдання «тотального контролю» медіаконтенту. Тобто основним завданням цензурної політики КНР є не контроль контенту повідомлень, а контроль засобів поширення цього контенту, максимально можливе ускладнення для користувачів пошуку в мережі інформації, небажаної для уряду та цензурних органів.

Крім того, на думку К. Ширкі (*Clay Shirky*), ставка робиться на «самоцензурування», сформоване та підкріплюване закликами до стриманого націоналізму, розуміння відповідальності перед суспільством і необхідності захисту суспільної моралі [412]. Р. Пітерс (*Robert Peters*) зазначає, що КНР завдяки подібній обмежувальній політиці створила інтернет-спільноту, що сповідує погляди й цінності, протилежні західним [389].

На думку китайських дослідників проблем інформаційної політики КНР, стратегія обмежень щодо мережі інтернет цілком вкладається в інформаційно-політичний контекст «керованої відкритості».

Систему «керованої відкритості» її дослідник Є. Євдокімов характеризує, з одного боку, як збереження централізованого контролю влади над основними інструментами формування суспільної думки всередині Китаю та апарату інформаційного впливу на закордонне суспільство, а з іншого – цей контроль вже не означає фізичного усунення носіїв альтернативних точок зору (арешти, закриття інформації, заборони на відвідування іноземцями окремих районів чи заходів). Таким чином, на думку Є. Євдокімова, не відмовляючись від здійснення політики обмеження свободи слова, КНР демонструє зрілість, кваліфікованість і технічну оснащеність китайського пропагандистського апарату, здатного витримувати конкуренцію з іноземною пропагандою та місцевими дисидентськими рухами бодай за деякими обраними напрямами інформаційного протиборства [74].

Чимало західних дослідників тематики «КНР та інтернет» покладали на інтернет «революційні» надії, вважаючи, що сама причетність КНР до Всесвітньої мережі спричинить у країні політичні зрушення в дусі ліберальних і неоліберальних теорій. Проте виявилося, що керівництву КНР вдається не тільки контролювати потенціал цього комунікативного інструменту, а й наочно демонструвати іншим світовим гравцям як інтернет можна використовувати з метою підтримки існуючої політичної системи.

Створену в КНР рестриктивно-цензурну (обмежувально-контрольну) систему розбудовують і американські інформаційно-циф-

рові компанії, які масово зайшли на китайський ринок на початку 2000-х років. Найвідоміший приклад співробітництва американських компаній з авторитарною китайською владою стосується збору даних про потенційних опонентів влади, які користувалися сервісом пошукового гіганта *Yahoo!* Починаючи з 2003 року компанія принаймні тричі ставала «відомою» через обвинувачення преси в тім, що вона надавала владі КНР відомості про своїх користувачів. У подальшому ці користувачі були визнані винними в скоєнні антидержавних злочинів[74]. У американському суспільстві така практика «колаборатства» інформаційних транснаціональних компаній з авторитарними політичними режимами викликає значний резонанс, що засвідчує, зокрема, сюжет на подібну тему відомого американського серіалу[75].

Цензурну політику в КНР піджвлює і контрольоване зростання систем телекомунікацій. Так, станом на 2003 рік у КНР було побудовано не більше ніж 10 мереж, більшість яких до того ж користувалася контрольованими китайським урядом ключовими інфраструктурними елементами [301].

Але попри політику КНР, спрямовану на блокування частини контенту закордонного походження (зокрема новинних ресурсів), «китайській інтернет» не позбавлений суто політичного змісту чи гострих обговорень актуальних тем, які стосуються діяльності уряду та міжнародної політики. Причому висновки, до яких доходять учасники форумів, далеко не завжди збігаються з позицією влади КНР [314]. Уже згадуваний китайський блогер М. Анті зазначає, що не варто думати, що лише через те, що китайці не мають доступу до «Великого інтернету», в Китаї немає публічної сфери. Він стверджує: «У КНР 300 млн мікроблогерів, які є справжнім кошмаром для офіційних осіб і які навіть на цензурованих майданчиках можуть обговорювати складні суто політичні питання. Так, іноді їм доводиться використовувати різноманітні натяки для позначення певних посадовців, однак всі розуміють, про кого йдеться. Коли ми говоримо про 300 млн

---

[74] Компанію *Yahoo!* звинувачують у принаймні трьох випадках такої співпраці, що призвели до ув'язнення політичних активістів чи журналістів. Один з найвідоміших – ув'язнення в 2005 році журналіста Ши Тао (*Shi Tao*), який вийшов на волю лише у 2014 році (більш докладно про це – див., наприклад [261].

[75] Ідеться про одну із серій популярного американського серіалу «Гарна дружина» (*The Good Wife*), в якій обігрується саме такий сюжет співпраці американської *IT*-компанії та уряду КНР, що призвела до ув'язнення китайського дисидента. Цікаво, що цей серіал у 2014 році потрапив до переліку серіалів, заборонених для ретрансляції у КНР.

користувачів лише системи мікроблогів, то розуміємо, що ефективно відцензурувати такий потік просто неможливо.» [239]. До речі, М. Анті (справжнє ім'я Чжао Цзін (*Zhao Jing*) був жертвою співробітництва уряду КНР з американськими компаніями, зокрема *Microsoft*, яка у 2005 році закрила його блог китайською мовою після того, як блогер оприлюднив серію статей про систему китайської цензури, яка здійснюється за участі західних компаній. У 2011 році адміністратори *Facebook* повністю видалили сторінку Чжао Цзіна в цій соціальній мережі під тим формальним приводом, що вона була зареєстрована з використанням псевдоніму, а не реального імені [117].

На нашу думку, проблему цензурування в китайському сегменті мережі доречно ставити не в універсальний контекст «безмежної свободи слова», а в специфічний китайський контекст обстоювання «азіатських цінностей». У цьому контексті цікаві оцінки китайської цензурної моделі пропонує Женьмінь Жібао. У січні 2013 року газета надрукувала статтю Ван Ївея (*Wang Yiwei*), який активно заперечує тезу щодо тотожності «західних» й «загальнолюдських» цінностей, вказуючи на існування трьох принципово різних ціннісних моделей [82]. Відповідно до першої, прозахідної, моделі розвиток КНР невдовзі зупиниться через брак «європейських» цінностей у китайців. Друга модель ґрунтується на думці про те, що в китайців є специфічні, однак не універсальні («не загальнолюдські») цінності. Третя модель виходить з розуміння рівнозначності західних і китайських цінностей як «загальнолюдських». Якщо ж Захід заперечує китайську ціннісну модель, то лише тому, що вона є загрозою для західної могутності. У програмній статті Ван Ївея порушується також проблема реглобалізації, потреба якої обґрунтовується тим, що домінантна модель глобалізації пов'язана із просуванням ліберальної парадигми та «західних» цінностей. Ван Ївей стверджує: «Нам потрібна глобалізація іншого порядку, глобалізація системи цінностей, яка в межах усього світу поважатиме та виражатиме всі існуючі культури, підходи та моделі розвитку, повністю відображатиме багатоманіття та багатство різних цивілізацій» [Там само].

Тези, сформульовані у статті з Женьмінь Жібао, не є принципово новими. По суті, вони відтворюють відомі положення лідера Сінгапуру Лі Куан Ю, який у своїх політичних трактатах протиставив конфуціанські цінності ліберальним цінностям Заходу.

На проблему утвердження китайських цінностей особливу увагу звернув у доповіді на 18-му з'їзді КПК Ху Цзіньтао. Він закли-

кав до розбудови соціалістичної культурної держави «з китайською специфікою», розвитку «високої традиційної моралі китайської нації» [160]. У доповіді Ху Цзіньтао пролунали також заклики до розбудови інфраструктури інтернету та поліпшення його наповнення, посилення управління мережевою спільнотою, просування його унормованого та впорядкованого функціонування інтернету на правовій основі; боротьби з порнографічною та нелегальною духовною продукцією; поширення наукових знань і посилення науковості й наукової підготовленості суспільства.

Залишаючи осторонь філософські питання несприйняття китайських цінностей західним світом, слід визнати, що осудні оцінки Заходу щодо внутрішньої політики КНР стосовно її власного кіберпростору часто-густо ґрунтуються не на науково-об'єктивному аналізі ситуації (зокрема щодо реальних можливостей держави здійснювати тотальній контроль за власним кіберпростором), а на суб'єктивних пересторогах, пов'язаних зі зростанням політичної ваги КНР на міжнародній арені та бажанням певних геополітичних гравців справляти вплив на цю країну.

Отже, критика регулятивної політики КНР щодо функціонування мережі інтернет може розцінюватися як складник глобального тиску, що здійснюється розвинутими країнами Заходу не тільки на КНР, а й на інші країни. Насаджування політики забезпечення прав людини, ліберальних цінностей, демократії тощо віддавна перетворилися для західних держав на чинник «м'якого» тиску.

Такі міркування не означають автоматичного схвалення регулятивної політики КНР щодо внутрішнього кібернетичного простору, яка насправді характеризується встановленням жорстких норм контролю персональних даних, надто суворих покарань за розміщення протиправного контенту. Водночас потрібно визнати факт: усе це не заважає стрімкому зростанню в Китаї загальної кількості користувачів інтернету й розвитку національного інформаційного простору. Але ставить під сумнів певні парадигмальні уявлення західних дослідників щодо взаємозв'язку питань інноваційного (інформаційного) розвитку та політичного режиму в країні. І це питання ще має бути додатково досліджене, оскільки не може бути повністю пояснене з погляду класичних неоліберальних уявлень про політичний та економічний розвиток.

Аналітичні оцінки досвіду КНР у сфері регулювання внутрішнього інформаційного (кібер) простору є важливими, зокрема, з огляду на спроби багатьох країн (розвинутих і тих, що розвиваються) виро-

бити власні стратегії забезпечення інформаційного суверенітету національних держав в умовах реконструкції (деструкції) традиційного розуміння державного суверенітету й трансформування підходів до сучасних воєнних протистоянь, які набувають характеру інформаційних (кібернетичних) і психологічних й мають, отже, виражений гуманітарно-технологічний вимір.

Значна кількість держав досі до кінця так і не визначилася з офіційною позицією щодо статусу кіберпростору та основних принципів його функціонування. За таких умов просування такими країнами, як КНР, проектів регулювання кіберсфери й правил поведінки, що стосуються міжнародної інформаційної безпеки й є альтернативними тим, що їх пропонують світовій спільноті держави Заходу (передусім США), формує базу для широкої дискусії з цього питання. Лобістом китайських альтернативних ініціатив і союзником КНР у цьому напрямі є Російська Федерація та низка інших держав.

12 вересня 2011 року чотири країни-члени ООН (КНР, РФ, Узбекистан і Таджикистан) звернулися до Генерального секретаря ООН з листом, в якому пропонували розглянути на 66-ій сесії Генеральної Асамблеї запропонований ними проект *A*/66/359 – Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки (*далі* – Правила) [262]. Хоча вказаний документ був надто лаконічним (його було сформульовано на 3 сторінках), однак деякі його ключові положення мали дійсно стратегічне значення для опонування домінантному західному підходу щодо недоторканності «вільних потоків інформації».

Так, уже в преамбулі Правил вказується, що «політичні повноваження у пов'язаних з інтернетом питаннях державної політики є суверенним правом держав; держави мають права та обов'язки стосовно пов'язаних з інтернетом питань державної політики міжнародного рівня» [Там само]. Фактично ця теза стверджує проекцію класичного державного суверенітету на інтернет-простір і його регулювання, тобто саме те, проти чого так активно виступають неоліберальні ідеологи та прихильники концепту «вільних потоків».

Правила стали відправною точкою й підґрунтям для ухваленої РФ Концепції зовнішньої політики Російської Федерації, затвердженої у лютому 2013 року. Концепція зазначає, зокрема, що Росія з метою посилення міжнародної безпеки «домагатиметься створення під егідою ООН правил поведінки у сфері забезпечення міжнародної інформаційної безпеки» [107].

З-поміж іншого, Правила звертають увагу на такі ключові моменти:

• забезпечення поваги «до основних прав та свобод людини, а також до багатоманітності історії, культури та соціального розвитку всіх країн» (пункт «*a*»);

• необхідність співпраці в «боротьбі зі злочинною чи терористичною діяльністю з використанням інформаційно-комунікаційних технологій <...> що підриває політичну, економічну та соціальну стабільність держав, їх культурне та духовне становище» (пункт «*c*») – відтворення ключової для КНР тези про необхідність захисту самобутніх духовних цінностей народу;

• «сприяння створенню багатосторонніх, демократичних міжнародних механізмів управління інтернетом, які <...> гарантували б його стабільне та безпечне функціонування» (пункт «*g*»).

В ООН сторони розпочали супровід своєї пропозиції в межах Першого та Третього комітетів. Під час 6-ої та 7-ої зустрічей Третього комітету[76] Генасамблеї ООН представник делегації КНР при ООН Лі Сяомей (*Li Xiaomei*) зазначила, що китайська сторона висловлює жаль із приводу відсутності на міжнародному рівні регулювальних документів, що мали б посприяти встановленню міжнародної інформаційної безпеки.

Основна дискусія відбулася в Першому комітеті[77] Генасамблеї під час 17-ої зустрічі, присвяченої обговоренню Правил. Посол КНР Ван Цюнь (*Wang Qun*) звернувся до учасників зустрічі зі вступним словом, у якому висвітлив позиції КНР з питання [415]. Загалом вони збіглися з позицією РФ, як з'ясувалося з виступу представника Росії А. Малова. Російська сторона наголосила на тім, що документ є передусім «запрошенням до діалогу», й ініціатори його внесення не наполягатимуть на голосуванні [40]. А. Малов також звернув увагу присутніх на те, що розроблена РФ Конвенція про забезпечення міжнародної інформаційної безпеки також є платформою для обговорення подібної міжнародної проблематики, й що вона згодом може стати не політичною декларацією (якою є Правила), а реальним міжнародно-правовим документом. Цю позицію підтримав і представник Білорусі [39].

Негативно з приводу Правил висловилися представники США та Австралії. В. Рейд (*Walter S. Reid*) від імені США зазначив, що пи-

[76] Опікується соціальними та гуманітарними питаннями, а також питаннями культури.

[77] До його компетенції належать питання роззброєння та міжнародної безпеки.

тання кіберсфери виходять поза межі обговорення у форматі ООН і потребують задіяння міжнародного гуманітарного законодавства як бази обговорення подібних ініціатив. Фактично аналогічної позиції дотримувався і представник Австралії П. Вулкотт (*Peter Woolcott*), який зазначив, що обговорення кібертематики в ООН буде надзвичайно складним, а багатоаспектність проблеми унеможливлює її обговорення в межах Комітету[78]. Крім того, П. Вулкотт зазначив, що Австралія повністю підтримує багатосторонній підхід до управління інтернетом і принципово заперечує державний контроль за мережею[79].

Більш розгорнутими й категоричними були оцінки Правил з боку представників держструктур США. Зокрема, М. Маркофф (*Michele Markoff*), старший радник Держдепартаменту з питань інтернету, висловила думку про те, що подібні проекти є спробою домогтися від ООН схвалення дій щодо посилення контролю над інтернет-простором [46]. Крім того, вона «нагадала» про факт укладення договору між 15 країнами включно із США, Росією та Китаєм щодо колективного обговорення питань інформаційної політики у зв'язку з поширенням інформаційних технологій, зазначивши, що в цьому контексті заява КНР і Росії сприймається як вихід з переговорного процесу. Аналогічну позицію посів також помічник Держсекретаря М. Познер: «Якщо такий кодекс буде прийнятий, це майже неминуче підірве свободу ЗМІ та спричинить перехід від кіберпростору, що розвивається пересічними людьми, до системи централізованого контролю з боку урядів. Це не дуже добра ідея» [38].

Не менш однозначним було зауваження з боку Кіберкомандування США, керівник якого генерал К. Александер, висловився проти того, щоб ООН регулювала інтернет, вважаючи, що в цілому це ослабить загальну безпеку в мережі.

Китайсько-російська ініціатива спричинила також негативну реакцію у відповідь з боку представника ОБСЄ з питань свободи ЗМІ Д. Міятович (*Dunja Mijatovic*), яка заявила, що подібні ініціативи є неприпустимими, оскільки потенційно можуть бути використані для спорудження бар'єрів на шляху потоків інформації чи обміну думками [141]. Вона звернула увагу країн-подавачів на те, що в червні

[78] У цьому контексті варто згадати, що нещодавно (вересень 2011 року) між США та Австралією було укладено додаткові угоди щодо спільної протидії кіберзагрозам і посилення двосторонньої співпраці з даного питання.

[79] Позиція була висловлена практично тими самими словами, якими вона записана в Міжнародній стратегії для кіберпростору (США).

2011 року представники ООН, ОБСЄ, Організації американських держав і Африканської комісії з прав людини і народів ухвалили Спільну декларацію про свободу вираження поглядів в інтернеті, зауваживши, що саме цей документ з даного питання має бути базовим.

У колективному листі від неурядових організацій на ім'я Голови 66-ої Генасамблеї ООН Насіра Абдулазіза Аль-Насера (*Nassir Abdulaziz Al-Nasser*) запропоновані Правила було піддано критиці за чотирма напрямами [387]:

• багатостороннє управління мережею, зазначене в пункті «*g*», не передбачає участі громадянського суспільства, що може перетворити таке управління на суто міждержавне;

• формування культури інформаційної безпеки, зазначене у пункті «*h*», передбачає провідну роль держави та державно-приватного партнерства на тлі відсторонення від цього процесу представників громадянського суспільства;

• «загальна повага до прав людини» містить суттєве уточнення – «повага до багатоманіття історії, культури та соціальної структури всіх країн», що може бути використано як привід для звуження універсальності прав людини, закріплених, зокрема, в документах Генасамблеї;

• боротьба зі злочинною чи терористичною діяльністю з використанням інформаційно-комунікативних технологій передбачає протидію діяльності, що «підриває політичну, економічну та соціальну стабільність держав, їх культурні та духовні традиції»; проте таке формулювання проблеми перевищує допустимі обмеження на свободу вираження думки, закладені статтею 19 (3) Міжнародного пакту про громадянські та політичні права та може бути використане для обмеження (цензурування) свободи слова.

Так само критично поставилися до Правил учасники міжнародної конференції з питань діяльності в кіберпросторі (Лондон, 1-2 листопада 2011 року), проведеній з ініціативи британського МЗС під девізом «Бачення. Сподівання. Побоювання» *(The Vision – The Hopes – The Fears*). Конференція зібрала 700 делегатів від урядових і комерційних структур ыз 60-ти країн [377].

Очікувалося, що під час проведення заходу Пекін і Москва спробують знайти точки дотику із західними партнерами щодо ухвалення запропонованої ними ініціативи на рівні Генасамблеї. Однак Лондонська конференція цих очікувань не виправдала. Міністр закордонних справ Великобританії У. Хейг (*William Hague*) у виступах під час від-

криття та закриття конференції підкреслив, що боротьба зі злочинністю та тероризмом не може виправдати спроби підпорядкування інтернету державним інтересам, явно маючи на увазі Пекін і Москву. Цю думку підтримав і британський прем'єр Д. Камерон (*David Cameron*): «Уряди країн світу не повинні використовувати кібербезпеку як привід для запровадження цензури» [356].

Офіційну позицію США на Лондонській конференції презентував американський віце-президент Дж. Байден, який категорично висловлювався проти політики країн, які під виглядом боротьби з кіберзлочинністю обмежують свободу діяльності в інтернеті і пропонують укласти «репресивний глобальний кодекс поведінки в інтернеті» (*repressive global code*) [444].

Прикметно, що до згаданої дискусії практично не долучалися країни ЄС, оскільки всередині Євросоюзу досі тривають дискусії щодо визначення меж свободи/контролю за контентом мережі (наприклад, у межах зазначеної вище ініціативи *The Great European Firewall project*).

Крім розглянутих Правил, існують також інші ініціативи, спрямовані на утвердження на міжнародному рівні правил гри в інтернеті. Вельми демонстративною є зазначена вище ініціатива Російської Федерації, яка не просто в окремих положеннях перегукується із Правилами, але є саме тим документом, який держава намагається реально закріпити на міжнародному рівні як бачення інформаційної безпеки, альтернативне західному.

Конвенція про забезпечення міжнародної інформаційної безпеки (КЗМІБ) [105], концепцію якої було представлено російською стороною під час Другої міжнародної зустрічі високих представників, що курують питання безпеки (20-21 вересня 2011 року, Єкатеринбург)[80], є значно більшою за обсягом, ніж Правила, і ґрунтовніше висвітлює те, що було лише контурно й частково окреслено китайсько-російським документом. Зокрема, в КЗМІБ, так само, як і у Правилах, акцентовано увагу на тім, що всі питання, пов'язані з державною політикою щодо мережі інтернет, є суверенним правом держав. Крім того, з-поміж загроз у сфері міжнародної інформаційної безпеки виокремлено такі:

• неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої ці ресурси розміщені;

[80] Учасниками були 52 країни. Рівень представництва – вищі особи, які відповідають за координування діяльності правоохоронних структур. Україну представляла Секретар РНБО України Р. Богатирьова.

• діяльність у інформаційному просторі з метою підриву політичної, економічної та соціальної системи іншої держави, психологічний вплив на населення, що дестабілізує суспільство;

• маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація та приховування інформації з метою викривлення психологічного та духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних та естетичних цінностей;

• протидія доступу до новітніх інформаційно-комунікативних технологій, створення умов технологічної залежності у сфері інформатизації на шкоду іншим державам[81];

• інформаційна експансія, набуття контролю над національними інформаційними ресурсами іншої держави.

Документ, запропонований Російською Федерацією для розгляду та обговорення ООН, жодною мірою не суперечить китайським підходам до інформаційної та кібербезпеки й відверто опонує відповідним американським документам і підходам. Можна припустити, що Росія та Китай активно консультувалися щодо своїх позицій, погоджували їх. Але, незважаючи на потужний супровід зазначеної ініціативи російським зовнішньополітичним відомством, вона так і не перетворилася на базу домовленостей між ключовими геополітичними гравцями включно із США та їх союзниками.

Висновки до розділу

На сьогоднішній проблематика майбутнього глобального кіберпростору є на перетині двох рівнозначних трендів. З одного боку, офіційні зусилля спрямовані на демілітаризацію кіберпростору та недопущення перетворення його на нове поле збройного протистояння, а з іншого – де-факто продовжується процес протистояння. Навіть у середовищі науковців та експертів відсутнє спільне бачення того, чи буде взагалі ефективним будь-який міжнародний механізм заборони мілітаризації кіберпростору чи нагляду за цим процесом.

[81] Хоча цей пункт кореспондує з тезами американської Стратегії кіберпростору, він має у російській версії принципово інший зміст. США, заперечуючи «обмеження доступу до технологій», мають на увазі обмеження урядами доступу до ІКТ для населення, тоді як РФ, вочевидь, має на увазі формальні та неформальні міждержавні обмеження. Зокрема обмеження, пов'язані з сумнозвісною поправкою Джексона-Веніка чи правилами, встановленими за років «холодної війни» (1949 р.) Координаційним комітетом з експортного контролю (*Coordinating Committee for Multilateral Export Controls, CoCom*), які згодом трансформувалися у Вассенарські домовленості (1996 р.)

Міжнародні структури на кшталт ООН, МСЕ чи *G*8 (*G*20), хоча й роблять спроби впливати на цей процес, однак ці спроби є фрагментарними та надто обережними. Незважаючи на цілу низку рішень і резолюцій, ООН так реально і не наблизилася до вироблення дієвого міжнародного документа, що зміг би впорядкувати кібербезпекову проблематику.

Не менш складними є і спроби ключових кібербезпекових держав (США та КНР) виробити внутрішні підходи до проблеми та запропонувати міжнародні ініціативи щодо майбутнього кіберпростору. Навіть побіжний огляд внутрішніх і зовнішніх ініціатив цих гравців робить очевидним той факт, що вони сповідують надто різні погляди з питання, і їм буде вкрай складно знайти точки дотику.

Розділ 4.

ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ УКРАЇНИ В ГЛОБАЛЬНОМУ ТА НАЦІОНАЛЬНОМУ КІБЕРПРОСТОРАХ

4.1. Ключові засади позиціювання України щодо кібербезпекової проблематики

4.1.1. Україна у вимірі сучасних кіберзагроз

Кіберзагрози Українській державі та суспільству умовно можна розділити на два ключових рівні. Перший – «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою. Хоча, звичайно, ціла низка кіберзлочинів має на меті й може скоюватися виключно для збагачення злочинців.

Можна констатувати, що в Україні в повному обсязі присутні всі ключові «класичні» кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо) і щороку їх кількість зростає.

Розглядаючи динаміку кількості карних справ, порушених Службою безпеки України за фактами виявлених кіберзлочинів, можна чітко прослідкувати їх істотне збільшення:

від 39 справ у 2005 році до 158 у 2011 році [55]. За результатами розгляду кримінальних справ у судових засіданнях за вказаний час винесено 20 судових вироків, з них у другому півріччі 2012 року – 14, у першому півріччі 2013 року – 6.

Ще наочнішими є дані МВС України. Стрімко зростає кількість шахрайств, здійснюваних за допомогою високих інформаційних технологій – лише за 6 місяців 2013 року їх було виявлено 986, у той час як за весь 2012 рік – 1663. Зростає кількість злочинів, пов'язаних з незаконними діями з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення: за весь 2012 рік виявлено 21 і стільки ж – за півроку 2013 року.

Ця динаміка стає найбільш очевидною на злочинах за ст.ст. 361, 361-1, 361-2, 362, 363 розділу XVI КК України[82]. Так, за ст. 361[83] у 2012 році було зареєстровано 74 злочини, а в 2013 році – 286. За ст. 362[84] спостерігається зростання – із 40 злочинів у 2012 році до 133 у 2013 році. Загалом можна констатувати, що кількість виявлених злочинів демонструє виразну тенденцію до зростання абсолютно за всіма основними статтями КК України, що стосуються злочинів, здійснюваних із використанням високих інформаційних технологій.

У структурі злочинів переважають різноманітні випадки шахрайств, основною жертвою яких є банківсько-фінансовий сектор та його клієнти. Так, у 2013 році кіберзлочинці намагалися привласнити з банківських рахунків 87 млн грн, «вдалими» стали шахрайства на 10 млн грн [19]. В Україні спостерігаються доволі високі показники розкриття кіберзлочинів у банківській сфері – до 80 % вкрадених коштів повертається господарям [120]. Хоча при оцінюванні рівня розкриваності фінансових кіберзлочинів варто зважати на високий рівень їх латентності – банківським установам переважно вигідніше закрити очі на вкрадені кошти й тихо компенсувати їх із власних ресурсів, ніж заявляти про це у правоохоронні органи [8]. Основною

---

[82] Статті Кримінального кодексу України, що входять до Розділу 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

[83] Ст. 361 – Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

[84] Ст. 362 – Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

причиною такої поведінки є потенційні іміджеві та репутаційні втрати, які для цього сектору є основними загрозами. Державі стає відомо лише про 5 % злочинів у кіберпросторі, а значна кількість потерпілих від них можуть тривалий час і не знати про те, що їх атакували. Іноді на виявлення факту «зламу» витрачаються місяці (якщо це спрямований «злам», здійснений фахівцями, – роки) [85].

Таким чином можна констатувати, що далеко не завжди держава реально обізнана з масштабами кіберзлочинності. І ця проблема наявна не лише в Україні, а й у всіх державах, де кіберзлочинність набирає обертів.

Зростають масштаби як традиційного кардингу[85], так і більш складних кіберзлочинів. Крім того, й досі значними за обсягами та збитками залишаються такі злочини, як поширення порнографії, порушення авторських прав, чому особливо активно протидіє МВС.

Якщо говорити про злочини, віднесені до групи геополітичних, чи міждержавних, механізмів боротьби (хактивізм, кібершпигунство та кібердиверсії), то загалом ситуація є такою. Україна вже активно залучається у протистояння хактивістів, в окремих випадках стає об'єктом кібершпигунських акцій, однак досі не було зареєстрованих випадків кібердиверсій.

Першим масованим випадком хактивізму, з яким зіткнулася Україна, були події довкола закриття файлообмінного сервісу *ex.ua*. Ідеться про масовані *DDoS*-атаки на ресурси органів державної влади, здійснювані різноманітними суб'єктами, переважно громадянами України. Після спроб правоохоронних органів втрутитися в роботу файлообмінного сервісу було здійснено *DDoS*-атаки на понад 10 інтернет-сайтів органів державної влади, зокрема на сайт Президента України та сайт Міністерства внутрішніх справ України (символічно, що сайт інституції, яка має опікуватися питаннями кіберзлочинності, виявився одним з найменш стійких до кібератак).

Атака розпочалася після того, як правоохоронні органи за позовом компаній *Microsoft*, *Adobe*, а також телеканалу «1+1» спочатку заблокували домен, а потім заарештували частину серверів компанії. Уже ввечері того ж дня внаслідок масштабних *DDoS*-атак було заблоко-

[85] Вид шахрайства, пов'язаний із використанням платіжних карток або їхніх реквізитів. Відповідні дані отримуються найрізноманітнішими способами: від фішингу та зараження персональних комп'ютерів вірусами до скіммінгу, тобто використання спеціальних «накладок» на банкомати, які знімають необхідні для зловмисників дані прямо у процесі легального використання банківських карток їх власниками.

вано роботу офіційних сайтів Президента України, уряду, Верховної Ради, СБУ, Національного банку України, Антимонопольного комітету, Державної податкової служби, Партії регіонів, Міністерства внутрішніх справ України. Певний час МВС було навіть змушене публікувати новини про свою діяльність на сторінках у соцмережах – ВКонтакте та *Facebook*.

У Всесвітній мережі (а також соціальних мережах) активно поширювалися інструкції про те, як саме можна здійснювати *DDoS*-атаки. Водночас, крім пересічних користувачів, які брали участь в атаці, в мережі було запущено спеціальний проект «Низькоорбітальна іонна гармата» (*Low Orbit Ion Cannon*), який мав полегшити проведення *DDoS*-атак. Через сайт *Low Orbit Ion Cannon* активувався скрипт, який починав серію звернень до визначених сайтів з метою виведення їх з ладу за рахунок дуже значної кількості відвідувань.

Уже 3 лютого *ex.ua* знов став доступним для користувачів, а згодом (у червні 2012 року) компанії повернули більшу частину вилученої техніки. Розслідування, проведене фахівцями СБУ засвідчило, що більшість атак здійснювали пересічні користувачі, з найбільш активними з яких було проведено «роботу». Водночас кримінальних справ чи інших процесуальних дій за результатами цих атак так і не було порушено [108], оскільки, по-перше, до МВС із відповідними заявами ніхто з постраждалих так і не звернувся, а по-друге, особливістю *DDoS*-атак щодо урядових ресурсів є те, що прямого економічного збитку державні органи від них не зазнають.

Історія довкола *ex.ua* вперше наочно продемонструвала, наскільки Українська держава не готова ані ідеологічно, ані технічно до подібних атак. Щоправда, саме відсутність прямих економічних збитків стала причиною того, що реальних висновків із тієї ситуації так і не було зроблено.

Наступною масштабною хактивістською кампанією стало політичне протистояння в жовтні 2013 року – лютому 2014 року довкола підписання/непідписання тодішньою владою Угоди про асоціацію між Україною та ЄС (події Євромайдану). Це протистояння активно відбувалося в соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток [12]. Наприклад, у *Twitter*, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Використовувалися також механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі).

Було «зламано» електронну пошту, аккаунт прес-секретаря Ю. Луценка Л. Сарган на *Twitter* та *Facebook*, аккаунти В. Кличка у *Facebook* та Вконтакте, «зламано» офіційний сайт партії «УДАР» та поштову скриньку й аккаунт на *Facebook* прес-секретаря Ю. Тимошенко М. Сороки [14]. Зі «зламаних» сторінок масово розсилалися фейкові[86] (підроблені) повідомлення, спрямовані на дезінформування суспільства. Загалом відбулася прицільна атака на ресурси та інструменти, які забезпечують комунікацію політиків із громадськістю та ЗМІ через інтернет.

Постраждали й електронні ЗМІ, які були головними інформаційними майданчиками, а заразом і рушійними силами акцій протесту. Кілька днів поспіль хакерських атак зазнавав сайт «Української правди» та «Главкому». Сайт інтернет-видання «Цензор.нет» було знищено хакерами [Там само]. Усе це змусило зазначені ЗМІ переносити свою активність до соцмереж. Наприклад, «Українська правда» почала розміщувати новини у *Twitter* та *Facebook* [121].

