АНАЛІТИЧНА ДОПОВІДЬ

Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців

НІСД 2012

З М І С Т

Автори:

Дубов Д.В. – завідувач відділу досліджень інформаційного суспільства та інформаційних стратегії НІСД

Ожеван М.А. – головний науковий співробітник відділу досліджень інформаційного суспільства та інформаційних стратегії НІСД

Вступ

Останні 10 років регулювання кіберпростору вже не є виключно «внутрішньою справою» окремих держав. Можливість використання кіберпростору організованими злочинними угрупованнями, зловмисниками-одинаками, формалізованими та неформалізованими деструктивними політичними групами, військовими та спеціальними службами держав з метою вчинення злочинів, здійснення хакерських атак за політичними мотивами, деструктивного впливу на військову та цивільну інфраструктуру (в тому числі критичну), збір чутливої інформації, а також пряме шпигунство в інтересах держави чи потужних корпорацій, робить неможливим ігнорування даної проблеми з боку світової спільноти.

Про рівень занепокоєності провідних геополітичних «гравців» щодо даного питання свідчать різноманітні дискусії (зокрема на найвищому рівні), що пропонують визнавати кібернапади «актом війни», кіберзброю прирівнювати до зброї масового ураження, а також відповідати на хакерську атаку звичними видами озброєнь (наприклад, ракетним ударом). Проблема додатково ускладнюється відсутністю єдиного погляду ключових «гравців» на кіберпростір та кібербезпеку в цілому, а також посиленням загальносвітової дискусій довкола забезпечення авторських та суміжних прав у мережі інтернет.

До останнього часу проблема кібербезпеки на міжнародному рівні була вирішена лише частково – у сфері протидії кіберзлочинності. Йдеться про прийняту Радою Європи у 2001 році Конвенцію про кіберзлочинність, що відносила до сфери кіберзлочинів такі.

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ до комп'ютерної системи або її частини; нелегальне перехоплення комп’ютерних даних; втручання в комп’ютерні дані; втручання у комп’ютерну систему; зловживання пристроями.
2. Правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами.
3. Правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією.
4. Правопорушення, пов'язані з порушенням авторських та суміжних прав.

Водночас далеко не всі країни (з-поміж тих, що входять до Ради Європи) ратифікували цей документ (зокрема принципову позицію з цього питання посіла Російська Федерація). Крім того, вказаний документ є регіональним, хоча до нього долучаються й інші країни світу, та не вирішує зазначених вище питань воєнного використання кіберпростору, глобальних міжнародних підходів до кібербезпеки тощо.

Невизначеність на глобальному рівні та відсутність єдиних підходів змушує керівництво держав формувати політику кібербезпеки на національному рівні. Більшість держав світу вже створили відповідні

підрозділи (як правоохоронні, так і військові), призначені для протидії кіберзагрозам та розроблення наступальних технологій.

З метою вирішення даної проблеми низка ключових світових держав (США, КНР, Російська Федерація) виступають з власними ініціативами щодо впорядкування на глобальному рівні питань кібербезпеки (інформаційної безпеки), однак запропоновані підходи не лише слабко узгоджуються між собою, а й подеколи протирічать одне одному. З огляду на те, що США зберігає статус єдиної наддержави низка ініціатив у її національному законодавстві цілком можливо вплине на міжнародну ситуацію з даного питання чи принаймні може задати основний тренд реформування національних законодавств в інших країнах.

Дана аналітична доповідь присвячена питанню висвітлення ключових міжнародних правових та політичних ініціатив (або таких національних ініціатив/законопроектів, що можуть мати суттєвий вплив на міжнародне правове поле) у сфері кібербезпеки, визначення можливих проблемних напрямів при реалізації таких ініціатив та можливої позиції щодо них України.

1. Ініціативи Сполучених Штатів Америки щодо майбутнього кіберпростору

США залишається одним з основних «гравців», що визначають перспективи розвитку кіберпростору та потенційні напрями його регулювання (або формування політики з цього питання).

Ключова зовнішньополітична ініціатива США щодо перспектив розвитку кіберпростору була оприлюднена 16 травня 2011 року з назвою **Міжнародна стратегія для кіберпростору** (International Strategy for Cyberspace – *далі* Стратегія)[1]. Даний документ не лише визначає принципові положення, що з них виходитимуть США при формуванні власної політики щодо кіберпростору, а й окреслює бажане «очікуване майбутнє» кіберпростору для США.

«Базовими принципами», що мають бути забезпечені при формуванні політики щодо кіберпростору, було визначено такі.

1. «Фундаментальні свободи» (можливість шукати, отримувати та передавати інформацію та ідеї через будь-які засоби зв'язку та незважаючи на кордони).
2. «Прайвесі» (усвідомлення користувачами кіберпрстору загроз їх персональній інформації та можливость вчинення проти них кіберзлочинів).
3. «Вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, адже вони лише створюють видимість безпеки. Кіберпростір має бути місцем інновацій та співпраці держави та бізнесу задля більшої безпеки).

Щодо **бажаного майбутнього** в кіберпросторі для США, то в контексті теми аналітичної доповіді особливий інтерес становлять тези, що стосуються міжнародного регулювання (або бачення в цілому) кіберпростору.

Документ виокремлює три стратегічні цілі, що мають бути досягнуті за реалізації Стратегії.

1. **Відкритість та сумісність**. Розвиток цифрових систем має невпинно спричинювати здешевлення доступу до кіберпростору дедалі більшій кількості людей. Для поширення цих процесів впроваджувані інновації мають бути сумісними між собою, а також активніше 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 за національними кордонами з метою заборони доступу до сучасного контенту великим групам людей через особливі політичні інтереси держав. Відповідно пріоритетом є розроблення нових інформаційних технологій, що засновані на міжнародних стандартах, які забезпечать зростання цифрової економіки та рух суспільства вперед.

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

2. **Безпека та надійність**. Користувачі мають бути впевнені в безпеці своїх даних. Забезпечення цього є завданням поліаспектним та таким, що потребує відповідальності на всіх рівнях починаючи від пересічних користувачів і закінчуючи державними органами та ефективної міждержавної співпраці. Ключовим питанням є встановлення міжнародних технічних стандартів (щодо програмного та апаратного забезпечення та систем управління інцидентами) та узгоджених міжнародних норм поведінки держав. Усе це потребуватиме розширення співпраці з питань обміну технічною інформацією між державним сектором та приватним, а також окремою державою та міжнародним співтовариством. Оскільки основним елементом надійності є безпека мереж, США готові інвестувати в них не лише на національному рівні, а й сприяти посиленню надійності мереж за кордоном.

