НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

МАЙБУТНЄ КІБЕРПРОСТОРУ ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ: НОВІ МІЖНАРОДНІ ІНІЦІАТИВИ ПРОВІДНИХ ГЕОПОЛІТИЧНИХ ГРАВЦІВ

Аналітична доповідь

Київ – 2012

УДК 004:327(477:470+571:510:73)
Д 79

Автори:
Дубов Д. В., к. політ. н., с. н. с.;
Ожеван М. А., д. філос. н., проф., заслужений діяч науки і техніки України.

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

Дубов Д. В.
Д 79 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.

ISBN 978-966-554-179-0

Розглянуто питання підходів основних геополітичних гравців (США, КНР і РФ) до майбутнього кіберпростору. Зазначено особливості таких підходів, форматів їхнього затвердження на міжнародному рівні та можливої позиції України щодо таких ініціатив. Проведено загальний аналіз міжнародних ініціатив на їхню відповідність національним інтересам України та на відповідність їхніх окремих положень вітчизняному законодавству.

ISBN 978-966-554-179-0

ВСТУП

Упродовж останніх десяти років питання регулювання кібернетичного простору перестає бути виключно «внутрішньою справою» окремих держав. Можливість використання кіберпростору організованими злочинними угрупуваннями, зловмисниками-одинаками, формалізованими та неформалізованими деструктивними політичними групами, військовими і спеціальними службами держав з метою вчинення злочинів, здійснення хакерських атак за політичними мотивами, деструктивного впливу на військову й цивільну інфраструктуру (у т.ч. – критичну), збір чутливої інформації, а також пряме шпигунство в інтересах держави чи потужних корпорацій, робить неможливим ігнорування цієї проблеми світовою спільнотою.

Про рівень занепокоєності провідних геополітичних гравців даним питанням свідчать різноманітні дискусії (у т.ч. – на найвищому рівні), що пропонують визнати кібернапади «актом війни», кіберзброю прирівняти до зброї масового знищення, а також надати право відповідати на хакерську атаку звичними видами озброєнь (наприклад – ракетним ударом). Проблема додатково ускладнюється двома потужними чинниками: відсутністю у головних гравців єдиного погляду на кіберпростір і кібербезпеку в цілому, а також посилення загальносвітової дискусій навколо забезпечення авторських і суміжних прав у мережі Інтернет.

До останнього часу проблему кібербезпеки на міжнародному рівні було вирішено лише частково – у сфері протидії кіберзлочинності. Йдеться про прийняту Радою Європи у 2001 р. Конвенцію про кіберзлочинність, що відносила до сфери кіберзлочинів такі види правопорушень:

- правопорушення проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, систему, зловживання пристроями);
- правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами);
- правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією;
- правопорушення, пов'язані з порушенням авторських та суміжних прав.

Водночас далеко не всі країни (з числа членів Ради Європи) ратифікували цей документ (у т.ч. принципову позицію з цього питання

зайняла РФ). Крім того, Конвенція є регіональним документом, хоча до нього долучаються й інші країни світу. Понад те, документ не вирішує зазначених вище питань військового використання кіберпростору, глобальних міжнародних підходів до кібербезпеки тощо.

Це змушує керівництво держав формувати власну політику кібербезпеки на національному рівні в умовах глобальної невизначеності й відсутності єдиних підходів. Більшість держав світу вже створили відповідні підрозділи (як правоохоронні, так і військові), що спрямовані на протидію кіберзагрозам і розроблення наступальних технологій.

З метою вирішення даної проблеми низка світових держав (США, КНР, РФ) виступають з власними ініціативами щодо впорядкування на глобальному рівні питань кібербезпеки (інформаційної безпеки), але спостерігаються докорінні відмінності в запропонованих підходах, що не лише мало узгоджуються між собою, а й суперечать один одному. Крім того, з огляду на те що США зберігають за собою статус єдиної наддержави, низка ініціатив в її національному законодавстві, цілком можливо, вплине й на міжнародну ситуацію в цій сфері чи, принаймні, може задати основний тренд реформування національних законодавств в інших країнах.

В аналітичній доповіді висвітлюються головні міжнародні правові й політичні ініціативи (або такі національні ініціативи/законопроекти, що можуть суттєво вплинути на міжнародне правове поле) у сфері кібербезпеки, визначаються можливі проблемні напрями при реалізації таких ініціатив та можлива позиція щодо них України.

1. ІНІЦІАТИВИ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ ЩОДО МАЙБУТНЬОГО КІБЕРПРОСТОРУ

США залишаються одним з основних гравців, що визначають перспективи розвитку кіберпростору й потенційні напрями в його регулюванні (або формуванні політики щодо даного питання).

Головна зовнішньополітична ініціатива США щодо перспектив розвитку кіберпростору була оприлюднена 16 травня 2011 р. під назвою **Міжнародна стратегія для кіберпростору** (*International Strategy for Cyberspace, далі* – Стратегія)[1]. Цей документ не лише визначає принципові положення, якими будуть керуватися США при форму-

[1] *International* Strategy for Cyberspace [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

ванні власної політики щодо кіберпростору, а й окреслює «очікуване майбутнє», яке вони планують побудувати в кіберпросторі.

Так, «базовими принципами», що мають бути забезпечені при формуванні політики щодо кіберпростору, Стратегія визначає:

• *«Фундаментальні свободи»* (можливість шукати, отримувати й передавати інформацію та ідеї через будь-які засоби зв'язку та незважаючи на кордони).

• *«Прайвесі»* (люди мають бути обізнані з загрозами їхній персональній інформації та про можливість здійснення проти них кіберзлочинів).

• *Вільні потоки інформації»* (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, оскільки вони створюють видимість безпеки, кіберпростір має бути місцем інновацій та співпраці держави й бізнесу задля більшої безпеки.

Цим документом установлено риси **бажаного майбутнього** в кіберпросторі для США. У контексті теми аналітичної доповіді особливий інтерес становлять тези, що стосуються міжнародного регулювання (або бачення в цілому) кіберпростору.

У документі виділено три стратегічні цілі, яких має досягти реалізація Стратегії.

1. Відкритість і сумісність. Зростання цифрових систем має поступово привести до здешевлення доступу до кіберпростору дедалі більшої кількості людей. Для розвитку впроваджувані інновації мають бути сумісними між собою, а також більш активно використовувати програмне забезпечення з відкритим кодом. Це дозволить створювати системи з єдиною логікою використання для всіх регіонів світу. Альтернатива цьому процесу є неприйнятною, оскільки передбачає фрагментування мережі Інтернет, де через особливі політичні інтереси держав великим групам людей буде заборонений доступ до сучасного контенту. Відповідно пріоритетом є розроблення нових інформаційних технологій, які засновані на міжнародних, загальноприйнятих стандартах, що забезпечить зростання цифрової економіки і рух суспільства вперед.

2. Безпека й надійність. Користувачі мають впевнитись у безпеці своїх даних. Забезпечення подібного стану – завдання поліаспектне й таке, що потребує загальної відповідальності на всіх рівнях суспільства (починаючи від простих користувачів і закінчуючи державними органами) та ефективної міждержавної співпраці. Головним питанням тут є встановлення міжнародних технічних стандартів (щодо програмного й апаратного забезпечення й систем управління інцидентами) та узгоджених міжнародних норм поведінки держав. Це потребуватиме розширення співпраці в питаннях обміну технічною інформацією з при-

ватним сектором і міжнародним співтовариством. Оскільки головним елементом надійності є безпека мереж, США готові інвестувати в них не лише на національному рівні, а й сприяти більшій надійності мереж за кордоном.

3. Стабільність через норми. Цей пункт становить особливий інтерес у контексті теми нашої аналітичної доповіді, оскільки дозволяє в цілому зрозуміти американське бачення і чинного міжнародного правового поля щодо кіберпростору, і орієнтирів його трансформації. Відповідно до тексту Стратегії вироблення єдиних правил поведінки у кіберпросторі – головне завдання й США готові працювати над виробленням консенсусної точки зору з приводу того, що таке «прийнятна поведінка», а також партнерство, в кіберпросторі. Відповідно до тексту Стратегії «*вироблення таких норм сприятиме передбачуваності поведінки держав, що дозволить попереджувати конфліктні ситуації чи непорозуміння*». Відповідно до тексту Стратегії, у США не бачать необхідності приймати принципово нові міжнародні документи, оскільки чинне міжнародне законодавство не є «*застарілим*» відносно реалій кіберпростору: «*розроблення правил поводження держави у кіберпросторі не потребує оновлення чинного міжнародного законодавства та не робить існуючі міжнародні норми застарілими. Багаторічні міжнародні норми, що визначають дії держави під час миру та війни, також стосуються кіберсередовища». Водночас визнається необхідність певного доопрацювання міжнародних норм: «унікальні характеристики мережевих технологій потребують додаткового опрацювання з метою з'ясування, яким чином ці норми слід використовувати та які додаткові тлумачення є необхідними. Ми продовжимо працювати на міжнародному рівні заради досягнення консенсусу щодо використання норм поведінки в кіберпросторі, усвідомлюючи важливість першого кроку в даному напрямі, та в очікуванні мирного й справедливого поводження у кіберпросторі»*.