DDOS-атак зазнали сайти органів державної влади. Офіційні сайти Міністерства внутрішніх справ, Кабінету Міністрів і Президента України зазнали хакерських атак.

Останнє на часі кіберпротистояння стосується загострення українсько-російських відносин. Частково воно є наслідком тієї суспільно-політичної кризи, яка охопила українське суспільство протягом грудня 2013 року – лютого 2014 року. Унаслідок цього протистояння було сформовано загони хактивістів, які йменують себе «Кіберберкутом» (*Cyberberkut* – віртуальна структура, що не визнає української влади, яка сформувалася після лютого 2014 р.)[87] та «Кіберсотнею Майдану», «Анонімусами» з російською або українською «прописко́ю» тощо.

Діяльність «кіберберкутівців» та інших інтернет-активістів (хактивістів) аналогічного ідеологічного спрямування зводиться переважно до *DDos*-атак на державні установи, мас-медіа й навіть комерційні

[86] Від англійського *fake*, що означає підробка, фальсифікація.

[87] http://cyber-berkut.org/
https://www.facebook.com/CyberBerkut
https://twitter.com/cyberberkut1
https://vk.com/cyberberkut1

структури. Наприклад, саме «Кіберберкут» взяв на себе відповідальність за атаки на сайти структур НАТО 15 березня 2014 року – було здійснено напади на офіційний сайт НАТО, а також на сайти Центру кіберзахисту НАТО в м. Таллінні (*The NATO Cooperative Cyber Defence Centre of Excellence – CCD COE*) та Парламентської асамблеї НАТО.

«Кіберберкут» здійснював не лише класичні *DDos*-атаки, а й дефейси, зазвичай розміщуючи на атакованих ними сайтах карту України, де західні області помічені нацистською свастикою, а з Криму виходять стріли напрямів «фронтових ударів» на Південь і Схід України. Популярними символами були звернені одна до одної голови змії (вочевидь, має символізувати ворога) й беркута.

Найбільш масованою атакою цієї групи на урядові інтернет-ресурси була атака, організована 3 березня 2014 року. Складнощі в роботі відчули численні (понад 100) сайти – як урядові (зокрема Верховної Ради України, Кабінету Міністрів України, РНБОУ), так і різноманітних інтернет-ЗМІ.

З боку лояльних до нової влади хакерських структур було проведено аналогічні кібератаки проти веб-сайту «Кремлін.Ру», сайтів Центробанку Росії, Міністерства іноземних справ РФ, *Russia Today* (RT), «Російської газети». Так само, як і «Кіберберкут», ці структури використовували дефейси. Наприклад, 4 березня 2014 року внаслідок такої атаки на сайт російського зовнішнього телемовника *RT* у заголовках новин усі слова *Russia* й *Russians* було змінено на *Nazi* й *Nazis* [342]. Іншим прикладом є дефейс сторінок сайту Держдуми РФ. Так, 10 квітня 2014 року було «зламано» сторінку депутата-комуніста М. Харитонова [215], а 15 квітня – голови Комітету з транспорту. В обох випадках від імені власників сторінок розміщувалися антиросійські звернення, які закінчувалися гаслом «Слава Україні!» [214].

DDos-атаки й досі є важливим інструментом протистояння хактивістів. Причому для цього останні не гребують залученням цілком кримінальних ресурсів. Наприклад, у квітні 2014 року було проведено низку потужних *DDos*-атак на урядові ресурси (зокрема сайти Кабінету Міністрів України та Генеральної прокуратури України), для чого активно використовувалися бот-мережі. За даними фахівців *CERT-UA* [50], для атаки на сайт Кабміну було задіяно щонайменше два ботнети. Цікаво, що після того, як фахівцям *CERT-UA* вдалося блокувати один із серверів управління бот-мережі (сервер, що коор-

динує роботу всіх заражених комп'ютерів), за допомогою якого координувалася *DDoS*-атака на веб-сайт Урядового порталу, власник/орендар цього серверу за 5 хвилин зв'язався зі своїм провайдером і вимагав пояснень щодо недоступності серверу. Так само бот-мережі використовувалися і в атаках на сайт Генпрокуратури України 4 квітня 2014 року [49]. Зазначимо, що ті самі бот-мережі використовуються й із суто кримінальною метою – для атаки цілей, що не мають жодного стосунку до політичного процесу.

В інтернет-протистоянні Росії з Україною проти України вперше було застосовано троянські програми, ключовою серед яких став вірус *Uroburos* [79]. З одного боку, завданням цього вірусу було формування бот-мережі із заражених комп'ютерів та отримання повноцінного доступу до їх наповнення, а з іншого – викрадення інформації з цих комп'ютерів. Об'єкти атаки також, вочевидь, були обрані не випадково – веб-ресурси органів державної влади (в тому числі силових структур), засобів масової інформації, фінансових установ, великих промислових підприємств.

Українські фахівці із *CERT-UA* виявили кілька особливостей цього вірусу:

• складність програмного коду (що обумовлює можливість його розроблення із залученням значної кількості людських, технічних і фінансових ресурсів (зокрема, це можуть бути науково-дослідні установи, *IT*-корпорації, державні установи, спецслужби тощо);

• наявність літер кирилиці у програмному коді;

• схожість за низкою характеристик (імена файлів, ключі шифру, основні можливості тощо) із троянською програмою, яку було знайдено в інформаційних системах ЗС США в 2008 році, що призвело до повної відмови ЗС США від використання *USB*-носіїв (через які вона поширювалася) в автоматизованих системах військового призначення);

• географія поширення вірусу [Там само].

Зважаючи на зазначені особливості, фахівці *CERT-UA* припускають, що до вироблення вірусу причетні іноземні спецслужби, а сам він очевидно пов'язаний зі зростаючою (на той час – середина березня) напруженістю в українсько-російських відносинах.

Можна дійти висновку, що основним мотивом ініціатора цієї кібератаки було бажання встановити прихований контроль за визначеними об'єктами для подальшого спостереження за інформаційним обміном із власної території. Щоправда, іноземні дослідники (зокре-

ма польські [310]) вважають, що всі функції *Uroburos*'у ще не до кінця вивчено та не виключено, що, можливо, він має значно більше завдань та можливостей.

Хоча діяльність вірусу *Uroburos* і є першим випадком цілеспрямованої атаки на державні інформаційні системи, однак Україна й раніше відчувала на собі діяльність вірусів, які можна класифікувати як кіберзброю.

Так, упродовж останнього періоду Україна вже ставала жертвою принаймні двох вірусів, які більшість фахівців характеризують як кіберзброю, – це розглянуті вище віруси *Duqu* та *MiniDuke*. Те, що більшість українців уповні не відчули на собі наслідки цих акцій, не є дивним і наразі лише до певної міри – прикрим. Адже причиною цього є вельми строкатий, неоднорідний рівень інформатизації України включно зі сферами державного управління та виробничих процесів, що є тимчасовим «природним» захистом держави від складних кібератак.

На щастя, Україна поки не зіткнулася з кіберзброєю, придатною для проведення кібердиверсій. Багато в чому це було обумовлено відсутністю (або прихованою природою) протягом усіх років незалежності суттєвих зовнішніх загроз чи екзистенційних загроз національній безпеці, що походять від потужних зовнішніх гравців, які мають необхідні можливості створення таких кіберозброєнь. Водночас події 2014 року (які, вочевидь, матимуть своє продовження в тій чи іншій формі наступними роками) дозволяють припустити, що слід очікувати на збільшення кіберзагроз для Української держави.

При цьому маємо враховувати, що на сьогодні кібербезпековий сектор держави лише частково готовий відповідати на масовані кібератаки, що доводить, зокрема, масштабність успішних *DDoS*-атак на урядові ресурси. Заклики окремих українських фахівців з інформаційної безпеки формувати своєрідні «кібердружини» [189] свідчать не стільки про рівень уваги до цієї проблеми, скільки про обмеженість можливостей держави. Загалом сумнівно, що Україна на сьогоднішньому етапі уваги до кібербезпекових питань дійсно буде спроможна щось протиставити на реальні масовані атаки.

Зовнішні гравці, як уже зазначалося в роботі, активно готуються до масштабних кіберпротистоянь, змінюючи свої підходи до самого розуміння кіберпростору, формуючи відповідні нормативно-правові, організаційні елементи, вкладаючи в це значні кошти. Глобальне геополітичне протистояння неодмінно спричинюватиме (і вже спричинює) підвищення якості наступальних кіберозброєнь, що є в розпо-

рядженні всіх геополітичних суб'єктів. Ідеться не лише про США та КНР, які є локомотивами гонки кіберозброєнь, а й про інші потужні держави – Росію, Індію, країни Азії та Європейського Союзу. Україна не може просто ігнорувати цю нову реальність, оскільки подальші процеси інформатизації лише підвищуватимуть вірогідність того, що від умовно небезпечних *DDoS*-атак супротивники України (а не виключено, що й сьогоднішні союзники) переходитимуть до більш жорстких дій – від кібершпигунства до кібердиверсій.

4.1.2. Геостратегічні чинники впливу на кібербезпекову політику України

Хоча Україна досі є на шляху розвитку, однак для неї проблеми глобалізованого кіберпростору не є чимось відірваним від політичної реальності. Понад те, що інтенсивніше розвивається інформаційне суспільство в Україні, то актуальнішою (як для держави в цілому, так і кожного громадянина зокрема) стає проблема самовизначення України щодо кіберпростору. Сам факт актуалізації кібербезпекового складника для нашої держави свідчить про певний рівень розвитку українського суспільства, який визначає на порядку денному нові загрози людині, суспільству, державі.

Можна більш-менш чітко артикулювати сутнісну зміну геополітичної реальності для Української держави. Ця зміна пов'язана із двома розглянутими вище панівними глобальними трендами: зростанням впливу КНР на міжнародній арені (і, відповідно, посиленням суперництва між Китаєм та США) та виокремленням кіберпростору у відносно самостійний «п'ятий» простір геополітики та геостратегування. Саме ці тренди створюють передумови «холодної війни *v*2.0.», а їх наслідком є стрімка мілітаризація кіберпростору.

Трансформаційні процеси України в цій новій реальності є наразі в точці біфуркації. А це означає, що навіть незначні безпосередні або опосередковані дії чи впливи спрацьовують за принципом «малі причини породжують великі наслідки» («ефект метелика»), тобто можуть вирішально позначитися на позиціюванні України в найближчому й більш віддаленому майбутньому.

Що далі просуватиметься Україна шляхом інформатизації та становлення інформаційного суспільства, то уразливішою вона буде перед кібератаками. І жодні її односторонні міжнародні зобов'язання (на зразок позаблоковості чи нейтралітету) не спроможні завадити подібній зловмисній діяльності. Її наслідком буде втягування Ук-

раїни в нову «холодну війну», позначену рисами хактивізму, кібершпигунства та кібердиверсій.

Україна, яка прагне бути не лише об'єктом, а й суб'єктом світової політики, має сформувати власну цілісну стратегію щодо кіберпростору (як глобального, так і локального), визначити щодо нього свої зовнішньополітичні пріоритети, ключові стратегії розбудови власної кіберпотужності та механізми захисту національного кіберпростору від атак. Усі ці елементи мають бути взаємопогоджені та перетворені не просто на один з елементів зовнішньо- та внутрішньополітичних стратегій, а на один з основних чинників формування оновлених національних інтересів держави в умовах становлення інформаційного суспільства.

Формуючи власну зовнішньо- та внутрішньополітичну стратегію в новому цифровому світі, Україна має виходити з таких довгострокових трендів.

1. Неоднозначні відносини між США та КНР, які весь час вагаються між співробітництвом (і суперництвом) та протистоянням, цілком можуть призвести до «холодної війни» оновленого формату. І цей глобальний зовнішньополітичний наратив – реальність, а не віддалена перспектива. Отже, Україна мусить покінчити зі своєю позірною багатовекторністю й віднайти власне місце в новому постбіполярному світі. Відповідно, вона має визначитися стосовно стратегічної перспективи у вимірах класичного для української зовнішньої політики трикутника інтересів «США – ЄС – Росія», який або доповниться четвертим учасником, або зазнає суттєвих і непередбачуваних поки що трансформацій.

2. Кіберпростір є не просто тлом протистоянь, а новим полем геополітичного суперництва. Особливість кіберпростору як нового геополітичного простору змушує держави витрачати додаткові кошти на недопущення його використання іншими учасниками в інтересах, які суперечать їхнім національним інтересам. Логічно та передбачувано це призводить до мілітаризації кіберпростору, що супроводжується посиленням недовіри між акторами, несформованістю міжнародного нормативно-правового поля та відчуттям нового протистояння в термінах ядерного стримування середини XX сторіччя.

3. Зростання катастрофічної свідомості й відчуття небезпеки, яке завжди було психологічним підґрунтям для реалізації гонки озброєнь. Але на відміну від гонки озброєнь доби залякування ядерними силами стримування, які сама їх природа робила проблематичними у за-

стосуванні, кіберозброєння застосовуватимуться надзвичайно часто й матимуть наслідки не лише в реальному світі (йдеться про реалізацію сценарію «цифрового Перл-Харбору»). І кожній державі, яка захоче принаймні не зазнавати важких наслідків цих «бойових» дій, доведеться вкладати сили й кошти в кібербезпеку та власні кіберозброєння.

4. Не варто очікувати на прийняття жодних реальних, а надто дієвих, міжнародних договорів щодо заборони кіберозброєнь. Якщо під час «холодної війни» між США та СРСР мали місце хоча б спроби взаємного стримування, роззброєння тощо, то цілком латентний характер створення кіберозброєнь унеможливлює контроль за ними з боку будь-якого авторитетного міжнародного органу.

5. Сплеск шпигунської активності, базованої на використанні кіберпростору, стане визначною прикметою кіберпротистоянь. «Шпигунські скандали» були характерними і для класичної «холодної війни», однак особливістю «холодної війни *v*2.0.» стане можливість «масованого» та часто «неспрямованого» шпигунства (можливості шпигунських програм дозволяють охоплювати не лише цільові об'єкти атаки, а й будь-які схожі об'єкти, розташовані в будь-яких інших місцях). Цей стан перманентної небезпеки опосередковано спричинюватиметься інтерконективністю сучасних технологій.

6. У світі «холодної війни *v*2.0.» нового значення набуде концепція національного виробника, принаймні щодо *IT*-сфери. Сама можливість здійснення кібершпигунських чи кібердиверсійних заходів обумовлюється вразливостями програмного забезпечення й використання заздалегідь встановлених на рівні програмного забезпечення чи навіть мікросхем «закладок» (таємно встановлених елементів програми, які дозволяють зловмисникам отримати несанкціонований доступ до ресурсів системи). Наразі проблема потенційних «закладок» турбує безпекові структури абсолютно всіх країн. Адже значна кількість експортерів програмних продуктів і технологічних рішень зосереджена в 2-3 країнах світу, які і є найактивнішими учасниками «холодної війни *v*2.0.». Відповідно, перед більшістю держав постає питання створення суто національних (створених вітчизняними фахівцями, на вітчизняному обладнанні, для вітчизняних потреб) продуктів, що їх уповноважені безпекові структури можуть ідентифікувати як дійсно безпечні. Це стосується всього спектра продукції, починаючи від мікросхем і закінчуючи національними антивірусами, операційними системами тощо. Незважаючи на такий, вочевидь неринковий, механізм функціонування держави в інформаційну добу,

саме до таких кроків вдаються навіть ті держави, які проголошують неоліберальні принципи розвитку, зокрема США. Не дивно, що країни більш «закриті» діють в аналогічний спосіб, формуючи політику інформаційної безпеки. До кола цих країн належать, зокрема, Росія та Іран. А в завершеному вигляді цей виразний тренд набуття цифрового суверенітету демонструє КНР.

7. Швидше за все, в кіберпросторі замість реалізації ідей «великого села» М. Маклюена (*Herbert Marshall McLuhan*) з'являться чітко окреслені «національні інтернети». На сьогодні модель такого «нацнету» існує лише в КНР, але можна очікувати, що у віддаленій перспективі аналогічним чином сегментуватимуться й інші елементи мережі, а перетинатимуться вони в доволі вузькому сегменті взаємодій. Понад те, навіть більшість експертів і науковців, погоджуючись зі стрімким зростанням кількості й ролі недержавних гравців як важливих учасників кіберпросторових процесів, зазначають, що основним гравцем тут залишаються саме держави. Нова модель світу, навіть незважаючи на зростання ролі недержавних суб'єктів, досі трактується як продержавна «кібер-Вестфальська епоха» [290], «нове Вестфальське павутиння» тощо (*The New Westphalian Web*) [362]. Дійсно, поки реальний контроль над фізичним рівнем кіберінфраструктури буде доменом держави, саме вона буде основним гравцем на цьому полі. Крім того, в жодному разі не варто забувати, що дійсно масштабні, продумані й добре підготовлені кібератаки найчастіше здійснюються фахівцями, вірогідність приналежності яких до спеціальних державних структур (розвідувальних, контррозвідувальних чи військових) має високий ступінь імовірності. Це вкотре засвідчили події, пов'язані з діяльністю Е. Сноудена, колишнього співробітника американського ЦРУ, який упродовж другого півріччя 2013 року безперервно постачав світовим медіа компромат на американські спецслужби.

Саме в такому світі Україна змушена обирати модель поведінки, яка дозволила б їй не лише «виживати», а й успішно розвиватися. Фактично йдеться про позиціювання України у «кібер-Вестфальську епоху» в координатах вестфальського світоустрою:

- підтвердження та забезпечення принципу національного суверенітету, передусім через вимоги невтручання в державні справи та забезпечення повноцінної влади на всій території держави;
- забезпечення балансу сил;
- рівність держав;
- обов'язковість дотримання сторонами укладених договорів.

Отже, зрештою йдеться про забезпечення державою цифрового суверенітету як ключового елементу більш загального інформаційного суверенітету[88]. Під *інформаційним суверенітетом* автор розуміє «сукупність організаційних, нормативно-правових, воєнних та зовнішньополітичних заходів, що спрямовані на забезпечення цілісності національного інформаційного простору, національної інформаційної інфраструктури та технологічної безпеки України, що здійснюється в інтересах забезпечення прав та свобод громадян України, суспільства та держави» [69]. А під *цифровим суверенітетом* – здатність держави самостійно й незалежно (в межах її технологічних можливостей) забезпечувати національні інтереси в кіберсфері, самостійно розпоряджатися власними інформаційними (цифровими) ресурсами та національною інформаційною інфраструктурою, а отже, гарантувати кібернетичну та інформаційну безпеку державі, суспільству та громадянам.

Цифровий суверенітет – це передусім стійкість і захищеність країни у кібервійнах, причому захищеність не тільки від вірусів, кібератак, «зламувань» («кряків»), витоків інформації та викрадень даних, спаму, а й від відключення вороже налаштованими зовнішніми силами певних об'єктів критичних інфраструктур.

Україна має забезпечити кіберсуверенітет, а отже, й оновлені національні інтереси щодо кіберпростору [63] як на фізичному рівні – (у спосіб створення власної базової інформаційно-телекомунікаційної інфраструктури), так і на контентному рівні – (через організаційні, інституційні, правові, політичні механізми).

На сьогодні концепція цифрового суверенітету є дискусійною і наукових розробок із цього питання бракує. Окремі напрацювання у цій сфері мають переважно французькі та російські дослідники.

Наприклад, відомий російський фахівець із нових медіа та інформаційної безпеки І. Ашманов запропонував таку систему елементів, що є основою «ідеального цифрового суверенітету» [84].

1. Електронний «щит»:

- власна апаратна платформа (мережева та ПК);
- власна чи контрольована програмна платформа (мережева та ПК);
- власна чи контрольована мобільна платформа.

---

[88] Поняття *цифрового суверенітету* досі залишається дискусійним. У багатьох випадках він розглядається як синонім понять *інформаційний суверенітет* та *кібернетичний суверенітет*. У роботі ми переважно використовуємо поняття *цифровий суверенітет* як більш містке за своїм наповненням, подеколи як його синонім може застосовуватися поняття *кібернетичний суверенітет*. Водночас, на нашу думку, *інформаційний суверенітет* є більш широким поняттям, ніж *цифровий суверенітет*.

2. Інформаційний «щит»:

• власна інтернет-інфраструктура;

• власна медійна структура ЗМІ, ТБ та інтернету;

• власна система й засоби пропаганди та ведення інформаційних війн;

• розвинена ідеологія, закони, ринок ідеологічних послуг.

На нашу думку, розвинена ідеологія, закони, ринок ідеологічних послуг з очевидністю має бути першою позицією. Під *ідеологією* будемо розуміти системно організовану сукупність ідей, поглядів, переконань, цінностей та установок, представлених у формі міфів, настанов, гасел, програмних документів партій, філософських концепцій тощо, яка виражає інтереси різних соціальних груп, класів, співтовариств, держави у цілому.

Кібернетична ідеологія – це усвідомлення й оцінка ставлення великих груп людей до соціальної дійсності кіберпростору, до соціальних проблем, нею викликаних, і можливих та бажаних способів розв'язання існуючих і потенційних «кібернетично вмотивованих» соціальних конфліктів. Така ідеологія також включає, вочевидь, цілі (програми) соціальної діяльності, спрямованої на закріплення або зміну існуючих суспільних і міжнародних відносин, пов'язаних із володінням кіберпростором або його фрагментами.

Хоча й не впритул, але до США за рівнем володіння кіберсуверенітетом наближається Китай, який має власні операційні системи, процесори, пошукові системи, пошту, месенджери, соціальні мережі, антивіруси, мережеве обладнання та програмне забезпечення, потужні зовнішні фільтри на зразок «Золотого щита» тощо. Третю позицію можна віддати Росії, яка вже розпочала вироблення власних процесорів Эльбрус-4С. Європейські країни та решта світу відстають.

На нашу думку, запропонована І. Ашмановим схема цифрового суверенітету багато в чому є логічною компонентою кібермогутності держави, оскільки зазначені параметри переважно є вимірюваними. Однак загалом ця схема не придатна для оцінки кібермогутності, бо є надто вузькою та лише частково відповідає реальним вимогам часу.

Цифровий суверенітет і кібермогутність базуються на сукупності змістовних чинників, до яких належать:

• інноваційний потенціал країни та її здатність самостійно створювати новітні технології;

• ступінь розвитку *IT*-компаній, а де-факто – наявність національних *IT*-ТНК;

• ступінь розвитку внутрішнього ринку (передусім відповідної вимогам сучасності IT-інфраструктури);

• гуманітарний показник впливу культури країни на загальний контент мережі;

• військовий потенціал держави (передусім можливість здійснювати кібератаки та захищатися від них);

• зовнішньополітична компонента (включно з можливостями впливу на міжнародні структури, задіяні в управлінні інтернетом).

Перші чотири елементи є звичайним предметом уваги сучасних держав, які вибудовують більш-менш цілісні стратегії розвитку інформаційного суспільства. Розвиток *IT*-компонентів безпекового та військового потенціалу є зазвичай засекреченим і забезпечується стратегічними й доктринальними документами безпекового та військового сектору, які, попри свою проголошену відкритість, є малоінформативними. Зовнішньополітична компонента кіберсуверенітету й кібермогутності узалежнюється базовими зовнішньополітичними документами, ухваленими в конкретній державі, та реальним станом справ у цій державі та її позиціювання на міжнародній арені.

Аксіоматичним є твердження про складність прогнозування можливості розвитку інших елементів кіберсуверенітету й кібермогутності без необхідного й достатнього (мінімального) «електронного щита», а де-факто – розвинутої кібернетичної інфраструктури. Усе зазначене має бути враховане у процесі побудови комплексних моделей кібернетичної безпеки, суверенітету й могутності держави, покликаних пов'язати всі основні елементи в єдину систему.

Загальний вигляд запропонованої схеми взаємопов'язування геостратегії держави щодо кіберпростору, цифрового суверенітету й кібермогутності представлений на рисунку стор. 255.

Законодавчо закріплений курс на інтеграцію України в європейські структури є, вочевидь, недостатньо адаптованим, якщо кіберпростір оцінювати у вимірі геополітичних стратегій держави. Адже, як уже підкреслювалося, з геополітичної точки зору, основними гравцями в кіберпросторі є США та КНР. Європейський Союз, Росія та низка інших країн, хоча і є важливими гравцями, однак, об'єктивно оцінюючи їх можливості, слід констатувати неспроможність «повноцінно втрутитися» в реальну конструкцію двостороннього суперництва в кіберпросторі на межі протистояння «холодна війна *v*2.0.».

Не зайве наголосити із цього приводу, що позиція України в міжнародному контексті кіберпростору та перспектив його розвитку має

бути проактивною. Наразі Україна поки що не розкрила свій потенціал розвитку в цій сфері. Виступаючи зі значущими зовнішньополітичними ініціативами у сфері убезпечення діяльності в кіберпросторі, вона насправді не використовує доступні їй механізми участі в дискусіях із питань міжнародної кібернетичної безпеки на найвищому рівні на всіх міжнародних майданчиках. Зокрема, Україна не скористалася можливостями головуючої в ОБСЄ країни у другому півріччі 2013 року та, на відміну від деяких країн-попередниць на цій посаді (Казахстан, Литва), не запропонувала світові жодних ініціатив у сфері міжнародної кібернетичної безпеки.

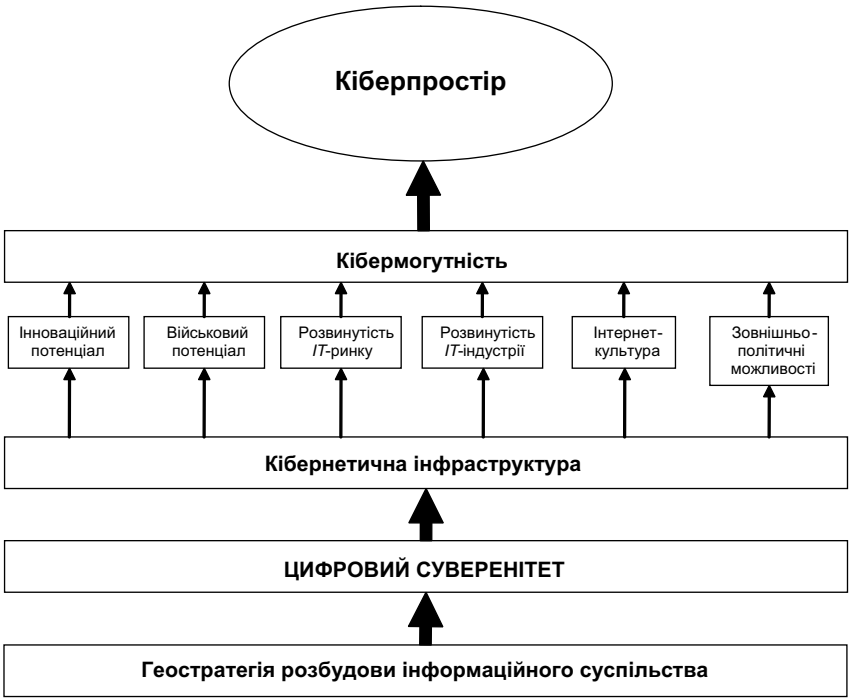

Рис. Взаємопов'язування геостратегії держави щодо кіберпростору, цифрового суверенітету й кібермогутності

Зазначене свідчить, що Україна має здійснити внутрішню світоглядну й ідеологічну революцію, спрямовану на подолання рутинного розуміння кіберпростору як «нейтральної території загального

безпечного користування» й вироблення ставлення до нього як до нетрадиційної території, що містить суттєву кількість загроз і викликів різних рівнів – від гуманітарного до суто технічного. Саме така базова настанова має бути засадою оцінювання реального стану кібернетичної сфери та прийняття будь-яких внутрішньо- й зовнішньополітичних рішень щодо перспектив її розвитку.

Наразі у плані кіберреалізму держава та бізнес (виразніше) демонструє певне розуміння даної проблеми, оскільки більше стикаються з нею. Однак для значної кількості українців, для багатьох з яких блага інформатизації є фрагментарними та ситуативними, а використання кіберпростору обмежується лише базовими можливостями, кіберзагрози на рівні сприйняття досі є відірваними від реальності буденного існування й буденної свідомості.

Не виключено, що вже в найближчому майбутньому Україна та українці будуть змушені, формуючи пріоритети безпеки для власних мереж та інформаційних технологій, виходити з позиції, запропонованої Д. Бреннером для американського військового й розвідувального сектору безпеки: «діяти та приймати рішення, виходячи з того, що всі службові мережі – включно із секретними – є «зламаними» [Цит. за: 246]. До цього варто додати, з огляду на викривальні заяви Е. Сноудена, ще й пересторогу, що всі мережі «прослуховуються» та потенційно уразливі для виходу з ладу через «закладки».

Як Україна осмислить себе в цьому новому геополітичному протистоянні, які цілі поставить (чи не поставить) перед собою і про яке орієнтовне «бажане майбутнє» заявить не на суто декларативному, а на матеріально-предметному рівні, зрештою, залежить від її вибору базових ідеологічних парадигм інформаційного суспільства. Кожна із цих парадигм є по-своєму привабливою, сказати б, «звабливою», однак ідеться про їх добір і поєднання, перегляд наявних концепцій розбудови інформаційного суспільства в Україні з погляду їх відповідності не лише ситуативним інтересам, а передусім довгостроковим національно-державним інтересам.

4.2. Пріоритети зовнішньополітичних стратегій України в кіберпросторі за умов посилення суперництва між основними геополітичними гравцями

Україна змушена у стислі строки сформувати цілісну позицію щодо кіберпростору як поля нового геополітичного протистояння, а державні зусилля у сфері зовнішньої політики природно мають бути

спрямовані на досягнення «бажаного майбутнього», яке б найповніше відповідало її довгостроковим інтересам.

Усі зазначені безпекові пріоритети мають реалізовуватися в суперечливих умовах:

• наявна в Україні модель інформаційного суспільства потребує перегляду з метою більш ефективного посилення цифрового суверенітету держави та зміцнення її кібермогутності;

• загальний рівень економічного розвитку не дозволяє спрямувати значні кошти у сферу подальшого розвитку *IT*-сфери, а отже, доводиться покладатися переважно на аутсорсингові потужності й співпрацю із провідними геополітичними гравцями (передусім зі США та ЄС, КНР і РФ) та інформаційними ТНК;

• вага України на міжнародній арені об'єктивно не дозволяє їй бути очільником концептуальних змін щодо майбутнього кіберпростору (хоча певний потенціал для цього зберігається). На це, зокрема, вказують автори аналітичної доповіді «Концептуальні засади зовнішньополітичної стратегії України»: «Протягом останніх років значення України для розвитку системи міжнародних відносин в Європі та світі вступає у суперечність з тією фактичною роллю, яку вона відіграє в цій системі. Йдеться про певну девальвацію міжнародної суб'єктності нашої держави, яка, внаслідок ряду внутрішніх і зовнішніх чинників, втрачала можливості впливати на процеси прийняття рішень у міжнародних політичних справах та у питаннях міжнародної безпеки» [155, с. 4];

• в Україні досі не сформовано образ «бажаного майбутнього», який має відповідати довгостроковим (стратегічним) інтересам нашої держави в кіберпросторі;

• законодавча основа здійснення зовнішньополітичної діяльності України майже повністю ігнорує значення проблематики кіберпростору в практичній політичній діяльності.

Говорячи про стратегічні інтереси Української держави щодо глобального кіберпростору як такого та перспективи міжнародної політичної дійсності з цього питання в інтересах України, необхідно виокремити такі моменти.

1. Україна зацікавлена в максимально демілітаризованому й мирному глобальному кіберпросторі, що стає запорукою стрімкого економічного та інноваційного розвитку держави.

2. Україна має докладати зусиль щодо якнайширшого представлення власних інтересів стосовно майбутнього кіберпростору на всіх

ключових міжнародних майданчиках. Важливим елементом цього має стати просування Україною ініціатив (чи приєднання до ініціатив, висунутих іншими гравцями), спрямованих на формалізацію термінології у сфері міжнародної кібербезпеки та відповідності цих термінів іншим міжнародним нормативно-правовим документам (передусім тим, що регламентують питання війни та права самозахисту держав).