3. **Стабільність через норми**. Ця мета дозволяє в цілому зрозуміти американське бачення чинного міжнародного правового поля щодо кіберпростору та орієнтирів його трансформації. Вироблення єдиних правил поведінки в кіберпросторі – ключове завдання, адже їх «*вироблення… сприятиме передбачуваності поведінки держав, що дозволить попереджувати конфліктні ситуації чи непорозуміння*», і США готові працювати над виробленням консенсусної точки зору щодо критеріїв «*прийнятної поведінки*», а також партнерства в кіберпросторі. При цьому США не бачать необхідності додатково ухвалювати принципово нові міжнародні документи, оскільки чинне міжнародне законодавство не є «*застарілим*» щодо реалій кіберпростору: «*розробка правил поводження держави у 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*». Водночас визнається необхідність певного доопрацювання зазначених 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 задля досягнення консенсусу щодо використання норм поведінки у кіберпросторі, усвідомлюючи важливість першого кроку у даному напрямку, та в очікуванні мирного та справедливого поводження у кіберпросторі*».

Пріоритетом для США є згадана **Конвенція з кіберзлочинності**. Саме 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 вказується, що США розглядає «*подальші дискусії щодо міжнародних норм*» протидії кіберзлочинності передусім як «*поширення чинних зусиль, таких як Будапештська конвенція*», на всіх учасників. Крім того, докладатимуться зусилля для налагодження двосторонньої співпраці

між державами. Другий пункт зазначеного розділу прямо вказує на необхідність узгодження національних нормативно-правових документів у сфері протидії кіберзлочинності з Будапештською конвенцією, яка, на думку авторів Стратегії, «*є моделлю для розробки та оновлення чинних законів*» у відповідній сфері. США, зі свого боку, зобов'язуються стимулювати інші країни приєднуватися до Конвенції.

Можна прогнозувати, що в разі довгострокового інтересу США до просування Конвенції з кіберзлочинності як основного документа для двостороннього та багатостороннього співробітництва докладатимуться зусилля з перетворення цього документа на своєрідний міжнародний договір.

Водночас у нинішній редакції Конвенція не зможе охопити всі країни, що відіграють ключову роль у питаннях кібербезпеки. Так, Російська Федерація не підписала[2] Конвенцію, і можна передбачити, що не зробить цього доти, доки з документа не буде прибрано низку положень, що не влаштовують російську сторону. До таких передусім належать положення Конвенції про те, що та чи інша країна може отримувати доступ до ресурсів, розташованих у мережах загального користування іншої держави, не повідомляючи про це таку державу[3]. Малоймовірно, що на таке положення погодиться й Китай, й ціла низка інших країн (докладніше позиції Російської Федерації та КНР з проблем розвитку кіберпростору буде наведено у Розділі 2 Доповіді).

Крім вищезазначеного, у Стратегії визначено орієнтовну модель поведінки держав стосовно Всесвітньої мережі та окремих аспектів її роботи:

- ***дотримання основних свобод***. Держави мають поважати свободи слова та зібрань, що так само актуальні для он-лайну, як і для офф-лайну;
- ***повага до власності***. Держави у своїх ініціативах мають поважати право на інтелектуальну власність, включно з патентами, торговими таємницями, товарними знаками та авторськими правами;
- ***цінність приватного життя***. Громадяни-користувачі інтернету мають бути захищені від довільного/незаконного втручання у їхнє приватне життя;
- ***захист від злочинів***. Держави мають виявляти та переслідувати кіберзлочинців, створювати таке законодавство та практики, що не дозволять зловмисникам переховуватися на їх території, а також сприяти співробітництву з міжнародними структурами, що переслідують таких злочинців;

[2] Convention on Cybercrime // http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[3] Йдеться 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».

- ***право на самозахист***. Відповідно до Статуту ООН держави мають право на самозахист, що може бути застосований у відповідь на агресивні дії у кіберпросторі;
- ***глобальна сумісність***. Держави мають вживати заходів, що сприятимуть максимальній сумісності та зручності використання мережі інтернет, а також її доступності якнайбільшій кількості громадян;
- ***мережева стабільність***. Держави мають поважати свободу потоків інформації у національних мережах та не втручатися в роботу тієї інфраструктури, що відноситься до такої, що тісно пов'язана з міжнародною функціональністю мережі;
- ***надійний доступ***. Держави не мають штучно заважати доступу громадян до мережі інтернет чи мережевих технологій;
- ***багатостороннє управління***. Управління мережею інтернет не має обмежуватися виключно урядами, а повинне здійснюватися й іншими стейкхолдерами;
- ***особлива увага до кібербезпеки***. Держави мають визнавати свою відповідальність за безпечність на надійність роботи власних сегментів мережі інтернет та відповідної інфраструктури.

На особливу увагу в цьому переліку заслуговують два пункти: «право на самозахист» та «надійний доступ» (а також пов'язаний з ним пункт про «дотримання основних свобод»).

Посилання на Статут ООН у пункті «право на самозахист» переводить проблему з площини суто карних злочинів на рівень національної безпеки та військових загроз. Стаття 51 Статуту ООН однозначно стверджує «*невід'ємне право на індивідуальний чи колективний самозахист, якщо відбудеться військовий напад на Члена Організації*». Крім того, варто зважати на артикульовану заступником міністра оборони США В. Лінном позицію щодо права США відповідно до законодавства цієї країни «*у відповідь на серйозну кібератаку застосування пропорційну та обґрунтовану військову відповідь у час та місце, яке ми оберемо самі*»[4].

Відповідно до резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 року «агресією» вважається «*застосування збройних сил державою проти суверенітету, територіальної цілісності чи політичної незалежності іншої держави, або будь-яким іншим способом, що несумісні з Статутом Організації Об'єднаних Націй, як це встановлено в цьому визначенні*» (стаття 1). У цій самій Резолюції (стаття 3) подано перелік дій, що будь-що кваліфікуватимуться як «воєнні акти»:

1) 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

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

нападу, або інша анексія з використанням сили території іншої держави чи її частини;
2) бомбування збройними силами держави території іншої держави чи використання будь-якої зброї державою проти території іншої держави;
3) блокада портів чи берегів держави збройними силами іншої держави;
4) напад збройними силами держави на сухопутні війська, морські та повітряні флоти іншої держави;
5) використання збройних сил однієї держави, що знаходяться на території іншої держави за її згодою, в порушення умов, що передбачені угодою, чи будь-яке продовження перебування на такій території після припинення дії угоди;
6) дія держави, яка дозволяє, щоб її територія, яку вона надала в розпорядження іншої держави, використовувалася для здійснення акту агресії проти третьої держави;
7) засилання державою чи від її імені озброєних банд, груп, іррегулярних сил чи найманців, які здійснюють акти використання 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 передбачають фізичний контакт двох держав, найчастіше – з використанням кінетичної зброї. Кібератаки (вже через саму невизначеність національного кіберпростору) є розпорошеними, встановити їх належність саме державним органам, а надто 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 буде застосовано можливі санкції.