Головним пріоритетом для США залишається **Будапештська Конвенція з кіберзлочинності**. Цей документ, на думку авторів Стратегії, має стати базовим для всіх подальших напрацювань у сфері вироблення норм поведінки в кіберпросторі. Про це свідчить і те, що розділ «Розширення співробітництва та верховенство права» (ст. 19–20 Стратегії) значною мірою присвячено саме Конвенції. Зокрема зазначається, що США розглядає важливе питання «*подальші дискусії щодо міжнародних норм*» протидії кіберзлочинності в першу чергу як проблему «*поширення чинних зусиль, таких як Будапештська конвенція*» на всіх учасників. Крім того, докладатимуться зусилля до налагодження двосторонньої співпраці між державами. Другий пункт цього розділу вказує на необхідність узгодження національних нормативно-правових документів

у сфері протидії кіберзлочинності з Будапештською конвенцією, яка, на думку авторів Стратегії, «*є моделлю для розроблення та оновлення чинних законів*» у цій сфері. США зі свого боку зобов'язуються стимулювати інші країни приєднуватися до Конвенції.

Можна прогнозувати, що у випадку довгострокового інтересу США до просування Будапештської конвенції в якості основного документа для дво- та багатостороннього співробітництва, будуть здійснюватися зусилля з трансформації цього документа у своєрідний міжнародний договір.

Водночас у своєму нинішньому вигляді Конвенція не зможе охопити дійсно всі країни, що відіграють головну роль в питаннях кібербезпеки. Так, РФ не підписала[2] Конвенцію. І, судячи з усього, не зробить цього доти, доки з неї не буде прибрано низку положень, що не влаштовують російську сторону. Серед таких, зокрема, положення Конвенції про те, що та чи інша країна може отримувати доступ до ресурсів, розташованих у мережах загального користування іншої держави, не повідомляючи її при цьому[3]. Малоймовірно, що на таке положення згодяться КНР і цілий ряд інших країн (більш докладно позиції РФ і КНР з проблем розвитку кіберпростору буде наведено у другому розділі доповіді).

Крім зазначеного питання в Стратегії сформульована орієнтовну модель поведінки держав щодо Всесвітньої мережі й окремих аспектів її роботи:

• *додержання основних свобод*. Держави мають поважати фундаментальні свободи слова та об'єднань, що так само актуальні і для онлайну, як і для офлайну;

• *повага до власності*. Держави у своїх ініціативах мають поважати право на інтелектуальну власність, включно з патентами, торговими таємницями, товарними знаками й авторськими правами;

• *цінність приватного життя*. Громадяни мають бути захищені від довільного чи незаконного втручання в їхнє приватне життя, коли вони користуються інтернетом;

• *захист від злочинів*. Держави мають виявляти й переслідувати кіберзлочинців, створювати таке законодавство і практики, що не дозво-

---

[2][Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[3]Мається на увазі ст. 32 Конвенції «Транскордонний доступ до комп'ютерних даних, що зберігаються, за згодою або у випадку, коли вони є публічно доступними»: будь-яка Сторона може, не отримуючи дозволу іншої Сторони, здійснювати доступ до публічно доступних (відкриті джерела) комп'ютерних даних, що зберігаються, не зважаючи на те, де такі дані знаходяться географічно.

лять зловмисникам переховуватись на їхній території, а також сприяти співробітництву з міжнародними структурами, які переслідують таких злочинців;

• *право на самозахист*. У відповідності до Статуту ООН держави мають право на самозахист, що може бути застосоване у відповідь на агресивні дії в кіберпросторі;

• *глобальна сумісність*. Держави мають вживати заходів, щоб допомогти досягти максимальної сумісності та зручності використання мережі Інтернет, а також її доступності найбільшому числу громадян;

• *мережева стабільність*. Держави мають поважати свободу потоків інформації в їх національних мережах, і не втручатись у роботу інфраструктури, що відноситься до такої, яка тісно пов'язана із міжнародною функціональністю мережі;

• *надійний доступ*. Держави не повинні заважати доступу громадян до мережі Інтернет чи інших мережевих технологій;

• *багатостороннє управління*. Управління мережею Інтернет не має обмежуватись виключно урядами, а має включати й інших стейкхолдерів;

• *особлива увага до кібербезпеки*. Держави мають визнавати свою відповідальність за безпеку й надійність роботи власних сегментів мережі Інтернет та відповідної інфраструктури.

Особливу увагу в даному переліку викликають два пункти: «право на самозахист» і «надійний доступ» (а також пов'язаний із ним пункт про «додержання основних свобод»).

Посилання на Статут ООН у пункті «право на самозахист» переводить проблему з площини карних злочинів на рівень національної безпеки і військових загроз. У ст. 51 Статуту ООН розглядається «*невід'ємне право на індивідуальний чи колективний самозахист, якщо відбудеться військовий напад на Члена Організації*». Крім того, варто враховувати артикульовану позицію заступника Міністра оборони США Вільяма Лінна відносно того, що «*США залишають за собою право, у відповідності до законодавства щодо військових конфліктів, у відповідь на серйозну кібератаку застосувати пропорційну й обґрунтовану військову відповідь у той час та в тому місці які ми оберемо самі*»[4].

Відповідно до резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 р., «агресією» вважається «*застосування збройних сил державою проти суверенітету, територіальної цілісності чи полі-*

[4] *William J. Lynn, III* Remarks on the Department of Defense Cyber Strategy As Delivered by Deputy Secretary of Defense, National Defense University, Washington, D. C., Thursday. – 2011. – July 14 [Електронний ресурс]. – Режим доступу: http://www.defense.gov/speeches/speech.aspx?speechid=1593

тичної незалежності іншої держави, або будь-яким іншим способом, що несумісні з Статутом Організації Об'єднаних Націй, як це встановлено у цьому визначенні» (ст. 1). У цій же Резолюції (ст. 3) надано список дій, що в будь-якому випадку будуть кваліфіковані як «акти війни»:

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

• бомбування 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 війська, морські й повітряні флоти іншої держави;

• використання збройних сил держави, що знаходяться на території іншої держави, за її згодою, в порушенні умов, що передбачені угодою, чи будь яке подовження перебування на території після припинення дії угоди;

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

• засилання державою чи від її імені озброєних банд, груп, іррегулярних сил чи найманців, які здійснюють акти використання збройної сили проти іншої держави і мають настільки серйозний характер, що це рівнозначно перерахованим вище актам, чи значна участь у них.

Як бачимо, більшість цих визначень так чи інакше передбачають фізичний контакт двох держав, частіше за все – із використанням кінетичної зброї. Кібератаки (вже через саму невизначеність національного кіберпростору) є розпорошеними, встановити їх належність саме державним органам, а тим більше збройним силам, 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 будуть застосовані потенційні санкції.

У таких умовах видається сумнівним, що кібератака згідно з чинними міжнародними документами може кваліфікуватись як «агресія» чи «напад» і, тим більше, тягнути за собою військову відповідь. Водночас у Стратегії безпосередньо йдеться про те, що США готові застосовувати «*дипломатичні, інформаційні, військові й економічні*» засо-

би для реагування на інциденти. На даний момент все ще залишається незрозумілим, яким чином подібне положення може бути реалізоване на практиці без внесення кардинальних змін до Резолюції ООН, що дає визначення «агресії». Поки що існують лише окремі наукові напрацювання у сфері міжнародного права, які пропонують або визнати кіберзброю зброєю масового знищення, або (що виглядає більш реально) виробити механізм оцінки наслідків від здійснення кібератак та порівнювати їх із можливими наслідками від застосування традиційних озброєнь.

