ПОЛІТИЧНІ НАУКИ

УДК 323.2:327

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СПІЛЬНА ЗАДАЧА СВІТОВОГО СПІВТОВАРИСТВА

Білоусов О.С.
Одеський національний політехнічний університет

У статті розглядаються проблеми вирішення правового регулювання наслідків розвитку інформаційного суспільства, які несуть серйозну загрозу світовому простору, створюючи небезпеку на міжнародному, регіональному та національному рівнях. Показано, що потреба до забезпечення кібербезпеки та створення засобів ведення кібервоєн стосуються не лише зовнішніх викликів. Усе частіше вони змушують уряди провідних держав переглядати також їхню внутрішню політику у кіберсфері. Обгрунтовано, що світовій спільноті вкрай важко дійти згоди та виробити спільні підходи з цілої низькі принципово важливих, актуальних питань політико-правового регулювання даної сфери через відмінність ідеологічних, політичних, релігійних, соціокультурних установок та розбіжність національних інтересів щодо них.
Ключові слова: безпека, міжнародна безпека, Інтернет, інформаційне суспільство, світовий простір, кіберсфера, кібербезпека.

Правове регулювання Інтернету як одному з основних ІКТ та його складових на міжнародному, регіональному та національному рівнях неможливе без урахування морально-етичних засад суспільства. Так, у будь-якому соціумі «для права важливо, щоб людина чітко уявляла ту міру свободи, що несе в собі заряд руйнування, зла і несправедливості. Інформаційні технології і комп'ютерні можливості загострюють ці проблеми» [1, с. 13]. Тому держава повинна використовувати правові засоби як страхові для позначення меж дозволеного.

Саме під таким кутом зору – упередження перетину «меж дозволеного» – за допомогою нових можливостей, що відкриваються внаслідок відкриття небувалих раніше можливостей через прихід інформаційного суспільства та експлуатацію новітніх ІКТ, відбувається найбільш інтенсивна правова нормотворча діяльність як на національному, так і на регіональному та глобальному рівнях. Адже, саме наявність нових викликів та загроз залишається чи не найпотужнішим стимулом до міжнародно-правового регулювання даної сфери. Як зазначають з цього приводу автори аналітичної доповіді «Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців», 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» [2, с. 3].

Метою статті є визначення необхідності захисту кіберпростору на міжнародному, регіональному та національному рівнях

Провідні держави світу у своїй практичній політиці щодо вирішення проблем забезпечення власної кібербезпеки все більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн. З цією метою, зокрема, на сьогоднішній день більшість впливових світових геополітичних акторів (таких як США, Росія, ЄС, Китай, Індія та інші) вже або створили, або перебувають у процесі створення спеціалізованих військових підрозділів для використання у той чи інший спосіб мережі Інтернет. Так, за даними керівника компанії «McAfee», оприлюдненими на Всесвітньому економічному форумі в Давосі у 2010 р., протягом тільки 2009-2010 рр. понад 20 країн здійснили різноманітні спеціальні інформаційні операції. Сформовані цими країнами спецпідрозділи, як правило, мають на меті ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника із використанням можливостей кіберпростору. Якщо навіть керуватися лише офіційними заявами, то подібні підрозділи вже створені у США (U.S. Cyber Command), Великобританії (урядовий Cyber Security Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Не могла, звісно, оминути своєю увагою проблему протидії кіберзагрозам й такий потужний військово-політичний блок, як НАТО, країни якого створили для цього спеціальний центр (Cooperative Cyber Defence Centre of Excellence) [3].

На думку більшості експертів з проблем кібербезпеки, найпотужнішими та найактивнішими вважаються на сьогодні військові кіберпідрозділи КНР і США. Так, хоча офіційні дані про потенціал, чисельність і завдання китайських кібервійськ практично відсутні, але про них можна скласти певне уявлення за даними секретного звіту, що висвітлює рівень розвитку кібервійськ КНР та вказує на загрози цього розвитку для

США, підготованого ФБР, які потрапили у розпорядження ЗМІ. Звіт називає КНР «найбільшою цілісною загрозою США у сфері кібертероризму» та силою, що вже зараз може володіти потенціалом достатнім, щоб «знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних». За даними ФБР, КНР на сьогоднішній день має армію у 180000 хакерів, які щоденно атакують кібермережі США і щорічно здійснюють майже 90000 атак проти комп'ютерів Міністерства оборони США. З 180 тис. хакерів 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору (працівники приватних компаній, що залучаються до виконання військових чи розвідувальних завдань в кіберпросторі), місією яких є отримання доступу до військових і комерційних секретів США та внесення розладу в діяльність урядових і фінансових служб [4].