За таких умов вкрай сумнівно, що кібератака згідно з чинними міжнародними документами дійсно може кваліфікуватися як «агресія» чи «напад», а надто спричинювати воєнну відповідь. Водночас у Стратегії безпосередньо йдеться про те, що США готові застосовувати «*дипломатичні, інформаційні, військові та економічні*» засоби для реагування на інциденти. На даний момент досі незрозуміло, яким чином подібне положення може бути реалізоване на практиці без внесення кардинальних змін до Резолюції ООН, що надає визначення «агресії». Поки існують лише окремі наукові напрацювання у сфері міжнародного права, що пропонують або визнати кіберзброю зброєю масового ураження, або (що виглядає реальніше) виробити механізм оцінки наслідків від здійснення кібератак та порівнювати їх з можливими наслідками від застосування традиційних озброєнь.

Проблемі «надійного доступу» та «дотримання основних свобод» присвячено розділ Стратегії «Інтернет-свобода: підтримуючи

фундаментальні свободи та прайвесі». У розділі наводиться чотири основних напрями зусиль США з цього питання.

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

2. **Співробітництво з громадянським суспільством та неурядовими організаціями щодо підвищення їх кібербезпеки** (зокрема їхніх електронних поштових адрес, веб-сайтів, мобільних телефонів, інших засобів).

3. **Сприяти міжнародному співробітництву для ефективнішого захисту конфіденційності комерційних**.

4. **Забезпечити наскрізну сумісність систем, задіяних у передачі інформації в мережі інтернет**.

Тематиці «основних свобод» в інтернеті було присвячено грунтовний **виступ Держсекретаря США Г. Клінтон** під час конференції про свободу в інтернеті, що відбулася 8 грудня 2011 року в Гаазі[5].

Держсекретар виступила з критикою практики затримання блогерів-громадських активістів (наприклад, О. Навального в Російській Федерації) та практики китайського уряду, пов'язаної з укладанням спеціальних угод із компаніями, що надають телекомунікаційні послуги[6].

Заяви пані Клінтон з приводу необхідності врегулювання зазначеного питання також цілком вкладаються в запропонований Стратегією формат забезпечення положень про «фундаментальні права»: *Виконання належного у стосунку інтернет-свободи вимагає спільних дій, і ми повинні зав'язати розпочати глобальну розмову на основі загальних принципів…* ***Ця справа не є питанням погодження на переговорах єдиного документу і оголошення, що роботу зроблено***. *Вона вимагає постійних зусиль, щоб враховувати нову*

[5] *Промова* Державного секретаря Гілларі Клінтон на конференції про свободу в інтернеті [Електронний ресурс]. – Режим доступу: http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html

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

реальність, в якій ми живемо, в цифровому світі, і робити це таким чином, щоб максимальними були переваги, який він обіцяє[7].

Водночас у промові було порушено три додаткові проблеми, що дозволяють дійти висновків про довгострокові плани США щодо кіберпростору.

1. **Приватний сектор має виконати свою роль у захисті інтернет-свободи**. На думку Г. 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** і не чекати 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 столітті розумні компанії повинні вживати заходів до того, як вони потраплять суперечливе становище***». Подібна позиція США концептуально не збігається з панівною (у публічному дискурсі) неоліберальною концепцією «вільного ринку», відповідно до якої роль держави полягає саме у встановленні граничних меж ринку, але не у саморегулюванні на основі «розумності» цього процесу.

2. **Недопущення 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 громадянами, 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*». Основна занепокоєність США полягає у можливості створення національних правил гри для окремих сегментів мережі, що порушує принцип сумісності в інтернеті. **В більш широкому сенсі США виступають категорично проти будь-яких бар'єрів у кіберпросторі, що можуть трактуватися як своєрідні «кордони держави в кіберпросторі»**. Причому Г. Клінтон рішуче відкидає зв'язок цієї проблеми з питаннями безпеки (протидією кіберзлочинності, запобіганням поширенню

[7] Тут і далі усі цитати з промови Г. Клінтон дослівно подано в перекладі, розміщеному на офіційному сайті Посольства Сполучених Штатів.

дитячої порнографії, боротьбою з кібертероризмом), наголошуючи, що ці проблеми мають вирішуватися у інший спосіб, не порушуючи «*динамізм інтернету*».

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 сьогоднішній день важко сказати, наскільки успішною буде практична реалізація Стратегії та чи отримає вона загальносвітову підтримку. **Можна очікувати, що більшість європейських країн та частина країн Східної півкулі (наприклад, Японія, Австралія, Нова Зеландія) пристануть до цього підходу**. Крім того, деякі з цих країн 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[8]. У вересні 2011 року Австралія та США включили проблему співробітництва з протидії кіберзагрозам до договору про взаємну оборону[9]. У жовтні 2011 року, під час спільної прес-конференції міністрів оборони США та Японії, очільник японського військового відомства Я. Ітікава зазначив, що сторони активно обговорюють питання поглиблення співробітництва у сфері кібербезпеки[10].

Активність США щодо розвитку міжнародної співпраці зіштовхується з певними складнощами. Доволі детально причини проблем співпраці з країнами-партнерами США щодо технологій та методів протидії кіберзагрозам висвітлив начальник розвідки кіберкомандування контр-адмірал С. Кокс, виступаючи в Джорджтаунському університеті на семінарі, присвяченому кібербезпеці. На його думку, однією з головних проблем є у слабка захищеність комп'ютерних систем союзників США по НАТО, що призводить до легкого доступу супротивників до інформації, якою США діляться із союзниками. Щоправда, С. Кокс публічно[11] не називав країни з вразливими комп'ютерними мережами, хоча зазначив, що з-поміж цих країн немає Канади, Великобританії, Австралії й Нової Зеландії, з якими США тісно співробітничають у військовій та безпековій сферах.

Ще однією проблемою, що гальмує співпрацю воєнних відомств країн НАТО та партнерських країн, є надмірна засекреченість військових технологій і технологій подвійного призначення, а також надто жорсткі американські закони щодо експортного контролю трансферу таких

[8] India, US ink an agreement on cyber security // http://economictimes.indiatimes.com/news/politics/nation/india-us-ink-an-agreement-on-cyber-security/articleshow/9282199.cms
[9] Cyber Cooperation Added To U.S.-Australia Treaty // http://www.officialwire.com/main.php?action=posted_news&rid=44771
[10] Japan-U.S. Defense Ministers' Joint Press Conference // http://www.mod.go.jp/e/pressconf/2011/10/111025_japan_us.html
[11] У США трудности с партнерами по противодействию киберугрозам [Електронний ресурс]. - Режим доступу: vestnik-sviazy.ru

технологій, відповідно до яких Пентагон часто не має права продавати чи надавати ці технології іншим країнам.

Є обґрунтовані сумніви, що Стратегію в повному обсязі сприймуть КНР та Російська Федерація. Незважаючи на те, що, на думку деяких експертів[12], співробітництво з питань кібербезпеки в трикутнику США-КНР-РФ налагоджується (зокрема з питань визначення термінології та пожвавлення діалогу), є кілька позицій, що можуть стати принциповим моментом, який найближчим часом ці держави не зможуть подолати.