Інший важливий аспект, пов'язаний із запропонованою моделлю поведінки держав по відношенню до Всесвітньої мережі, визначається пунктами «надійний доступ» та «додержання основних свобод». У Стратегії цій проблемі присвячено розділ «Інтернет-свобода: підтримуючи фундаментальні свободи та прайвесі». У даному розділі наводиться чотири основних напрями зусиль США з даного питання.

1. Підтримка громадянського суспільства в питаннях отримання надійних і безпечних платформ для забезпечення свободи слова та зібрань. США закликають усіх до максимально активного використання цифрових засобів зв'язку задля обміну думками, інформацією, моніторингу виборів, боротьби із корупцією, організацію суспільних і політичних рухів та засудження тих, хто переслідує, арештовує чи погрожує тим людям, які користуються цифровими засобами. США готові сприяти розширенню прав і можливостей громадянського суспільства, правозахисників і журналістів використовувати такі цифрові засоби, а також сприяти тим урядам, що «вирішують реальні загрози у кіберпросторі, а не нав'язують компаніям обов'язки щодо обмежень свободи слова чи вільних потоків інформації».

2. Співробітництво з громадянським суспільством і неурядовими організаціями щодо підвищення їх кібербезпеки (зокрема, їх електронних поштових адрес, веб-сайтів, мобільних телефонів тощо).

3. Сприяти міжнародному співробітництву для більш ефективного захисту комерційних конфіденційних даних.

4. Забезпечити наскрізну сумісність систем, що задіяні в передачі інформації у мережі Інтернет.

Тематиці «основних свобод» та Інтернету було присвячено розлогий **виступ держсекретаря США Гілларі Клінтон** під час конференції «Свобода інтернету», що відбулась 8 грудня 2011 р. у м. Гаазі (Нідерланди)[5].

---

[5][Електронний ресурс]. – Режим доступу: http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html

У своєму виступі держсекретар розкритикувала практику затримання блогерів – громадських активістів (наприклад, Олексія Навального в РФ) та практику китайського уряду, пов'язану з укладанням спеціальних угод із компаніями, що надають телекомунікаційні послуги[6].

Заяви Гілларі Клінтон з приводу необхідності врегулювання даного питання також цілком вкладається у запропонований Стратегією формат забезпечення положень про «фундаментальні права»: «*Виконання належного в стосунках 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 й оголошення, що роботу зроблено. Вона вимагає постійних зусиль, щоб враховувати нову реальність, у якій ми живемо в цифровому світі, й робити це таким чином, щоб максимальними були переваги, які він обіцяє*». Водночас у цій промові було піднято три додаткових проблеми, що дозволяють зробити висновки про довгострокові плани США щодо кіберпростору.

1. Приватний сектор має прийняти свою роль у захисті Інтернет-свободи. На думку Гілларі 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** й не чекати на відповідні рішення Держдепартаменту: «*Коли компанії продають обладнання для стеження агентствам безпеки Сирії або Ірану (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 накласти санкції, і це закриє проблему <...> санкції є частиною рішення, але вони не все рішення <...> Подвійні технології й продажі третіми сторонами не дозволяють режиму санкцій ідеально запобігати використанню технологій поганими дієвими особами із поганими намірами. Часом компанії говорять нам, Державному департаменту: «Просто скажіть, що робити, і ми будемо це робити». Але насправді не слід чекати розпоряджень. У XXI ст. розумні компанії мають вживати заходів до того, як вони потраплять*

[6]«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 вони вели мову про пропоновані китайському народу інтернет-послуги, і це було кодове формулювання про відповідність жорсткому урядовому контролю над Інтернетом» (з виступу держсекретаря Гілларі Клінтон у м. Гаазі).

у суперечливе становище». Подібна позиція США концептуально не співпадає із панівною (у публічному дискурсі) неоліберальною парадигмою «вільного ринку», коли роль держави полягає саме у встановленні граничних меж ринку, однак не саморегулюванні на основі «розумності» цього процесу.

2. Недопущення використання урядами тематики «управління інтернетом» з метою посилення «контролю за інтернетом»: «*Саме зараз на різних міжнародних форумах деякі країни працюють над тим, щоб змінити регулювання інтернету. Існуючий багатосторонній підхід, де в єдину глобальну мережу включені уряди, приватний сектор і громадяни, та забезпечується вільний обмін інформацією, яку вони хочуть замінити. Натомість вони прагнуть нав'язати систему, закріплену глобальним кодом, який розширює контроль над Інтернет-ресурсами, установами і змістом, та централізує таке управління в руках урядів*». Основна занепокоєність США полягає в можливості створення національних правил гри для окремих сегментів мережі, що порушує сам принцип сумісності в Інтернеті. **У більш широкому сенсі США виступають категорично проти будь-яких бар'єрів у кіберпросторі, що можуть тлумачитися як своєрідні «кордони держави в кіберпросторі»**. Гілларі Клінтон рішуче відкидає зв'язок даної проблеми з питаннями безпеки (протидії кіберзлочинності, розповсюдження дитячої порнографії, кібертероризмом), наголошуючи, що проблеми мають вирішуватись у інший спосіб, не порушуючи «динамізму розвитку Мережі».

3. Створення коаліції за «відкритий Інтернет». Фактично є продовженням другої тези, однак з практичною частиною: об'єднуватись у коаліцію держав, що не допустить обмежень мережі в окремих країнах.

На сьогодні важко сказати, наскільки успішною буде практична реалізація Стратегії, та чи знайде вона загальносвітову підтримку. **Можна очікувати, що більшість європейських країн, і частина країн Східної півкулі (наприклад Японія, Австралія, Нова Зеландія) приймуть даний підхід**. Крім того, деякі з цих країн розпочали більш інтенсивну двосторонню співпрацю із США. Так, у липні 2011 р. Індія й США досягли домовленостей щодо посилення співпраці у сфері протидії кіберзагрозам: відповідний меморандум про взаєморозуміння було підписано між Департаментом електроніки та інформаційних технологій Міністерства комунікацій та інформаційних технологій й Департаментом державної безпеки США[7]. У вересні 2011 р. Австралія

[7][Електронний ресурс]. – Режим доступу: http://economictimes.indiatimes.com/news/politics/nation/india-us-ink-an-agreement-on-cyber-security/articleshow/9282199.cms

й США включили проблему співробітництва з протидії кіберзагрозам до договору про взаємну оборону[8]. У жовтні 2011 р., під час спільної прес-конференції міністрів оборони США та Японії, очільник японського військового відомства Ясуо Ітікава відмітив, що сторони активно обговорюють питання поглиблення співробітництва у сфері кібербезпеки[9].

Незважаючи на активність США в напрямі міжнародної співпраці, і тут є певні складнощі. Доволі розлого причини виникнення проблем, з якими зустрілись у США при співпраці з країнами-партнерами щодо технологій та методів протидії кіберзагрозам, висвітлив у своєму виступі на семінарі, що був присвячений кібербезпеці, в Джорджтаунському університеті начальник розвідки кіберкомандування контр-адмірал Семюель Кокс. На його думку, одна з головних проблем США полягає в слабкій захищеності комп'ютерних систем низки союзників НАТО, що призводить до заволодіння супротивником інформацією, якою США ділиться із союзниками. Щоправда, Семюель Кокс публічно[10] не називав країни з вразливими комп'ютерними мережами, хоча, на його думку, до числа цих країн не входить четвірка країн (Канада, Велика Британія, Австралія й Нова Зеландія), з якими у США тісна співпраця у військовій та безпековій сферах.

Ще одна проблема, яка гальмує співпрацю воєнних відомств країн НАТО й партнерських країн, – надмірна засекреченість військових технологій та технологій подвійного призначення, а також надто жорсткі американські закони щодо експортного контролю трансферу таких технологій, за яких у багатьох випадках Пентагону не дозволяється продавати іншим країнам або ж ділитися з ними цими технологіями безкоштовно.

Є обгрунтовані сумніви, що Стратегію в повному обсязі приймуть КНР і РФ. Незважаючи на думку деяких експертів[11], співробітництво з питань кібербезпеки у трикутнику США–КНР–РФ налагоджується (зокрема у питаннях визначення термінології й пожвавлення діалогу), але є декілька позицій, що можуть стати принциповою точкою, яку найближчим часом ці держави не зможуть подолати.

