УДК 004.056(477):004.378.5:340.147

Сергій Кандауров,
гендиректор Інституту міжнародних досліджень
Української академії наук

ПРО ТЕНДЕНЦІЇ МІЖНАРОДНОЇ СПІВПРАЦІ ЩОДО МІНІМІЗАЦІЇ КІБЕРНЕТИЧНИХ ЗАГРОЗ ТА ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті окреслюються ключові розбіжності в позиціях країн-лідерів у сфері кібернетичного озброєння щодо механізмів міжнародного контролю за гонкою кіберозброєння та національної відповідальності за кіберпростір. Також порушуються окремі проблемні питання формування політики України у сфері інформаційної безпеки.

Ключові слова: інформаційна безпека, кібернетична безпека, кібернетичний простір, кіберозброєння, кібершпигунство, міжнародні угоди, політична довіра, міжнародна взаємодія.

Очевидно вперше з часів розробки ядерної зброї перед людством постала нова цивілізаційна проблема, викликана новим витком науково-технічного прогресу.

Динамічний розвиток інформаційних технологій, проникаюча здатність Інтернету в сукупності з політикою тотальної інформатизації розмили віртуальні кордони між суверенними державами. Усе це в сукупності із зростанням масштабів інформаційного протистояння, кіберзлочинності, кібертероризму і, відповідно, гонки інформаційних, у тому числі кібернетичних, озброєнь, стає новим чинником, що впливає на міжнародну безпеку та геополітичну стабільність.

Напрями міжнародної співпраці у сфері інформаційної безпеки та актуальні проблеми забезпечення національних інтересів України в умовах виникнення новітніх загроз національній безпеці були висвітлені в працях таких вітчизняних науковців, як Д. Дубов, М. Ожеван [1], О. Кісілевич-Чорнойван [2], О. Литвиненко [4], В. Ліпкан [7], О. Макаренко [5], В. Петров [6] та ін.

Досвід останнього десятиліття засвідчує, що інформаційна зброя, враховуючи її асиметричний характер, надає можливості – як окремим

терористичним групам, так і державам – розв'язувати повномасштабні інформаційні війни практично на рівних із провідними, високорозвинутими світовими державами.

У таких умовах ефективне забезпечення інформаційної безпеки не може бути досягнуто виключно технологічними методами. Необхідним елементом такої безпеки стає впровадження відповідних національних політик, а також міжнародне правове регулювання питань інформаційної безпеки.

На сьогодні очевидно проявили себе дві основні групи країн, які репрезентують західну та східну політику (умовне визначення) щодо кіберзагроз. З одного боку, це США з їх союзниками по блоку НАТО (західний підхід), а з іншого – Росія, Китай та низка країн, які перебувають у сфері їх впливу (східний підхід).

Офіційні позиції всіх країн визнають необхідність боротьби із зростаючою загрозою кібератак і кібервійн. Разом з тим більшість технологічно розвинутих країн активно розробляють новітні види кіберозброєння.

На сьогодні провідні держави світу (США, Росія, Китай, Індія) перебувають у процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет. Активно формуються спецпідрозділи з ведення розвідки, здійснення операцій щодо блокування інформаційних ресурсів противника в мережі Інтернет, захисту власних мереж та критично важливих ресурсів. Такі підрозділи створено в США, Великої Британії, Німеччині, Австралії, Індії – у цілому більш ніж у 20 країнах [1].

Таким чином, кіберпростір реально стає новим глобальним театром бойових дій.

Разом з тим країни східної та західної політики поки не змогли досягти консенсусу у фундаментальних питаннях щодо боротьби зі зростаючою загрозою кібератак, які можуть завдати серйозної шкоди комп'ютерним системам та Інтернету в цілому.

Росія пропагує ідею та принцип міжнародних угод (подібно переговорів з хімічної зброї) і наполягає на цьому підході. Натомість, США стверджують, що подібний договір не потрібний. Замість цього вони виступають за розширення співпраці в рамках міжнародних правоохоронних груп. Якщо ці групи будуть співпрацювати, то це зробить кіберпростір безпечнішим від злочинних вторгнень, окрім цього їх робота також буде зміцнювати безпеку кіберпростору під час військових кампаній [1].