По-перше, як вже згадувалося, ключовий, на думку США документ щодо поліпшення глобальної кібербезпеки - Конвенція з кіберзлочинності – щонайшвидше не буде підписана РФ до внесення суттєвих змін до її тексту, що своєю чергою видається малоймовірним у осяжній перспективі. Водночас навіть у разі подальшого розширення дії цього документа (за рахунок збільшення країн-учасників) можна очікувати, що аналогічну російській позицію посяде і КНР. Таким чином, зважаючи на акцентування уваги з боку США щодо продовження просування 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 збігається з поглядом РФ і КНР (а також деяких інших країн) на те, яким саме 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 входить не лише РФ та КНР, а й значна кількість європейських, латиноамериканських та африканських країн) - з іншого, зможуть знайти дійсно єдину (консолідовану) точку зору щодо проблеми управління інтернетом. США однозначно посяде позицію щодо продовження контролю за мережею корпорацією ICANN. Незважаючи на вихід корпорації з-під контролю американського уряду у 2009 році, більшість країн світу, передусім КНР, 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 (а фактично заміщують) кібербезпеку як ключову проблему інформаційної безпеки. Вони вважають, що кібербезпека має розглядатися виключно як частина інформаційної безпеки, яка б охоплювала і всю низку гуманітарних питань (що регулюватимуться державою відповідно до принципів забезпечення національної безпеки).

[12] США и Россия усиливают сотрудничество по кибербезопасности // http://inosmi.ru/social/20111005/175569908.html

2. Ініціативи Російської Федерації та Китайської Народної Республіки щодо майбутнього кіберпростору

Якщо значна частина держав ще не визначилася з офіційною позицією щодо кіберпростору та основних принципів його функціонування, деякі країни почали просування альтернативних проектів регулювання (правил поведінки) у кіберсфері (або за визначеннями деяких відповідних документів – «сфері міжнародної інформаційної безпеки»).

Основна концептуальна відмінність, що вирізняє ці альтернативні проекти від американських ініціатив – **фактична відсутність розрізнення кібербезпеки від більш широкого (а іноді й доволі абстрактного) поняття «інформаційно-психологічної безпеки»**. РФ послідовно обстоює позицію, що кібербезпеку не можна розглядати як напрям, що існує окремо від соціальних, політичних, економічних і військових наслідків застосування сучасних інформаційних технологій. Понад те, за такого підходу взагалі недоречно говорити про абсолютно «вільні потоки інформації», оскільки безпекова тематика охоплює і наслідки їх впливу на державу та її громадян. Отже, застосування поняття «кібербезпеки» (навіть у міжнародному контексті) є не зовсім правильним, адекватнішою назвою даної проблеми є «інформаційна безпека» чи «міжнародна інформаційна безпека».

РФ розпочала дискусію щодо необхідності затвердження норм і правил у сфері міжнародної інформаційної безпеки з 1998 року. Однак до 2009 року жодних реальних результатів так і не було досягнуто. Першим проміжним успіхом можна вважати створену в 2009 році (відповідно до Резолюції 60/45 Генасамблеї ООН) Групи урядових експертів ООН з міжнародної інформаційної безпеки[13]. Ця група за рік роботи підготувала звіт (червень 2010 року), в якому в загальному вигляді сформульовано основні ризики, загрози від використання сучасних ІКТ. І хоча в тексті звіту відсутні однозначні тези про гуманітарні та політичні загрози (крім положення про зростання використання ІКТ з військовою та розвідувальною метою), РФ, посилаючись саме на роботу Групи, намагається просувати свої проекти міжнародних документів у сфері забезпечення міжнародної інформаційної безпеки.

Одним з таких документів є **Конвенція про забезпечення міжнародної інформаційної безпеки**[14] (КЗМІБ), представлена під час Другої міжнародної зустрічі високих представників, що курують питання безпеки (20-21 вересня 2011 року, Єкатиренбург)[15]. Концепція документа повною

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

[14] Конвенция об обеспечении международной информационной безопасности (концепция) // http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

[15] Учасниками є 52 країни. Рівень представництва – вищі особи, що відповідають за координацію діяльності правоохоронних структур. Від України представником була Секретар РНБО України Р. Багатирьова.

мірою відповідає російським поглядам на інформаційну безпеку і значною мірою опонує вищезгаданим американським документам та підходам. Зокрема, в російській КЗМІБ звертається увага на те, 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 якого знаходяться ці ресурси;
- діяльність в інформаційному просторі з метою підриву політичної, економічної та соціальної системи іншої держави, психологічний вплив на населення, що дестабілізує суспільство;
- маніпулювання інформаційними потоками і інформаційним простором інших держав, дезінформація та втаємничення інформації з метою викривлення психологічної та духовної сфери суспільства, ерозія традиційних культурних, етичних та естетичних цінностей;
- протидія доступу до новітніх інформаційно-комунікативних технологій, створення умов технологічної залежності у сфері інформатизації, що може загрожувати іншим державам[16]. При цьому схоже, що цей пункт, незважаючи на співзвучність з тезами американської Стратегії, має принципово інший зміст. США кажуть про «*обмеження доступу до технологій*» у контексті обмеження доступу для населення з боку урядів, в той час як РФ вочевидь має на увазі формальні та неформальні міждержавні обмеження (наприклад, через поправку Джексона-Веніка);
- інформаційна експансія, встановлення контролю над національними інформаційними ресурсами іншої держави.

На думку деяких оглядачів[17], російський МЗС сподівається, що даний варіант КЗМІБ буде внесено (та прийнято) на розгляд Генасамблеї ООН вже в 2012 році.

Отже, російський документ принципово відрізняється від американського максимально розширюючи сферу «інформаційних загроз». **Понад те, з огляду на цілу низку положень даного документа він, щонайшвидше, не зможе бути основою обговорення для ключових геополітичних «гравців» (зокрема США та тих країн, що поділяють її підходи)**.

Вочевидь, проходження КЗМІБ через ООН буде непростим і малоймовірно, що до нього приєднається більшість країн (зокрема європейських).

Як більш «м'яку» версію КЗМІБ РФ спільно з КНР запропонувала для обговорення інший документ - **Правила поведінки у сфері забезпечення**

[16] Крім традиційних звинувачень з боку РФ на адресу Західних країн у штучному обмеженні доступу новітніх технологій до Росії, цікавим є нещодавній виступ помічника держсекретаря М. Познера, в якому він звернув увагу на те, що авторитарні режими (наводився приклад Лівії) використовують новітні технології, що розроблюються переважно у США, для переслідування своїх політичних опонентів.

[17] Байты наши быстры // http://newtimes.ru/articles/detail/44438/

міжнародної інформаційної безпеки[18]. Спільно з Узбекистаном та Таджикистаном Росія та КНР 12 вересня 2011 року звернулися до Генерального секретаря ООН з листом, в якому пропонують вже на 66-ій сесії Генеральної асамблеї розглянути запропонований ними проект (A/66/359).

Текст Правил є значно меншим за обсягом, ніж КЗМІБ, однак в цілому повторює ключові положення цього документа. Серед іншого Правила звертають увагу на такі моменти.