---

[8][Електронний ресурс]. – Режим доступу: http://www.officialwire.com/main.php?action=posted_news&rid=44771

[9][Електронний ресурс]. – Режим доступу: http://www.mod.go.jp/e/pressconf/2011/10/111025_japan_us.html

[10]*У США* трудности с партнерами по противодействию киберугрозам [Електронний ресурс]. – Режим доступу: http://www.vestnik-sviazy.ru/t/news.php?day.20120412

[11][Електронний ресурс]. – Режим доступу: http://inosmi.ru/social/20111005/175569908.html

По-перше, на думку США, головний документ у поліпшенні глобальної кібербезпеки – Конвенція про кіберзлочинність – скоріше не буде підписаний РФ, до внесення суттєвих змін у текст Конвеції, що видається малоймовірним в осяжній перспективі. Водночас навіть у випадку подальшого розширення дії цього документа (за рахунок включення нових країн у число учасників) можна очікувати, що аналогічну російській позицію займе і КНР. Таким чином, враховуючи, що США акцентують увагу в просуванні Конвенції, можна припустити, що результативної дискусії тут найближчим часом не відбудеться.

По-друге, теза про «вільні потоки інформації», що не можуть обмежуватись за будь-яких умов національними урядами, принципово не співпадає із поглядом РФ і КНР (а також деяких інших країн), на те, яким чином можуть бути використані ці інформаційні потоки (зокрема, для дестабілізації політичної, економічної та соціальної ситуації в країні). Частина пояснень тези про «вільні потоки» (наприклад щодо активної підтримки з боку США громадянського суспільства у всьому світі) ще більше переконує уряди цих країн у неможливості прийняти подібне твердження як базове.

По-третє, малоймовірно, що США 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 іншого, зможуть прийти до дійсно єдиної (консолідованої) точки зору щодо проблеми управління Інтернетом. США однозначно займають позицію щодо продовження підпорядкованості контролю за мережею Інтернет корпорації *ICANN*. Незважаючи на цілий ряд дій, що були здійснені керівництвом корпорації для позбавлення іміджу компанії, яка безпосередньо підпорядкована уряду США, більшість країн світу продовжують наполягати на передачі її повноважень та функцій спеціально створеному органу під егідою ООН.

По-четверте, КНР і РФ принципово не згодні з тим, що США виокремлюють кібербезпеку як головну проблему інформаційної безпеки (а фактично заміщуючи її). Вони вважають, що кібербезпека має розглядатись виключно як частина інформаційної безпеки, яка б охоплювала всю низку гуманітарних питань (що, відповідно, могли б регулюватись державою у відповідності до проблеми забезпечення національної безпеки).

2. ІНІЦІАТИВИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ТА КИТАЙСЬКОЇ НАРОДНОЇ РЕСПУБЛІКИ ЩОДО МАЙБУТНЬОГО КІБЕРПРОСТОРУ

Погляди США на кіберпростір і основні принципи його функціонування не завжди поділяються іншими геополітичними гравцями. І якщо значна частина держав перебуває в стадії роздумів щодо визначення своєї офіційної позиції з приводу таких ініціатив, деякі країни почали просування альтернативних проектів регулювання (правил поведінки) у кіберсфері (або в деяких з цих документів – «сфері міжнародної інформаційної безпеки»).

Основна концептуальна відмінність, що вирізняє ці альтернативні проекти від американської ініціатив, – **фактична відсутність розділення кібербезпеки з більш широким (а іноді й доволі абстрактним) поняттям «інформаційно-психологічної безпеки»**. РФ послідовно відстоює позицію, що кібербезпеку не можна розглядати як повністю самостійний напрям, що існує окремо від соціальних, політичних, економічних і військових наслідків застосування сучасних інформаційних технологій. Більше того, за такого підходу взагалі недоречно казати про абсолютно «вільні потоки інформації», оскільки безпекова тематика охоплює й наслідки їх впливу на державу та її громадян. Тому казати про «кібербезпеку» (навіть у міжнародному контексті) не зовсім вірно, в той час як більш адекватною назвою даної проблеми є «інформаційна безпека» чи «міжнародна інформаційна безпека».

Саме таку позицію РФ послідовно відстоює з 1998 р., коли нею була розпочата дискусія щодо необхідності затвердження норм і правил у сфері міжнародної інформаційної безпеки. Однак до 2009 р. жодних реальних результатів так і не було досягнуто. Першим проміжним успіхом можна вважати створену у 2009 р. (у відповідності до резолюції 60/45 Генасамблеї ООН) групи урядових експертів ООН з міжнародної інформаційної безпеки[12]. Дана група за рік роботи підготувала звіт (за червень 2010 р.), у якому в загальному вигляді сформульовано основні ризики, загрози від використання сучасних інформаційно-комунікативних технологій (*далі* – ІКТ). Хоча в тексті звіту відсутні однозначні тези про гуманітарні та політичні загрози (крім положення

[12]Група створена з 15 експертів із таких країн: Білорусь, Бразилія, КНР, Естонія, Франція, Німеччина, Індія, Ізраїль, Італія, Катар, Південна Корея, РФ, Південно-Африканська Республіка, Велика Британія та США. Керівником групи став представник РФ Андрій Крутських.

про зростання використання ІКТ з військовою й розвідувальною метою), РФ посилаючись на роботу даної групи намагається просувати свої проекти міжнародних документів у сфері забезпечення міжнародної інформаційної безпеки.

Одним із таких документів є **Конвенція про забезпечення міжнародної інформаційної безпеки**[13] (*далі* – КЗМІБ), яка була представлена під час Другої міжнародної зустрічі високих представників, що курують питання безпеки (20-21 вересня 2011 р. у м. Єкатиренбурзі)[14]. Концепція документа повною мірою відповідає російським поглядам на інформаційну безпеку і значною мірою опонує вищезгаданим американським документам та підходам. Зокрема, в російській КЗМІБ звертається увага, що розв'язок усіх питаннь, які пов'язані із державною політикою щодо мережі Інтернет, є суверенним правом держав. Крім того, серед загроз у сфері міжнародної інформаційної безпеки виділено такі:

• неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої знаходяться ці ресурси;

• діяльність в інформаційному просторі з метою підриву політичної, економічної й соціальної системи іншої держави, психологічна обробка населення, що дестабілізує суспільство;

• маніпулювання інформаційними потоками і інформаційним простором інших держав, дезінформація й утаємничення інформації з метою викривлення психологічної та духовної сфери суспільства, ерозія традиційних культурних, етичних та естетичних цінностей;

• протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності у сфері інформатизації, що може нести загрозу іншим державам[15]. Схоже, що в даному пункті, не зважаючи на співзвучність із тезами американської Стратегії, закладено принципово інший зміст. У США кажуть про «*обмеження доступу до технологій*» в контексті обмеження доступу для на-

---

[13][Електронний ресурс]. – Режим доступу: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

[14]Учасники – 52 країни. Рівень представництва – вищі особи, які відповідають за координацію діяльності правоохоронних структур. Від України представником була Секретар РНБОУ Раїса Багатирьова.

[15]Крім традиційних звинувачень з боку РФ на адресу Західних країн у штучному обмеженні доступу до новітніх технологій Росії, цікавим у цьому контексті є нещодавній виступ помічника Держсекретаря Майкла Познера, де він звертав увагу на те, що авторитарні режими (наводився приклад Лівії) використовують новітні технології, що розроблюються переважно в США, для подальшого переслідування свої політичних опонентів.

селення з боку урядів, тоді як РФ, вочевидь, має на увазі формальні й неформальні міждержавні обмеження (наприклад, через поправку Джексона-Веніка);

• інформаційна експансія, встановлення контролю над національними інформаційними ресурсами іншої держави.

На думку деяких оглядачів[16], МЗС РФ сподівається, що даний варіант КЗМІБ буде внесено й прийнято на розгляд Генасамблеї ООН ще у 2012 р.

Як уже зазначалося, російський документ принципово відрізняється від схожого американського, максимально розширюючи сферу «інформаційних загроз». **Понад те, з огляду на цілу низку положень даного документа він, скоріше, не зможе бути основою обговорення між основними геополітичними гравцями (зокрема для США й тих країн, що поділяють їхні підходи)**.