3. Одним із головних питань захисту національних інтересів Української держави в кіберпросторі є проблема забезпечення широкого міжнародного контролю за функціонуванням мережі інтернет, а отже, передання функцій управління та адміністрування його ключових елементів від *ICANN* легітимним міжнародним структурам, передусім наприклад, Міжнародному союзу електрозв'язку або іншим, яких визначить ООН. Водночас Україна має вітати ті процеси інтернаціоналізації управління інтернетом, які спостерігаються протягом останніх років. Важливим тут є недопущення вихолощування цього процесу та уникнення небезпеки відтворення наявної моделі управління, однак з іншими гравцями.

4. Зважаючи на дедалі виразніший тренд суверенізації окремих елементів мережі (зокрема, побудова де-факто «національного інтернету» в КНР чи анонсований проект «альтернативного інтернету» від країн БРІКС), Україна, з одного боку, має вживати заходів щодо недопущення подальшого загострення проблематики, пов'язаної з фрагментацією мережі, а з іншого – вибудовувати стратегії розвитку з урахуванням можливості їх повноцінної реалізації та необхідності визначати свою позицію в такому «кіберсегментованому» світі.

5. Жоден з наявних на сьогодні підходів (умовно «американсько-європейський» та «російсько-китайський») до забезпечення миру й стабільності в глобальному кіберпросторі навряд чи зможе стати реальною базою для обговорення, незважаючи на загальне загострення ситуації, пов'язане з викривальними заявами Е. Сноудена. Відповідно, Україні варто наважитися вийти із пропозиціями, що сприятимуть досягненню необхідного консенсусу.

Крім того, потрібен комплексний аналіз відповідності «американсько-європейського» та «російсько-китайського» підходів до визначення майбутнього мережі національним інтересам Української держави. Причому потрібно розуміти, що ці, діаметрально протилежні, підходи концентровано втілюють глибинні сутнісні геополітичні позиції держав, і передусім є проекцією «національної сили» на міжнародний кіберпростір.

Розглядаючи принципи «російсько-китайської» моделі, доречно звертатися до тексту Конвенції про забезпечення міжнародної інформаційної безпеки (КЗМІБ), яка, хоча й була подана в ООН російською стороною, однак чітко окреслює безпекові контури «російсько-китайської» моделі. Водночас для пояснення окремих моментів так само доречним є посилання на тези Правил міжнародної поведінки в кіберпросторі (ПМПК), які, як зазначалося, хоч і не повністю збігаються з КЗМІБ, однак мають очевидну схожість «за духом» та загальними месиджами. Для «американсько-європейського» підходу «базовим» є текст Міжнародної стратегії для кіберпростору.

Загалом порівняння двох ініціатив формує враження, що запропоновані американсько-європейською та російсько-китайською «сторонами» ініціативи[89], апелюючи до одних і тих самих ключових питань інформаційної (кібер) безпеки, мають на увазі різні речі або ж артикулюють окремі нюанси таких питань в антогоністичних площинах, що вкрай ускладнює взаємопогодження позицій.

Американська Стратегія кіберпростору передбачає, зокрема, «право на захист» відповідно до Статуту ООН (передусім ідеться про захист американської інформаційної інфраструктури від кібератак). Російсько-китайські ПМПК уже в першому пункті також вказують на необхідність «поважати Статут ООН та загальновизнані норми міжнародного права, що включають, поміж іншого, повагу до суверенітету, територіальної цілісності та політичної незалежності всіх держав» [262]. Однак навіть поверхові уточнення «російсько-китайської» ініціативи щодо «поваги до багатоманіття історії, культури та соціального укладу всіх країн» чітко засвідчує бажання отримати від провідних держав світу певні гарантії невтручання (навіть опосередкованого) у сферу політичних комунікацій у спосіб підбурювання чи активної підтримки «кольорових революцій» тощо як базис забезпечення політичної стабільності держави.

Крім того, зрозуміло, що без створення відповідної міжнародної нормативної бази чи суттєвого уточнення чинної визнання кібератак (а наразі й усього того, що можна витлумачити як кібератаку) «актом агресії» подібна одностороння позиція США виглядає неоднозначно загрозливою для країн, з територій яких здійснюють напади організовані хакерські групи. Адже метою таких атак можуть бути об'єкти

[89] Огляд відповідності ініціатив національним інтересам Української держави подається за роботою [72].

американської інфраструктури, зокрема інформаційної. Ідеться не лише про Україну, а й про цілу низку країн з високим рівнем підготовки *IT*-фахівців, які можуть вчиняти протиправні дії, що їх неспроможні попередити правоохоронні структури.

Те саме стосується «вільних інформаційних потоків», питання про які американська сторона порушила альтернативно ще в 80-ті роки XX сторіччя, коли ЮНЕСКО ініціювала програму створення Нового міжнародного інформаційного порядку (ініціатива комісії Ш. Мак-Брайда (*Sean MacBride*). Зрештою, демонстративний вихід США, Великобританії та Сінгапуру з ЮНЕСКО у 1984–1985 рр. із втратою майже третини бюджету цієї організації призвів до торпедування будь-яких подальших активних ініціатив цієї організації, спрямованих на суверенізацію міжнародного інформаційного простору.

Відповідно до американської ініціативи «держави мають поважати свободу потоків інформації в їх національних мережах та не втручатися в роботу тієї інфраструктури, що відноситься до такої, яка тісно пов'язана з міжнародною функціональністю мережі», тобто фактично роль держави у контролі за частиною інформаційного простору нівелюється.

Натомість «російсько-китайська» ініціатива (ПМПК) зауважує на тім, що свобода інформаційних потоків має враховувати національне законодавство кожної держави.

Саме з питання свободи інформації спостерігаються найбільші розбіжності між «російсько-китайським» та «американсько-європейським» підходами. Причому розбіжності такого ступеня, що стають абсолютно незрозумілими ймовірні шляхи та перспективи їх зближення. Позиція КНР – РФ щодо співробітництва держав «у <...> стримуванні поширення інформації <...>, яка підриває політичну, економічну та соціальну стабільність держави, її культурний та духовний уклад» навряд чи буде колись підтримана західними країнами, що вбачають у цьому потенційну загрозу обмеження свободи слова, цензури та впливу на активістів громадянського суспільства.

Ціла низка положень тієї ж Конвенції про забезпечення міжнародної інформаційної безпеки видаються сумнівними з погляду їх реального впровадження в міжнародне нормативно-правове поле.

Наприклад, поняття *інформаційна війна* визначається як «протиборство між двома або більше державами в інформаційному просторі з метою завдання шкоди інформаційним системам, процесам та ресурсам, критично важливим та іншим структурам, підриву політич-

ної, економічної та соціальної систем, масованого психологічного впливу на населення для дестабілізації суспільства та держав, а також примушення держав до прийняття рішень в інтересах протиборчої сторони». Отже, теоретично будь-яке повідомлення, що з'являється в мережі інтернет від імені держави і засуджує/висловлює незгоду з тією чи іншою політикою іншої держави, може бути витлумачене як вияв інформаційної війни з відповідними наслідками.

Також украй проблематичним уявляється забезпечення реального контролю за протидією *масованій психологічній обробці населення* (особливо закріплення такого положення на рівні національного законодавства), оскільки не зовсім зрозуміло, які саме критерії визначатимуть такий вплив та чи можливо взагалі визначити ці критерії. Бажання російської сторони врахувати психологічну компоненту інформаційної безпеки цілком зрозуміле і до певної міри виправдане, однак навіть у самій Російській Федерації відсутній консенсус із цього питання. Ще на початку 90-х років XX сторіччя у РФ було здійснено кілька невдалих спроб ухвалити федеральний Закон «Про інформаційно-психологічну безпеку». Останньою такою спробою було внесення відповідного Законопроекту на розгляд Держдуми 3 грудня 1999 року (19 червня 2001 року він був відкликаний самим суб'єктом законодавчої ініціативи).

Неоднозначною є також дефініція поняття *міжнародна інформаційна безпека*, що трактується як «стан міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав та світового співтовариства в інформаційному просторі».

Як зазначалося, положення КЗМІБ щодо визначення «неправомірного[90] використання інформаційних ресурсів іншої держави без погодження з державою, в інформаційному просторі якої ці ресурси розміщені» [105] як загрози міжнародній інформаційній безпеці суперечить також положенням проамериканської Конвенції про кіберзлочинність. Але ж країни, що підписали Конвенцію про кіберзлочинність (з Україною включно) вже погодилися з можливістю подібної ситуації.

Безумовно, з погляду традиційного розуміння загроз національній безпеці, зазначене положення КЗМІБ є конфліктним, оскільки заперечує де-факто необхідність захисту національного суверенітету.

---

[90] Конвенція не пояснює, що в даному контексті означає «неправомірне» – *Прим. авт.*

Водночас, зважаючи на специфічно інтернаціональний тип загроз, якими є кібератаки та кіберзлочинність у цілому, така добровільна відмова від частини інформаційного суверенітету уявляється виправданою платою на шляху до безпечнішої глобальної мережі.

Загалом текст КЗМІБ виглядає надто рестриктивним, оскільки в ньому перераховано значну кількість заборонювальних дій. До того ж значна частина цих дій є просто нереалістичною, оскільки не може бути формалізована нормативно-правовим чином задля забезпечення чітких критеріїв для їх подальшого відслідковування (моніторингу).

До таких заборон можна віднести, зокрема, «маніпулювання інформаційними потоками, дезінформацію та приховування інформації з метою викривлення психологічного та духовного середовища суспільства, ерозії традиційних культурних, моральних, етичних та естетичних цінностей». З тексту незрозуміло, яким чином держави мають на рівні національного законодавства визначати поточний стан «психологічного та духовного середовища суспільства», зафіксувавши при цьому «традиційні культурні, моральні, етичні та естетичні цінності» з метою подальшого їх захисту та надання кіберінциденту статусу інформаційної війни.

Разом з тим варто визнати, що деякі положення КЗМІБ відповідають положенням американської Стратегії, і є цілком доречними й актуальними для схвалення Україною. Зокрема, це стосується визначення певних загроз міжнародній безпеці та додаткових чинників, що посилюють небезпеку цих загроз:

• загроза протидії доступу до новітніх інформаційно-комунікативних технологій, створення умов технологічної залежності у сфері інформатизації з метою завдати збитків іншим державам;

• потенційна небезпека включення в інформаційно-комунікативні технології недекларованих деструктивних можливостей;

• відмінності в оснащеності інформаційно-комунікативними технологіями та їх безпеки в різних країнах («цифрова нерівність»);

• розбіжності в національних законодавствах і практиці формування безпечної та швидко відновлюваної інформаційної інфраструктури.

Крім того, КЗМІБ слушно порушує питання щодо меж суверенітету держави в інформаційному (кібер) просторі. На думку авторів КЗМІБ, «кожна держава-учасник має право встановлювати суверенні норми та управляти відповідно до національних законів своїм інформаційним простором. Суверенітет і закони поширюються на інформаційну

інфраструктуру, розташовану на території країни-учасниці, чи іншим чином входить до її юрисдикції». Наразі така позиція, найімовірніше, відповідає довгостроковим інтересам Української держави. На жаль, американська ініціатива лише побіжно висвітлює це питання, перекладаючи акцент на проблему сумісності технологічних рішень.

Загалом «російсько-китайська» модель міжнародної інформаційної (кібер) безпеки, на нашу думку, є більш наближеною до українських реалій і проголошених Україною безпекових цілей в інформаційній сфері. Сама концепція «азійських» чи «євразійських» цінностей дозволяє порушувати концептуальне питання про можливість мати власні ціннісні системи, відмінні від «універсальних». Однак ця модель потребуватиме, з одного боку, більших коштів на впровадження, а з іншого – не вповні відповідає європейському світоглядному базису (менталітету) Українського народу.

Натомість «американська» модель є більш привабливою, бо «тут і зараз» пропонує безліч готових рішень у всіх сферах інформатизації, причому на суто ринкових умовах, які є дійсно доступними та здійсненними за посередництвом приватних ініціатив. Понад те, США часто йдуть назустріч тим країнам, які роблять ставку на американські компанії у сфері інформатизації. Так, наприклад, корпорація *Microsoft* іде на поступки у сфері захисту інтелектуальної власності, формуючи більш привабливі пропозиції на українському ринку тощо.

Позиція України щодо ініціатив, які виходили впродовж останнього часу від основних гравців кіберпростору, є вкрай невизначеною та неартикульованою.

Це, безумовно, пов'язано передусім із характером цих ініціатив, дискусія довкола яких досі триває без виразних перспектив досягнення компромісу, попри спроби різноманітних громадських організацій та науково-аналітичних установ запропонувати реальні рішення (спільна ініціатива Інституту проблем інформаційної безпеки при МДУ РФ та американського *The EastWest Institute* тощо). Кожна із двох описаних моделей міжнародної (кібер) інформаційної безпеки декларує бажання зменшити рівень мілітаризації кіберпростору, однак при цьому нав'язавши іншій стороні (сторонам) неприйнятні для неї (них) правила гри.

Крім того, для України, яка знаходиться у вкрай складному становищі безпекових викликів, вибір найбільш прийнятної для неї моделі й досі залишається доволі непростим через відмінності між «дійсним» і «реальним». З одного боку, маємо чіткий курс на європейську

інтеграцію, активне співробітництво із країнами Заходу, що означає перевагу саме «американсько-європейських» підходів. З іншого – реальні потреби поточної воєнно-політичної обстановки потребують більш жорстких заходів, ніж це допускається зазначеним підходом, зате вповні вкладається в «російсько-китайський». При цьому обрання останнього означатиме втрати для іміджу нашої держави, що спричинюють зрештою втрати економічні.

Час працює не на самовизначення України щодо прийнятності/неприйнятності одного із запропонованих підходів до міжнародної інформаційної (кібер) безпеки. Ідеться, зрештою, про стратегічний вибір напряму формування позиції країни з питань кібербезпеки та перспектив розвитку світового кіберпростору не лише на міжнародному, а й на національному рівні. При цьому потрібно розуміти, що забезпечення безпеки України в кіберпросторі не є питанням найближчих двох-трьох років. Має бути сформована відповідна стратегічна «дорожня карта», що визначатиме головне: якою Україна бачить себе через 10–20 років: «неоколонією», яка постачатиме «метрополії» науковців і технології, чи країною, спроможною забезпечити суб'єктність на світовій арені. Під час її розроблення, зокрема, треба зважати на те, що неоліберальна парадигма не лише не передбачає виключного положення держави як такої на міжнародній арені, а й дедалі частіше апелює до нових геополітичних суб'єктів, якими є недержавні (позадержавні) актори у вигляді ТНК.

У цій ситуації Україні варто зосередитися не стільки на обранні варіантів «або-або», скільки на обстоюванні тих стратегічних цілей щодо глобального кіберпростору, досягнення яких повністю відповідає національним інтересам України, незважаючи на те, яким, власне, підходам це відповідатиме.

Передусім, Україна зацікавлена в демілітаризації кіберпростору та забезпеченні своєрідного «кіберстримування» найбільш потужних гравців, що або неможливо, або вкрай складно без відповідної міжнародної нормативно-правової бази, яка ще має бути напрацьована. І саме в цьому сенсі Україна могла б зробити свою політику більш проактивною [155, с. 5].

Потенційну демілітаризацію кіберпростору доцільно розпочати з питань, непов'язаних з антагоністичними суперечностями. Предметом відповідних договорів може бути протидія терористичним кібератакам, здійснюваним третіми сторонами. Знайдені на цьому шляху спільні позиції згодом можуть перетворитися на першооснову більш

масштабних договірних порозумінь (на зразок Заключного акта Гельсінської угоди 1975 року).

Як один зі світових загальновизнаних лідерів у сфері роззброєння (добровільна відмова від третього за величиною у світі ядерного арсеналу на початку 90-х років XX сторіччя) Україна могла б виступити з цього питання ініціатором обговорень, що, з одного боку, стало б природним продовженням політики ядерного роззброєння, а з іншого – дозволило б Україні посісти більш значущу позицію щодо процесів демілітаризації кіберпростору.

На жаль, Україна не використала для подібних ініціатив можливість, яку надавало їй головування в ОБСЄ в 2013 році, й про можливість чого говорили українські експерти [72]. Крім майданчика ОБСЄ, який був би цілком логічним для подібних ініціатив, Україна може звернутися до інших міжнародних майданчиків, передусім ООН, МСЕ, а з окремих питань – ЮНЕСКО, Ради Європи.

Поміж можливих механізмів посилення ролі України у світових дискусіях щодо майбутнього кіберпростору є проактивна роль вітчизняних дипломатів у Групі урядових експертів ООН з міжнародної інформаційної безпеки. Група об'єднує представників країн, які або хочуть трансформацій чинної ситуації, або принаймні зацікавлено спостерігають за динамікою дискусій у цьому напрямі. Важливою частиною відповідних зусиль України мали б стати кроки, спрямовані на погодження міжнародних підходів до термінології у сфері кібербезпеки. Серед ключових кроків на цьому шляху – закріплення в документах ООН однозначного розуміння кіберпростору як нового, унікального виду простору, створеного людиною, що функціонує завдяки відповідним практичним і теоретичним навичкам людини у сфері електронних телекомунікацій.

Демілітаризація кіберпростору має перетворитися не просто на один із численних напрямів зовнішньої політики України, а на її ключовий напрям поряд з європейською інтеграцією, курсом на розв'язання «заморожених» конфліктів, розбудовою стратегічних відносин із США та КНР, зміцненням міжнародної стабільності й миру [81].

Як зазначалося, важливим елементом попередження демілітаризації кіберпростору та зменшення можливості ескалації «холодної війни *v*2.0.», яка стає дедалі виразнішою, є необхідність упорядкування стратегічного питання щодо управління функціонуванням мережі. Нагадаємо, що з початку стрімкого розвитку інтернету більшість контрольних функцій належать *ICANN*, яка, попри укладені угоди, тісно

пов'язана з державними структурами США, а також іншим організаціям, «управлінський центр» яких або вони самі розташовані у США.

Будь-які спроби урядів інших країн передати управління мережею під міжнародний (міждержавний) контроль зі зрозумілих причин викликають жорстку протидію з боку США. Це протистояння є настільки тривалим, що навіть набуло своєрідної інституалізації через Форум з управління Інтернетом, який збирається щороку з 2006-го з очевидною метою акцентувати на нерозв'язаності проблеми міжнародного контролю за діяльністю мережі[91].

Ще одна серйозна спроба вплинути на позицію США з цього питання спостерігалася наприкінці 2012 року під час роботи Всесвітньої конференції з регулювання міжнародних телекомунікацій (*World Conference on International Telecommunications* 2012 – *WCIT*-12) [143]. Однак і там проблему не було вирішено.

Водночас у 2014 році США пішли на певні поступки міжнародній спільноті й заявили про готовність передати функції *IANA* міжнародному співтовариству, однак передусім – через реформування *ICANN* на засадах мультистейкхолдеризму. Ця передача здійснюватиметься за чотирма напрямами[92]:

• передача урядом США відповідального керівництва функціями *IANA* корпорації *ICANN*;

• посилення підзвітності *ICANN*;

• підтримка безпечної і стабільної реалізації оновлених кореневих зон;

• зміцнення двосторонніх відносин з директивними органами.

Цей процес навряд чи буде швидким та простим, адже і зараз є певні побоювання, що ця ідея є лише спробою змінивши формальну сторону взаємовідносин, зберегти за собою реальні функції контролю за організацією й надалі.

Неоднозначність чинної системи управління мережею інтернет яскраво унаочнює адміністрування домену «*.UA*». Наразі домен адмініструє ТОВ «Хостмайстер». Вона здійснює технічну підтримку доме-

[91] Показово, що поміж учасників, які фінансують цей захід [322], відсутні США чи його урядові структури. Основний тягар фінансування припав на європейські країни, частково – на інших зацікавлених гравців (Індію, Росію та міжнародні структури, наприклад МСЕ). Водночас активну участь, зокрема у фінансуванні заходу, бере *ICANN*, частка якої багато в чому залежить від результатів обговорень. Зважаючи на тісні взаємозв'язки між корпорацією *ICANN* та урядом США, можна з упевненістю констатувати активну участь уряду США в дискусіях.

[92] Див.: https://www.icann.org/news/blog/-b6714092-9ee6-40a0-b3bb-340e28151740

ну, право на яку цій структурі делегували громадяни США (приватні особи), визнані американською структурою *ICANN* адміністраторами домену «*.UA*» без будь-якого погодження з державними структурами України. Відповідний сервер системи доменних імен розташований у США.

При цьому будь-які спроби держави[93] (державних органів) долучитися до процесу (що виглядає логічним з огляду на важливість повноцінного функціонування домену для всієї держави) наражаються на незадоволення корпоративних структур, які зазвичай розв'язують в інтернет-виданнях справжню кампанію з дезавуації заяв офіційно уповноважених осіб[94]. При цьому представники громадянського суспільства небезпідставно звинувачують державні структури, уповноважені приймати рішення щодо міжнародних зобов'язань України у сфері телекомунікацій, у непрозорості й закритості, через що зацікавлені структури громадського сектору чи бізнесу часто не в змозі з'ясувати офіційну позицію держави та зрозуміти логіку прийняття тих чи інших рішень.

Невизначена позиція України щодо стратегії розвитку кіберпростору, а отже, відсутність можливості поступового обстоювання національних інтересів, зокрема щодо демілітаризації кіберпростору та контролю над інтернетом, є частиною загальної проблеми неунормованості визначення зовнішньополітичних інтересів України в інформаційній сфері.

Один із основних законів України при формуванні основ зовнішньої політики «Про засади внутрішньої та зовнішньої політики» від 1 липня 2010 року № 2411-VI [167] мінімально звертає увагу на інформаційну проблематику загалом, а поняття з частиною *кібер* у цьому документі взагалі не зустрічаються. Крім того, апелюючи до інформаційної тематики, Закон звертається переважно до внутрішньополітичних аспектів. Так, абзац перший пункт 1 статті 6 вказує на необхідність «забезпечення життєво важливих інтересів людини і громадянина, суспільства і держави, своєчасне виявлення, запобігання і нейтралізації реальних та потенційних загроз національним інтересам у зовнішньополітичній, оборонній, соціально-економічній,

[93] Однією зі спроб є переделегування повноважень ТОВ «Хостмайстера» приватно-державній структурі – «Українському мережевому інформаційному центру» (УМІЦ).

[94] Один із поглядів на цю проблему можна прочитати на сайті Українського мережевого інформаційного центру [202].

енергетичній, продовольчій, екологічній та інформаційній сферах» саме як на засади внутрішньої політики у сфері національної безпеки і оборони. Також до внутрішніх пріоритетів віднесено «забезпечення свободи засобів масової інформації та безперешкодного доступу громадян до інформації, створення умов для розвитку інформаційних технологій та інформаційного суспільства, широкої інтеграції і доступу громадян до світового інформаційного простору» (абзац 13, пункт 1 ст. 10) та «створення суспільного мовлення та надання державної підтримки національному інформаційному продукту, здійснення заходів щодо захисту національного інформаційного простору» (абзац 14, пункт 1 ст. 10).

До «основних засад зовнішньої політики» віднесена лише «підтримка інтеграції України у світовий інформаційний простір» (абзац 16, пункт 2 ст. 11). При цьому абзац 2 цього ж пункту цієї самої статті звертає увагу на необхідність «забезпечення дипломатичними та іншими засобами і методами, передбаченими міжнародним правом, захисту суверенітету, територіальної цілісності та непорушності державних кордонів України, її політичних, економічних, енергетичних та інших інтересів». На жаль, документ не розтлумачує, які саме «інтереси» віднесено до «інших», тоді як цілком доречно було б додати вказівку на необхідність забезпечення інформаційного та цифрового суверенітету держави, її інтересів у глобальному кіберпросторі.

Частково проблему розв'язує Доктрина інформаційної безпеки України[95]. Проте зазначені аспекти прописані в ній фрагментарно, без вказівки на реальні механізми їх реалізації. На нашу думку, навіть запропоновані Доктриною заходи забезпечення інформаційної безпеки України в зовнішньополітичній сфері є еклектичними й лише частково дійсно описують частину проблеми, яка стосується кібербезпеки держави.

З огляду на те, що кіберпроблематика (як, власне, й ціла низка інших новітніх загроз) украй побіжно згадується в концептуальних

[95] На момент написання монографії Доктрина інформаційної безпеки України була чинним документом. Водночас у Рішенні Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» було зазначено необхідність у тримісячний строк розробити нову її редакцію, а 6 червня 2014 року Доктрина втратила чинність (підстава – Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України» від 06 червня 2014 р. № 504/2014).

зовнішньополітичних безпекових документах України, доречним є прийняття розширеної та конкретизованої Концепції зовнішньої політики України. Її основною метою є деталізація та чітке артикулювання інтересів Української держави у сфері міжнародних відносин щодо розбудови глобального кіберпростору.

Зауважимо, що дедалі поширенішою є практика визначення й формалізації зовнішньополітичних пріоритетів через особливу акцентуацію в документах, що визначають пріоритети державної зовнішньої політики щодо глобального кіберпростору чи міжнародної інформаційної безпеки. Так, США в 2011 році оприлюднили Міжнародну стратегію для кіберпростору, Російська Федерація в серпні 2013 року – Основи державної політики РФ у сфері міжнародної інформаційної безпеки на період до 2020 року». Документ РФ є основою стратегічного планування діяльності РФ на відділену перспективу та «виділяє основні загрози у сфері міжнародної інформаційної безпеки, мету, завдання та пріоритетні напрями державної політики Російської Федерації у сфері міжнародної інформаційної безпеки, а також механізми їх реалізації» [149].

Україна з очевидністю також потребує подібного стратегічного документа, спроможного надати чіткі відповіді на запитання щодо її уявлень про «новий цифровий порядок» і кроків, до яких вона готова вдатися заради його становлення/протидії становленню.

Напрацювання подібних документів не є справою авторської творчості обдарованих аналітиків. Воно потребує формування консолідованого бачення майбутнього кіберпростору як на рівні політичного керівництва держави, так і людей, які на практичному рівні відповідають за здійснення зовнішньополітичної діяльності, передусім представників системи дипломатичної служби України.

Станом на жовтень 2013 року у структурі МЗС України був відсутній профільний департамент, який опікувався б проблемами кібербезпеки й державної політики у цій сфері. Частково відповідні функції покладено на Департамент міжнародної безпеки та роззброєння, який навіть проводить окремі публічні заходи (зокрема конференції) з цього приводу. Традиційна для інших держав практика визначення спеціального уповноваженого або заступника міністра закордонних справ з питань інформаційної (кібер) безпеки[96] досі не адаптована

[96] Наприклад, посаду Уповноваженого з питань кібербезпеки було запроваджено в МЗС Німеччини ще у 2013 році. Завданням Уповноваженого є обстоювання інтересів держави у сфері електронних комунікацій [23].

Україною. Аналогічно посад уповноважених з питань інформаційної (кібер) безпеки немає і в інших ключових українських органах державної влади включно з Кабінетом Міністрів України та Адміністрацією Президента України.

Таким чином, у сфері забезпечення зовнішніх національних інтересів України в кіберпросторі актуальним є вирішення таких завдань.

1. Покладання на одного із заступників очільника українського зовнішньополітичного відомства обов'язків з обстоювання інтересів держави у сфері електронних комунікацій (кіберпросторі);

2. Більш чітка артикуляція завдань, покладених на профільний департамент МЗС з питань кібербезпеки, з метою створення можливості для більш широкої участі в цій діяльності представників корпоративних і бізнесових *IT*-структур, *IT*-громадськості, збору експертних оцінок тощо.

3. Активізація діяльності українських дипломатичних репрезентантів, представлених в основних безпекових структурах (зокрема ООН, ОБСЄ, НАТО), щодо участі в робочих та експертних групах, діяльність яких спрямована на вирішення безпекових проблем глобального кіберпростору, їх періодична звітність перед представниками корпоративних і бізнесових *IT*-структур, *IT*-громадськості, експертного співтовариства.

4. Розроблення цілісного документа з питань зовнішньополітичної стратегії, який чітко артикулює сутність національних інтересів України у сфері подальшого розвитку глобального кіберпростору, формулює образ «бажаного майбутнього», пріоритети діяльності та чіткі механізми реалізації цих інтересів. Зазначений документ може бути прийнятий як деталізація окремих положень Стратегії національної безпеки України та Закону України «Про основи внутрішньої та зовнішньої політики».

4.3. Національні механізми протидії кіберзагрозам: стан і проблеми нормативно-стратегічного та організаційного забезпечення

Упродовж 2011–2013 років тематика кібербезпеки дедалі активніше артикулюється в Україні на найвищому рівні, хоча до реальних заходів стратегічного характеру Україна у цій сфері поки що не вдавалася. Загалом механізми, які були задіяні (найчастіше під тиском зовнішніх ініціатив і зобов'язань), були фрагментованими та несистемними.

Розв'язанню проблеми відсутності реальних кроків України в кіберпросторі жодним чином не сприяє недосконале чинне законодавство, яке досі виходить з парадигми штучного розширення предмета інформаційної безпеки на максимальну кількість сфер. Це, по-перше, розмиває сам предмет інформаційної безпеки, а по-друге, обумовлює відсутність частини *кібер* у вітчизняних нормативно-правових документах. Натомість використовується в суто пострадянському дискурсі поняття *інформаційна безпека* та низка інших, тісно з ним пов'язаних: *інформаційний суверенітет*; *інформаційна інфраструктура*» [66]; *інформаційні впливи* тощо. На виправдання зазначеного підходу зазвичай наводиться той аргумент, що терміни з частиною *кібер* акцентують виключно на формальній стороні інформаційних процесів, ігноруючи сторону змістову.

При цьому поняття інформаційної безпеки досить активно використовується в нормативно-правових документах усіх рівнів. Відповідно до ст. 17 Конституції України «захист суверенітету і територіальної цілісності України, забезпечення її економічної й інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Ст. 7 Закону України «Про основи національної безпеки» відносить до загроз національним інтересам і національній безпеці України в інформаційній сфері:

• вияви обмеження свободи слова та доступу громадян до інформації;

• поширення засобами масової інформації культу насильства, жорстокості, порнографії;

• комп'ютерну злочинність і комп'ютерний тероризм;

• розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави;

• намагання маніпулювати суспільною свідомістю, зокрема у спосіб поширення недостовірної, неповної або упередженої інформації.

Закон також згадує про необхідність забезпечення інформаційного суверенітету України, розвитку національної інформаційної інфраструктури та ресурсів, упровадження новітніх технологій у цій сфері, вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо. На нашу думку, вже на рівні цього, ключового

для забезпечення національних інтересів, документа можна побачити дуже широкий діапазон заходів, які на сьогодні відносять до політики національної безпеки в інформаційній сфері: від створення та підтримання позитивного іміджу держави та забезпечення інформаційних прав громадян до боротьби з корупцією.

Важко однозначно заперечувати слушність і цінність зазначеного підходу, але, на нашу думку, він не охоплює тих заходів, які в західній науковій та юридичній практиці стосуються саме проблем кібербезпеки. Передусім ідеться про протидію комп'ютерній злочинності й комп'ютерному тероризму. До речі, жодне з цих понять не отримало належного визначення в національному законодавстві, а тому незрозуміло, з чим, власне, пропонується «боротися».

Аналогічний підхід зберігається і в Доктрині інформаційної безпеки України. Доктрина зазначає, що основною метою реалізації її положень є створення в Україні розвиненого національного інформаційного простору та захист її інформаційного суверенітету. Перелік загроз інформаційній безпеці України, що їх визначає документ, є дуже широким: від недостатньої розвиненості інститутів громадянського суспільства та недосконалості партійно-політичної системи до відставання українського кінематографа, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвитку відповідних сфер у розвинутих державах. Таким чином, згідно з Доктриною інформаційна безпека стає всеосяжною «темою», яка може бути віднайдена в будь-якій сфері людського буття.

Подібна еклектичність розуміння поняття *інформаційної безпеки* притаманна не лише Україні, а й більшості країн пострадянського простору.

У вітчизняному нормативно-правовому полі визначення поняття *інформаційна безпека* зафіксоване в не зовсім профільному для безпекової сфери Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Закон фіксує інформаційну безпеку як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (ст. 13, розділ III).

На нашу думку, це визначення невиправдано розмиває предметне поле інформаційної безпеки та потребує суттєвого уточнення в май-

бутньому. Це нове розуміння має бути узгоджене з європейським (власне, традиційним для світової спільноти) підходом до інформаційної безпеки, що зафіксовано в редакції Стратегії національної безпеки від 2012 року. Ключовими завданнями держави у сфері забезпечення інформаційної безпеки Стратегія визначає:

• стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

• забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

• розроблення і впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність;

• створення національної системи кібербезпеки.