- Пункт «a» свідчить про «…повагу до основних прав та свобод людини, а також **багатоманітності історії, культури та соціального розвитку всіх країн**».
- Пункт «c» звертає увагу на необхідність співпраці в «боротьбі з злочинною чи терористичною діяльністю з використанням інформаційно-комунікаційних технологій… **що підриває політичну, економічну та соціальну стабільність держав, їх культурний та духовний стан**».
- Пункт «g» спрямований на «**сприяння створенню багатосторонніх, демократичних міжнародних механізмів управління Інтернетом**, які б … гарантували його стабільне та безпечне функціонування».

У самому ООН сторони розпочали супровід своєї пропозиції в межах Першого та Третього комітетів. Під час 6-ої та 7-ої зустрічей Третього комітету[19] Генасамблеї ООН представник делегації КНР при ООН Лі Ксяомеі (Li Xiaomei) зазначила, що китайська сторона висловлює жаль з приводу того, що до останнього часу на міжнародному рівні не було прийнято регулювальних документів, що мали б сприяти встановленню міжнародної інформаційної безпеки.

Однак основна дискусія відбулася в Першому комітеті[20] Генасамблеї під час 17-ої зустрічі (загалом зустріч була присвячена саме обговоренню Правил). Посол КНР Вонг Кун (Wang Qun) звернувся[21] до учасників зустрічі із вступним словом, в якому висвітлив позиції КНР з даного питання. Представник від Росії А. Малов наголосив[22] при цьому, що наданий документ є передусім «запрошенням до діалогу» і ініціатори його внесення не наполягатимуть на його винесенні на голосування. А.Малов також звернув увагу присутніх на те, що розроблена РФ КЗМІБ також є платформою для обговорення, сподіваючись, що вона зможе стати не лише політичною декларацією (якими згідно з власними положеннями мають стати Правила), а

[18] 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

[19] Опікується соціальними та гуманітарними питаннями, а також питаннями культури.

[20] До його компетенції належать питання розброєння та міжнародної безпеки.

[21] Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security // http://www.china-un.org/eng/hyyfy/t869445.htm

[22] Выступление представителя Российской Федерации Андрея Малова в Первом комитете ГА ООН (20 октября 2011) // http://www.unmultimedia.org/radio/russian/archives/98456

й дієвим міжнародним правовим документом. Цю позицію підтримав представник Білорусі[23].

Негативно з цього приводу висловилися представники США та Австралії. В. Рейд (Walter S. Reid, США) зазначив, що питання кіберсфери виходять за межі обговорення у форматі ООН та потребують врахування міжнародного гуманітарного законодавства як бази при обговоренні подібних ініціатив. Фактично аналогічної позиції дотримувався і П. Вулкот (Peter Woolcott, Автсралія), який зазначив, що обговорення кібертематики в ООН буде надзвичайно складним, а багатоаспектність проблеми робить неможливим її обговорення в межах комітету[24]. Крім того, він зазначив, що Австралія повністю підтримує багатосторонній підхід управління інтернетом і принципово проти державного контролю за мережею[25].

Більш розгорнутими та категоричними були оцінки зазначеної ініціативи з боку представників держструктур США. М. Маркофф (Michele Markoff), старший радник Держдепартаменту з питань інтернету, вважає[26], що **подібні проекти є спробою домогтися від ООН схвалення дій щодо посилення контролю над інтернет-простором**. Крім того, пані Маркофф зазначила, що минулого року був укладений договір між 15 країнами, включаючи США, Росію і Китай. Згідно з угодою країни погоджувалися колективно продовжувати обговорення з питання щодо подальшої інформаційної політики у зв'язку з дедалі більшим поширенням інформаційних технологій. У цьому контексті заява КНР та Росії сприймається як вихід з переговорного процесу. Приблизно аналогічну позицію висловив[27] і помічник Держсекретаря М. Познер: «**Якщо такий кодекс буде прийнятий, це майже неминуче підірве свободу ЗМІ** та викличе перехід від кіберпростору, що розвивається пересічними людьми, до системи централізованого контролю з боку урядів. Це не дуже добра ідея».

Не менш однозначним було зауваження з боку Кіберкомандування США (U.S. Cyber Command). Його керівник, генерал К. Александер (Keith B. Alexander), висловився проти того, щоб ООН регулювала інтернет, вважаючи, що це в цілому ослабить загальну безпеку в мережі.

Запропонована китайсько-російська ініціатива викликала доволі різку негативну реакцію також з боку ОБСЄ: представник ОБСЄ з питань свободи ЗМІ Д. Міятович (Dunja Mijatovic) заявила, що **подібні ініціативи є неприпустимими, оскільки потенційно можуть бути використані для**

---

[23] Выступление представителя Беларуси при ООН Игоря Угорича в Первом комитете ГА ООН (20 октября 2011) // http://www.unmultimedia.org/radio/russian/archives/98379

[24] У цьому контексті складно не згадати, що нещодавно (вересень 2011 року) між США та Австралією було укладено додаткові угоди щодо спільної протидії кіберзагрозам та посилення двосторонньої співпраці з даного питання.

[25] Цікаво, що дана позиція була висловлена практично тими самими словами, як вона записана в Міжнародній стратегії розвитку кіберпростору (США).

[26] Huffington Post: Госдеп США обвиняет Россию и Китай в попытках усилить контроль в интернете // http://www.centrasia.ru/newsA.php?st=1317282000

[27] Выступление помощника госсекретаря Познера о свободе слова в эпоху цифровых технологий // http://iipdigital.usembassy.gov/st/russian/article/2011/10/20111026103945x0.8727468.html#axzz1dIC9bFSK

зведення бар'єрів на шляху потоку інформації чи обміну думками[28]. Вона звернула увагу тих країн, що подали відповідне звернення, що в червні 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, і зазначила, що саме цей документ має бути базовим з цього питання.

У колективному листі від неурядових організацій[29] на ім'я Голови 66-ої Генасамблеї ООН Абд аль-Азіза ан-Насера запропонований Кодекс критикується за чотирма напрямами:

- 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, в той час як з цього процесу виключені елементи громадянського суспільства;
- «загальна повага до прав людини» містить суттєве уточнення - «повага до багатоманіття історії, культури та соціальної структури всіх країн», що може бути використано для звуження універсальності прав людини, закріплених, зокрема, в документах Генасамблеї;
- боротьба із 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*». 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 у Лондоні з питань діяльності в кіберпросторі, яка відбулася 1-2.11.2011 з девізом «Бачення. Надії. Страхи» ("the Vision, the Hopes, the Fears") з ініціативи британського МЗС й зібрала 700 делегатів (представників як урядових, так і комерційних структур) з 60-ти країн[30].