Вочевидь, проходження КЗМІБ через ООН буде непростим і малоймовірно, що до нього приєднається більшість країн (зокрема європейських). У якості більш «м'якої» версії КЗМІБ РФ спільно з КНР запропонували для обговорення інший документ: 12 вересня 2011 р. КНР і РФ спільно з Узбекистаном і Таджикистаном звернулися до Генерального секретаря ООН з листом, де пропонують на 66-й сесії Генеральної асамблеї розглянути запропонований ними проект «**Правил поведінки у сфері забезпечення міжнародної інформаційної безпеки**»[17] (A/66/359).

Текст Правил є значно меншим за обсягом, ніж КЗМІБ, однак у цілому повторює основні положення цього документа. З-поміж іншого, Правила звертають увагу на такі моменти:

• у пункті «*a*» йдеться про «...повагу до основних прав і свобод людини, а також **багатоманітності історії, культури і соціального розвитку всіх країн**»;

• пункт «*c*» звертає увагу на необхідність співпраці в «боротьбі зі злочинною чи терористичною діяльністю із використанням інформаційно-комунікаційних технологій <...> **що підриває політичну, економічну й соціальну стабільність держав, їх культурний та духовний стан**».

• у пункті «*g*» йдеться про «**сприяння створенню багатосторонніх, демократичних міжнародних механізмів управління Інтернетом**, які б гарантували його стабільне й безпечне функціонування».

---

[16][Електронний ресурс]. – Режим доступу: http://newtimes.ru/articles/detail/44438/

[17]*China*, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations. – 2011. – October 13 [Електронний ресурс]. – Режим доступу: http://www.fmprc.gov.cn/eng/zxxx/t858978.htm

В ООН сторони розпочали супровід своєї пропозиції в межах двох комітетів – Першого та Третього. Під час 6-ї та 7-ї зустрічей Третього комітету[18] Генасамблеї ООН представник делегації КНР при ООН Лі Ксяомеі зазначила, що китайська сторона висловлює жаль з приводу того, що до останнього часу на міжнародному рівні не було прийнято регулюючих документів, які мали б сприяти встановленню міжнародної інформаційної безпеки.

Однак основна дискусія відбулася в Першому комітеті[19] Генасамблеї під час 17-ї зустрічі (зустріч була присвячена саме обговоренню Правил). Посол КНР Вонг Кун звернувся[20] до учасників зустрічі зі вступним словом, в якому доніс позиції КНР з даного питання. Андрій Малов (представник від РФ) у контексті обговорення наголосив[21], що наданий документ, це передусім «запрошення до діалогу», й ініціатори не будуть наполягати на його винесенні на голосування. У своєму виступі Андрій Малов також звернув увагу присутніх, що розроблена РФ КЗМІБ є платформою для обговорення, і що вона зможе стати не лише політичною декларацією (якими згідно положень мають стати Правила), а й дієвим міжнародним правовим документом. Цю ж позицію підтримав білоруський представник[22].

Негативно з цього приводу висловились представники США й Австралії. Вальтер Рейд зазначив, що питання кіберсфери виходять за рамки обговорення в межах ООН і потребують масштабного врахування міжнародного гуманітарного законодавства як головної структури при обговоренні таких ініціатив. Фактично аналогічної позиції дотримувався й Пітер Вулкот, зазначивши, що обговорення «кібер»-тематики в ООН буде надзвичайно складним, а багатоаспектність проблеми робить неможливим її обговорення в межах комітету[23]. Крім того він зазначив, що Австралія повністю підтримує існуючий багатосторонній підхід управління Інтернетом і принципово проти державного контролю за Інтернетом[24].

---

[18]Займається соціальними та гуманітарними питаннями, а також культурою.

[19]Займається питаннями розброєння та міжнародної безпеки.

[20][Електронний ресурс]. – Режим доступу: http://www.china-un.org/eng/hyyfy/t869445.htm

[21][Електронний ресурс]. – Режим доступу: http://www.unmultimedia.org/radio/russian/archives/98456

[22][Електронний ресурс]. – Режим доступу: http://www.unmultimedia.org/radio/russian/archives/98379

[23]У цьому контексті складно не згадати, що у вересні 2011 р. між США та Австралією було підписано додаткові угоди щодо спільної протидії кіберзагрозам і посилення двосторонньої співпраці з даного питання.

[24]Цікаво, що дана позиція була висловлена практично в тих же словах, як вона записана в «Міжнародній стратегії розвитку кіберпростору» (США).

Більш розгорнутими й категоричними були оцінки даної ініціативи з боку представників держструктур США. Мішель Маркофф, старший радник Держдепартаменту з питань Інтернету вважає[25], що **подібні проекти спрямовані на спроби домогтися від ООН схвалення на посилення контролю над Інтернет-простором у своїх країнах**. Крім того, Мішель Маркофф зазначила, що минулого року був укладений договір між 15 країнами, включаючи США, РФ і КНР. Згідно з угодою, країни погоджувалися колективно продовжувати обговорення з питання того, яку політику слід застосовувати у зв'язку з більш широким поширенням інформаційних технологій. У цьому контексті заява КНР і Росії сприймається як вихід з переговорного процесу. Приблизно аналогічну позицію висвітлив[26] і помічник держсекретаря Майкл Познер: «**Якщо такий Кодекс буде прийнятий, це майже неминуче підірве свободу ЗМІ** й викличе перехід від кіберпростору, що розвивається рядовими людьми, до системи централізованого контролю з боку урядів. Це не дуже хороша ідея».

Не менш однозначним було зауваження з боку Кіберкомандування США. Його керівник, генерал Кіт Александер, висловився проти того, щоб ООН регулювала Інтернет, вважаючи, що це послабить загальну безпеку в мережі.

Крім США, запропонована китайсько-російська ініціатива викликала негативну реакцію з боку ОБСЄ: представник ОБСЄ з питань свободи ЗМІ Дуня Міятович заявила, що **подібні ініціативи є неприпустимими, оскільки потенційно можуть бути використані для зведення бар'єрів на шляху потоку інформації чи обміну думками**[27]. Вона звернула увагу тих країн, які подали відповідне звернення, що у червні 2011 р. представники ООН, ОБСЄ, Організації американських держав і Африканської комісії з прав людини і народів прийняли Спільну декларацію про свободу вираження поглядів в Інтернеті й зазначила, що саме цей документ має бути базовим у цьому питанні.

Не можна не згадати і про колективний лист від неурядових організацій[28] на ім'я Голови 66-ї Генасамблеї ООН Абд аль-Азіза ан-Насера, в якому запропонований Кодекс критикується за чотирма напрямами:

---

[25][Електронний ресурс]. – Режим доступу: http://www.centrasia.ru/newsA.php?st=1317282000

[26][Електронний ресурс]. – Режим доступу: http://iipdigital.usembassy.gov/st/russian/article/2011/10/20111026103945x0.8727468.html#axzz1dIC9bFSK

[27][Електронний ресурс]. – Режим доступу: http://www.uznews.net/news_single.php?nid=18024

[28][Електронний ресурс]. – Режим доступу: http://www.igcaucus.org/infosecurity-code

• у пункті «*g*» про багатостороннє управління мережею Інтернет не прописано участь громадянського суспільства, що може перетворити таке управління на суто міждержавне;

• у пункті «*h*» у формуванні культури інформаційної безпеки провідна роль належить державі й державно-приватному партнерству, у той час як з цього процесу виключені елементи громадянського суспільства;

• у пункті, що присвячений «загальній повазі до прав людини» присутнє істотне уточнення – «повага до багатоманіття історії, культури і соціальної структури всіх країн», що може бути використано для звуження універсальності прав людини, закріплених, у т.ч. у документах Генасамблеї;

• основну претензію викликав пункт «*c*», де разом з боротьбою зі злочинною чи терористичною діяльністю з використанням інформаційно-комунікаційних технологій пропонується включити протидію діяльності, що «*підриває політичну, економічну й соціальну стабільність держав, їх культурні та духовні традиції*». У такій постановці питання дане положення перевищує допустимі обмеження на свободу вираження думки, що закладені в ст. 19 (3) Міжнародного пакту про громадянські й політичні права й може бути використане для обмеження (цензурування) свободи слова.

Такий саме критичний характер мало і обговорення Правил під час міжнародної конференції з питань діяльності в кіберпросторі, що відбулася 1-2 листопада 2011 р. у Лондоні під девізом «Бачення. Надії. Страхи» (*The Vision, the Hopes, the Fears*) з ініціативи британського МЗС яка зібрала 700 делегатів із 60-ти країн, що представляли як урядові, так і комерційні структури[29].