Стратегія зазначає, що поширення кіберзлочинності є чинником, що загрожує глобальній міжнародній стабільності й негативно позначається на безпековому середовищі України. Увага акцентується й на тому, що на тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, що характеризується, зокрема, нездатністю України протистояти новітнім викликам національній безпеці (явищам і тенденціям, що можуть за певних умов перетворитися на загрози національним інтересам), пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам.

На сьогодні зберігається дуже розгалужена (при цьому сталою є тенденцію до зростання кількості суб'єктів) система залучення державних інституцій у забезпеченні кібернетичної безпеки України[97].

1. Президент України.

2. Рада національної безпеки і оборони України.

3. Кабінет Міністрів України.

---

[97] Перелік і повноваження наводяться за доповіддю Начальника управління Служби безпеки України В. Хлевицького під час міжнародних експертних консультацій «Україна – НАТО» з питань кібернетичного захисту (м. Ялта, 2011 рік).

4. Служба безпеки України (захист законних інтересів держави та прав громадян в інформаційній сфері від протиправних посягань організацій, груп та осіб на інформаційну безпеку держави, інших протиправних дій у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку, які безпосередньо становлять загрозу життєво важливим інтересам України; виявлення, попередження та припинення протиправних зазіхань на державні електронні інформаційні ресурси; виявлення, попередження та припинення проявів комп'ютерної злочинності й комп'ютерного тероризму, які здійснюються вітчизняними і транснаціональними злочинними угрупуваннями хакерів).

5. Міністерство внутрішніх справ України (дізнання й досудове слідство у справах про комп'ютерні злочини; забезпечення особистої безпеки громадян, захист від протиправних посягань).

6. Державна служба спеціального зв'язку та захисту інформації (формування вимог до захисту інформації в інформаційно-телекомунікаційних системах; проведення державних експертиз комплексних систем захисту; експлуатація загальнодержавних спеціальних інформаційно-телекомунікаційних систем; контроль за виконанням вимог із захисту інформації; визначення напрямів розвитку сфери телекомунікацій та інформатизації; встановлення стандартів і норм телекомунікацій; сертифікація обладнання телекомунікацій).

7. Міністерство оборони України (захист інформаційної інфраструктури держави у сфері оборони).

8. Національна комісія, що займається регулюванням зв'язку та інформатизації (ліцензування господарської діяльності у сфері телекомунікацій; оформлення дозволів на використання радіочастотного ресурсу; контроль за виконанням норм у сфері телекомунікацій).

9. Національний банк України (формування вимог до захисту інформації в інформаційно-телекомунікаційних системах банківських установ).

10. Державне агентство з питань науки, інновацій та інформатизації (визначення вимог до формування та використання національних електронних інформаційних ресурсів).

11. Науково-дослідні установи, позаурядові структури, оператори і провайдери телекомунікацій.

Крім цього, в Україні діє спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації

України – *CERT-UA* (*Computer Emergency Response Team of Ukraine* – команда реагування на комп'ютерні надзвичайні події України). Ця команда є частиною *CERT* (*Computer Emergency Response Team*) та акредитованим членом *FIRST* (*Forum for Incident Response and Security Teams* – Форум команд реагування на інциденти інформаційної безпеки). Одним з основних завдань *CERT-UA* є координування діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ та організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Водночас, незважаючи на значну кількість відомств, задіяних у забезпеченні кібербезпеки держави, основні функції належать обмеженому колу виконавців: Службі безпеки України, Міністерству внутрішніх справ України, Державній службі спеціального зв'язку та захисту інформації, Міністерству оборони України.

Традиційно у структурі **Служби безпеки України** інтереси держави у сфері інформаційної безпеки було покладено на Департамент контррозвідувальної діяльності. Однак Указом Президента України від 25 січня 2012 року № 34/2012 створено спеціальний Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Його основними завданнями є «сприяння концентрації сил і засобів, вирішенні завдань із захисту законних інтересів держави і прав громадян в інформаційній сфері від розвідувально-підривної діяльності іноземних спецслужб, протиправних посягань організацій, груп та осіб» [164]. Крім того, до функцій Департаменту також належить «захист урядових телекомунікаційних систем, державних інформаційних ресурсів, критичних об'єктів інформаційної інфраструктури держави; боротьба з кібертерроризмом; боротьба з кіберзлочинністю, що становить загрозу життєво важливим інтересам держави; контроль за обігом спеціальних технічних засобів негласного одержання інформації»[98].

Увагу СБУ до проблематики кібербезпеки засвідчують ті факти, що Службу в цій рольовій функції часто згадують у виступах її очіль-

[98] Наводиться за доповіддю Начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України В. Біка під час міжнародних експертних консультацій «Україна – НАТО» з питань кібернетичного захисту (м. Ялта, 2013 рік).

ників, а проблематика кібербезпеки дедалі частіше висвітлюється її керівниками. Так, в одному з інтерв'ю екс-голова Служби безпеки України І. Калінін, зазначив, що «статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів» [188].

Крім того, СБУ здійснює доволі широку міжнародну співпрацю в цій сфері. Так, у жовтні 2010 року спільно з ФБР і спецслужбами 9 інших країн світу було проведено операцію *Trident breach* з нейтралізації злочинного хакерського міжнародного угруповання, що несанкціоновано втручалося з території України в роботу закордонних банківських установ, яким у результаті було завдано збитків на суму близько 170 млн дол. США. Цю спільну операцію відзначено у щорічному звіті за результатами діяльності ФБР у 2010 році. У червні 2011 року Служба безпеки України спільно з правоохоронними органами США, Великобританії, Нідерландів, Франції, Німеччини, Кіпру, Литви та інших (загалом 10 країн) припинила незаконну діяльність міжнародного злочинного хакерського угруповання під прикриттям комерційної структури, що діяла легально та координувалася громадянами України. За попередніми оцінками, в результаті злочинної діяльності вказаного угруповання збитки перевищили 72 млн дол. США. У серпні 2011 року Служба безпеки України в межах спільної операції зі спецслужбами США припинила незаконну діяльність українського осередку міжнародного злочинного хакерського угруповання, члени якого викрали із закордонних банківських установ, підроблюючи кредитні картки, понад 20 млн дол. США. У 2013 році СБУ спільно з ФСБ РФ провело операцію із затримання розробників троянської програми *Carberp*, що завдала збитків на суму 250 млн дол. США [27].

Крім того, СБУ також ініціювала розвиток контактів у сфері протидії комп'ютерної злочинності із Францією, Білоруссю, Італією, Ізраїлем, Швецією, Румунією, Молдовою, Угорщиною, Єгиптом, Японією, Алжиром та Спеціальним комітетом НАТО. На регулярній основі відбуваються експертні консультації експертів Україна – НАТО з питань кіберзахисту.

Важливу частину роботи з убезпечення громадян від найбільш поширених кіберзлочинів здійснює **МВС,** у структурі якого створено спеціальне Управління боротьби з кіберзлочинністю, на яке покладено низку завдань, поміж яких участь у формуванні та забезпеченні реалізації державної політики щодо попередження і протидії кримінальним

правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням (*далі* – сфера боротьби з кіберзлочинністю). У тому числі: кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (*далі* – протиправного контенту); економіки, яка включає в себе фінансові й торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері (*далі* – електронної комерції); надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище кримінальних правопорушень) [205].

Поміж профільних завдань **Державної служби спеціального зв'язку та захисту інформації** є такі:

• забезпечення формування та реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем криптографічного й технічного захисту інформації, використання та захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; участь у формуванні й реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні й упровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

• забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку та Національної системи конфіденційного зв'язку;

• здійснення державного контролю за станом криптографічного й технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена

законом, протидії технічним розвідкам, а також за додержанням технічних вимог керівних документів у сфері надання послуг електронного цифрового підпису;

• розроблення та здійснення заходів щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності й сталого функціонування [148].

У структурі **Міністерства оборони України** принаймні два основних управління відповідають за питання кібербезпеки держави. Зокрема, цю функцію виконує Управління інформаційних технологій, підпорядковане заступникові міністра оборони України – керівнику апарату.

У структурі Генерального штабу Збройних сил України функціонує Головне управління зв'язку та інформаційних систем, на яке, крім іншого, покладено такі обов'язки:

• організація зв'язку й автоматизованого управління військами у Збройних силах України та здійснення оперативного управління телекомунікаційними мережами України в інтересах оборони держави;

• підготовка системи зв'язку та автоматизації управління військами Збройних сил України й контроль за підготовкою телекомунікаційних мереж України в інтересах оборони держави;

• участь у реалізації державної політики у сфері захисту інформації та протидії кіберзагрозам в інформаційно-телекомунікаційних системах Збройних сил України;

• участь у військовому співробітництві з питань, пов'язаних із розвитком системи та засобів зв'язку Збройних сил України, захисту інформації та протидії кіберзагрозам [44].

Крім того, на Головне управління розвідки у структурі Міністерства оборони України покладено завдання вжиття спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, воєнній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного й науково-технічного розвитку, захисту та охорони державного кордону [133].

Водночас кібербезпекова тематика лише побіжно згадується у стратегічних документах воєнного сектору. Наприклад, у Воєнній доктрині України йдеться про кібернетичний складник або в контексті поширення тероризму (зокрема кібертероризму), або як про елемент переліку дій, які Україна вважає необхідними умовами для виникнення воєнного конфлікту та застосування воєнної сили –

«проведення акцій, що порушують безпеку функціонування об'єктів ядерної, хімічної промисловості, оборонно-промислового комплексу, об'єктів, на яких зберігаються озброєння, військова техніка, боєприпаси, інших потенційно небезпечних об'єктів, у тому числі кібернетичних атак на зазначені об'єкти» [165]. Аналогічно незначна увага приділяється питанням кібербезпеки у Стратегічному оборонному бюлетені України. Документ визначає кібернетичні загрози як один із прогнозованих викликів національній безпеці України на довгостроковий період і підкреслює необхідність «забезпечення високого ступеня захисту та живучості систем управління, військ (сил) і важливих об'єктів від ударів різноманітних засобів ураження, насамперед високоточної зброї, від диверсій, радіоелектронних перешкод, інформаційного впливу, у тому числі кібернетичних атак» [194].

Розв'язати проблеми стратегічного значення кібербезпекової сфери неможливо без однозначного розуміння стану, в якому перебуває умовний «вітчизняний кібербезпековий сектор». Принциповий огляд має більш-менш однозначно й директивно вказати на системні проблеми та можливі способи їх розв'язання, на моменти дублювання функцій відомствами, причетними до інформаційної (кібер) безпеки або на функції, непритаманні певним відомствам, а також на елементи кібербезпекової сфери, які залишилися поза увагою цього сектору безпеки.

Оскільки питання кібербезпеки є для України відносно новими та зачіпають інтереси не лише державних інститутів, а й приватного сектору, громадянського суспільства та кожної особи зокрема, доцільно використати відповідну європейську кібербезпекову практику, яка передбачає:

• створення Зеленої книги, метою якої є формулювання порядку денного;

• винесення питання визначеного порядку денного на широке обговорення та привернення уваги широких верств громадян;

• створення Білої книги, покликаної надати відповіді на ключові проблемні питання, визначити способи їх розв'язання [70].

Зауважимо, проте, що для вітчизняної політичної практики подібні механізми вироблення політики з певного питання є доволі новими, а набутий у цій сфері досвід не завжди був успішним. Українські державні структури мають досвід написання «білих книг» (особливо з питань реформування державних органів), однак їх реальний вплив на зміни у відповідних сферах був мінімальним. Це можна по-

яснити не останньою чергою відсутністю усталеної практики наступності політики, якою в Україні нехтується на всіх рівнях державно-управлінського процесу від початку створення Української держави.

Своєрідним наслідком відсутності цілісного обговорення кібербезпекових питань у якомога ширшому колі є відсутність в Україні системних нормативних документів, що описували б загрози Україні в кіберпросторі, визнавали їх існування й формували цілісну державну політику кібербезпеки.

Стратегія національної безпеки України (від 12 лютого 2007 року) зазначає, що Україна має «розробляти та впроваджувати національні стандарти й технічні регламенти застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». Однак, по-перше, сама Конвенція про кіберзлочинність (ратифікована парламентом України ще 2005 року), хоча і стосується проблеми убезпечення кіберпростору, проте зосереджена переважно на протидії кримінальним діям (шахрайство, підроблення, поширення дитячої порнографії, порушення авторських прав тощо) з використанням комп'ютерної техніки й різноманітних мереж. А по-друге, у самій Конвенції відсутнє визначення поняття *кіберзлочинність*. До того ж кримінальне переслідування кіберзлочинців передбачає Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. Саме цей розділ (ст.ст. 361–363) традиційно розуміється в Україні як «кібербезпековий».

І хоча нова редакція Стратегії національної безпеки (2012 року) в певному обсязі звертає увагу на кібербезпекову проблематику, цілісна термінологічна система, спроможна сформувати єдиний понятійно-категоріальний апарат у сфері кібербезпеки, в Україні досі відсутня. Це призводить до того, що навіть спеціальні підрозділи силових відомств, у назві яких присутні слова *кіберзлочинність*, *кібербезпека*, не вповні забезпечені відповідними нормативними документами для визначення предмета своєї роботи. Відповідні визначення відсутні навіть на рівні окремих відомств (щонайліпше вони узгоджені на рівні окремих підрозділів, однак внутрішньовідомчими документами не закріплені).

Певною мірою термінологічні проблеми кібербезпекової сфери пов'язані з особливостями створення та ухвалення нормативних до-

кументів різного рівня (у тому числі законів та указів і розпоряджень Президента України). Хоча слід визнати, що у 2011–2013 рр. розпочалися процеси унормування даної проблематики та пошуку способів вирішення відповідних питань через створення відповідних нормативних документів.

Пріоритетним у полі створення цілісного законодавства з кібербезпеки є прийняття Стратегії забезпечення кібернетичної безпеки України, зобов'язання щодо розроблення якої Україна взяла на себе перед закордонними партнерами. Цей документ має визначити основні поняття у сфері, загрози, принципи та напрями забезпечення кібербезпеки й, зокрема, заходи щодо вдосконалення державного управління та нормативно-правового поля у сфері кіберзахисту. Це саме той шлях, яким активно просуваються провідні країни світу, передусім країни – члени НАТО.

Зазначимо, що певні напрацювання стосовно розроблення Стратегії забезпечення кібернетичної безпеки України вже існують. Зокрема, один із проектів був підготовлений у 2012 році фахівцями Національного інституту стратегічних досліджень.

Крім проблем суто нормативно-правового напряму, доводиться констатувати брак міжвідомчого координування з питань забезпечення кібербезпеки держави. Наразі в Україні відсутні загальнонаціональні міжвідомчі координаційні структури, спроможні узгоджувати й координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створення ефективної системи захисту вітчизняного кіберпростору (в тому числі у військовій сфері).

На нашу думку, зважаючи на кількість залучених до цієї сфери суб'єктів, зазначена проблема постає не просто як «одна з», а швидше, як центральна.

Координування з питань забезпечення кібербезпеки держави має відбуватися на двох рівнях – стратегічному та оперативному. Стратегічне координування вочевидь є зоною відповідальності Ради національної безпеки і оборони, оперативне – спеціально уповноваженої структури (можливо, новоствореної спеціально для цих цілей). Невиконання цієї вимоги матиме результатом небажання окремих структур сектору безпеки співпрацювати з іншими уповноваженими відомствами через законодавчу (нормативну) невизначеність прав та обов'язків цих структур чи невідповідність певних нормативних документів вимогам часу. Ця ситуація вже має місце, а в тих випадках, коли така співпраця існує, найчастіше вона здійснюється на рівні

міжособистісних зв'язків керівників відповідних підрозділів. З погляду довгострокової перспективи така ситуація є прямою загрозою кібербезпеці держави.

У період 2010–2012 рр. певні спроби здійснення координування здійснювалися на базі Апарату РНБО України. Щоправда, це відбувалося в межах діяльності Робочої підгрупи Спільної робочої групи Україна – НАТО високого рівня з питань кібернетичного захисту, створеної як підгрупа Спільної робочої групи з питань військової реформи. Робоча підгрупа поєднала зусилля основних відомств, задіяних у сфері кібербезпеки держави (принаймні на рівні інституцій, що формують політику в цій сфері). Проте, на нашу думку, подібні «напівршення» не є дійсно системними та довгостроковими, що й продемонструвало подальше припинення діяльності Робочої підгрупи. Певні надії покладалися на відновлення повноцінної роботи Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України. Однак ця структура до останнього часу, незважаючи на певні ініціативи в цьому напрямі, так і не запрацювала й не стала ефективно діючим майданчиком для обговорення зазначених проблем. Частково ці питання можуть потрапити в поле зору створеного при Апараті РНБО України Оперативно-аналітичного центру, однак кібербезпекові питання безпосередньо не віднесено до його основних завдань.

Кібербезпека – це передусім людський ресурс. Проте, на думку більшості представників відомств, задіяних у системі забезпечення кібербезпеки України, кадрове забезпечення відомств відповідними фахівцями у сфері кібернетичної безпеки є незадовільним. Незважаючи на те, що низка вищих військових, цивільних і відомчих навчальних закладів здійснюють підготовку фахівців за різноманітними спеціальностями, які можна віднести до сфери інформаційної безпеки, якість їх підготовки не відповідає вимогам. Крім того, рівень матеріальних і нематеріальних стимулів унеможливлює залучення висококласних фахівців (молодих спеціалістів) до силових структур, задіяних у забезпеченні безпеки вітчизняного кіберпростору.

В Україні жодного разу не проводилися комплексні навчання з проблеми кібербезпеки (на кшталт навчань «Кіберштурм», що проводяться у США, або аналогічних навчань, що проводяться ЄС) із залученням усіх відомств, які належать до системи забезпечення кібербезпеки держави.

Майже відсутні поліпрофільні науково-дослідні інститути, задіяні в *комплексних* дослідженнях інформаційної безпеки. Переважно дослідження з відповідної тематики стосуються проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки; про соціально-гуманітарний компонент, а надто поєднання технологічних та гуманітарних складників, не йдеться.

Ще одна проблема полягає в тому, що, незважаючи на зусилля спеціально уповноважених відомств, Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово уразливою до кіберзагроз і не останньою чергою через надмір широке транслювання іноземних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможливлюється через залежність Української держави від згаданих продуктів, що вийшла на дійсно загрозливий для національної безпеки рівень на всіх рівнях і в усіх сферах.

Досі актуальною є така критично важлива проблематика:

• створення національної операційної системи (принаймні для її використання в системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом існують суттєві зауваження з боку головних вітчизняних безпекових організацій);

• відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем);

• стимулювання з боку держави створення національного антивірусу тощо.

Фактично йдеться про створення повноцінного кібернетичного суверенітету держави, без якого країна буде змушена весь час перебувати у стані наздоганяючої трансформації безпекового сектору. Значна частина реалізації цього питання зосереджена у сфері ефективної геостратегії розбудови інформаційного суспільства та елементів кібермогутності держави.

Ще одне критично важливе питання, характерне не лише для України, а й для всього пострадянського простору, пов'язане із традиційно низьким рівнем взаємодії органів державної влади з приватним сектором, а також неурядовими організаціями та громадянським суспільством у цілому. Якщо подібна взаємодія налагоджена в межах інституційованих форм співробітництва у традиційних сферах держав-

ного управління, то у сфері кібербезпеки вони щойно з'являються. Водночас саме це питання є головним для повноцінного розвитку зазначеної сфери, зважаючи на те, що значна кількість інформаційної інфраструктури, в тому числі критичної, є в приватній власності. Навіть пересічні громадяни відіграють дедалі значущу роль у забезпеченні кібербезпеки держави.

Поліаспектна взаємодія у трикутнику «держава – бізнес – суспільство (НДО)» в жодній країні не відбувається без обмежень і компромісів, адже потребує визначення припустимих меж втручання держави в діяльність приватних структур і життя звичайних громадян. Однак логіка останніх подій (передусім масштабних кібератак, викривальних заяв Е. Сноудена тощо) вказує на те, що баланс поступово зміщується в бік широкої участі держави, однак за умов посилення її зобов'язань перед своїми громадянами та бізнес-структурами.

Необхідність залучення «другого сектору» до кібербезпекових питань розуміють навіть найбільш кіберпотужні держави, незалежно від того, яка модель розбудови інформаційного суспільства в них упроваджується та якою є їх політична система. Вони активно сприяють процесу залучення приватних організацій до загальнодержавних програм реагування на кіберзагрози. Найбільш показовим прикладом такого взаємопроникнення є згаданий комерційний проект *FIRST*, з яким активно співпрацюють державні структури в межах *CERT*.

Дедалі більшу роль у глобальних протистояннях у кіберпросторі, передусім у відстежуванні та подальшому аналізі кібератак, відіграють різноманітні приватні безпекові організації, які часто поєднують свою діяльність з виробництвом антивірусних продуктів. Поміж таких компаній *McAfee*, *Avast*, *Kaspersky Lab*, *ESET*, *F-Secure* та інші, які завдяки більшій свободі діяльності порівняно з державними є викривальниками масштабних кібероперацій включно із *Stuxnet, Flame* та *Red October*. В Україні організацій приватних кібербезпекових організацій подібного масштабу немає, а чи не єдиний антивірус національного виробництва (*Zillya!*) лише намагається потрапити на цей ринок в умовах активної протидії з боку незацікавлених у цьому іноземних структур. Відсутні в Україні й мінімально потужні *IT*-ТНК (хоча б на рівні російських *Mail.ru* чи *Yandex*), на які припадала б значна частина задоволення інформаційних потреб громадян, а отже, й можливостей ефективно впливати на їх безпеку.

Суттєвою проблемою взаємодії держави з приватним сектором є недовіра між бізнесом та урядом. Бізнесові структури не переконані,

що уряд не передасть дані (або створить умови для їх отримання) про кібератаки компаніям-конкурентам або третім особам або оприлюднить їх. Можливість не повідомляти урядові структури про кібератаки обумовлена латентним характером останніх. Відповідно, держава не вживає необхідних заходів.

Важливість цієї проблеми продемонстрували відповідні кроки уряду США. Фактично йшлося про примусові дії у спонуканні приватних компаній до сповіщення урядових безпекових структур про здійснені кібератаки. Масштаб наявних суперечностей засвідчила спроба створення спеціального центру, передбаченого законопроектом *Cybersecurity Act* 2012, де мала накопичуватися подібна інформація про кібератаки. Натомість в Україні під час розроблення проектів Закону України «Про кібернетичну безпеку» питання взаємовідносин між урядовими структурами сектору безпеки та приватним сектором були виписані мінімально, а подеколи взагалі ігнорувалися.

Так само невиписаними є можливості й перспективи взаємодії держави з НДО. Водночас останні також могли б впливати на посилення кібербезпеки держави, здійснюючи в цій сфері зовнішні незалежні дослідження. Це допомогло б урядовим структурам ухвалювати більш виважені рішення, ґрунтуючись на широкому спектрі експертних думок. Наприклад, у США згадуваний документ «Безпека кіберпростору для 44-го президента» [409] дійсно суттєво вплинув на політику Білого Дому й неодноразово згадувався в урядових матеріалах, присвячених кібербезпековій проблематиці. Розробник документа продемонстрував й іншу реальну можливість залучення НДО: за ініціативи та посередництва Інституту Бжезинського вже декілька років поспіль проводяться кібернавчання між військовими США та КНР.

На жаль, в Україні сфера державно-приватного партнерства є найбільш нереалізованою, і тут спостерігаються певні національні особливості, пов'язані з тим, що в Україні майже відсутні дійсно фахові НДО безпекового спрямування. Наявні організації натомість мають надто широку сферу діяльності, що унеможливлює налагодження з ними конструктивних відносин щодо проблем кібербезпеки. В окремих випадках ідеться про вкрай низький рівень аналітичних матеріалів, підготовлених профільними НДО, які до того ж не напрацювали дійсно ефективних механізмів донесення своїх розробок і пропозицій до посадових осіб. Не останньою проблемою є й надто тісна залежність більшості вітчизняних НДО від іноземних (переважно американських) джерел фінансування.

Таким чином, для України актуальною є ціла низка проблемних питань, розв'язання яких потребуватиме часу та певних зусиль як з боку держави, так і бізнесу/НДО.

4.4. Стан і напрями вдосконалення нормативно-правової бази щодо розбудови Національної системи кібернетичної безпеки

Чинна нормативно-правова база не охоплює всі основні елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Однією з важливих проблем у цій сфері є вже неодноразово вказана термінологічна невизначеність.

Ціла низка законів України та інших нормативних документів різних рівнів загалом охоплює проблеми забезпечення кібербезпеки держави:

• Закон України «Про основи національної безпеки України»;

• Закон України «Про інформацію»;

• Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

• Закон України «Про державну таємницю»;

• Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та інші.

Крім того, в межах даної проблематики чинними є два стратегічних документи:

• Стратегія національної безпеки України;

• Доктрина інформаційної безпеки України.

Важливе нормативно-стратегічне значення має також ратифікована Верховною Радою України Конвенція про кіберзлочинність.

Водночас спостерігається надто довільне використання значної кількості кібербезпекових понять (та їх синонімів), часто неузгоджених між собою.

Так, у Законі України «Про основи національної безпеки України» згадуються *комп'ютерна злочинність* і *комп'ютерний тероризм*, причому жоден із цих термінів не отримав визначення ані в цьому, ані в інших нормативних документах.

У Законі України «Про боротьбу з тероризмом» поняття *комп'ютерний тероризм* не згадується зовсім, а причетні до нього елементи прописані виключно як складники *технологічного тероризму*.

У Доктрині інформаційної безпеки України також згадуються *комп'ютерна злочинність* та *комп'ютерний тероризм*, але без жодних

пояснень чи посилань (відсилань) до таких пояснень. У Доктрині згадуються також *кібератаки*, але без спроб визначення даного поняття.

Неунормованість понятійно-категоріальної бази, відсутність правового визначення зон відповідальності відомств, залучених до сфери забезпечення кібербезпеки, слабке координування їх діяльності щодо реагування та попередження кіберзлочинів, брак правового закріплення взаємовідносин урядових безпекових структур із бізнесом і «третім сектором» на тлі зростання кількості й масштабності (зокрема за наслідками) кіберзагроз вимагає створення комплексного нормативно-правового документа, що забезпечуватиме безпеку в кіберсфері.

Наприкінці 2010 року (Указ Президента України від 10 грудня 2010 року № 1119/2010) набуло чинності Рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році». Відповідно до цього Рішення поставлене завдання розробити за участю та подати у двомісячний строк на розгляд Ради національної безпеки і оборони України пропозиції щодо створення єдиної загальнодержавної системи протидії кіберзлочинності» та «розробити за участю та затвердити перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак.

На виконання цих завдань мав бути розроблений **Закон України «Про кібернетичну безпеку України»**, покликаний:

- зафіксувати основні терміни у сфері кібербезпеки;
- визначити поняття *об'єкт критичної інфраструктури* та *механізм захисту об'єктів критичної інфраструктури;*
- визначити принцип побудови Єдиної загальнодержавної системи протидії кібернетичним загрозам та її складових елементів;
- вирішити проблеми міжвідомчого координування та повноваження суб'єктів забезпечення кібернетичної безпеки держави.

Підтвердження зобов'язань України з розроблення Закону відображено в Річній національній програмі співробітництва Україна – НАТО на 2012 рік, у якій проблематиці кібербезпеки відведено окремий параграф [168].

Однак станом на кінець 2014 року погоджений зацікавленими відомствами варіант так і не було створено. Хоча протягом 2010–2014 рр. зроблено принаймні чотири спроби створення документа,

жодна з яких не закінчилася заключним обговоренням. Причинами такої ситуації можна назвати принаймні три.

1. Правильне в цілому базове «відсилання» до необхідності впорядкувати кібербезпекову проблематику мало наслідком намагання негайного прийняття відповідного закону України, який мав би вирішити мало не всі проблеми кібербезпекової сфери. Перепоною задоволення вимоги терміновості прийняття закону та його практичної реалізації стали різноманітні проблеми, поміж яких не останнє місце посідають питання міжвідомчої неузгодженості. А запланована універсальність Закону зіштовхнулася з дещо іншими уявленнями про кібербезпеку з боку суб'єктів законодавчої ініціативи. Майже **в усіх редакціях насправді йдеться не про «кібербезпеку» як таку, а швидше, про «кіберзахист», причому в суто вузькому сегменті цього ключового поняття як захисту критичної інфраструктури**. Безумовно, ця проблема є дуже важливою, однак існує ще ціла низка супутніх проблем, пов'язаних, зокрема, з гуманітарними аспектами кібербезпеки. Їх ігнорують майже всі законопроекти та редакції законопроектів з кібербезпеки. Зокрема, лише подеколи «повноцінно» згадується проблема підготовки фахівців з кібербезпеки (при цьому на одне із «зацікавлених відомств» покладено повноваження Міносвіти).

2. Фактично **в жодному з проектів законів про кібербезпеку не розглядаються як повноцінні партнери держави громадянське суспільство та приватний сектор** (який реально є власником більшості потенційних об'єктів кіберзахисту). А якщо й згадуються, то не як повноцінні й рівноправні з державою суб'єкти, а лише як об'єкти державного управління. Подібний підхід повністю суперечить світовим тенденціям убезпечення кіберпростору і, власне, логіці реальної діяльності із забезпечення кібербезпеки держави.

3. Намагаючись створити нормативно-правовий документ із проблем кібербезпеки, кожен із суб'єктів (а це представники щонайменше чотирьох відомств) **виходив із власного корпоративно-відомчого розуміння загроз, небезпек, пріоритетів захисту й понятійно-категоріального апарату**. У результаті, незважаючи на те, що при підготовці кожного з цих документів та їх редакцій створювалися консультаційні групи й неформально залучалися експерти, забезпечити необхідну єдність поглядів (консенсус) щодо основних рис системи кібербезпеки як такої так і не вдалося.

Частково система державної кібербезпеки мала бути розроблена ще на той час, коли згаданим вище Указом Президента України

«Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 було поставлене завдання створити єдину загальнодержавну систему протидії кіберзлочинності. Однак на той час реалізація цього завдання так і залишилася на рівні робочих обговорень.

Наступним кроком стала запропонована Службою безпеки України у 2011 році модель організаційної структури й діяльності системи кібербезпеки, яка функціонально уподібнювалася до єдиної державної системи запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[99].

На наступному етапі, який тривав з 2011-го по 2013 рік, українські уповноважені структури створили принаймні кілька нормативно-правових документів у форматі проектів закону України. Робоча група на базі Державної служби спеціального зв'язку та захисту інформації запропонувала Концепцію Проекту закону України «Про кібернетичну безпеку України», яка заохочувала всі зацікавлені сторони до дискусії щодо власне предмету захисту. В базовому варіанті документа, підготовленого Державною службою спеціального зв'язку та захисту інформації України, зазначалася необхідність захищати критичну інфраструктуру.

Наприкінці 2011 – початку 2012 років з'явився документ, пов'язаний зі ще одним проектним баченням Закону України «Про кібернетичну безпеку України», запропонований Службою безпеки України. У Проекті зміст діяльності у сфері кібербезпеки значною мірою зводився до убезпечення національної критичної інфраструктури, яка визначалася через систему потенційних наслідків від впливу чинників загроз (у тому числі надзвичайна ситуація техногенного характеру, блокування роботи державних органів, розголошення державної таємниці, масові заворушення, що супроводжуються насильством тощо). Відповідно до запропонованої моделі перелік об'єктів національної критичної інфраструктури мав визначати Кабінет Міністрів України, а Реєстр систем об'єктів Національної критичної інфраструктури – створюватися й підтримуватися запропонованим Національним центром протидії кібернетичним загрозам при Службі безпеки України в порядку, визначеному Кабінетом Міністрів України.

---

[99] Положення про цю систему було затверджено Постановою Кабінету Міністрів України від 3 серпня 1998 р. № 1198, яка втратила чинність 31 січня 2014 року.

І хоча за такого підходу є певні принципові розходження з безпосереднім визначенням об'єктів «національної критичної інфраструктури», однак, на нашу думку, їх «динамічне» визначення через можливі згубні наслідки є перспективнішим і гнучкішим, аніж жорстке «статичне».