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

Фактично вже початок заходу не залишив надії на таке обговорення: міністр закордонних справ Великобританії У. Хейг (William Hague) у виступах під час відкриття та закриття конференції підкреслив, що боротьба

---

[28] ОБСЕ обеспокоена желанием Узбекистана контролировать интернет // http://www.uznews.net/news_single.php?nid=18024

[29] Open letter to President of the UN General Assembly on International Code of Conduct for Information Security // http://www.igcaucus.org/infosecurity-code

[30] Офіційний сай конференції: http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/ Nations discuss cyber security. November 1st, 2011 [Електронний ресурс]. – Режим доступу: http://www.cyberwarnews.info/2011/11/01/nations-discuss-cyber-security/

зі злочинністю та тероризмом не може виправдати спроби підпорядкування інтернету, явно маючи на увазі Пекін і Москву. Цю думку підтримав британський прем'єр Д. Камерон: "Уряди країн світу не повинні використовувати кібербезпеку як привід для запровадження цензури»[31].

Офіційну позицію США на Лондонській конференції представляв американський віце-президент Д. Байден (Joseph Biden), який прямо висловився проти політики країн, які під виглядом боротьби з кіберзлочинністю обмежують свободу діяльності в інтернеті й пропонують укласти «*репресивний глобальний кодекс поведінки в Інтернеті*» ("repressive global code").

До останнього часу до цієї дискусії практично не долучалися країни ЄС. Це може бути пояснено, серед іншого, тим, що в ЄС досі тривають внутрішні дискусії щодо визначення меж свободи/контролю за контентом мережі (наприклад, у межах ініціативи «віртуального шенгену»). Хоча можна очікувати, що вже найближчим часом члени ЄС також приєднаються до цієї дискусії як активні «гравці».

3. Міжнародні ініціативи щодо кіберпростору та національні інтереси України: проблеми реалізації та перспективи

Останніми роками в Україні значно зросла увага до проблем забезпечення кібербезпеки держави та боротьби з кіберзлочинністю. Так, за даними голови Служби безпеки України І. Калініна, вже зараз «*статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів*»[32]. Про актуальність даної проблеми свідчить і зростання кількості злочинів, що кваліфікуються за статтями 361-363 Кримінального кодексу України. Згідно з даними Єдиного державного реєстру судових рішень щодо судових рішень за 16 розділом Кримінального кодексу України за останні 2 роки було прийнято 342 судових рішення (з них 89 - вироки).

Наприкінці 2010 року (10 грудня 2010 року №1119/2010) Указом Президента України 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 було поставлене завдання «*розробити за участю та подати у двомісячний строк на розгляд Ради національної безпеки і оборони України пропозиції*

[31]London hosts cyberspace security conference [Електронний ресурс]. – Режим доступу: http://www.bbc.co.uk/news/technology-15533786. Зазначимо, що подібні заяви з боку Д. Камерона виглядали дивно (про що зауважила 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 та соціальні мережі у разі масових заворушень. Так само є окремі інформаційні повідомлення про те, що уряди західних країн задіяні в блокуванні комунікації усередині популярного нині на Заході антикапіталістичного руху «Окупуй Уол-Стріт!».

[32] СБУ: Головні проблеми для України - тероризм і кіберзлочинність // http://www.pravda.com.ua/news/2012/03/23/6961285/

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*»[33].

На виконання цих завдань наразі розробляється **Закон України «Про кібернетичну безпеку України»**, що має зафіксувати ключові терміни у сфері кібербезпеки, визначити поняття об'єкта критичної інфраструктури та механізми захисту таких об'єктів, 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 знайшли своє відображення у Річній національній програмі співробітництва Україна - НАТО на 2012 рік, у якій проблемі кібербезпеки відведено окремий параграф[34].

Зазначимо також посилення міждержавної співпраці у сфері протидії кіберзлочинності та кіберзагрозам. У жовтні 2010 року СБУ спільно з ФБР і спецслужбами 9 інших країн світу провело операцію «Trident breach» з нейтралізації злочинного хакерського міжнародного угруповання, що з території України несанкціоновано втручалося в роботу закордонних банківських установ, у результаті чого завдано збитків на суму близько 170 млн доларів США. Ця спільна операція була відзначена в щорічному звіті за результатами діяльності ФБР у 2010 році. В червні 2011 року Служба безпеки України спільно з правоохоронними органами США, Великобританії, Нідерландів, Франції, Німеччини, Кіпру, Литви (загалом 10 країн), припинила незаконну діяльність міжнародного злочинного хакерського угруповання під прикриттям комерційної структури, що діяла легально та координувалася громадянами України. За попередніми оцінками у результаті злочинної діяльності вищевказаного угруповання збитки перевищили 72 млн доларів США.

У серпні 2011 року Служба безпеки України в рамках 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. доларів США.

Крім того, українська сторона ініціювала розвиток контактів у сфері протидії комп'ютерної злочинності з ДСТ Франції, КДБ РБ, СІСДе Італії, МГБ Ізраїлю, Національною радою правоохоронних органів Швеції, РСІ Румунії, СІБ Республіки Молдова, ВНБ Угорщини, спеціальними службами

[33] Указ Президента «Про Рішення Ради національної безпеки і оборони України «Про виклики та загрози національній безпеці України у 2011 році» (№1119/2010 від 10.12.2010) // http://zakon2.rada.gov.ua/laws/show/n0008525-10

[34] Указ Президента України № 273/2012 «Про затвердження Річної національної програми співробітництва Україна - НАТО на 2012 рік» // http://www.president.gov.ua/documents/14697.html

Єгипту, Національною поліцією Японії, ДРБ МО Алжиру й Спеціальним комітетом НАТО. На регулярній основі відбуваються експертні консультації експертів Україна-НАТО з питань кібернетичного захисту.

Водночас до останнього часу позиція України щодо запропонованих міжнародних ініціатив є невизначеною і чітко не артикульованою. Безумовно, не в останню чергу це пов'язано із самим характером цих ініціатив, дискусія довкола яких досі не набула значного резонансу. Однак вже зараз Україна має чітко визначитися щодо прийнятності певного із запропонованих підходів і напряму формування позиції країни з питань кібербезпеки (та розвитку кіберпростору) саме на міжнародному рівні.

Розглядаючи можливість підтримання (включеності) Україною тих чи інших міжнародних ініціатив варто зосередитися 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**. Йдеться про фактичну спробу часткового заміщення чинної Конвенції про кіберзлочинність (Рада Європи) міжнародною Конвенцією про забезпечення міжнародної інформаційної безпеки (КЗМІБ).

Безумовно, такий поділ є досить умовним, оскільки деякі з цих ініціатив поєднують обидва рівні.