Цікавим є те, що світові наддержави не схильні розглядати проблему через призму кібербезпеки (кібероборони), а скоріше через призму

кібервійни (кібернаступу). Саме тому представники США не виявляли інтересу до участі в консультаціях експертів Україна – НАТО з питань кібернетичної безпеки, створеної у 2009 р. під егідою Спільної робочої групи Україна – НАТО з питань воєнної реформи. Росія, зі зрозумілих причин, тоді в цих консультаціях участі теж не брала. Разом з тим Росія та США на регулярній основі проводять спільні науково-практичні консультації, зокрема 22–25 квітня 2013 г. у м. Гармиш-Партенкірхен (Німеччина) при підтримці МГУ ім. М. В. Ломоносова, академії РАН відбувся VII Міжнародний форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» та Сьома наукова конференція Міжнародного дослідницького консорціуму інформаційної безпеки. У роботі форуму взяли участь представники 18 країн: Росії, Австралії, Австрії, Азербайджану, Бахрейну, Білорусі, Болгарії, Великої Британії, Індії, Канади, Китаю, Куби, США, Франції, Німеччини, Швейцарії, Естонії та Японії.

Експерти США стверджують, що неузгодженість підходів перешкоджає міжнародному співробітництву правоохоронних органів, особливо враховуючи значну частку кібератак на об'єкти, підконтрольні американському уряду, які походять з Китаю та Росії [1].

З російської точки зору, відсутність такого договору є запуском свого роду гонки кіберозброєнь з потенційно небезпечними наслідками.

Будь-яка угода щодо кіберпростору має ряд специфічних проблем, оскільки зачіпає такі питання, як цензура в Інтернеті, суверенітет і суб'єкти, які не можуть бути предметом договору.

Справа в тому, що східна та західна політика у сфері кіберзагроз не завжди сумісні. Вони являють різні філософські (а можливо цивілізаційні) підходи.

Ще у 2010 р. Росія сформувала свою позицію як основу для роззброєння в кіберпросторі. Пропонований Росією договір, зокрема, вводитиме заборону для країн таємно закладати шкідливі коди або схеми («логічні бомби»), які можуть бути активовані віддалено в разі війни, а також заборону на кібершпигунство. Інші російські пропозиції включають застосування гуманітарного права для заборони нападів на некомбатантів та обману під час проведення операцій у кіберпросторі. Дана ініціатива є спробою боротьби з проблемою анонімних атак. Росіяни також закликали до більш широкого міжнародного й державного контролю за Інтернетом [6].

США традиційно чинять опір угодам, які давали б урядам право

застосовувати цензуру в Інтернеті, вважаючи, що такі дії забезпечать прикриття для тоталітарних режимів. Вони також вважають, що договір буде неефективним, оскільки майже неможливо визначити, чи інтернет-атака організована певним урядом, чи лояльними уряду хакерами, чи «гравцями», що діють самостійно, тим більше, що не існує дієвих механізмів оперативної взаємодії на міждержавному рівні щодо цього [1].

Американці невдоволені тим, що російська позиція має занадто широкі рамки. Зокрема, ідеться про пропозицію Росії заборонити кібершпигунство. США підозрюють, що вона має радше пропагандистський характер, адже, на їхню думку, пропозиція заборони кібершпигунства надійшла від держави з досить високим рівнем майстерності в цій сфері, держави, яку регулярно підозрюють в організації кібероперацій проти інших країн, держави, яка чи не найслабше веде боротьбу з кіберзлочинністю на власній території та не підписала жодної міжнародної угоди щодо негативної кіберактивності [3].

Разом з тим США дуже стурбовані швидким розвитком кібершпигунства. У той час як шпигунство, метою якого є державні системи, може вийти з-під контролю, справжнім головним білем для технологічно розвинутих держав, зокрема США, є інтелектуальна власність. Скажімо, китайські хакери крадуть результати досліджень, витрачаючи один цент на мільярд, вкладений іншими країнамив ці дослідження, а потім виводять продукт на ринок… Серйозність кіберзагрози з боку Китаю змусила США зробити це питання ключовим під час останньої зустрічі Б. Обами та С. Цзіньпіна в Каліфорнії 8 червня 2013 р. Причому питання розглядалося в контексті вибудовування «нової моделі двосторонніх відносин» зокрема у військовій сфері, що саме по собі є унікальним явищем. Китай наполягає, що і сам потерпає від кіберзагроз.

США намагаються зміцнити кібербезпеку (а точніше, організувати оборону в кіберпросторі) шляхом посилення зв'язків з міжнародними правоохоронними агентствами. Як модель може слугувати Конвенція Ради Європи про кіберзлочинність, прийнята Комітетом міністрів Ради Європи в листопаді 2001 р.