В альтернативному варіанті Проекту закону України «Про основи кібернетичної безпеки України», підготовленому в 2012 році фахівцями Апарату РНБО України, йшлося про широке коло питань кібербезпеки включно з питаннями протидії *кіберзлочинам*. Як і попередні варіанти законопроектів, цей документ був зосереджений на проблемах безпеки об'єктів критичної інфраструктури, майже не зачіпаючи інших питань (на кшталт порядку взаємодії держави з власниками цих об'єктів). Суттєвою вадою Законопроекту було й те, що він пропонує фактично потрійну схему визначення об'єкта критичної інфраструктури: *по-перше,* часткове визначення самого об'єкта; *по-друге*, через сукупність ознак таких об'єктів; *по-третє*, через критерії віднесення до об'єкта за можливими наслідками реалізації загроз. На нашу думку, це могло призвести до невиправданого розширення кількості об'єктів, що визначаються як критичні. Проте обидва законопроекти (СБУ й Апарату РНБО України) не було подано до Верховної Ради України.

Абстрагуючись від тематики міжвідомчих суперечностей, які виникли під час обговорення кожної редакції зазначених документів, варто зауважити на проблемах погодження цих документів в Апараті Верховної Ради України. Вони виникали переважно через низку розбіжностей у поглядах щодо термінології та способів вирішення нормативно-правових проблем кібербезпекової сфери.

Зокрема, один зі способів вирішення нормативно-правових проблем стосується ідеї внесення до ВРУ не цілковито нових законопроектів, а змін до чинної нормативно-правової бази. Саме у такий спосіб намагався дійти народний депутат А. Деркач, коли наприкінці серпня 2013 року зареєстрував у парламенті Законопроект «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». 12 грудня 2013 року ініціатор Законопроекту відкликав його.

Раціональним моментом Законопроекту була пропозиція розділення понять *об'єкт критичної інфраструктури* та *об'єкт критичної інформаційної інфраструктури*. Перше поняття включало самі об'єкти інфраструктури, вплив на які (зокрема через об'єкти критич-

ної інформаційної інфраструктури) може мати наслідки, що безпосередньо зачіпають національну безпеку. Друге – власне інформаційно-телекомунікаційні системи, які забезпечують роботу подібних критичних об'єктів.

До проміжних варіантів законотворчого вирішення кібербезпекової проблематики можна віднести Проект закону «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» (відкликаний 27 лютого 2014 року). Цей документ пройшов усі етапи міжвідомчого обговорення та був внесений на розгляд парламенту. Хоча формально цей документ було внесено Кабінетом Міністрів України, однак основним його «ідеологом» було МВС України.

Так само, як і «проект Деркача», проект КМУ пропонував внесення змін до чинного Закону України «Про основи національної безпеки України». Зокрема, як і в попередніх законопроектах, пропонувалося кілька принципових визначень для сфери кібербезпеки: власне *кіберпростір* та *кібербезпека*, а проблема критичної інфраструктури вирішувалася через необхідність забезпечення «належного рівня надійності і захищеності національної інформаційної інфраструктури в умовах надзвичайних ситуацій».

Таке обережне оперування поняттям *національна інформаційна інфраструктура* в кібербезпековому законодавстві слід визнати зваженим і доцільним, оскільки воно дозволяє вирішити проблему неспіввіднесеності питань захисту критичної інфраструктури та її убезпечення від кібератак.

Перевагою використання поняття *національна інформаційна інфраструктура* є його чітка визначеність у чинному законодавстві. Зокрема, таке визначення пропонує Закон України «Про Концепцію Національної програми інформатизації»: «Обчислювальна та комунікаційна техніка, телекомунікаційні мережі, бази і банки даних та знань, інформаційні технології (*IT*), система інформаційно-аналітичних центрів різного рівня, виробництво технічних засобів інформатизації, системи науково-дослідних установ та підготовки висококваліфікованих фахівців.» [169].

Ще одна спроба прийняття профільного кібербезпекового законодавства пов'язана з внесенням на розгляд Верховної Ради України Проекту закону України «Про кібернетичну безпеку України» [170] за авторством народних депутатів В. Олійника, Ю. Самойленка та О. Кузьмука (зареєстрований 6 червня 2013 року, 19 грудня 2013 року

відкликаний). Законопроект містив чимало нових для українського законодавства термінів і положень, що викликали жорстку дискусію майже за всіма пунктами документа починаючи від визначення основних загроз кібернетичній безпеці України і закінчуючи переліком суб'єктів забезпечення кібернетичної безпеки, їх основних функцій та повноважень. Відповідно, його відкликання стало очікуваним наслідком.

На нашу думку, головною вадою більшості вітчизняних офіційних нормативних документів у сфері національної безпеки щодо кібербезпекових питань є те, що вони не відповідають на ключові запитання: як саме держава як провідний актор національної безпеки тлумачить проблему кібербезпеки і чи керується вона у своїх діях чітко вибудуваною стратегією протиборства в кіберпросторі.

Важливо підкреслити, що значна частин труднощів із проходженням усіх проектів законів України, в яких зачіпалося поняття *кібербезпека*, стосувалася навіть не різних філософій і бачень, які закладалися їх авторами, а були наслідком жорстких дискусій довкола використаної термінології. Адже, як зазначалося, незважаючи на широке використання в науковій, публіцистичній та офіційній мові понять з частиною *кібер*, проблема формування кібербезпекової понятійно-категоріальної бази досі залишається в Україні нерозв'язаною, причому не лише на офіційно-державному, а й на науковому рівні.

Відповідні термінологічні проблеми намагалися вирішити як окремі науковці, так і експертно-наукові структури. Зокрема, в 2011 році Національний інститут стратегічних досліджень проводив дослідження, одним із завдань якого було визначення підходів до тлумачення основних термінів у кіберпросторі [64]. Результатом дослідження стало створення дефініцій таких понять, як *кіберпростір*, *кіберпростір держави*, *інформаційна інфраструктура*, *інформаційна інфраструктура держави*, *критична інформаційна інфраструктура держави*, *інформація про критичні об'єкти інфраструктури*, *критична інформація*, *кібербезпека*, *кіберзахист*, *кібератака*, *кіберзлочин*, *кібершпигунство*, *кібердиверсія*, *кібертероризм*. Щодо останнього поняття, то автори дослідження зазначають, що виокремлення *кібертероризму* як самостійного поняття є однією з найбільш дискусійних проблем у кібербезпековій сфері. Це обумовлено, по-перше, надзвичайною політизацією поняття, а по-друге, необхідністю чітко та правозастосовно виписати його ключові параметри так, щоб під їх дію не можна було підвести звичайні комп'ютерні злочини чи комп'ютерне хуліганство.

На жаль, українські дослідники не завжди здатні надати кваліфіковану допомогу законодавцю. Їхні дослідження пропонують таке розуміння окремих термінів (понять, категорій), яке, по-перше, часто не відповідає чинному українському законодавству, а по-друге, не має дійсно цілісних тлумачень підходів та оперує розпливчастими поняттями на кшталт «звичайні кібератаки» [162], «засоби інформаційного насильства» [124]. Як зазначають українські дослідники кібербезпекових проблем, в окремих випадках науковці пропонують і вочевидь хибні методологічні підходи до розуміння даної проблематики [67]. Проте «обережне дефініціювання» не є надто перспективним способом вирішення термінологічних проблем, хоча й забезпечить українських правоохоронців мінімально необхідним переліком визначень, потрібних у їх повсякденній роботі. Однак з погляду забезпечення інтересів довгострокового стратегування сфери кібербезпеки, таких рішень вочевидь недостатньо.

На проблему довгострокового стратегування сфери кібербезпеки опосередковано звертає увагу і Законопроект «Про кібернетичну безпеку» від 4 червня 2013 року, в якому зазначається, що «[однією з] основних функцій суб'єктів забезпечення кібернетичної безпеки є вироблення і періодичне уточнення Стратегії кібернетичної безпеки України», організувати розроблення такої має Кабінет Міністрів України [170].

Україна дійсно потребує цілісної, пророблені й такої, що відповідає потребам часу, Стратегії забезпечення кібербезпеки України – концептуального документа, який зміг би задати загальну логіку не лише подальшої нормотворчої діяльності, а й сутнісно сформулювати бачення Україною нових геополітичних умов існування держави, передусім щодо її ролі в глобальному та національному кіберпросторах. Документи аналогічного змісту вже давно ухвалено на Заході, і вони, хоча б у загальних рисах, зосереджені саме на зазначених питаннях, узгоджуючи їх із пріоритетами розвитку внутрішньодержавних систем кібербезпеки.

Проект такої Стратегії [64] (багато в чому вона використовувала напрацювання із зазначеного вище дослідження НІСД), максимально наближеної до європейських практик створення стратегічних безпекових документів, був створений у 2012 році фахівцями Національного інституту стратегічних досліджень (за участю автора роботи).

Поміж іншого, цей документ важливий як з огляду на євроінтеграційні прагнення української держави, так і з огляду на необхідність

на суто практичному рівні віднайти спільне бачення згаданих проблем з іноземними колегами. Крім того, в зазначеному документі здійснено спробу узгодити, з одного боку, інтереси ключових відомств, задіяних у сфері забезпечення кібербезпеки держави, а з іншого – зберегти науково-аналітичне бачення проблеми та основних способів її вирішення. Документ складається із семи основних розділів.

1. Визначення.
2. Загальні положення.
3. Основні принципи забезпечення кібернетичної безпеки України.
4. Загрози в сфері кібернетичної безпеки.
5. Основні напрями забезпечення кібернетичної безпеки.
6. Удосконалення державного управління та нормативно-правового поля у сфері кіберзахисту.
7. Етапи реалізації Стратегії.

Чи не найбільша кількість пропозицій, які надійшли від різних відомств до проекту Стратегії, стосувалися його першого розділу – «Визначення». Найбільш жваві дискусії також було присвячено саме цьому розділу. Стратегія запропонувала коректні та зрозумілі визначення таких понять:

- кіберпростір;
- кіберзагроза;
- кібербезпека;
- суб'єкти забезпечення кібернетичної безпеки;
- суб'єкти забезпечення кіберзахисту;
- кіберзлочинність;
- кіберзлочин;
- кібертероризм;
- кібершпигунство;
- кібервійна;
- національна критична інформаційна інфраструктура.

У пропонованому переліку саме поняття *національна критична інформаційна інфраструктура* є наріжним каменем державного інтересу у сфері кібербезпеки, який становить сутність державної безпекової політики щодо попередження та ліквідації (ослаблення) кіберзагроз. Менш важливими в даному контексті, на нашу думку, є загальні питання, які стосуються «об'єктів критичної інфраструктури», проблеми забезпечення безпеки яких виходять поза межі проблем кіберзахисту й кібербезпеки. Причому йдеться не про

будь-які «критичні об'єкти», а саме про ті, які є полем максимальної концентрації державного та приватного (загальнонаціонального) інтересу.

Розділ «Загальні положення» описує стан забезпечення кібербезпеки держави на поточному етапі, формулює в загальному вигляді основні завдання держави у цій сфері, джерела загроз і засади подальшого вдосконалення державної політики.

Проект більш-менш виразно артикулює принципові позиції України щодо кіберпростору та забезпечення кібербезпеки.

По-перше, зазначає, що «Україна виходить з того, що кіберпростір є відкритим простором – відкритим до інновацій, вільного розповсюдження ідей, інформації та обміну думками» [64].

По-друге, що «заходи із забезпечення кібербезпеки жодним чином не можуть суперечити принципу гарантування прав та свобод українських громадян, в тому числі права на недоторканість приватного життя та свободи спілкування». При цьому зауважено, що обов'язковою умовою ефективного забезпечення кібербезпеки є «узгоджений та комплексний підхід на чолі з державою, однак у тісному співробітництві з приватним сектором та громадянським суспільством, без яких неможливо вирішити дане завдання».

Це засадниче положення відображене також у розділі «Основні принципи забезпечення кібернетичної безпеки України», в якому, поміж іншого, увага акцентується на:

- пріоритеті дотримання прав і свобод людини та громадянина;
- пріоритеті запобіжних заходів;
- партнерстві держави, інституцій громадянського суспільства та приватного сектору у справі забезпечення кібернетичної безпеки держави;
- необхідності міжнародної співпраці для вироблення єдиних підходів та ефективної взаємодопомоги для протидії кіберзагрозам.

Розділ «Загрози в сфері кібернетичної безпеки» визначає загрози у сфері кібернетичної безпеки й не містить деталізації загроз, виходячи з переліку, визначеного положеннями Закону України «Про основи національної безпеки». Натомість проект Стратегії використовує загальноєвропейські підходи, відповідно до яких загрози розбито на три великі групи:

- кіберзлочини;
- кібертероризм;
- кібершпигунство та кібервійна.

У п'ятому розділі «Основні напрями забезпечення кібернетичної безпеки» сформульовано основні стратегічні пріоритети. Виокремлено 28 напрямів розбудови ефективної системи кібербезпеки, які стосуються, зокрема, проблем:

• військової сфери;

• підготовки кадрів;

• подальшої імплементації Україною положень Конвенції про кіберзлочинність;

• інноваційного розвитку;

• залучення до безпекової діяльності приватного сектору і громадянського суспільства.

Проект акцентує на комплексності вирішення безпекових проблем, охоплюючи соціальні, економічні, освітні, технологічні, інноваційні, нормативно-правові питання, а також питання міжнародного співробітництва. Зауважує, що успіх залежить від делегування державою відповідальності не лише профільним відомствам, а й усім державним органам, а також від їх узгодженої діяльності.

Розділ «Удосоналення державного управління та нормативно-правового поля у сфері кіберзахисту» стосується вдосконалення державного управління та нормативно-правового поля у сфері кіберзахисту. Основною тезою даного розділу є необхідність створення державного органу для забезпечення своєчасного виявлення, запобігання й нейтралізації кібернетичних загроз, а також усунення передумов їх виникнення та наслідків реалізації. Цей орган покликаний розв'язати проблеми міжсуб'єктного координування в забезпеченні кібернетичної безпеки, усунути паралелізм у роботі й дублювання функцій.

З метою виконання покладених на нього завдань зазначений орган має вжити таких заходів:

• організовувати взаємодію суб'єктів забезпечення кібернетичної безпеки включно із проведенням заходів щодо визначення можливих наслідків реалізації кібернетичних загроз, усунення передумов для їх настання та негативних наслідків їх реалізації;

• вести реєстр об'єктів національної критичної інформаційної інфраструктури, розробляти критерії визначення ступенів важливості, вразливості, захисту таких об'єктів, а також методику прогнозування наслідків, що можуть настати в результаті реалізації кібернетичних загроз щодо вказаних об'єктів;

• надавати методичну допомогу та рекомендації суб'єктам забезпечення кібернетичної безпеки щодо виявлення й усунення причин

вчинення кібернетичних злочинів і нейтралізації умов, які сприяють таким злочинам;

• надавати дозволи на впровадження в об'єктах національної критичної інформаційної інфраструктури відповідного безпекового програмного забезпечення та обладнання;

• контролювати в межах компетенції дотримання власниками об'єктів національної критичної інформаційної інфраструктури вимог чинного законодавства у сфері технічного захисту інформації.

Саме ця структура, за задумом проекту Стратегії, спроможна бути наріжним каменем у структурі майбутньої Національної системи кібербезпеки, оскільки в межах її повноважень можна буде вирішувати значну частину проблемних питань у сфері безпосереднього кіберзахисту.

Досі дискусійними є питання щодо кінцевої відомчої підпорядкованості як новопропонованої структури, так і інших елементів, які визначатимуться як ключові в Національній системі кібербезпеки.

Зважаючи на те, що до основних загроз у сфері кібернетичної безпеки віднесено питання кібервійни, природно, що основною контрольною та спрямовуючою силою в Національній системі кібербезпеки має бути інститут Президента України як Головнокомандувача, що своєю чергою впливатиме на розбудову інших елементів згаданої системи.

У цьому ж розділі вказується перелік законів, а також основних змін до них, які потрібно внести з метою впорядкування нормативно-правового поля національної кібербезпеки.

Сьомий розділ «Етапи реалізації Стратегії» присвячено трьом етапам реалізації Стратегії, перші два з яких має бути завершено протягом двох років, а заключний зорієнтований на підбиття підсумків.

Перший етап є критичним у плані забезпечення готовності держави відповісти на нові виклики безпеці. Саме на нього припадає значна частина заходів, спрямованих на розбудову Національної системи кібербезпеки, вдосконалення нормативно-правового поля, особливо в тій частині, яка стосується створення умов співробітництва між державним і недержавним сектором безпеки в питаннях протидії кіберзагрозам.

Під час *другого етапу* має завершитися основна частина розбудови Національної системи кібербезпеки, коли буде активізовано заходи щодо міжнародного співробітництва та вдосконалення міжнародного законодавства, здійснено оптимізацію програми підготовки кадрів

та розвитку необхідної для кібербезпекового сектору інноваційної продукції.

Третій етап та наступні роки – підведення підсумків реалізації двох попередніх етапів та з, огляду на динамічність сфери кібербезпеки та актуалізацію нових викликів і загроз, вжиття заходів щодо коригування Стратегії.

Висновки до розділу

Україна змушена у стислі строки сформувати цілісну позицію щодо кіберпростору як поля нового геополітичного протистояння.

Маючи чіткий курс на європейську інтеграцію, активне співробітництво із країнами Заходу, Україна має надавати перевагу «американсько-європейським» підходам, але реальні потреби поточної воєнно-політичної обстановки потребують більш жорстких заходів. Обрання російсько-китайської моделі означатиме втрати для іміджу нашої держави, що, зрештою, спричинюють втрати економічні. У цій ситуації Україні варто зосередитися не стільки на обранні варіантів, скільки на обстоюванні тих стратегічних цілей щодо глобального кіберпростору, досягнення яких повністю відповідає її національним інтересам.

У загальному вигляді «бажане майбутнє» передбачає максимально демілітаризований кіберпростір, посилення ролі на всіх основних міжнародних майданчиках, передання функцій управління та адміністрування ключових елементів інтернету від компаній типу *ICANN* легітимним міжнародним структурам, мінімізацію практик, спрямованих на фрагментацію мережі.

Поміж імперативів побудови ефективної стратегії кібербезпеки України можна виділити внесення змін до Закону України «Про засади внутрішньої та зовнішньої політики» і Доктрини інформаційної безпеки України.

Також доречним є прийняття цілком нових документів, таких як Стратегія забезпечення кібернетичної безпеки України, закони України «Про кібернетичну безпеку України» та «Стратегічні напрями зовнішньої політики України щодо глобального інформаційного простору та кіберпростору».

На тлі формування нового простору людського буття – кіберпростору – геополітика як наукова та практична сфера пояснення глобальних міждержавних процесів набуває якісно іншого виміру. Класичні геополітичні підходи багато в чому можуть бути застосовані до кіберпростору, але за умови їх певного корегування. Проте мине час, перш ніж класична геополітика визнає кіберпростір новим простором міждержавних протистоянь (критична геополітика робить це вже зараз). Таке несприйняття обумовлюється переважно незвичністю рис кіберпростору, складністю виявлення його ключових елементів, розмежування кордонів тощо. Усе це ще має бути концептуалізовано в науковому колі.

Дедалі більше дослідників вважають за необхідне зосередити наукові дослідження на проблемі кібермогутності держав як здатності втілювати їх волю та забезпечувати національні інтереси в кіберпросторі. Про важливість і актуальність проблеми свідчить активне її обговорення та спроби розв'язання дослідниками з тих країн, які найчастіше згадуються в контексті нового глобального геополітичного протиборства – США та КНР.

Проблема наукового осмислення та практичного використання кіберпростору супроводжується суттєвими термінологічними та нормативно-правовими питаннями. Наразі не існує загальноприйнятого визначення навіть базового поняття кіберпростору, не кажучи про інші, ціла низка яких настільки активно застосовується в публіцистиці, що поступово губиться можливість їх наукового осмислення. Багато питань постає й довкола спроб перенести класичні види протистоянь і загроз (тероризм і війна) у реальність кіберпростору. Вже стало очевидним, що механічне застосування

понять кібертероризму та кібервійни як проекцій класичного тероризму та війни в кіберпросторі не відповідає реальному стану речей.

Нормативно-правові проблеми є природним наслідком термінологічних, однак виводять їх із суто наукового обговорення до сфери практичних міждержавних відносин. При цьому досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім похідним від нього поняттям сфери безпеки, принципово не визначено правовий статус кіберпростору (існує щодо всіх інших просторів), відсутній будь-який міжнародний далекосяжний консенсус щодо правил поведінки в кіберпросторі та загальноприйняті методики оцінювання наслідків кібератак та їх «прив'язування» до міжнародних норм і правил.

Спроби впорядкувати ці проблеми в межах нормативно-правового поля можна вважати лише частково успішними. Єдиним реальним документом кібербезпекового характеру є Конвенція про кіберзлочинність, однак вона, по-перше, присвячена доволі вузькому сегменту кіберзагроз (кіберзлочинам у сфері комп'ютерної інформації), а по-друге є, по-суті, регіональним документом, що до того ж не сприймається значною кількістю геополітичних гравців. Спроби КНР і Росії просувати власні ініціативи (наприклад Конвенцію про забезпечення міжнародної інформаційної безпеки) стикаються з очікуваним спротивом США та їх союзників.

На цьому тлі глобальної невизначеності небезпечними є спроби окремих країн та організацій (зокрема НАТО) трактувати кібератаки як «акти війни», адже це може призвести до систематичних порушень чинного міжнародного законодавства. При цьому, найшвидше, без змін Статуту ООН і закріпленого в ньому поняття *агресія* такі спроби і надалі перебуватимуть поза міжнародним нормативно-правовим полем. І це незважаючи на особливу актуальність проблеми, спричинену реальною мілітаризацією кіберпростору, активним нарощуванням значною кількістю держав їхніх військових кіберпотенціалів попри численні публічні заклики до «мирного кіберпростору». Дедалі більше країн чи не офіційно починають займатися розробленням кіберозброєнь, вкладають мільярдні кошти в кібербезпековий сектор (лише США в 2013 році вклали в кіберсферу 14 млрд дол.), що спричинює нову гонку озброєнь і збільшення взаємної недовіри між геополітичними гравцями.

За таких реалій дві найпотужніші держави сьогодення – КНР і США – вступають у довготривале суперництво, яке має глобаль-

ний характер і виявляється майже на всіх рівнях. Зокрема – в кіберпросторі.

Могутність цих країн (економічна, військова, зовнішньополітична, культурна) та їх взаємозалежність робить практично неможливим відкрите протистояння, змушуючи шукати альтернативні форми суперництва, за яких кожна з країн може збільшити свою перевагу або принаймні знизити ефективність дій суперника. За таких умов кіберпростір стає одним з важливих просторів протиборства, в т.ч. через його нормативно-правову невизначеність. Це формування створює умови для розгортання «холодної війни *v*2.0.» з усіма ознаками «класичної» «холодної війни»: високим рівнем латентних загострень на міжнародній арені, непрямими методами боротьби (передусім активізацією розвідувальної діяльності з обох сторін), винесенням конфліктів на територію третіх країн (наприклад у формі протистоянь за сфери впливу) та гонкою озброєнь. Уже сьогодні ми бачимо, як кібершпигунство стає повсякденним явищем у взаємовідносинах КНР – США, а дискусії щодо зменшення протистояння в кіберпросторі ведуться на найвищому політичному рівні. «Оновлена» гонка кіберозброєнь має важливу особливість: вона є принципово латентною та прихованою, що обумовлено самою природою кіберзброї.

В історичній ретроспективі можна побачити, що це суперництво/протистояння в кіберпросторі та довкола кіберпростору розпочалося ще в 2008–2009 рр., однак у реальні міждержавні взаємовідносини увійшло з 2010 року і відтоді є їх постійним чинником. Хоча протягом останніх 3-4 років сторони робили певні спроби знизити рівень взаємного напруження в кіберпросторі, однак досі вони залишаються невдалими і, з огляду на принциповий характер суперництва, найшвидше, такими й залишаться. На практиці це протистояння виражається в масштабних діях хактивістів (від них страждають обидві сторони), кібершпигунстві (всесвітньо відомою стала кібершпигунська атака на *Mitsubishi Heavy Industries* або функціонування таких програм, як *Duqu*, *Flame*, *Gauss*, *MiniDuke*, *Red October*), а в окремих випадках – у кібердиверсіях (на кшталт дії *Wiper* та *Stuxnet*). Від того, чи зможуть КНР і США виробити ефективний статус-кво щодо діяльності в кіберпросторі, може залежати доля не лише цих країн, а й практично всього глобалізованого світу.

Ситуація, що склалася, природно спричинює масштабні міжнародні фахові дискусії щодо можливості вироблення ефективних заходів, спрямованих на демілітаризацію кіберпростору. Результати

таких дискусій наражаються на практичну неможливість контролю за виробленням/недопущенням вироблення чи обліком кіберозброєнь, спричинену їх природою. Фактично майже будь-яке програмне забезпечення, як, власне, й всі *IT*-технології, є технологіями подвійного призначення, а отже, потребують або тотального контролю, або принципово іншого підходу, ніж сучасне ставлення до «традиційних» подвійних технологій. Крім того, будь-яка ініціатива, спрямована на демілітаризацію кіберпростору, стикатиметься із вже згаданим невизначеним нормативно-правовим статусом кіберпростору, відсутністю для нього правил ведення війни, а також відповідності воєнних дій у кіберпросторі «класичним» воєнним діям. Адже, незважаючи на алармістські настрої значної частини фахівців, масштабні кібератаки все-таки не можуть бути повністю еквівалентними «класичним» кінетичним атакам, надто ядерним. Хоча саме досвід ядерного стримування 60-90 рр. XX сторіччя став би надзвичайно корисним у намаганнях стримати неконтрольовану мілітаризацію кіберпростору. Ідеться передусім про заходи щодо зміцнення довіри та політику «малих кроків».

Маємо визнати, що міжнародні організації наразі, вочевидь, недостатньо готові до діяльності в умовах нової кіберпросторової реальності. Такі міжнародні інститути, як ООН, *G*7 та інші, поки що не змогли посісти ту однозначну позицію щодо процесів у кіберпросторі, на яку очікує міжнародна спільнота. Багато в чому це пояснюється відносною ефективністю та нереформованістю цих структур на теперішньому етапі їх розвитку, однак і нинішні свої потенційні можливості й доступні механізми впливу на ситуацію вони використовують недостатньо повно. Меншою мірою це стосується діяльності Міжнародного союзу електрозв'язку, який на практичному рівні задіяний у пошуку відповідей на глобальні кібервиклики, однак, як засвідчують події в Дубаї 2012 року, навіть у цієї організації виникають суттєві проблеми із пошуком балансу інтересів.

За відносної неспроможності міжнародних структур суттєво вплинути на глобальні питання розвитку кіберпростору США і КНР роблять в цьому напрямі суттєві кроки, причому як щодо національного, так і міжнародного кіберпростору. Зокрема, США з першої каденції Б. Обами на посаді президента розпочали масштабні програми, спрямовані на посилення кібербезпеки країни. Було вжито заходів щодо вдосконалення нормативно-правового поля (зокрема ухвалено низку профільних нормативно-правових документів), організаційної

структури протидії кіберзагрозам (сформовано Кіберкомандування США, посилено кібербезпекові підрозділи ЦРУ, ФБР, АНБ і МВБ), активізовано работу із співпраці безпекових структур з приватним сектором. Показово, що на тлі скорочень військового бюджету США та часткового перегляду його пріоритетів чи не єдиною статтею видатків, що не скорочується, є використання *IT* у військовому секторі, передусім у кібербезпековій сфері. У межах зовнішньополітичних ініціатив США щодо кіберпростору в 2011 році було прийнято Міжнародну стратегію для кіберпростору, положення якої держава послідовно обстоює на всіх рівнях.

Розвиток кіберпростору є сталим пріоритетом стратегій розвитку КНР, в тому числі в межах п'ятирічних планів розвитку. При цьому політика КНР щодо кіберпростору акцентує передусім на механізмах забезпечення державного суверенітету над національним сегментом мережі інтернет. Керівництво КНР через спеціально уповноважені органи прискіпливо спостерігає за дотриманням національного законодавства під час поширення певних видів інформації національними та західними компаніями, без вагань вдаючись до протистояння в разі виявлення порушень. Подібний жорсткий контроль за контентом, що циркулює в національному сегменті кіберпростору, китайське керівництво пояснює передусім необхідністю захистити традиційні азіатські цінності. Сама політика щодо контенту здійснюється відповідно до принципу «керованої відкритості».

Поміж зовнішньополітичних ініціатив КНР щодо майбутнього кіберпростору найбільш важливими є Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки, які передбачається закріпити через інститути ООН. Багато в чому цей документ є референованою версією іншого, більш масштабного документа, що просувається Російською Федерацією – Міжнародної конвенції про забезпечення міжнародної інформаційної безпеки.

З огляду на суттєві відмінності в поглядах на кіберпростір і на те, де проходять межі влади держави в цьому просторі, малоймовірно, що США та КНР домовляться про спільне бачення майбутнього для глобалізованого кіберпростору.

В умовах глобального суперництва США та КНР змушена формувати свою політику щодо кіберпростору Україна. При цьому вона має зважати на те, що попри заклики всіх провідних гравців до демілітаризації кіберпростору, цей процес так і не буде розпочатий, принаймні в її традиційному історичному розумінні поняття *демілітаризація*.

Гонка кіберозброєнь є практично невідворотною, що обумовлює необхідність дуже серйозно поставитися до питань кібербезпеки держави та її громадян. Кібершпигунство і надалі буде важливою домінантою міждержавного суперництва і з розвитком *IT*-сектору лише посилюватиметься.

Можна очікувати, що на певному етапі подібні виклики глобальному кіберпростору спричинять його сегментацію на певні «національні інтернети». Це висуває перед державою глобальне питання розбудови власного кіберсуверенітету, який розуміється як можливості національних держав самостійно і незалежно визначати внутрішні та зовнішні, політичні й геополітичні національні інтереси в кіберсфері, їх спроможність самостійно визначатися з курсом внутрішньої і зовнішньої інформаційної політики, самостійно розпоряджатися власними інформаційними ресурсами та інфраструктурою національного інформаційного простору, а відтак, гарантувати кібернетичну та інформаційну безпеку державі, суспільству та громадянам.

Зазначені реалії порушують перед Україною низку питань як у сфері зовнішньополітичних зусиль, так і щодо оптимізації нормативно-правової та організаційної бази забезпечення кібербезпеки держави.

Передусім мають бути сформульовані її стратегічні інтереси щодо глобального кіберпростору як такого та визначені перспективи міжнародної політичної дійсності з цього питання в інтересах України. Ідеться передусім про вжиття заходів щодо максимально можливої демілітаризації кіберпростору (незважаючи на відсутність практичної перспективи таких дій, зусиль у цьому напрямі має бути докладено); якнайширше представлення власних інтересів щодо майбутнього кіберпростору на всіх ключових міжнародних майданчиках; забезпечення широкого міжнародного контролю за функціонуванням мережі інтернет (у тому числі передання функцій управління та адміністрування його ключових елементів до МСЕ); вжиття заходів щодо недопущення подальшого загострення проблематики, пов'язаної з фрагментацією Світової мережі (при цьому потрібно розробляти стратегії розвитку, зважаючи на можливості повноцінної реалізації таких «проектів» та необхідність визначати свою позицію в «кіберсегментованому» світі); потребу виходити з того, що жоден з наявних на сьогодні підходів до забезпечення миру та стабільності у глобальному кіберпросторі (умовно «американсько-європейський» та «російсько-китайський») навряд чи зможе стати реальною базою для обговорення. Україна має виступати на міжнародному рівні з більш активними

ініціативами, спрямованими на визначення майбутнього кіберпростору. Цьому суттєво сприятиме ухвалення профільних нормативно-правових документів і запровадження профільних посад заступників міністра в Міністерстві зовнішніх справ.

Зусилля держави щодо розбудови ефективної системи кібербезпеки мають бути зосереджені, зокрема, на визначенні та закріпленні в нормативно-правовому полі ключових термінів і понять кібербезпекової сфери та уточненні чинних безпекових документів (зважання в них на проблеми кібербезпеки). Доцільно розглянути питання комплексного огляду вітчизняного сектору кібербезпеки (у форматі Зеленої книги), забезпечити прийняття Стратегії забезпечення кібернетичної безпеки України та Закону України «Про кібернетичну безпеку України». Важливо сформувати загальнонаціональні міжвідомчі координаційні структури, спроможні узгоджувати та координувати діяльність різних силових відомств на час розслідування злочинів у кіберпросторі, та створити ефективну систему захисту вітчизняного кіберпростору (зокрема у військовій сфері). Сам кібербезпековий сектор має бути на якісно новому рівні забезпечений ресурсами (фінансовими, кадровими, технічними), в тому числі через створення національної операційної системи та «антивірусу», а також через відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. З огляду на те, що значна кількість об'єктів критичної інфраструктури наразі є у приватній власності, конче важливим є посилення взаємодії органів державної влади з приватним сектором, а також неурядовими організаціями та громадянським суспільством у цілому.