Усі ініціативи, апелюючи до одних і тих самих питань, мають на увазі різні речі або артикулюють окремі нюанси таких питань, що вкрай ускладнює погодження позицій щодо них. Американська Стратегія передбачає «право на захист» відповідно до Статуту ООН (передбачаючи передусім захист своєї інформаційної інфраструктури від кібератак). Російсько-китайські Правила вже в першому пункті також свідчать про необхідність «*поважати Статут ООН та загальновизнані норми міжнародного права, що включають, поміж іншого, повагу до суверенітету, територіальної цілісності та політичної незалежності всіх держав*». Однак уточнення російсько-китайської ініціативи щодо «*поваги до багатоманіття історії, культури та соціального укладу всіх країн*» свідчить про бажання отримати гарантії невтручання (навіть опосередкованого) у сферу політичних комунікацій, що забезпечують політичну стабільність держави. Крім того, як зазначалося вище, без створення відповідної міжнародної нормативної бази (чи уточнення чинної) щодо визнання кібератак «актом агресії» (а разом і того, що взагалі можна трактувати як «кібератаку») подібна одностороння позиція США (що була додатково пояснена очільниками американського військового відомства) виглядає дещо неоднозначно для тих країн, на території яких функціонують організовані хакерські групи, що можуть здійснювати атаки на об'єкти американські інформаційної (та звичайної) інфраструктури. І в цьому разі йдеться не лише про Україну, а й про цілу

низку країн з високим рівнем підготовки ІТ-фахівців, які, проте, не завжди мають можливість попередити їх протиправні дії.

Те саме стосується і питання про «вільні інформаційні потоки». Якщо відповідно до американської ініціативи «*держави мають поважати свободу потоків інформації в їх національних мережах* ***та не втручатись*** *в роботу тієї інфраструктури, що відноситься до такої, яка тісно пов'язана із міжнародною функціональністю мережі*», тобто фактично роль держави у контролі за частиною інформаційного простору нівелюється, то російсько-китайська ініціатива уточнює, що вільність цих потоків має враховувати «*національне законодавство кожної держави*». Саме з цього питання спостерігається чи не найбільше розходження зазначених ініціатив. Позиція РФ-КНР щодо співробітництва держав « *у… стримуванні поширення інформації… яка підриває політичну, економічну та соціальну стабільність держави, їх 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. Водночас зазначимо, що відповідно до **Доктрини інформаційної безпеки України**[35] захист «*духовних та моральних засад суспільства*» є напрямом державної політики у сфері інформаційної безпеки України[36].

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

Принципово, що Україна не лише підписала (23.11.2001), а й ратифікувала (07.09.2005) Конвенцію про кіберзлочинність (набула чинності 01.07.2006). Відповідно Україна є активним учасником засідань Комітету Конвенції про кіберзлочинність, що проводить щорічні зустрічі (як на рівні експертів, так і на рівні представників профільних владних установ) та визначає пріоритети подальшого поширення Конвенції, передусім на країни, що входять до Ради Європи[37]. 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 разі прийняття та необхідності подальшої ратифікації КЗМІБ, яка, з одного боку, стосується питань більш широкого спектра, але з іншого - стосується кібербезпекової проблематики, може виникнути колізія з чинною Конвенцією про кіберзлочинність.

Крім того, ціла низка положень КЗМІБ видаються сумнівними з точки зору реального впровадження в практику нормативного поля. Наприклад, поняття «**інформаційна війна**» визначається як «*протиборство між двома або більше державами в формаційному просторі з метою заподіяння шкоди інформаційним системам, процесам та ресурсам, критично важливим та*

[35] Указ Президента України «Про Доктрину інформаційної безпеки України» // http://zakon1.rada.gov.ua/laws/show/514/2009/print1332746452509988

[36] Експерти з питань інформаційної безпеки вже неодноразово звертали увагу на необхідність суттєвого доопрацювання Доктрини.

[37] T-CY: The way forward // http://www.coe.int/t/dghl/standardsetting/t-cy/tcy2011/TCY_2011_4E_Rev_BU_Way_forward_V4.pdf

іншим структурам, підриву політичної, 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 (її органів) і засуджує/висловлює незгоду з тією чи іншою політикою іншої держави, може трактуватися як вияв «інформаційної війни» з відповідними наслідками.

Також вкрай проблематичним буде забезпечення реального контролю за протидією «**масованій психологічній обробці**» (і особливо закріплення такого положення на рівні національного законодавства), оскільки не зовсім зрозуміло, які саме критерії визначатимуть такий «вплив» та чи можливо це взагалі. Бажання російської сторони врахувати психологічну компоненту цілком зрозуміле і до певної міри виправдане, однак навіть у самій Російській Федерації відсутній консенсус з цього питання. Варто згадати, що ще з початку 90-х років XX ст. у РФ кілька разів намагалися ухвалити федеральний Закон «Про інформаційно-психологічну безпеку». Останньою спробою стало внесення його на розгляд Держдуми 3 грудня 1999 року, а 19 червня 2001 року він був відкликаний самим суб'єктом законодавчої ініціативи.

Неоднозначним є й дефініція самого 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*».

Один з пунктів КЗМІБ протирічить положенням Конвенції про кіберзлочинність. Так, до загроз, що призводять до порушення міжнародного миру та безпеки (а отже, можуть розглядатися як порушення міжнародної інформаційної безпеки), відноситься «*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, вже погодилися з можливістю подібної ситуації і сприймають її як свідомий крок на шляху до безпечнішої мережі. Безумовно, з точки зору традиційних загроз таке положення Конвенції видається конфліктним щодо захисту національного суверенітету, водночас, зважаючи на специфічний тип загроз, якими є кібератаки та кіберзлочинність в цілому, подібне положення виглядає як виправдане. Таким чином, малоймовірно, що КЗМІБ отримає схвальні відгуки з боку держав-підписантів.

Загалом текст КЗМІБ виглядає надмірно рестриктивним (забороняючим), вміщуючи значний перелік забороняючих дій, значна частина яких просто не може бути відслідкована та процесуально закріплена. До таких заборон можна віднести і «*маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація та 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 та духовного середовища суспільства», зафіксувати «традиційні культурні, моральні, етичні та естетичні цінності» з метою подальшого їх захисту та можливості визначення статусу «інформаційної війни».

Хоча деякі пункти КЗМІБ відповідають положенням американської ініціативи і є цілком доречними і актуальними для української сторони. Такими пунктами, зокрема, є:

- 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 та практиці формування безпечної та швидко відновлюваної інформаційної інфраструктури.

Крім того, КЗМІБ знов порушує питання про межі суверенітету держави щодо інформаційного (кібер) простору. На думку авторів КЗМІБ, «*кожна держава-учасник має право встановлювати суверенні норми та керувати відповідно до національних законів своїм інформаційним простором. Суверенітет та закони поширюються на інформаційну інфраструктуру, розташовану на території країни-учасника чи іншим чином входить до його юрисдикції*». На сьогодні така позиція, щонайшвидше, відповідає довгостроковим інтересам Української держави. На жаль, американська ініціатива лише побіжно висвітлює це питання, роблячи акцент 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 за умови достовірного встановлення джерела загрози та адекватності дій у відповідь*». У такій редакції подібна норма є більш прийнятною (порівняно з американським варіантом), однак все одно постає питання щодо конкретних механізмів визначення «достовірного джерела» та обсягу «адекватності дій у відповідь».