За деякими припущеннями очікувалось, що під час даного заходу Пекін і Москва спробують знайти точки дотику із західними партнерами щодо ухвалення запропонованої ними ініціативи на рівні Генасамблеї. Однак Лондонська конференція не підтвердила звернених до неї очікувань.

Фактично початок заходу не залишив надії на таке обговорення: міністр закордонних справ Великої Британії Вільям Хейг у виступах під час відкриття й закриття конференції підкреслив, що боротьба зі злочинністю й тероризмом не може бути виправданням для спроб наведення порядку в Інтернеті, маючи на увазі Пекін і Москву. Йому

[29] *Офіційний* сайт конференції: Nations discuss cyber security. – 2011. – November 1 [Електронний ресурс]. – Режим доступу: http://www.cyberwarnews.info/2011/11/01/nations-discuss-cyber-security/

вторив британський прем'єр Девід Камерон: «Уряди країн світу не повинні використовувати кібербезпеку як привід для запровадження цензури»[30].

Офіційну позицію США на лондонській конференції представляв американський віце-президент Джозеф Байден, який у своєму виступі висловив спротив політиці тих країн, які під виглядом боротьби з кіберзлочинністю обмежують свободу діяльності в Інтернеті й пропонують укласти «**репресивний глобальний кодекс поведінки в Інтернеті**».

Останнім часом до цієї дискусії практично не долучались країни ЄС. Це може бути пояснено, тим, що в ЄС тривають внутрішні дискусії щодо визначення меж свободи/контролю за контентом мереж (наприклад у рамках ініціативи «віртуального шенгену»). Хоча можна очікувати, що вже найближчим часом члени ЄС приєднаються до цієї дискусії в якості активних гравців.

3. МІЖНАРОДНІ ІНІЦІАТИВИ ЩОДО КІБЕРПРОСТОРУ Й НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ: ПРОБЛЕМИ РЕАЛІЗАЦІЇ ТА ПЕРСПЕКТИВИ

За останні роки в Україні значно зросла увага до проблем забезпечення кібербезпеки держави й боротьби із кіберзлочинністю. Так, за даними голови Служби безпеки України Ігоря Калініна, вже зараз «*статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів*»[31]. Про актуальність даної проблеми свідчить і зростання кількості злочинів, що кваліфікуються за ст.ст. 361–363 Кримінального Кодексу України. Згідно з даними Єдиного державного реєстр судових рішень, з посиланнями на Розділ XVI Кримінального Кодексу України за останні два роки прийнято 342 судових рішення (з них 89 – вироки).

[30]Варто зазначити, що подібні заяви зі сторони Девіда Камерона виглядали дивно (це відмітила британська й світова преса) зважаючи на те, що ще у серпні 2011 р., під час масових виступів британської молоді, він категорично виступав за надання урядові права роз'єднувати мобільні й соціальні мережі у випадках масових заворушень. Так само є окремі інформаційні повідомлення про те, що уряди західних країн задіяні у блокуванні комунікацій всередині популярного нині на Заході антикапіталістичного руху «Окупуй Уол-Стріт!» *London hosts* cyberspace security conference. – 2011. – November 1 Електронний ресурс]. – Режим доступу: http://www.bbc.co.uk/news/technology-15533786

[31][Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/

Наприкінці 2010 р. Указом Президента України від 10 грудня 2010 р. №1119/2010 було введено в дію рішення Ради національної безпеки і оборони України від 17 листопада 2010 р. «Про виклики та загрози національній безпеці України у 2011 році». Відповідно до цього рішення було поставлено 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*» й «*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*»[32].

На виконання цих завдань у процесі розроблення знаходиться Закон України «**Про кібернетичну безпеку України**», що має зафіксувати основні терміни у сфері кібербезпеки, визначити поняття про об'єкт критичної інфраструктури й механізми захисту таких об'єктів, принцип побудови єдиної загальнодержавної системи протидії кібернетичним загрозам та її складових елементів, вирішить проблеми міжвідомчої координації та повноваження суб'єктів забезпечення кібернетичної безпеки держави. Підтвердження зобов'язань України із розроблення цього закону знайшли своє відображення в «Річній національній програмі співробітництва Україна–НАТО на 2012 рік», де проблемі кібербезпеки відведено окремий параграф (4.7)[33].

Не можна не відзначити і посилення міждержавної співпраці у сфері протидії кіберзлочинності й кіберзагрозам. У жовтні 2010 р. СБУ спільно із ФБР США й спецслужбами дев'яти інших країн світу провели операцію *Trident breach* з нейтралізації злочинного хакерського міжнародного угруповання, що з території України несанкціоновано втручалося в роботу закордонних банківських установ, у результаті чого нанесло збитків на суму близько 170 млн дол. США. Указана спільна операція була відзначена в щорічному звіті за результатами діяльності ФБР США за 2010 р. У червні 2011 р. СБУ, в координації із правоохоронними органами США, Великої Британії, Нідерландів, Франції, Німеччини, Кіпру, Литви (усього десять країн), припинена незаконна діяльність міжнародного злочинного хакерського угруповання під прикриттям комерційної структури, що легально діяла та координувалася громадянами України. За попередніми оцінками, в

[32][Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/n0008525-10

[33][Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/14697.html

результаті злочинної діяльності вищевказаного угруповання збитки становили понад 72 млн дол. США.

У серпні 2011 р. СБУ, в рамках спільної операції зі спецслужбами США припинено незаконну діяльність українського осередку міжнародного злочинного хакерського угруповання (серед членів якого – чотири громадянина України), яке викрало із закордонних банківських установ шляхом підробки кредитних карток указаних фінансових інститутів, понад 20 млн дол. США.

Крім того, українською стороною ініційований розвиток контактів у сфері протидії комп'ютерної злочинності з Дирекцією стеження за територіями Франції (*DST*), Комітетом державної безпеки Республіки Білорусь (КДБ РБ), Службою інформації й демократичної безпеки Італії (*SISDE*), Національною радою правоохоронних органів Швеції, Розвідувальною службою інформації Румунії (*SRI*), Службою інформації й безпеки Республіки Молдова (СІБ РМ), спеціальними службами Єгипту, Національною поліцією Японії та Спеціальним комітетом НАТО. На регулярній основі відбуваються Консультації експертів Україна–НАТО з питань кібернетичного захисту.

До останнього часу позиція Україна щодо запропонованих міжнародних ініціатив залишається не визначеною й чітко не артикульованою. Безумовно, не останньою чергою це пов'язано із самим характером цих ініціатив, дискусія навколо яких досі не набула дійсно значного резонансу. Однак вже зараз Україна має більш чітко визначитися щодо того, які із запропонованих підходів є для неї більш прийнятними і в якому напрямі має формуватись позиція України з питань кібербезпеки (і розвитку кіберпростору) на міжнародному рівні.

Розглядаючи можливість підтримання (включеності) Україною тих чи інших міжнародних ініціатив варто зосередитись на двох рівнях таких пропозицій.

1. **Політичні ініціативи**, що не потребують безпосередніх змін у національному законодавстві. Йдеться про Міжнародну стратегію для кіберпростору (США) та «Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки» (РФ–КНР).

2. **Ініціативи, що мають нормативний характер**. Мова йде про спробу часткового заміщення чинної Конвенції про кіберзлочинність (Рада Європи) на міжнародну Конвенцію про забезпечення міжнародної інформаційної безпеки (КЗМІБ), яку запропонувала РФ.

Безумовно, такий поділ є досить умовним, оскільки деякі з цих ініціатив об'єднують у собі обидва рівні.

Цікавим є те, що всі ініціативи, апелюючи до одних і тих самих питань, мають на увазі різні речі, або ж артикулюють окремі нюанси

таких питань, що вкрай ускладнює погодження позицій в них. Американська Стратегія передбачає «право на захист» у відповідності до Статуту ООН (маючи на увазі захист своєї інформаційної інфраструктури від кібератак). У пункті Китайсько-російських правил ідеться про необхідність «*поважати Статут ООН і загальновизнані норми міжнародного права, що включають, з-поміж іншого, повагу до суверенітету, територіальної цілісності та політичної незалежності всіх держав*». Однак очевидно, що сторони по-різному розуміють частину цих положень. І уточнення китайсько-російської ініціативи щодо «*поваги до багатоманіття історії, культури та соціального укладу всіх країн*» свідчить про бажання отримати гарантії не втручання (навіть опосередкованого) у сферу політичних комунікацій, що забезпечують політичну стабільність держави.