Використана література

1. *Австралия* отказала китайской компании Huawei [Електронний ресурс]. – Режим доступу: http://ntdtv.ru/news/avstraliya-otkazala-kitaiskoi-kompanii-huawei

2. *Америка* не будет закупать китайское *IT*-оборудование [Електронний ресурс]. – Режим доступу: http://www.cy-pr.com/news/other/6843/

3. *Американские* спецслужбы обвинили Китай в осуществлении кибератак на Пентагон [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/430508.php

4. *Американским* компаниям запретили замалчивать информацию о кибератаках [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/17oct2011/uscyberattckrpr

5. *Американцы* потратят $130 млн. на виртуальный военный полигон [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/405997.php?sphrase_id=1139540

6. *АНБ* США получит право регулировать киберпространство США [Електронний ресурс]. – Режим доступу: http://www.cybersecurity.ru/armament/65241.html

7. *Андрианов В. Л.* Формирование «Большого Китая»: Геополитическое измерение : автореф. дис. ... к.і.н. : 07.00.03 / В. Л. Андрианов [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/formirovanie-bolshogo-kitaya-geopoliticheskoe-izmerenie

8. *Банкам* выгоднее закрывать глаза на украденные деньги, чем сообщать о кибератаках на их ресурсы [Електронний ресурс]. – Режим доступу: http://112.ua/politika/bankam-vygodnee-zakryvat-glaza-na-ukradennye-dengi-chem-soobschat-o-kiberatakah-na-ih-resursy-ekspert-20442.html

9. *Барлогу Д. П.* Декларация независимости Киберпространства [Електронний ресурс]. – Режим доступу: http://www.zhurnal.ru/1/deklare.htm

10. *Бергстен Ф.* Китай. Что следует знать о новой сверхдержаве / Ф. Бергстен, Б. Гилл, Н. Ларди, Д. Митчел; пер. с англ. – изд. 2-е, перераб. и доп. – М. : Институт комплексных стратегических исследований, 2007. – 256 с.

11. *Беттс Р.* Утраченная логика сдерживания // Россия в глобальной политике / Р. Беттс [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/number/Utrachennaya-logika-sderzhivaniya-15954

12. *Боти* намагаються засмічувати інформаційне поле #євромайдан – як з цим боротись [Електронний ресурс]. – Режим доступу: http://v-n-zb.livejournal.com/6379558.html

13. *Британцы* занялись разработкой кибероружия [Електронний ресурс]. – Режим доступу: http://actualcomment.ru/news/25319637/

14. *Булгак П.* Кібервійна та Євромайдан: репетиція 2015 / П. Булгак [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/articles/2013/11/27/7003178/

15. *Бутузов В. М.* Протидія комп'ютерній злочинності: деякі аспекти міжнародного досвіду (на прикладі діяльності правоохоронних органів США та Німеччини) / В. М. Бутузов // Інформаційна безпека: людини, суспільства, держави. – 2009. – № 1. – С. 30–38.

16. *Бутузова А.* Могущество, интересы и ценности в международных отношениях / А. Бутузова [Електронний ресурс]. – Режим доступу: http://www.geopolitica.ru/article/mogushchestvo-interesy-i-cennosti-v-mezhdunarodnyh-otnosheniyah#.UjLKhX8fj_c

17. *Бывший* глава АНБ США: Россия и Китай используют кибершпионаж для хищения технологических секретов чаще остальных [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/418571.php

18. *Бэкдор* MiniDuke размером 20 КБ «вынес мозг» Евгению Касперскому [Електронний ресурс]. – Режим доступу: http://www.xakep.ru/post/60229/

19. *В 2013 году* мошенники похитили с банковских счетов предприятий 10,5 млн гривен [Електронний ресурс]. – Режим доступу: http://112.ua/kriminal/v-2013-godu-moshenniki-pohitili-s-bankovskih-schetov-predpriyatiy-10-5-mln-griven-18956.html

20. *В Gartner* борьбу с киберугрозами считают финансовой пирамидой [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/443716.php

21. *В Голландии* хотят легализовать DDoS-атаки [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/426205.php

22. *В Китае* заявляют, что напугали Google [Електронний ресурс].– Режим доступу: http://m.hitech.newsru.com/article/18Jan2010/cngoogle

23. *В МИД* ФРГ появится должность уполномоченного по кибербезопасности [Електронний ресурс]. – Режим доступу: http://antivirus.ua/node/3041

24. *В Минске* раскрыли секреты избирательной кампании Барака Обамы [Електронний ресурс]. – Режим доступу: http://www.interfax.by/article/40963

25. *В мире* два десятка стран занимаются кибероружием – McAfee [Електронний ресурс]. – Режим доступу: http://www.cybersecurity.ru/armament/86546.html

26. *Война* в киберпространстве – вопрос времени? [Електронний ресурс]. – Режим доступу: http://www.golos-ameriki.ru/content/cyber-wars-in-future/1681528.html

27. *В Украине* арестованы разработчики трояна Carberp [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/439271.php

28. *В ходе учений* по «кибервойне» курсанты американских военных вузов победили специалистов АНБ [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/23apr2013/uscdx

29. *В этом году* доходы китайских хакеров году могут превысить $1,5 млрд [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=63065

30. *WikiLeaks:* Германские эксперты посоветовали США атаковать Иран вирусом Stuxnet [Електронний ресурс]. – Режим доступу: http://www.newsru.com/world/19jan2011/stuxnet.html

31. *Василенко И. А.* Геополитика современного мира : учеб. пособие / И. А. Василенко. – М. : Гардарика, 2006. – 340 с.

32. *Ведущая* японская военная корпорация подверглась хакерской атаке [Електронний ресурс]. – Режим доступу: http://vz.ru/news/2011/10/10/528966.html#

33. *Взломан* Национальный реестр плотин США [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/440120.php

34. *Возможности* Китая в проведении кибероперацій и шпионаже. Как это видит Конгресс США? [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/blog/personal/tsarev/21111.php

35. *Вознюк Ю. С.* Геополітична свідомість як феномен культури постмодерну: історичний аспект / Ю. С. Вознюк // Політологічний вісник. – 2012. – № 60. – С. 341–353.

36. *Волков Я. В.* Геополитика и ее влияние на обеспечение безопасности в современном мире : автореф. дис. ... к.політ.н. : 23.00.01 / Я. В. Волков [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/geopolitika-i-ee-vliyanie-na-obespechenie-bezopasnosti-v-sovremennom-mire

37. *Воронянський О. В.* Проблема визначення політичного змісту категорії «національні інтереси» / О. В. Воронянський // Політологічний вісник. – 2011. – № 54. – С. 241–246.

38. *Выступление* помощника госсекретаря Познера о свободе слова в эпоху цифровых технологий [Електронний ресурс]. – Режим доступу: http://iipdigital.usembassy.gov/st/russian/article/2011/10/20111026103945x0.8727468.html#axzz1dIC9bFSK

39. *Выступление* представителя Беларуси при ООН Игоря Угорича в Первом комитете ГА ООН [Електронний ресурс]. – Режим доступу: http://www.unmultimedia.org/radio/russian/archives/98379

40. *Выступление* представителя Российской Федерации Андрея Малова в Первом комитете ГА ООН [Електронний ресурс]. – Режим доступу: http://www.unmultimedia.org/radio/russian/archives/98456

41. *Gauss* спонсировали госструктуры [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/428343.php

42. *Гаджиев К. С.* Геополитика / К. С. Гаджиев. – М. : Юрайт, 2011. – 480 с.

43. *Голдштейн Э.* Китай: прямая и явная угроза / Эвери Голдштейн // Россия в глобальной политике. – 2013. – № 5.– Т. 11. – С. 77–84.

44. *Головне* управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України [Електронний ресурс]. – Режим доступу: http://www.mil.gov.ua/index.php?part=department&lang=ua&sub=guz_is

45. *Гольцов А. Г.* Геостратегія держав світу: основні рівні і типи / А. Гольцов // Наукові праці МАУП. – 2011. – Вип. 1(28). – С. 21–26.

46. *Госдеп США* обвиняет Россию и Китай в попытках усилить контроль в интернете [Електронний ресурс]. – Режим доступу: http://www.centrasia.ru/newsA.php?st=1317282000

47. *Гримська М. І.* Еволюція зовнішньої політики КНР в умовах реалізації стратегії «чотирьох модернізацій» : автореф. дис. ... к.політ.н. : 23.00.04 / М. І. Гримська; Київ. нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – К., 2009. – 16 с.

48. *22–25 апреля* 2013 года в г. Гармиш-Партенкирхене (Германия) состоялись Седьмой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» [Електронний ресурс]. – Режим доступу: http://www.iisi.msu.ru/news/news70/

49. *DDoS-атака* на веб-сайт Генеральної прокуратури України [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?p=506

50. *DDoS-атака* на веб-сайт Кабінету Міністрів України [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?p=714

51. *Duqu* – вредоносная матрёшка [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/159669/

52. *Duqu* использовал критическую 0day уязвимость в Windows [Електронний ресурс]. – Режим доступу: http://www.xakep.ru/post/57692/

53. *Декларация* принципов ВСИО [Електронний ресурс]. – Режим доступу: http://www.un.org/russian/conferen/wsis/dec.pdf

54. *Дергачев В. А.* Геополитический словарь-справочник / В. А. Дергачев. – К. : КНТ, 2009. – 592 с.

55. *Доповідь* про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/?q=system/files/sites/default/files/images/dop.doc

56. *Дорошко М.* Геополітичне середовище та геополітична орієнтація країн СНД : навч. посібник / М. Дорошко, Н. Шпакова. – К. : Центр учбової літератури, 2011. – 204 с.

57. *Достижения* в сфере информатизации и телекоммуникации в контексте международной безопастности : резолюция A/RES/53/70 [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/ods.asp?m=A/RES/53/70

58. *Достижения* в сфере информатизации и телекоммуникации в контексте международной безопастности : доклад Генерального Секретаря ООН [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/ods.asp?m=A/54/213

59. *Достижения* в сфере информатизации и телекоммуникаций в контексте международной безопасности : резолюция ООН A/

RES/56/19 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement

60. *Дубов Д.* Американо-китайское соперничество в киберпространстве: новая «холодная война» / Д. Дубов // Проблемы национальной стратегии. – 2013.– № 6 (21). – С. 111–125.

61. *Дубов Д.* Демилитаризация киберпространства и проблемы «киберсдерживания»: возможные решения // ბიზნესი და კანონმდებლობა.– 2014. – № 1. – С. 41–48.

62. *Дубов Д.* Доктрина Барака Обами: нова «Стратегія національної безпеки» США / Д. Дубов, М. Ожеван // Актуальні проблеми міжнародних відносин : зб. наук. праць / Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка. – К., 2010. – Вип. 94; Ч. І. – С. 16–20.

63. *Дубов Д.* Забезпечення національних інтересів держави в інформаційному суспільстві: трансформація пріоритетів / Д. Дубов // Стратегічні пріоритети. – 2012. – № 3. – С. 120–125.

64. *Дубов Д.* Кібербезпека: світові тенденції та виклики для України / Д. Дубов, М. Ожеван. – К. : НІСД, 2011. – 30 с.

65. *Дубов Д.* Кібербезпекова політика в контексті трансформації політики безпеки США за адміністрації Б. Обами / Д. Дубов // Політичний менеджмент. – 2010. – № 1. – С. 156–163.

66. *Дубов Д.* Модернізація інформаційної інфраструктури як чинник забезпечення національних інтересів України / Д. Дубов // Стратегічні пріоритети. – 2013. – № 2. – С. 90–96.

67. *Дубов Д.* Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – № 5. – С. 19–30.

68. *Дубов Д.* Політика Китаю щодо регулювання внутрішнього інформаційного простору / Д. Дубов // Політичний менеджмент. – 2010. – № 4. – С. 94–102.

69. *Дубов Д.* Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні : аналіт. зап. / Д. Дубов [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1466/

70. *Дубов Д.* Стратегічні аспекти кібербезпеки України / Д. Дубов // Стратегічні пріоритети. – 2013. – № 4. – С. 119–126.

71. *Дубов Д.* Сучасні тенденції забезпечення кібербезпеки на міжнародному рівні / Д. Дубов // Стратегічні пріоритети. – 2011. – № 4. – С. 5–11.

72. *Дубов Д. В.* Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2012. – 32 с.

73. *Дугин А.* Основы геополітики / А. Дугин. – М. : АРКТОГЕЯ-центр, 2000. – 928 с.

74. *Евдокимов Е. В.* Основные направления стратегии внешнеполитической пропаганды КНР в отношении США : автореф. дис. ... к.політ.н. : 23.00.04 / Е. В. Евдокимов [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/osnovnye-napravleniya-strategii-vneshnepoliticheskoi-propagandy-knr-v-otnoshenii-ssha

75. *Евтихевич Н. С.* Концепция «безопасности личности и общества»: канадский подход / Н. С. Евтихевич, Е. В. Исраелян [Електронний ресурс]. – Режим доступу: http://www.imemo.ru/ru/period/pathways/2013/N01/13008_02.pdf

76. *Ерёмин Я. И.* Роль и место США во внешнеполитической стратегии Китая: политологический аналіз : автореф. дис.. ... к.полит.н. : 23.00.04 / Я. И. Ерёмин [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/rol-i-mesto-ssha-vo-vneshnepoliticheskoi-strategii-kitaya-politologicheskii-analiz

77. *Жданова Н. А.* Стратегия расширения геополитического влияния КНР на рубеже XX–XXI веков : автореф. дис.. ... к.і.н. : 07.00.03 / Н. А. Жданова [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/strategiya-rasshireniya-geopoliticheskogo-vliyaniya-knr-na-rubezhe-xx-xxi-vekov

78. *Зайцев Ю.* Stuxnet / Юрий Зайцев [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/blog/personal/Zuis-blog/7.php

79. *Зараження* вірусом Uroburos [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?p=344

80. *Зевелёв И.* Реализм в XXI веке // Россия в глобальной политике / И. Зевелёв [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/number/Realizm-v-XXI-veke-15792

81. *Зовнішньополітичні* пріоритети [Електронний ресурс]. – Режим доступу: http://mfa.gov.ua/ua/about-ukraine/foreign-policy

82. *Ивей Ван.* Китайская модель разрушает гегемонию «общечеловеческих ценностей» [Електронний ресурс]. – Режим доступу: http://inosmi.ru/world/20130114/204595110.html#ixzz2Hx7crG9v

83. *Ильин М.* Этапы становления внутренней геополитики России и Украины / М. Ильин // Политические исследования. – 1998. – № 3. – С. 82–95.

84. *Информационный* суверенитет – новая реальность [Електронний ресурс]. – Режим доступу: http://iforum.ua/docs/biz/

85. *Інфографіка:* злами інформаційних систем, а також час виявлення та реагування на них [Електронний ресурс]. – Режим доступу: https://scontent-a.xx.fbcdn.net/hphotos-prn1/t1.0-9/1604423_617599488319664_1554722890_n.jpg

86. *«Кибероружейному»* вирусу Flame дали команду на самоуничтожение [Електронний ресурс]. – Режим доступу: http://news.yottos.com/ShowNews/

87. *Кефели И. Ф.* Философия геополитики / И. Ф. Кефели. – СПб. : Изд. дом «Петрополис», 2007. – 208 с.

88. *Кибератаки* на Mitsubishi Heavy Industries, RSA и Lockheed Martin могла осуществить одна и та же хакерская группа [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/407517.php

89. *Кибербезопасность* – в центре повестки дня женевского форума [Електронний ресурс]. – Режим доступу: http://www.unmultimedia.org/radio/russian/archives/138951/

90. *Кибербезопасность* [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/ecosoc/itu/cybersecurity.shtml

91. *Кибервойска РФ* рождаются в Генштабе [Електронний ресурс]. – Режим доступу: http://file–rf.ru/news/12209

92. *Кибершпион* вирус – Красный октябрь – Red October [Електронний ресурс]. – Режим доступу: http://www.youtube.com/watch?v=C2i7ENSgkXw

93. *Кирьянов О.* Китайский генерал поспорила с главой Пентагона / О. Кирьянов [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2013/06/02/general-site-anons.html

94. *Киссинджер Г.* Будущее американо-китайских отношений / Г. Киссинджер [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/number/Buduschee-amerikano-kitaiskikh-otnoshenii

95. *Китай* «не создавал» шпионской киберсети [Електронний ресурс]. – Режим доступу: http://news.bbc.co.uk/hi/russian/sci/tech/newsid_7973000/7973063.stm

96. *Китай* и США объявили о сотрудничестве в предотвращении информационной холодной войны [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/424306.php

97. *Китай* и США совместно проводили киберучения [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/42339.php

98. *Китай* объединится с США в борьбе с киберпреступностью [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/399387.php

99. *Китай* официально опроверг ведение кибервойн против США [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/406028.php

100. *Китай* собирается вводить новые правила борьбы с международным кибершпионажем [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/438546.php

101. *Китайские* власти заблокировали YouTube [Електронний ресурс]. – Режим доступу: http://www.lenta.ru/news/2009/03/youtube/

102. *Китайские* военные взломали компьютерную сеть Пентагона [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/04Sep2007/china

103. *Китайские* эксперты сообщили об увеличении числа хакерских атак на государственные сайты [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/405062.php

104. *Китайцы* взломали Пентагон [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=34060

105. *Конвенция* об обеспечении международной информационной безопасности (концепция) [Електронний ресурс]. – Режим доступу: http://www.mid.ru/bdomp/ns–osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

106. *Конвенція* про кіберзлочинність // Офіційний вісник України. – 2007. – № 65; 10 верес. – С. 107.

107. *Концепция* внешней политики Российской Федерации [Електронний ресурс]. – Режим доступу: http://www.mid.ru/brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F

108. *Криміналу* за фактом хакерських атак на сайт МВС не буде [Електронний ресурс]. – Режим доступу: http://24tv.ua/home/showSingleNews.do?kriminalu_za_faktom_hakerskih_atak_na_sayt_mvs_ne_bude&objectId=185800

109. *Куткин В. С.* Геополитика как объект социально-философского анализа : автореф. дис. ... к.філос.н. : 09.00.11 / В. С. Куткин [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/geopolitika-kak-obekt-sotsialno-filosofskogo-analiza

110. *Лебідь В.* Американо-китайські відносини: тенденції та перспективи / В. Лебідь // Дослідження світової політики : зб. наук. праць. – 2011. – Вип. 2. – С. 115–126.

111. *Лежун Ц.* Онлайновые СМИ КНР в 1995–2001 гг. : автореф. дис. ... к.філол.н. : 10.01.10 / Цзя Лежу [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/onlainovye-smi-knr-v-1995-2001-gg

112. *Ленський П. С.* Центральноазійський вектор політики КНР у галузі регіональної безпеки в постбіполярний період : автореф. дис. ... к.політ.н. : 23.00.04 / П. С. Ленський; НАН України, Ін-т світ. економіки і міжнар. відносин. – К., 2010. – 21 с.

113. *Ломанов А.* Флаги китайских отців // Россия в глобальной политике / А. Ломанов [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/number/Flagi-kitaiskikh-ottcov-15183

114. *Ломанов А.* Чжунго хэпин цзюэци (Мирное возвышение Китая) // Россия в глобальной политике / А. Ломанов [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/book/n_424682347

115. *Лукьянович Н. В.* Геополитика России: теоретико-методологические основы, генезис, особенности формирования и развития в условиях глобализации : автореф. дис. ... к.політ.н. : 23.00.04/Н. В. Лукьянович [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/geopolitika-rossii-teoretiko-metodologicheskie-osnovy-genezis-osobennosti-formirovaniya-i-ra

116. *Луценко А. В.* Оцінка впливу кібертероризму на зовнішню політику держав: нові підходи до стратегії «м'якої сили» у геополітиці США / А. В. Луценко // Актуальні проблеми міжнародних відносин. – 2009. – Вип. 85 (Ч. 2). – С. 78–82.

117. *Люлько Л.* Ирония судьбы, или Собака Цукерберга / Л. Люлько [Електронний ресурс]. – Режим доступу: http://www.pravda.ru/society/how/14-03-2011/1069840-bloggerchina-0/

118. *MiniDuke* – новая вредоносная программа для кибершпионажа в государственных структурах по всему миру [Електронний ресурс]. – Режим доступу: http://www.kaspersky.ru/news?id=-207733960

119. *Майбутнє* кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2012. – 32 с.

120. *Максим Літвінов*: Об'єднавши зусилля, ми досягнемо високих результатів у боротьбі з кіберзлочинністю / Максим Літвінов [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/915190

121. *Максим Савaневський* #євромайдан: українська цифрова революція та останній шанс аналоговим політикам стати цифровими Саваневський Максим [Електронний ресурс]. – Режим доступу: http://watcher.com.ua/2013/11/yevromaydan-ukrayinska-tsyfrova-revolyutsiya-ta-ostanniy-shans-analohovym-politykam-staty-tsyfrovymy/

122. *Манжай О. В.* Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай // Право і безпека. Науковий журнал. – 2009. – № 4. – С. 142–149.

123. *Маринченко А. В.* Геополитика : учеб. пособие / А. В. Маринченко. – М. : ИНФРА-М, 2010. – 429 с.

124. *Марченко А. В.* Соціальні наслідки кібертерористичної небезпеки в епоху інформаційних технологій / А. В. Марченко // Методологія, теорія та практика соціологічного аналізу сучасного суспільства : зб. наук. праць Харків. нац. ун-ту імені В. Н. Каразіна. – 2008. – № 1. – С. 355–360.

125. *Масляк П. О.* Країнознавство : підруч. / П. О. Масляк. – К. : Знання, 2007. – 292 с.

126. *Мерзлякова А.* Русские держатели знания / Анна Мерзлякова [Електронний ресурс]. – Режим доступу: http://sibforum.sfu-kras.ru/node/311

127. *Минобороны* Беларуси создает элитное подразделение кибервойск [Електронний ресурс]. – Режим доступу: http://www.bezpeka.com/ru/news/2013/09/18/belarus-cyberforce.html

128. *Миссия* Сноудена: Тайная мировая кибервойна получает официальные технические параметры [Електронний ресурс]. – Режим доступу: http://www.regnum.ru/news/polit/1675640.html#2ZyQEuVMR

129. *Михайлов Т. А.* Эволюция геополитических идей / Т. А. Михайлов. – М. : б.и.,1999. – 179 с.

130. *Момот А. С.* Інформаційні чинники впливу на сталий розвиток світосистеми // А. С. Момот // Нова парадигма. – 2011. – Вип. 104. – С. 67–77.

131. *На Black* Hat запретили рассказывать о возможностях китайской кибермии [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/396433.php

132. *На защиту* компьютерных сетей США потратят 233 млн долларов [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/404983.php?sphrase_id=1139540

133. *Напрями* діяльності ГУР МОУ [Електронний ресурс]. – Режим доступу: http://www.gur.mil.gov.ua/content/directions.html

134. *Наступает* время кибертерроризма, кибероружия и кибервойн. – Касперский [Електронний ресурс]. – Режим доступу: http://www.iplife.com.ua/news/stuxnet-kasperskiy

135. *НАТО* в 2020 году: Гарантированная безопасность, динамичное взаимодействие [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/ru/natolive/official_texts_63654.htm

136. *О второй* международной встрече высоких представителей, курирующих вопросы безопасности [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/news/674.html

137. *О третьей* международной встрече высоких представителей, курирующих вопросы безопасности [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/news/720.html

138. *О чем* будут говорить на американо-китайском саммите Барак Обама и Си Цзиньпин? [Електронний ресурс]. – Режим доступу: http://www.mk.ru/politics/world/article/2013/06/02/3-o-chem-budut-govorit-na-amerikanokitayskom-sammite-barak-obama-i-si-tszinpin.html

139. *О'Туатайл Г.* Геополитические условия постмодерна: государства, государственное управление и безопасность в новом тысячелетии / Герард О'Туатайл [Електронний ресурс]. – Режим доступу: http://www.geopolitica.ru/article/geopoliticheskie-usloviya-post-moderna-gosudarstva-gosudarstvennoe-upravlenie-i-bezopasnost-v#.UgxGIawRTDd

140. *Оборонные* предприятия Японии и США могли атаковать одни и те же хакеры [Електронний ресурс]. – Режим доступу: http://digit.ru/it/20110927/384386034.html#ixzz2wVkrcsWp

141. *ОБСЕ* обеспокоена желанием Узбекистана контролировать интернет [Електронний ресурс]. – Режим доступу: http://www.uznews.net/news_single.php?nid=18024

142. О*жеван М. А.* Доктрина Барака Обами: нова «стратегія національної безпеки» США / М. А. Ожеван, Д. В. Дубов // Актуальні проблеми міжнар. відносин. – 2010. – Вип. 94; Ч І. – С. 16–20.

143. *Ожеван М.* Спроби впровадження міжнародного контролю за діяльністю в Інтернеті під егідою ООН: нові можливості реалізації Україною інформаційного суверенітету / М. Ожеван [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1093/

144. *Олійник О.* Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави / О. Олійник, О. Соснін, Л. Шиманський [Електронний ресурс]. – Режим доступу: http://old.niss.gov.ua/book/Sosnin_2.htm

145. *Операция* 'Red October' – обширная сеть кибершпионажа против дипломатических и государственных структур [Електронний ресурс]. – Режим доступу: http://www.securelist.com/ru/blog/207764382/Operatsiya_Red_October_obshirnaya_set_kibershpionazha_protiv_diplomaticheskikh_i_gosudarstvennykh_struktur

146. *Определение* агрессии : утв. Резолюцией 3314 (XXIX) Генеральной Ассамблеи ООН 14 декабря 1974 года [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml

147. *Определения* и терминология, связанные с укреплением доверия и безопасности при использовании информационно-коммуникационных технологий // Резолюция МСЭ 181 (новая) [Електронний ресурс]. – Режим доступу: http://www.itu.int/net/itunews/issues/2010/09/20-ru.aspx

148. *Основні* завдання Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=-89831&cat_id=89828

149. *Основы* государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/114.html

150. *От масштабной* кибератаки пострадали компьютеры ведущей корпорации Японии Mitsubishi Heavy Industries [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/19sep2011/mitsubishi

151. *Отчет* о доступности сервисов и данных [Електронний ресурс]. – Режим доступу: http://www.google.com/transparencyreport/removals/government/countries/?t=table&p=2012-12&r=CH

152. *Отчет* о Тунисском этапе Всемирной встречи на высшем уровне по вопросам информационного общества, Тунис, Kram Palexpo, 16–18 ноября 2005 года / ООН [Електронний ресурс]. – Режим доступу: http://www.itu.int/wsis/docs245/tunis/off/97rev179-ru.doc

153. *Отчет* о Тунисском этапе Всемирной встречи на высшем уровне по вопросам информационного общества / Исполнительный комітет СНГ [Електронний ресурс]. – Режим доступу: http://cis.minsk.by/page.php?id=3536

154. *Панченко Ж. О.* Геополітичне позиціонування України в процесах євроінтеграції : автореф. дис. ... к.політ.н. : 23.00.03 / Ж. О. Панченко; Київ. нац. ун-т ім. Т.Шевченка. – К., 2006. – 19 с.

155. *Парахонський Б.* Концептуальні засади зовнішньополітичної стратегії України : аналіт. доп. / Б. Парахонський, Г. Яворська. – К. : НІСД, 2011. – 41 с.

156. *Паркер Ж.* Преемственность и изменения геополитической мысли Запада / Ж. Паркер // Междунар. журн. соц. наук. – 1993. – № 3. – С. 22–30.

157. *Пентагон* вложит 500 млн долларов в исследования в области кибербезопасности [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/404867.php?sphrase_id=1139540,

158. *План* действий ВСИО [Електронний ресурс]. – Режим доступу: http://www.un.org/russian/conferen/wsis/plan.pdf

159. *Погорецький М.* Поняття кіберпростору як середовища вчинення злочинів / М. Погорецький, В. Шеломенцев // Інформаційна безпека людини, суспільства, держави. – 2009. – № 2. – С. 77–81.

160. *Полный* текст доклада, с которым выступил Ху Цзиньтао на 18-м съезде КПК [Електронний ресурс]. – Режим доступу: http://www.cntv.ru/2012/11/19/ARTI1353295006286632.shtml

161. *Понимание* киберпреступности : руководство для развивающихся стран [Електронний ресурс]. – Режим доступу: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf

162. *Порфирович О.* Віртуальний криміналітет: від хакера до терориста (портрет явища) / О. Порфирович // Актуальні питання масової комунікації. – Вип. 9. – 2008. – С. 25–34.

163. *Почему* Китай создал «сетевую синюю армию»? // Жэньминь Жибао [Електронний ресурс]. – Режим доступу: http://russian.people.com.cn/31521/7421675.html

164. *Пояснювальна* записка до проекту Закону України «Про внесення змін до деяких законів України щодо структури та порядку обліку кадрів Служби безпеки України» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=41867

165. *Про Воєнну* доктрину України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/648/2004/print-1361272038412688

166. *Про Доктрину* інформаційної безпеки України : указ Президента України від 08.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009

167. *Про засади* внутрішньої і зовнішньої політики : закон України від 01.07.2010 р. № 2411–VI [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2411–17

168. *Про затвердження* Річної національної програми співробітництва Україна – НАТО на 2012 рік [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/14697.html

169. *Про Концепцію* Національної програми інформатизації : закон України від 4.02.1998 р. № 75/98-ВР) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/75/98-%D0%B2%%80

170. *Про кібернетичну* безпеку України : Проект закону [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240

171. *Про основи* національної безпеки України : закон України від 19.06.2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

172. *Про Стратегію* національної безпеки України // Офіційний вісник України. – 2007. – № 11. – С. 7.

173. *Продажи* кибероружия будут ограничены [Електронний ресурс]. – Режим доступу: http://www.3dnews.ru/788165

174. *Промова* Державного секретаря Гілларі Клінтон на конференції про свободу в інтернеті [Електронний ресурс]. – Режим доступу: http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html

175. *Путин* обсудил с премьером Индии тему международного терроризма... [Електронний ресурс]. – Режим доступу: http://www.newsru.com/arch/russia/21oct2013/put_ter.html

176. *Резолюция* 50 – Кибербезопасность / Всемирная ассамблея по стандартизации электросвязи, Йоханнесбург, 21–30 окт., 2008 г. [Електронний ресурс]. – Режим доступу: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-R.pdf

177. *Романчук Ю. В.* Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти : дис. ... к.політ.н. : 23.00.04 / Ю. В. Романчук. – К. : Ін-т світ. екон. та міжнар. віднос., 2009. – 203 с.

178. *Димлевич Н.* Россия – Болгария: информационное сотрудничество и информационная безопасность / Н. Димлевич [Електронний ресурс]. – Режим доступу: http://www.fondsk.ru/article.php?id=2506

179. *Россия* и США обсуждают кибербезопасность [Електронний ресурс]. – Режим доступу: http://www.cybersecurity.ru/armament/83820.html

180. *Россия,* США и Китай могут воссоздать «Красный телефон» в киберпространстве [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/423808.php

181. *Русанова М. І.* Постімперська геостратегія Великої Британії: глобальна стратегія Кінгстона-Маклорі / М. І. Русанова // Політологічний вісник. – 2012. – № 60. – С. 429–437.