Таким чином, незважаючи на те, що з формальної точки зору обидві політичні ініціативи викладені відповідно до класичних трактувань демократичного устрою, ані американська, ані російсько-китайська ініціативи не стануть дійсно загальносвітовими, оскільки кожна з них містить підходи, що є неприйнятними для певного, щоразу визначеного, кола країн. У поточній редакції зазначених документів ці ініціативи видаються не до кінця прийнятними і для України, яка має отримати чіткіші роз'яснення від авторів документів щодо окремих положень таких ініціатив і особливо щодо механізмів використання воєнних засобів реагування на кібератаки.

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

У цьому контексті актуальним є питання того інституту (організації), на базі якої мають напрацьовуватися ці правила. Незважаючи на статус ООН як ключової організації з питань миру та безпеки, прийняття рішень у рамках цієї організації щороку ускладнюється. Крім того, ймовірність прийняття обов'язкового для виконання документа (яким є Конвенція) з питань кібербезпеки оцінюється експертами як низька. Ще менше перспектив мають односторонньо проголошені ініціативи, які також, щонайшвидше, не будуть одностайно схвалені іншими країн, які дедалі більше тяжіють до вироблення спільних рішень та ініціатив. Усе це обумовлює необхідність пошуку інших форм міжнародних домовленостей, у межах яких кожна країна зможе мати рівнозначний голос, а сама міжнародна домовленість не виглядатиме як нав'язана однією зі сторін.

Зважаючи на вищевикладене, оптимальним варіантом організації, від імені якої має виходити відповідна 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 (у результаті підписання в 1975 році Заключного акту Ради з безпеки та співробітництва в Європі), чим сприяла зменшенню напруження в міжнародних відносинах та налагодженню конструктивного співробітництва між країнами-підписантами, може стати одним з чинників успішності ініціативи щодо кібербезпекового питання. Начебто «європейський» (регіональний) аспект діяльності організації насправді є доволі умовним, оскільки з організацією співпрацюють і африканські, і азіатські країни.

У 2013 році Україна головуватиме в ОБСЄ, і цілком доречно, що саме проблема вироблення прийнятного міжнародного договору з проблеми кібербезпеки може стати однією з основних ініціатив, запропонованих Україною в безпековій сфері. Вбачається реальним протягом 2013 року напрацювати таку редакцію відповідного документа, яка в цілому задовольнятиме всіх учасників ОБСЄ та ті країни, що переймаються кбербезпековою проблематикою.

Перевагами цього документа можуть стати такі.

1. Рівень ініціації (загальновизнана організація з питань безпеки).
2. Характер взятих зобов'язань (добровільність, зобов'язання політичного характеру).
3. Відображення найсуттєвіших для всіх країн проблем, що не викликають протиріч учасників.

Важливим моментом є і те, що ОБСЄ вже має певні напрацювання щодо кібербезпекової проблематики. У травні 2011 року у Вені відбулася конференція «Комплексний підхід до кібербезпеки: роль ОБСЄ», на якій обговорювалися питання кібербезпеки (військово-політичні, кіберзлочини та

тероризм, глобальна відповідальність, регіональна відповідальність, потенційна роль ОБСЄ).

Головуючи в ОБСЄ, Україні доцільно ініціювати проведення в Києві відповідну міжнародну конференцію з даної тематики, на якій мають бути обговорені як наявні міжнародні ініціативи, так і запропоновано власний проект консенсусного документа з міжнародних правил використання кіберпростору.

ВИСНОВКИ

Зазначаючи високий рівень активності та зацікавленості міжнародного співтовариства у стратегічному вирішенні проблем розвитку кіберпростору та його майбутнього на віддалену перспективу, враховуючи останні ініціативи США, КНР та Російської Федерації щодо майбутнього (зокрема безпекового) кіберпростору, можна дійти таких висновків.

1. Геополітичні «гравці» активно пропонують свій порядок денний щодо майбутнього кіберпростору: своє бачення того, що є дійсно «правилами поведінки» держав у кіберпросторі та які стратегічні цілі мають переслідуватися при його розбудові.
2. Пропоновані американською стороною ініціативи, щонайшвидше, так і не будуть реалізовані в повному обсязі в загальносвітовому масштабі, й не в останню чергу через неприйнятність окремих положень цих ініціатив для інших країн. Поміж таких «дискусійних положень» можна визначити окремі пункти Конвенції про кіберзлочинність, неготовність деяких країн прийняти тезу про абсолютно «вільні інформаційні потоки» та триваюча дискусія з проблеми «управління інтернетом» (як у аспекті визначення «управлінця», так і змістовного наповнення цього поняття).
3. США обрали результативну стратегію налагодження двосторонньої співпраці (Австралія, Японія, Індія) у межах своєї Стратегії та розширення дії Конвенції про кіберзлочинність як чинного міждержавного правового документа, який вже підписаний та ратифікований низкою країн, а отже, вже функціонує і формує політику кібербезпеки низки країн. Важливою частиною загальної позиції США з цього питання є відсутність необхідності розроблення нових документів у сфері кібербезпеки.
4. Сумнівними є перспективи ініціатив РФ та КНР (як Правил, так і КЗМІБ). Стратегічно прийняття міжнародного документа (як на рівні політичної декларації, так і міжнародного правового документа у вигляді Конвенції) є правильним кроком до посилення загальносвітової стабільності в кіберпросторі, однак малоймовірним на практиці через неприйнятність цілої низки положень запропонованих документів окремими країнами. Малоймовірним є також його прийняття саме в межах ООН.
5. Певна абстрактність (невизначеність) деяких із зазначених документів (зокрема запропонованої РФ КЗМІБ) зробить неможливим (чи вкрай складним) впровадження її у практику на національному рівні.
6. Усі запропоновані ініціативи в їх нинішніх редакціях не вповні відповідають національним інтересам України і навряд чи зможуть дійсно ефективно вплинути на формування міжнародного консенсусу з питання майбутнього кіберпростору. А отже, навряд чи Україна зможе їх підтримати.

7. Створення реального міжнародного консенсусу з проблем кіберпростору між ключовими геополітичними «гравцями» є об’єктивною необхідністю, адже унеможливить подальше стрімке зростання кіберзагроз як на національному, так і міжнародному рівні. Окремі положення розглянутих ініціатив мають спільні риси та однаково трактують певні загрози. Відповідно саме ці проблеми та спільні підходи мають стати основою для широкого діалогу щодо формування консенсусу.
8. Україна як країна, що вже сьогодні зазнає впливу кіберзлочинності, об’єктивно зацікавлена в тому, щоб брати в цих дискусіях активну участь і не лише на рівні чинних дискусійних майданчиків (на кшталт Комітету Конвенції з кіберзлочинності), а й у профільних групах експертів.
9. Вироблення консенсусного документа з проблем кіберпростору цілком може стати провідною темою під час головування України в ОБСЄ в 2013 році. Саме ця структура, зважаючи, зокрема, на історію її створення, є однією з найбільш реальних основ, на базі якої може бути віднайдено необхідні точки перетину інтересів ключових геополітичних «гравців».