Крім того, як вже зазначалось вище, без створення відповідної міжнародної нормативної бази (чи уточнення поточної) щодо визнання кібератак «актом агресії» (а заразом і того, що взагалі можна трактувати як «кібератаку») подібна одностороння позиція США (що була додатково пояснена очільниками американського військового відомства) виглядає неоднозначно для тих країн, на території яких функціонують організовані хакерські групи, що можуть здійснювати атаки на об'єкти американської інформаційної (й звичайної) інфраструктури. Йдеться не лише про Україну, а й про низку країн, з високим рівнем підготовки *IT*-фахівців, які не завжди мають можливість попередити їх протиправні дії.

Те саме стосується й питання про «вільність інформаційних потоків». Якщо американська ініціатива каже про те, що «*держави мають поважати свободу потоків інформації в їх національних мережах,* і не втручатися *в роботу тієї інфраструктури, що відноситься до такої, яка тісно пов'язана із міжнародною функціональністю Мережі*», а фактично, нівелюючи роль держави у контролі над частиною інформаційного простору, то китайсько-російська ініціатива уточнює, що вільність цих потоків має враховувати «*національне законодавство кожної держави*». У цьому питанні спостерігається чи не найбільше розходження даних ініціатив. Позиція КНР–РФ відносно того, що держави мають «*співробітничати у <...> стримуванні розповсюдження інформації <...>, яка підриває політичну, економічну й соціальну стабільність держави, їх культурний та духовний уклад*» навряд чи буде колись підтримана західними країнами, що вбачають саме в цьому пункті потенційний шлях до обмеження свободи слова, цензури і впливу на активістів громадянського суспільства. Водночас не можна не зазначити, що у відповідності до **Доктрини інформаційної безпе-**

ки України[34], захист «*духовних і моральних засад суспільства*» є одним із напрямів державної політики у сфері інформаційної безпеки України[35].

Ще більш неоднозначним є розгляд можливості прийняття КЗМІБ, запропонованою російською стороною.

У даному випадку принциповим є той факт, що Україною не лише підписано (23 листопада 2001 р.), а й ратифіковано (7 вересня 2005 р.) Конвенцію про кіберзлочинність (яка набула чинності 1 липня 2006 р.) Відповідно, Україна є активним учасником засідань Комітету Конвенції про кіберзлочинність, що проводить щорічні зустрічі (як на рівні експертів, так і представників профільних владних установ) та визначає пріоритети подальшого поширення Конвенції, передусім на країни, що входять до Ради Європи[36]. На сьогодні у вітчизняне законодавство вже імплементовано низку положень Конвенції про кіберзлочинність (наприклад щодо контактного центру 24/7) і є проекти щодо подальшої імплементації. У випадку прийняття й необхідності подальшої ратифікації КЗМІБ, яка з одного боку стосується питань більш широкого спектру, але водночас стосується й кібербезпекової проблематики, може виникнути протиріччя із чинною Конвенцією про кіберзлочинність.

Крім того, цілий ряд положень з російського варіанту КЗМІБ видаються сумнівними з точки зору реального впровадження в практику нормативного поля. Наприклад, поняття «**інформаційна війна**» трактується як «*протиборство між двома або більше державами у формаційному просторі з метою нанесення шкоди інформаційним системам, процесам та ресурсам, критично важливим та іншим структурам, підриву політичної, економічної й соціальних систем, масованої психологічної обробки населення для дестабілізації суспільства та держав, а також примушення держав до прийняття рішень в інтересах протиборчої сторони*». За такого визначення, теоретично будь-яке повідомлення, що з'являється в мережі Інтернет від імені держави (її відомств), в якому засуджується/висловлюється незгода з тією чи іншою політикою іншої держави може трактуватись як «інформаційна війна» із відповідними наслідками.

---

[34][Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/514/2009/print1332746452509988

[35]У цьому контексті варто згадати, що експерти з питань інформаційної безпеки вже неодноразово звертали увагу на необхідність суттєвого доопрацювання Доктрини.

[36][Електронний ресурс]. – Режим доступу: http://www.coe.int/t/dghl/standardsetting/t-cy/tcy2011/TCY_2011_4E_Rev_BU_Way_forward_V4.pdf

Проблематичним буде забезпечити реальний контроль за протидією «**масованій психологічній обробці населення**» (й особливо – закріпити положення на рівні національного законодавства), оскільки не зовсім зрозуміло, що буде виступати в якості критеріїв визначення такої «обробки» та чи можливо це взагалі. Бажання російської сторони врахувати психологічний компонент цілком зрозуміле й до певної міри виправдане, однак навіть у РФ відсутній консенсус щодо цього питання.

Варто згадати, що з початку 90-х років XX ст. у РФ декілька разів намагались прийняти Федеральний Закон «Про інформаційно-психологічну безпеку». Останньою спробою стало внесення його на розгляд Держдуми 3 грудня 1999 р., а 19 червня 2001 р. він був відкликаний самим суб'єктом законодавчої ініціативи. Неоднозначним є визначення самого поняття «міжнародна інформаційна безпека», що тлумачиться як «*стан міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав і світового співтовариства в інформаційному просторі*».

Один із пунктів КЗМІБ входить у протиріччя із положеннями Конвенції про кіберзлочинність. Так з-поміж загроз, що призводять до порушення міжнародного миру й безпеки, (а отже, можуть розглядатися як порушення міжнародної інформаційної безпеки) є і «*неправомірне використання інформаційних ресурсів іншої держави без погодження з державою, в інформаційному просторі якої розташовані ці ресурси*» (без пояснення того, що в даному контексті означає «неправомірне»). Країни, що підписали Конвенцію про кіберзлочинність, уже погодилися з можливістю подібної ситуації й сприймають її як свідомий крок на шляху до більш безпечної мережі. Безумовно, з погляду традиційних загроз подібне положення Конвенції про кіберзлочинність видається конфліктним щодо захисту національного суверенітету, водночас враховуючи специфічний тип загроз, якими є кібератаки і кіберзлочинність в цілому, подібне положення виглядає як виправдане. Таким чином малоймовірно, що КЗМІБ отримає схвальні відгуки з боку цих держав.

Варто зауважити, що текст КЗМІБ є надмірно рестриктивним (забороняючим), вміщуючи в собі значний перелік заборонених дій, значна частина яких просто не може бути відслідкована й процесуально закріплена. До таких заборон можна віднести «*маніпулювання інформаційними потоками у інформаційному просторі інших держав, дезінформація й втаємничення інформації з метою викривлення психологічного та духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних та естетичних цінностей*». Не зовсім

зрозуміло, яким чином держави мають на рівні національного законодавства визначати поточний стан «психологічного й духовного середовища суспільства», зафіксувати «традиційні культурні, моральні, етичні та естетичні цінності» з метою подальшого їх захисту й можливості визначення статусу «інформаційної війни».

Деякі пункти КЗМІБ є спільними для американської ініціативи і цілком доречними й актуальними для української сторони. З-поміж них виділимо такі:

• загроза протидії доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності у сфері інформатизації на збиток іншим державам;

• потенційна небезпека включення до інформаційно-комунікаційних технологій не декларованих деструктивних можливостей;

• відмінності в ступені оснащеності інформаційно-комунікаційними 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 піднімає питання про межі суверенітету держави щодо інформаційного (кібер) простору. На думку авторів КЗМІБ, «*кожна держава-учасник має право встановлювати суверенні норми і керувати у відповідності із національними законами своїм інформаційним простором. Суверенітет і закони розповсюджуються на інформаційну інфраструктуру, що розташована на території країни-учасника чи іншим чином входить у його юрисдикцію*».

На сьогодні така позиція скоріше відповідає довгостроковим інтересам Української держави. На жаль, американська ініціатива лише побіжно висвітлює дане питання, зупиняючись на проблемі «сумісності» технологічних рішень.

Водночас у КЗМІБ, як і в американській Стратегії, присутня теза про те, що «*кожна держава-учасник має невід'ємне право на самозахист перед обличчям агресивних дій в інформаційному просторі при умові достовірного встановлення джерела загрози і адекватності зворотних дій*». У такій редакції подібна норма є більш прийнятною (відносно американського варіанту), однак виникає питання щодо конкретних механізмів визначення «достовірного джерела» та обсягу «адекватності зворотних дій».