На сьогодні Конвенцію підписали 46 країн, ратифікували – 30 (Україна – з 2006 р.), у тому числі неєвропейські країни – США, Канада, Японія, Мексика, ПАР, Філіппіни, Чилі, Коста-Ріка, Домініканська Республіка та ін. Ані Росія, ані Китай досі не згодні приєднуватися до Конвенції.

Зокрема, Росія заперечує проти того, що Європейська конвенція про кіберзлочинність надає правоохоронним органам можливості розпочинати розслідування справ щодо злочинів у Інтернеті, які походять

з іншої країни, без інформування місцевих органів влади, порушуючи тим самим традиційні принципи суверенітету.

Очевидно, що один з магістральних шляхів, який дасть змогу досягти прогресу на шляху наведення контролю над кіберозброєнням, це зміцнення політичної довіри між урядами.

У Європі мета політики інформаційної безпеки полягає в тому, щоб захистити цілісність інформації та інформаційних систем, гарантувати належні умови її обігу та цінність. Вирішення проблем інформаційної безпеки в межах ЄС передбачає створення загальної стратегії європейської інформаційної безпеки, протидії кібервійнам, інформаційному тероризму та боротьбі з інформаційною злочинністю [2].

Російська сторона неодноразово пропонувала резолюції, що закликають до підписання договору про роззброєння в кіберпросторі в рамках ООН. США послідовно виступають проти цієї ідеї.

Так, на 60-й сесії Генеральної Асамблеї ООН планувалося прийняти проект міжнародної конвенції з міжнародної інформаційної безпеки. Причини неухвалення цього документа пов'язані з неузгодженістю позицій групи урядових експертів з таких питань, як практичні заходи із запобігання розробкам, виробництву, використанню та поширенню інформаційних озброєнь у межах глобального режиму міжнародної інформаційної безпеки. До міжнародного договору передбачалося додати положення про ознаки та класифікацію інформаційних озброєнь та дотичних засобів; заходи з обмеження обігу інформаційних озброєнь; заходи з запобігання інформаційним війнам; визнання інформаційних озброєнь зброєю масового ураження; забезпечення свободи інформаційних потоків; гармонізація міжнародного права та національних законодавств з міжнародної інформаційної безпеки тощо [2].

Враховуючи швидкість, з якою розвивається ситуація в цій сфері, якщо найближчим часом західний чи східний підходи до політики контролю над кіберозброєннями не будуть прийняті на міжнародному рівні, світова спільнота досягне «точки неповернення» в запобіганні гонки кіберозброєнь.

Разом з тим це буде означати лише те, що політичні аргументи цієї суперечки не стали переконливими й тоді підійде черга економічних аргументів, які, як правило, здатні остудити перегріті амбіціями голови політиків.

Специфікою сучасного інформаційного світу є стрімке посилення ролі та впливу окремих національних і транснаціональних компаній на розвиток і функціонування кіберпростору. Ідеться, насамперед, про

провідних виробників апаратних засобів, програмного забезпечення, провайдерів телекомунікаційних мереж.

Видається, що настав час переглянути деякі традиційні норми та підходи міжнародного (дипломатичного) протоколу до інформаційної епохи.

Зокрема, чи не пора найбільшим суб'єктам інформаційного бізнесу стати суб'єктами міжнародного права, що регулює інформаційні взаємовідносини, отримати свої унікальні права та обов'язки в забезпеченні світової інформаційної безпеки.

Кожна держава не тільки має право всіма доступними засобами забезпечувати безпеку власних інформаційних ресурсів та критичної інфраструктури, а й зобов'язана нести відповідальність за це, у тому числі перед міжнародним співтовариством.

Маючи гіркий досвід техногенних катастроф світового масштабу, Україна має повною мірою усвідомлювати таку відповідальність.

Враховуючи вищевикладене, скоріше за все, Україна буде намагатися знайти золоту середину між принциповими позиціями США, ЄС, Росії та Китаю, і видається, що це цілком можливо. Тим більше, що загрози, мотиви, технології та засоби кібератак найчастіше мають транскордонний характер, що створює умови для міжнародної взаємодії країн. Україна, зокрема, стала першою з позаблокових країн, яка розпочала з НАТО експертні консультації на високому рівні з питань кібербезпеки та заявляла про зацікавленість у розробці універсальних міжнародно-правових документів, що стосуються цієї сфери. Очевидно, варто продовжувати цю роботу, щоправда, розширити коло учасників, запросивши до участі в консультаціях країни СНД, зокрема учасників ОДКБ. У цьому контексті варто скористатися можливостями, які надає Україні її головування в СНД у 2014 р. Принаймні можна створити паралельні консультації, а потім ініціювати спільні консультації двох робочих груп, або приєднатися до регулярних консультацій, які вже започатковані між цими країнами.