182. *Siemens* призналась в распространении Stuxnet [Електронний ресурс]. – Режим доступу: http://www.xakep.ru/post/53423/

183. *Sony* извинилась за утечку личных данных 77 млн клиентов сети PlayStation [Електронний ресурс]. – Режим доступу: http://www.rbc.ua/rus/top/show/sony-izvinilas-za-utechku-lichnyh-dannyh-77-mln-klientov-seti-01052011150000

184. *Spiegel* обвинил Китай в шпионской кибер-атаке на правительство Германии» [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/27Aug2007/china

185. *Stuxnet* против центрифуг: в США выходит книга о кибервойне против Ирана [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/04jun2012/dvdsanger

186. *Stuxnet:* война 2.0. [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/105964/

187. *Самый* строгий антипиратский закон смягчили [Електронний ресурс]. – Режим доступу: http://therunet.com/news/1045-samyy-strogiy-antipiratskiy-zakon-smyagchili

188. *СБУ:* Головні проблеми для України – тероризм і кіберзлочинність [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/

189. *Седаков П.* Первый украинский киберфронт: кто и зачем объявил IT-мобилизацию? / П. Седаков, Д. Филонов [Електронний ресурс]. – Режим доступу: http://www.forbes.ru/tekhnologii/internet-i-svyaz/251623-pervyi-ukrainskii-kiberfront-kto-i-zachem-obyavil-it-mobilizatsi

190. *Смарт-позиция*, «3D» и гибкая дипломатия администрации Обамы [Електронний ресурс]. – Режим доступу: http://russian.people.com.cn/95181/6675672.html

191. *Сноуден* сделал правильный ход [Електронний ресурс]. – Режим доступу: http://www.inosmi.ru/world/20130627/210428985.html

192. *Створення* глобальної культури кібербезпеки : резолюция A/RES/57/239 [Електронний ресурс]. – Режим доступу: http://daccess-

dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement

193. *Страны* защищают компьютерные сети и веб-сайты [Електронний ресурс]. – Режим доступу: http://www.america.gov/st/peacesec-russian/2009/October/20091002140506sjhtrop0.8408167.html

194. *Стратегічний* оборонний бюлетень України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/771/2012/print1361272038412688

195. *США* готовы ответить на атаки хакеров военным ударом – заявил Пентагон [Електронний ресурс]. – Режим доступу: http://www.newsru.com/world/13may2010/cybercommand.html

196. *США* и Китай обсудят правила кибершпионажа [Електронний ресурс]. – Режим доступу: http://www.pd.rsoc.ru/press-service/subject1/news2161.htm

197. *США* и Россия усиливают сотрудничество по кибербезопасности [Електронний ресурс]. – Режим доступу: http://inosmi.ru/social/20111005/175569908.html

198. *США* признались в применении кибероружия [Електронний ресурс]. – Режим доступу: http://news.nur.kz/207185.html

199. *Сяотун Юй*. Стратегический баланс сил в АТР на рубеже XX–XXI вв. : автореф. дис.. ... к.політ.н. : 23.00.04 / Юй Сяотун [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/strategicheskii-balans-sil-v-atr-na-rubezhe-xx-xxi-vv

200. *У США* трудности с партнерами по противодействию киберугрозам [Електронний ресурс]. – Режим доступу: vestnik-sviazy.ru

201. *Україна* у світі, що змінюється : стратегія національної безпеки України // Офіційний вісник України. – 2007. – № 11. – С. 7.

202. *Український* мережевий інформаційний центр [Електронний ресурс]. – Режим доступу: http://uanic.net/

203. *Уотермэн Ш*. Компьютерный вирус Duqu угрожает важнейшим промышленным объектам / Ш. Уотермэн [Електронний ресурс]. – Режим доступу: http://www.inosmi.ru/usa/20111025/176563164.html

204. *Управления* общего учета США обвиняет Пентагон в нерациональном финансировании ИТ-проектов [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/398149.php?sphrase_id=1139696

205. *Управління* боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754

206. *Устав* Организации Объединенных Наций [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/charter/index.shtml

207. *F-Secure:* Человечество стоит на пороге развития гонки кибервооружения [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/428659.php

208. *ФБР* получит $ 234 миллиона на новые средства слежки за Интернетом [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/15jun2009/fbi

209. *Федорова Ю.* Структурування та інноваційна вербалізація понятєвих вузлів англомовної картини світу у галузі комп'ютерних технологій / Юлія Федорова // Наук. зап. Кіровоград. держ. пед. ун-ту імені Володимира Винниченка. – 2009. – С. 56–59. – (Сер. Філологічні науки; вип. 81(4).210).

210. *Федорук П.* Культурно-цивілізаційний контекст геополітичних пріоритетів України / П. Федорук // Нова парадигма. – 2012. – Вип. 107. – С. 181–191.

211. *Феоктистов В. М.* Культурно-цивилизационные ценности концепции национальной безопасности КНР в условиях глобализации : автореф. дис. ... к.філос.н. : 09.00.13 / В. М. Феоктистов [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/kulturno-tsivilizatsionnye-tsennosti-kontseptsii-natsionalnoi-bezopasnosti-knr-v-usloviyakh-

212. *Формирование* организационно-правовой системы защиты национальной инфраструктуры от киберугроз / В. В. Бик, А. А. Климчук, В. Н. Панченко, В. В. Петров. – К. : Академпресс, 2013. – 200 с.

213. *Хакеры* взломали доступ к самому дорогому проекту Пентагона [Електронний ресурс]. – Режим доступу: http://top.rbc.ru/society/21/04/2009/295893.shtml

214. *Хакеры* взломали сайт Госдумы РФ и украсили его лозунгом «Слава Украине!» [Електронний ресурс]. – Режим доступу: http://ru.tsn.ua/politika/hakery-vzlomali-sayt-gosdumy-rf-i-ukrasili-ego-lozungom-slava-ukraine-360843.html

215. *Хакеры* украсили официальный сайт Госдумы лозунгом «Слава Украине!» [Електронний ресурс]. – Режим доступу: http://www.unian.net/politics/906584-hakeryi-ukrasili-ofitsialnyiy-sayt-gosdumyi-lozungom-slava-ukraine.html

216. *Халецька Л.* Еволюція поняття «могутність» у політичній думці Франції кінця XX – початку XHI століття / Л. Халецька //

Дослідження світової політики : зб. наук. праць. – 2011. – Вип. 2. – С. 177–188.

217. *Хилдрет С. А.* Кибертерроризм : материалы Исследовательской службы Конгресса // Кибервойна : доклад Исследовательской службы Конгресса RL30735 / С. А. Хилдрет [Електронний ресурс]. – Режим доступу: http://www.infousa.ru/information/bt-1028.htm.

218. *Цыганков П. А.* Геополитика: последнее прибежище разума? / П. А. Цыганков // Вопросы философии. – 1994. – № 7–8 [Електронний ресурс]. – Режим доступу: http://philosophy.ru/library/vopros/66.html

219. *Цымбурский В.* Геополитика как мировидение и род занятий // Русский Архипелаг. Сетевой проект Русского Мира / В. *Цымбурский* [Електронний ресурс]. – Режим доступу: http://www.archipelag.ru/text/196.htm

220. *Цымбурский В. Л.* Остров Россия. Геополитические и геохронологические работы. 1993–2006 / В. Л. Цымбурский. – М. : РОССПЭН, 2007. – 544 с.

221. *Червь* Stuxnet [Електронний ресурс]. – Режим доступу: http://www.symantec.com/ru/ru/theme.jsp?themeid=stuxnet

222. *Черненко Е.* Холодная война 2.0? // Россия в глобальной политике / Е. Черненко [Електронний ресурс]. – Режим доступу: http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874

223. *Что это* там был за Wiper? [Електронний ресурс]. – Режим доступу: https://www.securelist.com/ru/blog/207764148/Chto_eto_tam_byl_za_Wiper

224. *«Шпионский»* вирус Flame искал чертежи и PDF-документы на зараженных ПК [Електронний ресурс]. – Режим доступу: http://www.digit.ru/technology/20120604/392310510.html

225. *Шевченко М. М.* Еволюція геостратегії держави в контексті цивілізаційних трансформувань другої половини XX століття / М. М. Шевченко // Актуальні проблеми бойового забезпечення авіації та застосування космічних систем : темат. збірн. стат. за мат. наук.-технічн. семінару «Актуальні проблеми створення, застосування та експлуатації авіаційних систем». – К. : НАОУ, 2004. – С. 70–79.

226. *Шевчук О. В.* Зовнішньополітична стратегія США та РФ щодо КНР : автореф. дис. ... д.політ.н. : 23.00.04 / О. В. Шевчук; Ін-т світ. економіки і міжнар. відносин НАН України. – К., 2009. – 33 с.

227. *Шенгенская* интернет-зона: немцы предложили ввести «национальную маршрутизацию» интернета [Електронний ресурс]. – Режим доступу: http://focus.ua/tech/287113/

228. *Эксперимент:* опечатка – тоже угроза безопасности [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/12sep2011/typesquot

229. *Эстония* примет центр НАТО против кибер-атак [Електронний ресурс]. – Режим доступу: http://news.bbc.co.uk/hi/russian/international/newsid_7402000/7402761.stm

230. *Якунин В. И.* Механизм разработки геостратегий в современном российском государстве: На примере транспортно-железнодорожной сферы : автореф. дис.. ... к.політ.н. : 23.00.02 / В. И. Якунин [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/mekhanizm-razrabotki-geostrategii-v-sovremennom-rossiiskom-gosudarstve-na-primere-transportn

231. *A BILL* To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes [Електронний ресурс]. – Режим доступу: http://homeland.house.gov/sites/homeland.house.gov/files/Cybersecurity.pdf

232. *A BILL* To enhance the security and resiliency of the cyber and communications infrastructure of the United States [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf

233. *A Message* About CISPA [Електронний ресурс]. – Режим доступу: http://www.facebook.com/notes/facebook-washington-dc/a-message-about-cispa/10150723305109455

234. *Action* plan to combat high-tech crime [Електронний ресурс]. – Режим доступу: http://www.irational.org/APD/CCIPS/action.htm

235. *Addicott J.* Cyberterrorism: Legal Policy Issues / Jeffrey F. Addicott // Legal Issues in the Struggle against Terrorism / ed. by John N. Moore, Robert F. Turner. – Durham, NC : Carolina Academic Press, 2010. – P. 592.

236. *Air* Force Cyber Command Strategic Vision [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/cgi–bin/GetTRDoc?AD=ADA479060&Location= U2&doc=GetTRDoc.pdf

237. *Alexander B. Keith.* Warfighting in Cyberspace / K. Alexander B. [Електронний ресурс]. – Режим доступу: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf

238. *Alexander* Will Be Last Intel Officer To Head NSA, Hayden Says [Електронний ресурс]. – Режим доступу: http://defense.aol.com/2011/09/07/alexander-will-be-last-intel-officer-to-head-nsa-hayden-says/

239. *Anti M.* Behind the Great Firewall of China / M. Anti [Електронний ресурс]. – Режим доступу: http://www.youtube.com/watch?v=-yrcaHGqTqHk

240. *Arquilla J.* Cyber Fail / John Arquilla // The Foreign Policy [Електронний ресурс]. – Режим доступу: http://www.foreignpolicy.com/articles/2012/09/05/cyber_fail

241. *Average* Attack Bandwidth up 718 percent [Електронний ресурс]. – Режим доступу: http://www.prolexic.com/news-events-pr-giant-ddos-attacks-overwheliming-appliances-isps-carriers-content-delivery-networks-q1-2013-report.html

242. *Beidleman W. S.* Defining and deterring cyber war / Scott W. Beidleman [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf

243. *Bendiek A.* European Cyber Security Policy / Annegret Bendiek [Електронний ресурс]. – Режим доступу: http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf

244. *Blumenthal D.* How to Win a Cyberwar with China / Dan Blumenthal // The Foreign Policy [Електронний ресурс]. – Режим доступу: http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china?page=0,0

245. *Brennan J. O.* Shoring up cyberdefenses / J. O. Brennan // The Washington Post. – 2012. – April 16. – P. A13.

246. *Brenner J.* America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare / J. Brenner. – N. Y. : The Penguin Press, 2011. – 320 p.

247. *Broad W. J.* Israeli Test on Worm Called Crucial in Iran Nuclear Delay / William J. Broad, John Markoff and David E. Sanger // The New York Times. – 2011. – 16 Jan. [Електронний ресурс]. – Режим доступу: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&pagewanted=1

248. *Brown D.* A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Confict / Davis Brown // The Harvard International Law Journal Online [Електронний ресурс]. – Режим доступу: http://www.harvardilj.org/wp-content/uploads/2010/10/HILJ_47-1_Brown.pdf

249. *Brzezinski Z.* Game Plan: A Geostrategic Framework for the Conduct of the U.S.-Soviet Contest / Zbigniew Brzezinski. – Boston : Atheneum, 1986. – 288 p.

250. *Bumgarner J.* Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008 / John Bumgarner and Scott Borg [Електронний ресурс]. – Режим доступу: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

251. *Cameras* Draw Closer to Beijing's Internet Cafes [Електронний ресурс]. – Режим доступу: http://blogs.wsj.com/china-realtime/2008/10/17/cameras-draw-closer-to-beijings-internet-cafes/tab/article/

252. *Candidates* answer cybersecurity questions at CBS [Електронний ресурс]. – Режим доступу: http://dailycaller.com/2011/11/14/candidates-answer-cybersecurity-questions-at-cbsnational-journal-debate/

253. *Carnesale A.* Living with Nuclear Weapons / A. Carnesale. – 5th ed. – Harvard : Harvard University Press, 1983. – 288 p.

254. *Carr J.* Inside Cyber Warfare: Mapping the Cyber Underworld / J. Carr. – 2th. ed. – Sebastopol : O'Reilly Media, Inc., 2010. – 318 p.

255. *Cavelty M. D.* Cyberwar: concept, status quo, and limitations / Myriam Dunn Cavelty [Електронний ресурс]. – Режим доступу: www.sta.ethz.ch

256. *Central* America, Cyber-Security and Electromagnetic Pulse Attack Identified As Overlooked National Security Threats [Електронний ресурс]. – Режим доступу: http://cnsnews.com/news/article/central-america-cyber-security-and-electromagnetic-pulse-attack-identified-overlooked

257. *Chabrow E.* Cybersecurity as a Campaign Issue / E. Chabrow [Електронний ресурс]. – Режим доступу: http://www.govinfosecurity.com/blogs.php?postID=1161&opg=1

258. *Charles J. D., Jr.* Perspectives for cyber strategists on law for cyberwar/ J. D., Jr. Charles // Strategic Studies Quarterly. – 2011. – №5(1). – P. 81–99.

259. *China* accuses US of using cyberwarfare // The Financial Times [Електронний ресурс]. – Режим доступу: http://www.ft.com/cms/s/0/092d5ab6-08fc-11df-ba88-00144feabdc0.html?nclick_check=1

260. *China* becomes biggest net nation [Електронний ресурс]. – Режим доступу: http://news.bbc.co.uk/2/hi/technology/7528396.stm

261. *China* frees journalist jailed over Yahoo emails [Електронний ресурс]. – Режим доступу: http://www.theguardian.com/world/2013/sep/08/shi-tao-china-frees-yahoo

262. *China*, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations [Електронний ресурс]. – Режим доступу: www.fmprc.gov.cn/eng/zxxx/t858978.htm

263. *China's* First Twitter Novel [Електронний ресурс]. – Режим доступу: http://blogs.wsj.com/chinarealtime/2010/03/11/chinas-first-twitter-novel/

264. *China's* National Defense in 2002 [Електронний ресурс]. – Режим доступу: http://www.china.org.cn/e-white/20021209/II.htm

265. *China's* National Defense in 2008 [Електронний ресурс]. – Режим доступу: http://www.fas.org/programs/ssp/nukes/2008Defense-WhitePaper_Jan2009.pdf

266. *China's* Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/full/

267. «*Chinese* government has supported cyberattack...» [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/articles/2010/01/13/the-great-google-coverup.html

268. *Christopher R. Hughes.* The Internet and Censorship in China: Politics of the Digital Leap Forward / Christopher R. Hughes, Gudrun Wacker. – London : Routlege, 2003. – 192 p.

269. *Clarke R.* Cyber War: The Next Threat to National Security and What to Do About It / Richard A. Clarke, Robert K. Knake. – N. Y. : HarperCollins Publishers, 2010. – 320 p.

270. *Clinton H.* Remarks on Internet Freedom [Russian] / H. Clinton [Електронний ресурс]. – Режим доступу: http://www.state.gov/documents/organization/135878.pdf

271. *Convention* on Cybercrime [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?-NT=185&CM=&DF=&CL=ENG

272. *Convention* on Cybercrime : Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy [Електронний ресурс]. – Режим доступу: http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf

273. *Creveld M. van.* Command in War / M. van Creveld. – Cambridge : Harvard University Press, 1985. – 352 p.

274. *Cyber* Atlantic 2011 [Електронний ресурс]. – Режим доступу: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011

275. *Cyber* Cold War Looming for U.S. // USA Today [Електронний ресурс]. – Режим доступу: http://www.questia.com/library/1G1-245805413/cyber-cold-war-looming-for-u-s

276. *Cyber* Cooperation Added To U.S.-Australia Treaty [Електронний ресурс]. – Режим доступу: http://www.officialwire.com/main.php?action=posted_news&rid=44771

277. *Cyber* Defence Exercises [Електронний ресурс]. – Режим доступу: https://www.ccdcoe.org/353.html

278. *Cyber* Defense Exercise [Електронний ресурс]. – Режим доступу: http://www.usna.edu/Cyber/cdx.htm

279. *Cyber* Europe 2012 Key Findings and Recommendations [Електронний ресурс]. – Режим доступу: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report/at_download/fullReport

280. *Cyber* Intelligence Sharing and Protection Act of 2011 [Електронний ресурс]. – Режим доступу: http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523:

281. *Cyber* Security and American Cyber Competitiveness Act of 2011 [Електронний ресурс]. – Режим доступу: http://thomas.loc.gov/cgi-bin/query/z?c112:S.21:

282. *Cyber* Storm: Securing Cyber Space [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/cyber-storm-securing-cyber-space

283. *Cyber* Threats: Law Enforcement and Private Sector Responses [Електронний ресурс]. – Режим доступу: http://www.judiciary.senate.gov/hearings/hearing.cfm?id=0c8be511696c80844b851734969e83e5266d

284. *Cyber-attackers* could have stolen defense contractor's passwords. – 2011 [Електронний ресурс].– Режим доступу: http://ajw.asahi.com/article/economy/technology/AJ2011100813764

285. *Cyberpower* and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. – Washington, D.C. : Potomac Books, 2009. – 642 p.

286. *Cybersecurity* as a Campaign Issue [Електронний ресурс]. – Режим доступу: http://www.govinfosecurity.com/blogs.php?postID=11-61&pg=1

287. *Cyberspace* Policy Review [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_ Review_final.pdf

288. *Cyberspace* Presents Complex Global Challenges [Електронний ресурс]. – Режим доступу: http://www.securityconference.de/Program.425+M58b8d057766.0.html?&L=1

289. *Define* geostatics // Askdefine Online Dictionary [Електронний ресурс]. – Режим доступу: http://geostrategic.askdefine.com/

290. *Demchak Chris C.* Rise of a cybered westphalian age / Chris C. Demchak, Peter Dombrowski // Strategic Studies Quarterly. – 2011. – №5(1). – P. 32–61.

291. *Directorate-General* F. Press Communication Transparency // Digital Civil Rights in Europe [Електронний ресурс]. – Режим доступу: http://www.edri.org/files/cover_note.pdf

292. *Dodds K.* Political geography III: critical geopolitics after ten years / K. Dodds // Progress in Human Geography. – 2001. – P. 469–484.

293. *Dodson E.* Cracks in the Golden Shield: the rising challenge of expanding chinese internet censorship technologies / E. Kathleen Dodson [Електронний ресурс]. – Режим доступу: http://repository.library.georgetown.edu/bitstream/handle/10822/553476/dodsonElizabeth.pdf?sequence=1

294. *Dolman E. C.* New Frontiers, Old Realities / Everett Carl Dolman // Strategic Studies Quarterly 6.1. – 2012; spring. – P. 78–96.

295. *Duhigg C.* How the U.S. Lost Out on iPhone Work / C. Duhigg // The New York Times [Електронний ресурс]. – Режим доступу: http://www.nytimes.com/2012/01/22/business/apple-america-and-a-squeezed-middle-class.html?_r=4&pagewanted=all&

296. *Efferink L. van* The Definition of Geopolitics – Classical, French and Critical Traditions / Leonhardt van Efferink [Електронний ресурс]. – Режим доступу: http://www.exploringgeopolitics.org/Publication_Efferink_van_Leonhardt_The_Definition_of_Geopolitics_Classicial_French_Critical.html

297. *EU* Cybersecurity plan to protect open internet and online freedom and opportunity [Електронний ресурс]. – Режим доступу: http://europa.eu/rapid/press-release_IP-13-94_en.htm

298. *Exposing* One of China's Cyber Espionage Units [Електронний ресурс]. – Режим доступу: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

299. *Fact* sheet: Mitt Romneys Strategy ensure American century [Електронний ресурс]. – Режим доступу: http://www.mittromney.com/blogs/mitts-view/2011/10/fact-sheet-mitt-romneys-strategy-ensure-american-century

300. *Fahrenkrug T. D.* Cyberspace Defined / T. D. Fahrenkrug [Електронний ресурс]. – Режим доступу: http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

301. *Fallows J.* China's Internet Censorship is Effective / James Fallows // Censorship: Opposing Viewpoints / ed. by Scott Barbour. – Farmington Hills, MI : Greenhaven Press, 2010. – 217 p.

302. *First* pan-European cyber security simulation [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/dgs/jrc/index.cfm?id=2820&obj_id=561&dt_code=HLN&lang=en

303. *Foreign* Ministry Spokesperson Hong Lei's Regular Press Conference. – 2011 [Електронний ресурс]. – Режим доступу: http://www.fmprc.gov.cn/eng/xwfw/s2510/2511/t861151.htm

304. *Foreign* Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on «Internet Freedom» [Електронний ресурс]. – Режим доступу: http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t653351.htm

305. *G8* Foreign Ministers' meeting statement [Електронний ресурс]. – Режим доступу: http://www.g8.utoronto.ca/foreign/formin-130411.html

306. *Gauss:* Nation-state cyber-surveillance meets banking Trojan [Електронний ресурс]. – Режим доступу: http://www.securelist.com/en/blog?weblogid=208193767

307. *Gayle D.* Obama BANS U.S. government from buying Chinese-made computer technology over cyber-attack fears / Damien Gayle [Електронний ресурс]. – Режим доступу: http://www.dailymail.co.uk/news/article-2300518/Obama-BANS-U-S-government-buying-Chinese-technology-cyber-attack-fears.html

308. *Goodin D.* Hackers of Japanese military contractor fluent in Chinese / Dan Goodin [Електронний ресурс]. – Режим доступу: http://www.theregister.co.uk/2011/09/22/japan_military_hack_follow_up/

309. *Google* может прекратить работу в Китае [Електронний ресурс. – Режим доступу: http://www.securitylab.ru/news/389714.php

310. *Górecki P.* Cyberatak na Ukrainę. Trudno będzie udowodnić, że to Rosja / Paweł Górecki // Gazecie Wyborczej [Електронний ресурс]. – Режим доступу: http://wyborcza.pl/1,75477,15614511,Cyberatak_na_Ukraine__Trudno_bedzie_udowodnic__ze.html#ixzz2vqhakLz

311. *Gorman S.* U.S. Plans Cyber Shield for Utilities, Companies / S. Gorman [Електронний ресурс]. – Режим доступу: http://online.wsj.com/news/articles/SB10001424052748704545004575352983850463 10

8?mg= reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704545004575352983850463108.html

312. *Halliday J.* WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank / Josh Halliday // The Guardian. – 2011 [Електронний ресурс]. – Режим доступу: http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear

313. *Harth A.* Geopolitics and grand strategy: Foundations of American national security / Anthony Christian Harth. – University of Pennsylvania : ProQuest, UMI Dissertations Publishing, 2003. – 463 p.

314. *Harwit E.* Government Policy and Political Control over China's Internet / Eric Harwit and Duncan Clark // Chinese Cyberspaces: Technological Changes and Political Effects / eds. Jens Damm and Simona Thomas. – N.Y. : Routlege, 2006. – 204 p.

315. *Hearing* to receive testimony on U.S. Strategic Command and U.S. Cyber Command in review of the defense authorization request for fiscal year 2013 and the future years defense program [Електронний ресурс]. – Режим доступу: http://armed-services.senate.gov/Transcripts/2012/03%20March/12-19%20-%203-27–12.pdf

316. *Hersh S. M.* The Online Threat / Seymour M. Hersh // The New Yorker [Електронний ресурс]. – Режим доступу: http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all

317. *Horgan J.* Don't Believe Scare Stories about Cyber War / John Horgan [Електронний ресурс]. – Режим доступу: http://blogs.scientificamerican.com/cross-check/2011/06/03/dont-believe-scare-stories-about-cyber-war/

318. *House J. D.* Internet censorship in China / Joseph David House [Електронний ресурс]. – Режим доступу: http://aladinrc.wrlc.org/handle/1961/11051

319. *House* to take up cybersecurity bill with revisions / Diane Bartz [Електронний ресурс]. – Режим доступу: http://feeds.reuters.com/~r/reuters/technologyNews/~3/qnWZadguowc/us-cybersecurity-congress-idUSBRE8391FY20120410

320. *How* Censorship Works in China : A Brief Overview [Електронний ресурс]. – Режим доступу: http://www.hrw.org/reports/2006/china0806/3.htm

321. *Hulme G. V.* Industry on Cybersecurity Act of 2012: Not so fast / G. V. Hulme [Електронний ресурс]. – Режим доступу: http://www.csoonline.com/article/700595/industry-on-cybersecurity-act-of-2012-not-so-fast

322. *IGF*. Funding [Електронний ресурс]. – Режим доступу: http://www.intgovforum.org/cms/funding

323. *India*, US ink an agreement on cyber security [Електронний ресурс]. – Режим доступу: http://www.infowar-monitor.net/2011/07/india-us-ink-an-agreement-on-cyber-security/

324. *Information* Operations : Joint Publication 3–13, 27 Nowember, 2012 [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

325. *International* Strategy for Cyberspace [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

326. *Internet* World Stats – Internet Usage in Asia [Електронний ресурс]. – Режим доступу: http://www.internetworldstats.com/

327. *ITU-T* X.1205 (04/2008) [Електронний ресурс]. – Режим доступу: http://handle.itu.int/11.1002/1000/9136-en

328. *Janczewski L. J.* Cyber Warfare and Cyber Terrorism / Lech J. Janczewski, Andrew M. Colarik. – Hershey, PA : Information Science Reference, 2008. – 532 p.

329. *Japan* cyber attack silence may breach arms contracts [Електронний ресурс]. – Режим доступу: http://ajw.asahi.com/article/economy/AJ2011092011372

330. *Japan* to prep for cyber-attack by sending 'infected' e-mail to staff [Електронний ресурс]. – Режим доступу: http://news.asiaone.com/News/Latest%2BNews/Science%2Band%2BTech/Story/A1Story20111008-303888.html

331. *Japans* Mitsubishi Heavy Industries by hackersbut not a secret leaked [Електронний ресурс]. – Режим доступу: http://www.newso.org/ITNews/Trade/Japans-mitsubishi-heavy-industries-by-hackersbut-not-a-secret-leaked/490e790d-2300-4e48-a256-519a6fae6677

332. *Japan-U.S.* : Defense Ministers' Joint Press Conference. – 2011[Електронний ресурс].– Режим доступу: http://www.mod.go.jp/e/pressconf/2011/10/111025_japan_us.html

333. *Jeffrey L. C.* Cyberdeterrence and cyberwar / L. C. Jeffrey // Strategic Studies Quarterly. – 2011. – № 5(1). – P. 148–150.

334. *Jellenc E.* Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory / Eli Jellenc // Proseedings of the 11th European Conference on Information Warfare and Security, July 5–6, 2012 [Електронний ресурс]. – Режим доступу: http://academic-conferences.org/pdfs/ECIW_2012-Abstract-booklet.pdf

335. *Joint* meeting of the Law Enforcement Working Party and the Customs Cooperation Working Part [Електронний ресурс]. – Режим доступу: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%20 7181%202011%20INIT

336. *Jones T. Y.* Cyber attacks hurt China's credibility: U.S. official / T. Y Jones [Електронний ресурс]. – Режим доступу: http://uk.reuters.com/article/2013/04/09/us-china-usa-cyber-idUKBRE93806620130409

337. *Kash W.* Lessons from the cyberattacks on Estonia / Wyatt Kash [Електронний ресурс]. – Режим доступу: http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx

338. *Klimburg A.* The Whole of Nation in Cyberpower / Alexander Klimburg [Електронний ресурс]. – Режим доступу: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/News/The_Whole_of_Nation_in_Cyberpower_AK.pdf

339. *Kramer D. F.* Cyber Influence and International Security / D. F. Kramer, L.Wentz // Defense Horizons. – 2008. – № 61. – P. 1–11 [Електронний ресурс]. – Режим доступу: http://www.carlisle.army.mil/DIME/documents/Kramer%20and%20 Wentz%20Cyber%20 Influence%20and%20International%20Security%5D.pdf

340. *Krauthammer C.* The irrelevance of START / Charles Krauthammer // The Washington Post [Електронний ресурс]. – Режим доступу: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/25/AR2010112502232.html

341. *Krebs B.* DHS Seeking 1,000 Cyber Security Experts / B. Krebs // The Washington Post [Електронний ресурс]. – Режим доступу: http://voices.washingtonpost.com/securityfix/2009/10/dhs_seeking_1000_cyber_securit.html

342. *Kremlin* website hit by "powerful" cyber attack [Електронний ресурс]. – Режим доступу: http://www.reuters.com/article/2014/03/14/russia-kremlin-cybercrime-idUSL6N0MB2B620140314

343. *Kroes N.* EU firewall? The EU Commission has NO such intentions! / *N. Kroes* [Електронний ресурс]. – Режим доступу: https://twitter.com/NeelieKroesEU/status/70835778216931328

344. *Lawrence L.* Cyberwarfare a Viable Nonviolent Alternative to Military Strikes / L. Lawrence, Jr. Muir [Електронний ресурс]. – Режим доступу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-a-viable-nonviolent-alternative-to-military-strikes

345. *Lawson S.* Cyberwarfare Treaty Would Be Premature, Unnecessary, and Ineffective / Sean Lawson [Електронний ресурс]. – Режим доступу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-treaty-would-be-premature-unnecessary-and-ineffective

346. *Lewis J.* A Cybersecurity Treaty Is a Bad Idea / James Lewis [Електронний ресурс]. – Режим доступу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/a-cybersecurity-treaty-is-a-bad-idea

347. *Li Z.* A Chinese perspective on cyber war / Li Zhang // International Review of the Red Cross. New Technologies and Warfare. – 2012. – Jun. – P. 801–807.

348. *Libicki M.* Cyberdeterrence and Cyberwar / Martin C. Libicki. – Washington D. C. : RAND Corporation, 2009. – 238 p.

349. *Libicki M.* Cyberwar as a Confidence Game / Martin C. Libicki // Strategic Studies Quarterly. – 2011. – № 5(1). – P. 132–146.

350. *Libicki M.* Setting International Norms on Cyberwar Might Beat a Treaty / Martin Libicki [Електронний ресурс]. – Режим доступу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty

351. *Libisky M.* The Emerging Primacy of Information / M. Libisky // Orbis. – 1996. – 40/2. – P. 261–276.

352. *Liepman M. J., Jr.* Cyberspace: The Third Domain / James M. Liepman, Jr. [Електронний ресурс]. – Режим доступу: https://www.hsdl.org/?view&doc=89385&coll=public

353. *Lin H.* Escalation dynamics and conflict termination in cyberspace / H. Lin // Strategic Studies Quarterly. – 2012. – № 6(3). – 46–70.

354. *Lindsay J.* International Cyberwar Treaty Would Quickly Be Hacked to Bits / Jon Lindsay [Електронний ресурс]. – Режим доступу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/international-cyberwar-treaty-would-quickly-be-hacked-to-bits

355. *Lockheed* wins $31M cyber contract [Електронний ресурс]. – Режим доступу: http://www.bizjournals.com/washington/stories/2009/09/28/daily110.html

356. *London* hosts cyberspace security conference [Електронний ресурс]. – Режим доступу: http://www.bbc.co.uk/news/technology-15533786

357. *Lynn W. J.* Defending A New Domain: The Pentagon's Cyberstrategy / William J. Lynn // Foreign Affairs. – 2010. – September/ October [Електронний ресурс]. – Режим доступу: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

358. *Lyons D.* China's Golden Shield Project: myths, realities and context / D. Lyons [Електронний ресурс]. – Режим доступу: http://www.scribd.com/doc/15919071/Dave-Lyons-Chinas-Golden-Shield-Project

359. *MacDonald F.* Anti-Astropolitik – outer space and the orbit of geography / Fraser MacDonald // Progress in Human Geography. – 2007. – № 31. – P. 592–615.