Таким чином, незважаючи на те що з формального погляду обидві політичні ініціативи викладені у відповідності до класичних трактувань демократичного устрою, очевидно, ані американська, ані китайсько-російська ініціативи не стануть дійсно загальносвітовими, оскільки кожна з них містить підходи, що є неприйнятними для низ-

ки країн. У нинішній редакції ініціативи видаються не до кінця прийнятними для України, яка має отримати більш чіткі роз'яснення від авторів документів щодо окремих положень таких ініціатив і особливо стосовно механізмів використання військових засобів реагування на кібератаки.

Водночас, оскільки ініціативи містять низку спільних положень, що не викликають суперечності сторін, доречно було б зосередитися саме на тезах, які б могли стати основою для вироблення спільної ініціативи щодо кіберпростору.

У цьому контексті актуальним є питання того інституту (організації), на базі якого мають напрацьовуватися правила. Незважаючи на статус ООН як головної організації з питань миру й безпеки, прийняття рішень у межах цієї організації з кожним роком дедалі більше ускладнюється. Крім того, ймовірність прийняття обов'язкового для виконання документа (яким є Конвенція) з питань кібербезпеки оцінюється експертами як низька. Мало перспективними є проголошені односторонні ініціативи, що, скоріше, не знайдуть повноцінного схвалення серед інших країн, які дедалі більше тяжіють до вироблення спільних рішень та ініціатив. Усе це обумовлює необхідність пошуку інших форм міжнародних домовленостей, у межах яких кожна з країн зможе мати рівний голос, а сама міжнародна домовленість не буде виглядати як нав'язана однією зі сторін.

Зважаючи на вище викладене, оптимальним варіантом організації, від імені якої має виходити дана ініціатива, є Організація з безпеки і співробітництва в Європі. Сама історія організації, що виникла як елемент добровільно взятих на себе потужними геополітичними гравцями політичних зобов'язань (унаслідок підписання у 1975 р. заключного акту Ради з безпеки і співробітництва в Європі), чим сприяла зменшенню напруги у міжнародних відносинах і налагодженню конструктивного співробітництва між країнами-підписантами, може стати одним із факторів успішності ініціативи щодо питання кібербезпеки. Начебто «європейський» (регіональний) аспект діяльності організації, насправді є доволі умовним, оскільки з організацією співпрацюють африканські та азійські країни.

Україна у 2013 р. обійме головування в ОБСЄ, тому вбачається цілком доречним, що саме вироблення прийнятного міжнародного договору з проблеми кібербезпеки може стати однією з основних ініціатив, що будуть запропоновані Україною в безпековій сфері. Вбачається реальним протягом 2013 р. напрацювати редакцію документа, що буде в цілому задовольняти всіх учасників ОБСЄ та країни, що переймаються кібербезпековою проблематикою.

Перевагою цього документа може стати:

• рівень ініціації (загально визнана організація з питань безпеки);

• характер взятих зобов'язань (добровільність, зобов'язання політичного характеру);

• відображення найбільш суттєвих для всіх країн проблем, що не викликають протиріч між учасниками.

Важливим моментом є те, що ОБСЄ вже має певні напрацювання щодо кібербезпекової проблематики. У травні 2011 р. в м. Відні (Австрія) відбулась конференція «Комплексний підхід до кібербезпеки: роль ОБСЄ», на якій обговорювалося широке коло питань із проблем кібербезпеки (військово-політичні, кіберзлочини і тероризм, глобальна відповідальність, регіональна відповідальність, потенційна роль ОБСЄ).

У межах головування України в ОБСЄ видається цілком доцільним ініціювати проведення в Києві у 2013 р. відповідної міжнародної конференції з даної тематики, що має обговорити як наявні міжнародні ініціативи, так і запропонувати власний проект консенсусного документа з міжнародних правил використання кіберпростору.

ВИСНОВКИ

Відмічаючи високий рівень активності й зацікавленості міжнародного співтовариства щодо стратегічного вирішення проблем розвитку кіберпростору та його майбутнього на віддалену перспективу, враховуючи останні ініціативи США, КНР і РФ щодо майбутнього (у т.ч. безпекового) кіберпростору, можна зробити наступні висновки.

1. Геополітичні гравці активно пропонують свій порядок денний щодо майбутнього кіберпростору. Кожен з них пропонує своє бачення того, що є дійсно «правилами поведінки» держав у кіберпросторі, та які стратегічні цілі мають переслідуватись при його розбудові.

2. Пропоновані американською стороною ініціативи, скоріше, так і не будуть реалізовані в повному обсязі у загальносвітовому масштабі, й не в останню чергу – через неприйнятність окремих положень цих ініціатив для інших країн. Серед таких «дискусійних положень» можна відмітити окремі пункти Конвенції про кіберзлочинність, неготовність деяких країн прийняти тезу про абсолютну «вільність інформаційних потоків» та дискусію з проблеми «управління Інтернетом» (як в аспекті підпорядкованості такого управління, так і самого наповнення цього поняття).

3. Водночас США обрали результативну стратегію налагодження двосторонньої співпраці (Австралія, Японія, Індія) в межах своєї Стратегії й розширення дії Конвенції про кіберзлочинність, як чинного міждержавного правового документа, що вже підписаний та ратифікований низкою країн, а отже, функціонує і формує політику кібербезпеки цих країн. Важливою частиною загальної позиції США з даного питання є відсутність необхідності розроблення нових документів у сфері кібербезпеки.

4. Сумнівними виглядають і перспективи ініціатив РФ та КНР. У стратегічній перспективі прийняття міжнародного документа (і на рівні політичної декларації, і міжнародного правового документа у вигляді Конвенції) є вірним кроком до посилення загальносвітової стабільності в кіберпросторі, однак малоймовірним на практиці, через неприйнятність цілої низки положень запропонованих документів окремими країнами. Додатково малоймовірним є його прийняття в межах ООН.

5. Не можна не відмітити і певну абстрактність (невизначеність) деяких із цих документів (зокрема запропонованої РФ Конвенції), що зробить неможливим (чи вкрай складним) впровадження її на практиці на національному рівні.

6. Варто зауважити, що всі запропоновані ініціативи у їхніх нинішніх редакціях не повною мірою відповідають національним інтересам України і навряд чи зможуть дійсно ефективно вплинути на формування міжнародного консенсусу з питання майбутнього кіберпростору. У нинішній редакції малоймовірно, що Україна зможе їх підтримати.

7. Водночас створення реального міжнародного консенсусу з проблем кіберпростору між основними геополітичними гравцями є об'єктивною необхідністю, що унеможливить подальше стрімке зростання кіберзагроз, як на національному, так і міжнародному рівні. Окремі положення всіх розглянутих ініціатив мають спільні риси і однаково трактують певні загрози. Відповідно, ці проблеми і спільні підходи мали б стати основою для широкого діалогу щодо формування консенсусу.

8. Україна, як країна, що вже сьогодні зазнає впливу кіберзлочинності, об'єктивно зацікавлена в тому, щоб приймати в цих дискусіях більш активну роль, і не лише на рівні чинних дискусійних майданчиків (на кшталт Комітету Конвенції з кіберзлочинності), а й у профільних групах експертів. Проблема вироблення консенсусного документа з проблем кіберпростору може стати провідною темою під час головування України у 2013 р. в ОБСЄ. Саме ця структура, зважаючи на історію її виникнення, є одним з найбільш реальних варіантів, на базі якого може бути віднайдено необхідні точки перетину інтересів головних геополітичних гравців.

ЗМІСТ

Наукове видання

Дубов Дмитро Володимирович
Ожеван Микола Андрійович

МАЙБУТНЄ КІБЕРПРОСТОРУ ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ: НОВІ МІЖНАРОДНІ ІНІЦІАТИВИ ПРОВІДНИХ ГЕОПОЛІТИЧНИХ ГРАВЦІВ

Аналітична доповідь

Літературний редактор: *В. М. Сизонтов*
Коректор: *Є. Ю. Стрижеус*
Комп'ютерне верстання: *Є. Ю. Стрижеус*

Відповідальний за випуск: *В. М. Сизонтов*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел. (044) 234-50-07

Формат 60x84/16. Ум. друк. арк. 1,86. Обл.-вид. арк. 2,08.
Тираж 200 пр. Зам. № 12-554.

Віддруковано ПП «Вид-во «ФЕНІКС»
вул. Шутова, 13-Б, м. Київ, 03680
Тел. (044) 501-93-01
Свідоцтво суб'єкта видавничої справи ДК № 271 від 07.12.2000