Для України, вимогою часу є розвиток національного законодавства шляхом максимальної його гармонізації зі світовими трендами. Починаючи з 2008 р, Україна значно активізувалася в цьому напрямі: слідом за Доктриною інформаційної безпеки України, затвердженої Указом Президента України № 514 від 8 липня 2009 р., яка заклала правове підґрунтя в цій сфері, зараз триває робота над іншими ключовими нормативними документами, зокрема Законом України «Про забезпечення кібернетичної безпеки України».

Підбиваючи підсумок, варто відзначити кілька проблемних питань, на які Україні потрібно буде відповісти, формуючи свою позицію на міжнародній арені, під час обговорення питань кібербезпеки.

По-перше, враховуючи, що організація контролю над кіберозброєнням не забезпечуватиме скорочення його арсеналів, чи варто нам включатися в гонку цих озброєнь?

По-друге, яку позицію зайняти у питанні кібершпигунства, який, з одного боку, практично не може бути верифікованим, але є дієвим засобом контролю справжніх намірів країн – учасників угоди, а з іншого – створює можливості для підготовки театру бойових дій, а також промислового шпигунства? Чи будемо ми наполягати на припиненні будь-якої діяльності, пов'язаної зі встановленням «логічних бомб» та інших шпаринок у цивільних мережах інших країн?

По-третє, чи здатні ми самотужки вдатися до оборонних заходів у разі кібератаки на цивільні об'єкти критично важливої інфраструктури, і які саме види об'єктів ми запропонуємо для включення до списку міжнародної угоди про ненапад?

По-четверте, які міжнародні санкції Україна готова підтримати для встановлення «національної відповідальності за кіберпростір»?

І нарешті, варто пам'ятати, що, навіть якщо напад почнеться в кіберпросторі без солдат і кровопролиття, навряд чи на цьому все й закінчиться. Якщо кіберзброя вже «висить» в інфраструктурних мережах інших країн, війна може розгорітися дуже легко.

Глобальні загрози інформаційної безпеки ще тільки набирають силу, тому зараз важливо вжити застережливих заходів, щоб не повторити помилок недавнього історичного минулого, коли провідні світові держави в гонитві за примарою світового панування втягнули світ у виснажливу гонку ядерних і космічних озброєнь.

Список використаних джерел

1. *Дубов Д. В.* Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь [Електронний ресурс] / Д. В. Дубов, М. А. Ожеван // НІСД. – К., 2011. – С. 3–10. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf. – Назва з екрана.

2. *Кісілевич-Чорнойван О. М.* Міжнародне інформаційне право / О. М. Кісілевич-Чорнойван. – К.: ДП «Вид. дім "Персонал"», 2011. – С. 109–115.

3. Кларк Р. Третья мировая война: какой она будет? [Електронний

ресурс] / Р. Кларк, Р. Нейл. – Изд-воПитер, 2011. – С. 48. – Режим доступу: http://sv-scena.ru/athenaeum/tretjya-mirovaya-vojna-kakoj-ona-budet.glava-7-kibermir.Razdel-1–1-1–9-48.html#Razdel-1–1-1–9-48. – Назва з екрана.

4. *Литвиненко О. В.* Інформаційна безпека Європи : конспект лекцій до курсу лекцій для студ. спец. «Міжнародна інформація» спеціалізації «Європейські комунікації» / Київ. ун-т ім. Т. Шевченка, Ін-т міжнар. відносин, Центр європейських студій, Кафедра міжнар. комунікацій та зв'язків із громадськістю. – К., 1999. – 61 с.

5. *Макаренко Є. А.* Міжнародна інформаційна безпека: сучасні виклики та загрози / Є. А. Макаренко, М. М. Рижиков, М. А. Ожеван [та ін.]. – К. : Центр вільної преси, 2006. – 916 с.

6. *Петров В. В.* Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн : автореф. дис. ... канд. політ. наук : 21.01.01 / Петров В. В. ; Рада нац. безпеки і оборони України, НІПМБ. – К., 2010. – 19 с.

7. *Ліпкан В. А.* Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський // Київ. нац. ун-т внутрішніх справ, Кафедра міжнар. відносин та нац. безпеки. – К. : КНТ, 2006. – 280 с.