360. *MacKinnon R.* China's new online video regulation: reading the tea leaves / Rebecca MacKinnon [Електронний ресурс]. – Режим доступу: http://rconversation.blogs.com/rconversation/2008/01/chinas-new-onli.html

361. *MacKinnon R.* China's «Green Dam Youth Escort» software / R. MacKinnon [Електронний ресурс]. – Режим доступу: http://rconversation.blogs.com/rconversation/2009/06/chinas-green-dam-youth-escort-software.html

362. *Maher K.* The New Westphalian Web Web / Katherine Maher // Foreign Policy [Електронний ресурс]. – Режим доступу: http://www.foreignpolicy.com/articles/2013/02/25/the_new_westphalian_web

363. *Matsubara M.* Japan's Cybercrime Problem / Mihoko Matsubara // The Diplomat [Електронний ресурс]. – Режим доступу: http://thediplomat.com/2011/07/japans-cybercrime-problem/

364. *McConnell M.* How to Win the Cyber-war. We're Loosing / Mike McConnell // The Washington Post [Електронний ресурс]. – Режим доступу: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

365. *Media* watchdog concerned over US cyber security bill : BBC Monitoring World Media Supplied by BBC Worldwide Monitoring, April 9, 2012 [Електронний ресурс]. – Режим доступу: http://www.accessmylibrary.com/article-1G1-285841675/media-watchdog-concerned-over.html

366. *Meena K.* What is the difference between geo-politics and geo-strategy? / Krishnendra Meena [Електронний ресурс]. – Режим доступу: http://idsa.in/askanexpert/geopoliticsandgeostrategy

367. *Miles D.* Gates Establishes New Cyber Subcommand / D. Miles [Електронний ресурс]. – Режим доступу: http://www.defenselink.mil//news/newsarticle.aspx?id=54890

368. *Military* and Security Deployments Involving the People's Republic of China [Електронний ресурс]. – Режим доступу: http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf

369. *Military* and Security Developments Involving the People's Republic of China 2013 / Departament of Defence [Електронний ресурс]. – Режим доступу: http://www.cfr.org/china/department-defense-military-security-developments-involving-peoples-republic-china/p28408

370. *Missile* Data Targeted in Mitsubishi Heavy Cyber Attack // India Gazette [Електронний ресурс]. – Режим доступу: http://www.indiagazette.com/index.php/sid/49315126/scat/5e8a9e9456185a7e#sthash.58YWkFKz.dpuf

371. *Mulvenon J.* Golden Shields and Panopticons: Beijing's Evolving Internet Control Policies / James Mulvenon // Georgetown Journal of International Affairs. – 2008. – Summer; 9.2. – P. 115–120.

372. *Nakashima E.* Stuxnet was work of U.S. and Israeli experts, officials say / Ellen Nakashima and Joby Warrick // The Washington Post [Електронний ресурс]. – Режим доступу: http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials

373. *National* Cyberspace Strategy [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

374. *National* Military Strategy for Cyberspace Operations [Електронний ресурс]. – Режим доступу: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

375. *National* Plan for Information Systems Protection [Електронний ресурс]. – Режим доступу: www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

376. *National* Security Strategy USA [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

377. *Nations* discuss cyber security, November 1st, 2011 [Електронний ресурс]. – Режим доступу: http://www.cyberwarnews.info/2011/11/01/nations-discuss-cyber-security/

378. *NATO* Defence Ministers adopt new cyber defence policy [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/en/natolive/news_75195.htm

379. *Nazario J.* Estonian DDoS Attacks – A summary to date / Jose Nazario [Електронний ресурс]. – Режим доступу: http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

380. *New Romney* adviser: NSA key to ensuring cybersecurity [Електронний ресурс]. – Режим доступу: http://www.nextgov.com/nextgov/ng_20111007_3294.php

381. *NSA leak:* Source believes exposure, consequences inevitable // Washington Post [Електронний ресурс]. – Режим доступу: http://www.washingtonpost.com/video/thefold/nsa-leak-source-believes-exposure-consequences-inevitable/2013/06/07/fb15c0fe-cf94-11e2-8845-d970ccb04497_video.html

382. *NSA* slides explain the PRISM data-collection program // Washington Post [Електронний ресурс]. – Режим доступу: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

383. *Nye J.* Nuclear lessons for cyber security? / Joseph S. Nye // Strategic Studies Quarterly. – 2011. – № 5(4). – P. 18–38.

384. *Nye J. S., Jr.* The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone / *J. S. Nye Jr.* . – Oxford & N.Y. : Oxford University Press, 2002. – P. 62.

385. *O'Tuathail G.* The Geopolitics Reader / Gearoid O'Tuathail, Simon Dalby, Paul Routledge. – Routledge : s.n., 2006. – 320 p.

386. *Occupying* the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage [Електронний ресурс]. – Режим доступу: http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

387. *Open* letter to President of the UN General Assembly on International Code of Conduct for Information Security [Електронний ресурс]. – Режим доступу: http://www.igcaucus.org/infosecurity-code

388. *Ottis R.* Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective / Rain Ottis [Електронний ресурс]. – Режим доступу: https://docs.google.com/file/d/0B7yq33Gize8yNjEzNDkxMGMtOWMyNS00ZDJhLTg4MDUtZDUwODQ2YjQwOTIw/edit?pli=1&hl=en

389. *Peters R.* China, Democracy, and the Internet / Robert Peters // Information Technology and World Politics / ed. by Michael J. Mazaar. – N.Y : Palgrave MacMillan, 2002. – 192 p.

390. *President* Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview/

391. *President* Obama Names Vivek Kundra Chief Information Officer [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/

392. *Principles* to combat high-tech crime : Communique annex [Електронний ресурс]. – Режим доступу: http://www.irational.org/APD/CCIPS/principles.htm

393. *Protecting* the information society: addressing the phenomenon of cybercrime : Proseedings of the United Nations Conference on Trade and Development [Електронний ресурс]. – Режим доступу: http://unctad.org/en/docs/sdteecb20051ch6_en.pdf

394. *Qiu J. L.* Working-Class Network Society: Communications and the Information Have-Nots in Urban China / Jack Linchuan Qiu. – Cambridge, MA : The MIT Press, 2009. – 320 p.

395. *Radcliff D.* Cyber Cold War / Deb Radcliff // SC Magazine. – 2012. – Sep. – P. 24–26.

396. *Reed J.* DOD requests $4.7 billion to help fund offensive cyber teams / John Reed // The Foreign Policy [Електронний ресурс]. – Режим доступу: http://killerapps.foreignpolicy.com/posts/2013/04/10/dod_cyber_budget_request_increased_to_47_billion_to_help_fund_offensive_cyber_teams

397. *Reed J.* How many cyber troops does the U.S. have? / John Reed // The Foreign Policy [Електронний ресурс]. – Режим доступу: http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have

398. *Remarks* by President Obama and President Xi Jinping of the People's Republic of China after bilateral meeting [Електронний ресурс]. – Режим доступу: http://shanghaiist.com/2013/06/08/transcript_barack_obama_xi_jinping_remarks_bilateral_meeting_sunnyvale_california.php

399. *Remarks* by the President on securing our nation's cyber infrastructure [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

400. *Remarks* by the Vice President at the ceremonial swearing-in of Leon E. Panetta as director of the CIA [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_press_office/Remarks-by-the-Vice-President-at-the-ceremonial-swearing-in-of-Leon-E-Panetta-as-D/

401. *Romney* takes swipe at Obama over new defense strategy // The Hill [Електронний ресурс]. – Режим доступу: thehill.com/...strategy/203457-romney-takes-swipe-at-obama-over-new-defense-strategy

402. *Rothkopf D.* The Cool War / David Rothkopf // The Foreign Policy [Електронний ресурс]. – Режим доступу: http://www.foreignpolicy.com/articles/2013/02/20/the_cool_war_china_cyberwar

403. *Sanger D.* Pentagon plans new arm to wage cyberspace wars / D. Sanger, T. Shanker // The New York Times [Електронний ресурс]. – Режим доступу: http://www.nytimes.com/2009/05/29/us/politics/29cyber.html?_r=1

404. *SARFT*, MII Co-Issue Online Video Regulation [Електронний ресурс]. – Режим доступу: http://www.marbridgeconsulting.com/marbridgedaily/2007-12-29/article/7063/sarft_mii_co_issue_online_video_regulation

405. *Schmitt M. N.* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework / Michael N. Schmitt // Columbia Journal of Transnational Law. – 1998–99. – Vol. 37 [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA471993

406. *Schmitt M. N.* Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict / Michael N. Schmitt // Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US. Policy. – Washington : National Academies Press, 2010.

407. *Schmitt M. N.* The Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. Schmitt [Електронний ресурс]. – Режим доступу: http://www.ccdcoe.org/249.html

408. *Schneier B.* It will soon be too late to stop the cyberwars / Bruce Schneier // Financial Times. – 2010. – 2 Dec. [Електронний ресурс]. – Режим доступу: http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzzl 9cNCeszp

409. *Securing* Cyberspace for the 44th Presidency / ed. by A. J. Lewis [Електронний ресурс]. – Режим доступу: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

410. *Shakarian P.* The 2008 Russian Cyber Campaign Against Georgia / Paulo Shakarian // Military Review. – 2011. – Nov/Dec. – P. 63–68.

411. *Sheldon J. B.* Deciphering cyberpower strategic purpose in peace and war / J. B. Sheldon // Strategic Studies Quarterly. – 2011. – № 5(2). – P. 95–112.

412. *Shirky C.* The Political Power of Social Media / Clay Shirky // Foreign Affairs. – 2011. – № 90. – P. 28–41.

413. *Smith D. J.* Lieberman and McCain, Cybersecurity and Secure IT Bills / David J. Smith [Електронний ресурс]. – Режим доступу: http://pipscyberissues.wordpress.com/2012/03/02/lieberman-and-mccain-cybersecurity-and-secure-it-bills-lets-get-it-right/#more-229

414. *Speech* by Dr. Bernd Pfaffenbach, State Secretary in the Federal Ministry of Economics and Labour of Germany [Електронний ресурс]. – Режим доступу: http://www.itu.int/wsis/tunis/statements/docs/g-germany/1.html

415. *Speech* by H. E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security [Електронний ресурс]. – Режим доступу: http://www.china-un.org/eng/hyyfy/t869445.htm

416. *Statement* by H. E. Mr. Yoshio Utsumi Secretary-general of the International Telecommunication Union [Електронний ресурс]. – Режим доступу: http://www.itu.int/wsis/tunis/statements/docs/io-itu-opening/1.html

417. *Statement* by the President on the White House Organization for Homeland Security and Counterterrorism [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_press_office/Statement-by-the-President-on-the-White-House-Organization-for-Homeland-Security-and-Counterterrorism/

418. *Statement* by Vice premier Huang Ju the State Council of the People's Republic of China [Електронний ресурс]. – Режим доступу: http://www.itu.int/wsis/tunis/statements/docs/g-china/1.html

419. *Stephens W. O.* A History of Sea Power / William Oliver Stephens, Allan Westcott [Електронний ресурс]. – Режим доступу: http://www.gutenberg.org/files/24797/24797-h/24797-h.htm

420. *Strategic* Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation [Електронний ресурс]. – Режим доступу: http://www.nato.int/lisbon2010strategic-concept-2010-eng.pdf

421. *Stuxnet* Questions and Answers [Електронний ресурс]. – Режим доступу: http://www.f-secure.com/weblog/archives/00002040.html

422. *Stuxnet:* Ahmadinejad admits cyberweapon hit Iran nuclear program / Mark Clayton // The Christian Science Monitor. – 2010 [Електронний ресурс]. – Режим доступу: http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program

423. *Sustaining* U. S. Global Leadership: Priorities for 21st Century Defense [Електронний ресурс]. – Режим доступу: http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

424. *Tang L.* New Approaches to Information Security / Lan Tang // Contemporary International Relations. – 2010. – Vol. 20; № 3. – P. 41–49.

425. *Taylor P. A.* From hackers to hacktivists: speed bumps on the global superhighway? / Paul A. Taylor // New Media and Society. – 2005. – Vol. 7; Iss. 5. – P. 625–646.

426. *Text* of Mitt Romney's Speech on Foreign Policy at The Citadel [Електронний ресурс]. – Режим доступу: http://blogs.wsj.com/washwire/2011/10/07/text-of-mitt-romneys-speech-on-foreign-policy-at-the-citadel/

427. *Thackrah J. R.* Dictionary of Terrorism / Thackrah J. R. – NY. : Taylor & Francis, 2004. – 318 p.

428. *The Cold* War is history. Now it's the Cool War // The Guardian [Електронний ресурс]. – Режим доступу: http://www.guardian.co.uk/commentisfree/2013/feb/24/cool-war-cyber-conflict

429. *The Flame:* Questions and Answers [Електронний ресурс]. – Режим доступу: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

430. *The MiniDuke* Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor [Електронний ресурс]. – Режим доступу: http://www.securelist.com/en/downloads/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf

431. *The national* strategy to secure cyberspace [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

432. *The senate* is still trying to jam through its hugely controversial cybersecurity bill [Електронний ресурс]. – Режим доступу: http://bgr.com/2014/06/17/cispa-is-back-2014/

433. *The United* States Cyber Challenge [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%28updated%205-8-09%29.pdf

434. *Thomas J.* Ethics of Hacktivism / Julie Thomas [Електронний ресурс]. – Режим доступу: http://www.giac.org/paper/gsec/530/ethics-hacktivism/101266

435. *Thomas T.* Russian Information-Psychological Actions: Implications for U.S. PSYOP / Timothy Thomas // Special Warfare. – 1997, Winter. – Vol. 10; № 1. – P. 12–19.

436. *Toward* the Single Secure. European Cyberspace [Електронний ресурс]. – Режим доступу: http://www.edri.org/files/virtual_schengen.pdf.

437. *Tracking* GhostNet: Investigating a Cyber Espionage Network [Електронний ресурс]. – Режим доступу: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

438. *U.S.* says worried by cyber-attacks; committed to Asia [Електронний ресурс]. – Режим доступу: http://www.reuters.com/article/2011/06/04/us-singapore-defence-idUSTRE7530O920110604

439. *U.S.-China* Relations: The Obama-Xi California Summit [Електронний ресурс]. – Режим доступу: http://www.brookings.edu/blogs/up-front/posts/2013/06/03-us-china-relations-obama-xi-california-summit-lieberthal

440. *U.S.-JAPAN* SECURITY SUB-COMMITTEE MEETING [Електронний ресурс]. – Режим доступу: http://wikileaks.org/cable/2010/02/10TOKYO228.html

441. *US* embassy cables: Germany ready to support Iran sanctions // The Guardian. – 2011. – 18 Jan. [Електронний ресурс]. – Режим доступу: http://www.guardian.co.uk/world/us-embassy-cables-documents/244617

442. *US* oil industry hit by cyberattacks: Was China involved? [Електронний ресурс]. – Режим доступу: http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

443. *US,* Chinese Presidents Cap Summit with Vows of New Cooperation [Електронний ресурс]. – Режим доступу: http://www.voanews.com/content/us-chinese-presidents-wrap-up-california-summit/1678033.html

444. *VP's* Remarks to London Cyberspace Conference [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace#transcript

445. *W32.Duqu*. The precursor to the next Stuxnet [Електронний ресурс]. – Режим доступу: http://aroundcyber.files.wordpress.com/2012/11/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf

446. *Waugh R.* A very modern theatre of war: The IT men whose mission is to rescue the world from cyberterrorists / Rob Waugh [Електронний ресурс]. – Режим доступу: http://www.dailymail.co.uk/home/moslive/article-1341142/Cyber-attack-The-IT-men-rescue-world-cyberterrorists.html#ixzz19J8v5k4e

447. *What* If There Was a Cold War Between the U.S. and China? [Електронний ресурс]. – Режим доступу: http://world.time.com/2012/11/28/what-if-there-was-a-cold-war-between-the-u-s-and-china/

448. *What* is Flame? [Електронний ресурс]. – Режим доступу: http://www.kaspersky.com/flame

449. *White* House review finds no evidence of spying by Huawei [Електронний ресурс]. – Режим доступу: http://www.reuters.com/article/2012/10/17/us-huawei-spying-idUSBRE89G1Q920121017

450. *Wolchok S.* Analysis of the Green Dam Censorware System / Scott Wolchok, Randy Yao, J. Alex Halderman [Електронний ресурс]. – Режим доступу: http://www.cse.umich.edu/~jhalderm/pub/gd/

451. *Woolley P.* Defining Cyberspace as a United States Air Force Mission / P. Woolley [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453972& Location=U2&-doc=GetTRDoc.pdf

452. *Working* Towards Rules for Governing Cyber Conflict [[[Електронний ресурс]. – Режим доступу: http://dl.dropbox.com/u/869038/US-Russia.pdf

453. *Yannakogeorgos P.* Technogeopolitics of Militarization and Security in Cyberspace / Panayotis Alexander Yannakogeorgos. – s.l.: ProQuest, UMI Dissertation Publishing, 2011. – 288 p.

454. *Zhao Y.* Communication in China: Political Economy, Power, and Conflict / Yuezhi Zhao. – s.l. : Rowan & Littlefield Publishers, 2008. – 384 p.

455. 国务院关于印发»十二五»国家战略性新兴产业发展规划的通知 // Gov.cn. – 2012. – Guo Fa № 28 [Електронний ресурс]. – Режим доступу: http://www.gov.cn/zwgk/2012-07/20/content_2187770.htm

Кіберпростір – середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності.

Кібератака (кібернапад) – цілеспрямовані дії, що реалізуються в кіберпросторі (або за допомогою його технічних можливостей), які призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, спостережності й доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психічний стан громадян).

Кіберзагрози – наявні та потенційно можливі явища й чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури.

Кіберінцидент – подія, яка фактично або потенційно призводить до негативних наслідків роботи інформаційної системи або порушує цілісність інформації, яка в цій системі обробляється, зберігається, передається, і яка може викликати необхідність зворотних дій для пом'якшення наслідків.

Кіберзлочин – суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних і комунікаційних технологій, відповідальність за вчинення якого встановлена кримінальним законодавством.

Кібертероризм – суспільно небезпечна діяльність, що здійснюється в кіберпросторі (або з використанням його технічних можливостей) з терористичною метою і полягає у свідо-

мому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров'я людей.

Кібердиверсія – це суспільно небезпечні діяння в кіберпросторі, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження стратегічних об'єктів у спосіб втручання в роботу інформаційно-телекомунікаційних систем.

Кібершпигунство – передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей з обмеженим доступом, яке здійснюється в кіберпросторі.

Кіберозброєння – спеціально створені для протиправних цілей програмні чи/та апаратні комплекси, спрямовані на несанкціоноване отримання інформації з інформаційно-телекомунікаційних мереж, а також використання таких мереж для контролю над об'єктами, в яких вони використовуються та/чи завдання шкоди таким об'єктам.

Кібервійська – спеціальні підрозділи збройних сил держави, діяльність яких спрямована на централізоване здійснення кібервоєнних операцій (кібервійни), управління й захист військових комп'ютерних мереж.

Кібервійна – використання державою чи групою держав спеціальних засобів (кіберозброєнь) проти країни (групи країн) в кіберпросторі, спрямоване на порушення стабільної роботи інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і мереж об'єктів критичної інфраструктури.

Кібермогутність – здатність до використання кіберпростору для створення переваг і справляння впливу в усіх інших операційних просторах через інструменти могутності.

Кібернетичний (цифровий) суверенітет – здатність держави самостійно й незалежно забезпечувати національні інтереси в кіберсфері, самостійно розпоряджатися власними інформаційними ресурсами та інфраструктурою національного інформаційного простору, а відтак, гарантувати кібернетичну й інформаційну безпеку державі, суспільству та громадянам.

***DDoS*-атаки** – кібератака на обчислювальну систему з метою доведення її до відмови в роботі, тобто створення умов, за яких легальні користувачі системи не можуть отримати доступ до системних ресурсів (сервісів) або цей доступ ускладнений.

Фішинг (англ. *fishing*) – вид злочинної діяльності, метою якого є отримання доступу до персональних даних користувачів за допо-

могою використання сайтів і масових поштових розсилок начебто від імені відомих брендів, знайомих або інших джерел, що можуть викликати в отримувача довіру до змісту сайту (листа).

Соціальна інженерія – використання маніпулятивних заходів (передусім у процесі спілкування зловмисника з жертвою) з метою вивідування даних.

SCADA – програмний комплекс, призначений для розроблення чи забезпечення роботи в режимі реального часу систем збору, оброблення, відображення та архівування інформації про об'єкт моніторингу чи управління. Використовується на системах моніторингу та управління промисловими, інфраструктурними та сервісними процесами на нафтопроводах, електростанціях, потужних системах зв'язку, аеропортах, судах і військових об'єктах.

0*day* (*zeroday*)-уразливість – нові уразливості програмного продукту, які до цього часу не були виявлені жодним із дослідників безпеки.

Бекдор (англ. *back door*) – програма, яка забезпечує зловмиснику можливість повторного доступу до системи «зламаного» комп'ютера.

Хактивізм – використання інформаційно-комунікаційних технологій з метою просування політичних лозунгів і закликів. Найчастіше виражається у формі «зламу» титульної сторінки сайту-цілі з подальшим розміщенням на ній політичних закликів.

Фаєрвол (англ. *firewall*) – пристрій або набір пристроїв (іноді програм), сконфігурованих так, щоб допускати, відмовляти, шифрувати, пропускати через спеціальний елемент (проксі) весь комп'ютерний трафік з набором певних правил та інших критеріїв. Використовується для додаткової захищеності мереж і комп'ютерів від шкідливої інформації чи кібератак.

Операції в комп'ютерних мережах – використання комп'ютерних мереж для атаки на інформацію, розміщену на комп'ютерах і в комп'ютерних мережах, або на самі комп'ютери та мережі.

Закладки (англ. *beetle*) – таємно (несанкціоновано) встановлені в комп'ютерні програми чи апаратну частину елементи, які дозволяють зловмисникам отримати несанкціонований доступ до ресурсів системи.

А

А. Бутузова *12, 47*
А. Вайнштайн *13*
А. Весткотт *44*
А. Гольцов *12, 28*
А. Деркач *260*
А. Клімбург *12, 47, 48*
А. Коларік *12, 75, 76*
А. Крокер *13*
А. Ломанов *13*
А. Малов *204*
А. Маринченко *36*
А. Марченко *12*
А. Мехен *12, 21, 44, 47*
А. Погорецький *72*
А. Рабкін *114*
А. Рафф *13, 103*
А. Соболєв *12*
А. Шупраде *12, 18*

Б

Б. Баді *42*
Б. Клінтон *173*
Б. Мітчел *44*
Б. Обама *10, 15, 48, 53, 54, 56, 57, 91–94, 113, 173–182*
Б. Парахонський *12*
Б. Шнаєр *13, 145*

В

В. Адріанов *12, 20*
В. Бік *245*
Ван Ївей *201*
В. Герасімов *51*
В. Дергачов *12, 26*
В. Кличко *214*
В. Куткін *12, 25*
В. Олійник *261*

В. Петров *12, 13*
В. Пилипчук *12, 13*
В. Рейд *204*
В. Скалацький *13*
В. Стефенс *44*
Ван Цюнь *204*
В. Хлевицький *243*
В. Цимбурський *12, 27*
В. Шарп *13*
В. Шахов *12*
В. Шеломенцев *12, 72*
В. Шерстюк *176, 177*
В. Якунін *12, 18*

Г

Г. Вакер *13, 194*
Г. Галілей *45*
Ген Янишен *53*
Г. Кіссинджер *13, 97*
Г. Раттрей *12, 36, 47, 144*
Г. Рейд *58*
Г. Рейнгольд *13*
Гу Цзянь *110*
Г. Шмідт *53, 181*
Г. Яворська *12*

Д

Д. Аддікотт *13, 145*
Д. Аткінсон *25*
Д. Барлоу *38*
Д. Блюменталь *114*
Д. Браун *13, 151*
Д. Бреннан *57, 175*
Д. Віджесекер *13*
Д. Галушкевич *117*
Д. де Вільпен *42*
Ден Сяопін *92*
Дж. Байден *173, 207*
Дж. Безо *65*

Дж. Бреннер *149*
Дж. Буш-мол. *15, 64, 75, 92, 173, 177, 179*
Дж. Дуе *44*
Дж. Егню *12, 19*
Джек Лінчуан Цю *198*
Д. Жирар *153*
Дж. Ліберман *56, 58*
Дж. Ліндсей *13, 150*
Дж. Ліпман *12, 13, 69, 73*
Дж. Льюїс *12, 13, 70, 150, 179*
Дж. Маккейн *58, 59*
Дж. Менгучі *109*
Дж. Міллер *51*
Дж. Міхаелья *13*
Дж. Най-мол. *12, 13, 15, 42, 141, 142, 152–155, 177*
Дж. Оруелл *10*
Дж. Паркер *12, 27*
Дж. Чарлз *13, 145, 146*
Д. Камерон *13, 207*
Д. Каплан *60*
Д. Куел *12, 71, 74*
Д. Лангрен *61*
Д. Ліндсей *150*
Д. Міхель *12*
Д. Міятович *205*
Д. Мульвенон *13, 193*
Д. Рабкін *114*
Д. Редкліф *13, 102*
Д. Рід *55*
Д. Рокфеллер *56*
Д. Роткопф *13, 101–103*
Д. Томас *115*
Д. Файнстайн *56*
Д. Фахренкург *12*
Д. Шелдон *12, 38, 142, 143, 148*

Е

Е. Голдштейн *96, 99*
Е. Джелленк *13, 103, 105*

Е. Додсон *196*
Е. Долман *12, 13, 17, 26, 98*
Е. Сноуден *68, 94, 99, 221, 226, 228, 254*
Е. Тоффлер *13*
Е. Шмідт *65*

Є

Є. Євдокімов *199*
Є. Замятін *10*
Є. Касперський *130, 136*
Є. Черненко *13*

Ж

Ж. Панченко *12*
Ж. О'Туатайль *12, 22, 23, 24*

З

Зб. Бжезинський *12*

І

І. Ашманов *222, 223*
І. Василенко *12, 25*
І. Данілін *13*
І. Зевельов *13, 92*
І. Кефелі *12, 18, 34*
І. Коротченко *103*
І. Лакосте *12, 23*
І. Ньютон *45*
І. Педак *13*

Й

Й. Суорант *13*
Й. Уцумі *165*

К

К. Александер *13, 53, 56, 59, 174, 176, 181, 205*
К. Гаджієв *12, 23*
К. Демчак *12, 40, 139*

К. Джілібренд *56*
К. Доддс *12, 24, 25*
К. Лагард *65*
К. Лібертал *94*
К. Міна *12, 27*
К. Хаусхофер *12, 18*
К. Ширкі *199*
К. Шмітт *36*

Л

Л. Алманн *117*
Л. Вентц *12, 13, 34*
Л. Жанчевскі *12, 75, 76*
Л. Івашов *99*
Лі Джанг *12, 45, 46*
Лі Куан Ю *15, 201*
Лі Сяомей *204*
Л. Мюїр *13, 150*
Л. Панетта *111, 173*
Л. Сарган *214*
Л. Тенг *152*
Л. Халецька *41*
Лян Гуанлє *111*

М

М. Анті *29, 200, 201*
М. Ахмедініжад *15, 135*
Ма Чжаосю *32*
М. Бангеманн *13*
М. ван Кревельд *148*
М. Гнатюк *12*
М. Гримська *13*
М. Єжеєв *12*
М. Ільїн *12*
М. Каветлі *12, 76, 77*
М. Капур *13*
М. Лібіцкі *12, 70, 74, 143, 150, 156, 157*
М. Макконнелл *157*
М. Маклюен *13, 221*

М. Маркофф *205*
М. Ожеван *12, 13*
М. Олбрайт *51*
М. Погорецький *12*
М. Познер *205*
М. Рижков *12*
М. Роджерс *59*
М. Ромні *178, 179, 180*
М. Русанова *12, 28*
М. Сорока *214*
М. Харитонов *215*
М. Хайден *179–181*
М. Хатавей *175*
М. Хеффернан *24*
М. Хіппонен *103*
М. Цукерберг *65*
М. Чертофф *180, 181*
М. Шмітт *13, 81, 84–86, 147, 151*

Н

Насір Абдулазіз Аль-Насер *206*
Н. Гінгріч *13*
Н. Жданов *13*
Н. Кроес *67*
Н. Саркозі *65*
Н. Спайкмен *12, 34*

О

О. Волошин *12*
О. Воронянський *35*
О. В. Шевчук *95*
О. Гостєв *122, 123, 129*
О. Дзьобань *13*
О. Ірхін *12*
О. Кузьмук *261*
О. Ломанов *91*
О. Манжай *12, 72*
О. Навальний *187*

О. Порфимович *12*
О. Резнікова *12*
О. Сноу *56*
О. Хакслі *10*
О. Шевчук *13*

П

П. Боніфас *42*
П. Відаль де ла Блаш *12, 21*
П. Вулкотт *205*
П. Вуллей *69*
П. Галлуа *12, 19, 20*
П. Домбровський *12, 40, 139*
П. Ленський *13*
П. Масляк *12, 27*
П. Тейлор *115*
П. Федорук *22*
П. Циганков *12, 18*

Р

Р. Арон *12, 41*
Р. Барбрук *13*
Р. Богатирьова *207*
Р. Беттс *13, 94*
Р. Гейтс *111, 176*
Р. Діперт *13, 102*
Р. Елдер *69*
Р. Маккінон *13, 195*
Р. Мердок *65*
Р. Олдріч *13*
Р. Оттіс *117*
Р. Пітерс *13, 199*
Р. Хорматс *114*
Р. Челлен *12, 16–18, 21*

С

С. Бейделман *12, 73, 74*
С. Василенко *12*
С. Делбі *12, 23*

С. Жижек *13*
Сі Цзіньпін *93, 94*
С. Кокс *111, 189*
С. Коллінс *51*
С. Старр *12, 34, 44, 45*
С. Хілдрет *74*
С. Юрченко *12*
Ся Ліпін *13, 92*

Т

Т. Ваден *13*
Т. Вінгфілд *13*
Т. Гоббс *10*
Т. Донілон *94*
Т. Дрейк *180*
Т. Михайлов *12, 18*

У

У. Лінн *104, 145*
У. Хейг *206*

Ф

Ф. Бланк *68*
Ф. Крамер *12, 13*
Ф. Макдоналд *12, 17, 141*
Ф. Махлуп *13*
Ф. Міллрах *13*
Ф. Пелерін *64*
Ф. Ратцель *12, 16, 17, 21*
Ф. Рігер *136*
Ф. Фукуяма *13*

Х

Хабіб Ельганян *137*
Х. Клінтон *31, 32, 177, 187, 188, 189*
Х. Лін *13, 105, 154, 157*
Х. Маккіндер *12, 34*
Ху Цзіньтао *15, 92, 201, 202*

Ц

Цзянь Сіюань *13, 92*
Цзян Юй *32*
Ці Сяндун *107*
Цуй Тянькай *111*

Ч

Чжань Веньму *96*
Чжао Цзін *201*
Чжен Біцзянь *92*
Ч. Краутхаммер *145*
Ч. Хейгел *98*

Ш

Ши Тао *200*
Ши Янхун *93*
Ш. Лоусон *13, 150*
Ш. МакБрайд *230*

Ю

Ю. Вознюк *12, 27*
Юй Сяотун *90*
Ю. Луценко *214*
Ю. Павленко *13*
Ю. Самойленко *261*
Ю. Тимошенко *214*
Ю. Федоров *12*
Ю. Хаясі *13*
Ю. Шмаленко *12*

Я

Я. Бремор *13, 100*
Я. Волков *12, 18, 34*
Я. Єрьомін *13*
Я. Ітікава *189*
Яо Юньчжу *98*

Наукове видання

ДУБОВ Дмитро Володимирович

КІБЕРПРОСТІР ЯК НОВИЙ ВИМІР ГЕОПОЛІТИЧНОГО СУПЕРНИЦТВА

Монографія

Літературний редактор: *І. О. Коваль*
Коректори: *О. В. Москаленко*, *І. О. Коваль*
Комп'ютерне верстання: *Є. Ю. Стрижеус*

Відповідальна за випуск: *І. О. Коваль*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел/факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua

Формат 60x90/16. Ум. друк. арк. 20,5.
Обл.-вид. арк. 15,38. Наклад 300 пр. Зам. № 549.

ДП «НВЦ «Пріоритети»
01014, м. Київ, вул. Командарма Каменєва, 8, корп. 6
тел./факс: 254-51-51

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 3862 від 18.08.2010