Як підкреслює відомий німецький футуролог К.-Х. Штайнмюллер, «Очевидна загроза майбутнього – небезпека кібервійни, яка в Інтернеті, або в тому, що прийде йому на зміну – розмиє кордони між холодним і гарячим кофліктом» [5, с. 159].

Небезпечність кібератак дійшла вже такого рівня, що спеціаліст з військової етики Державного університету в Буффало (штат Нью-Йорк, США) Ренделл Діперт у своїй статті «Етичні питання кібервійни» пропонує навіть подумати про необхідність створення аналогу Женевської конвенції щодо кібервійни. «Кіберпротивники прагнуть знищити бази даних, відключити системи зв'язку, очистити банківські рахунки, занурити в пітьму цілі міста, зупинити виробництво, внести хаос в систему охорони здоров'я і так далі до нескінченності. Але на відміну від звичайних воєн кібербитва не регулюється нічим, що хоча б віддалено нагадувало Женевську конвенцію. Не існує ніяких меж, ніяких стандартів міжнародного права, що обмежують кібервоєнних злочинців», – застерігає Р. Діперт. При цьому, вчений вважає, що просто взяти і перенести положення Женевської конвенції (якою, як відомо, вже тривалий час регулюються правила ведення звичайних війн) на цифрові військові дії неможливо. Адже в основі цього документа лежать моральні міркування, які не мають очевидних аналогів, коли мова заходить про кібервійни [6].

Розглянувши новітні тенденції розвитку міжнародного тероризму на глобальному та регіональному рівнях, М. Г. Гуцало приходить до висновку, що, зокрема, одним з основних напрямів діяльності терористичної мережі «Аль-Каїда» є «...посилення інформаційно-пропагандистської діяльності лідерами терористичної мережі шляхом прямих звернень до аудиторії через мережу Інтернет, створення нових веб-сайтів, збільшення кількості періодичних видань (зокрема спеціалізованих для жінок, молоді, дітей), розповсюдження відеофільмів, комп'ютерних ігор, анімаційних фільмів тощо. Так, значну активність на цьому напрямі демонструє новий лідер «Аль-Каїди», який зосереджує увагу своїх прибічників та послідовників на недопущенні роздроблення мережі після загибелі У. бен Ладена та спонукає цільову аудиторію до здійснення терактів в ініціативному порядку. Зокрема, у зверненні до мусульман країн Заходу «Не втрачайте сили і не занепадайте духом» новий лідер «Аль-Каїди» закликає до масштабної «інтелектуальної битви» з використанням засобів комунікації шляхом активного ведення дискусій в Інтернет-просторі. З цією метою активно використовуються онлайн-форуми, які є «ефективним» і доступним джерелом продукування екстремістської ідеології, розповсюдження пропагандистських матеріалів та психологічної обробки мусульман усього світу» [7, с. 176].

Виходячи з вище наведених даних, зрозуміло, чому таку надзвичайну увагу приділяє питанням кібербезпеки як на стратегічному, так і на тактичному рівнях блок НАТО. Так, ще під час Празького саміту на початку XX1 століття цієї організації було прийнято рішення про створення Сил і засобів реагування НАТО на комп'ютерні інциденти (NATO Computer Incident Response Capability – NCIRC). Зусилля НАТО у сфері кіберзахисту тоді були зосереджені переважно на захисті систем зв'язку, що належать і експлуатуються Альянсом. Пізніше політика НАТО з кіберзахисту була переглянута і доповнена засобами допомоги в посиленні кіберзахисту країн – членів Альянсу.

У Стратегічній концепції НАТО відзначається, що кібератаки стають дедалі частішими, організованішими та збитковішими і можуть досягти критичного рівня, який загрожує національному і євроатлантичному процвітанню, безпеці і стабільності. Джерелом таких атак можуть бути іноземні військові і розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи». Тому було визнано доцільним «розвивати можливості щодо запобігання, захисту і відновлення від кібератак шляхом використання процесу планування НАТО для поліпшення та координації національних можливостей з кіберзахисту, охоплюючи всі органи НАТО централізованим кіберзахистом, а також краще інтегруючи кіберобізнаність, попередження і реагування НАТО з державами – членами Альянсу.

На виконання положень цієї Стратегічної концепції була розроблена й затверджена Концепція НАТО з кіберзахисту під час засідання Північноатлантичної Ради (ПАР) на рівні міністрів оборони країн – членів НАТО у березні 2011 р. Нова Концепція визначає захист власних мереж НАТО як головну відповідальність Альянсу у сфері кіберзахисту, необхідність інтеграції кіберзагроз в оборонне планування НАТО, а також наголошує на важливості співпраці з партнерами та іншими міжнародними організаціями. Вона стала концептуальною основою переглянутої політики НАТО з кіберзахисту. Нова Політика НАТО з кіберзахисту (NATO Policy on Cyber Defence) була схвалена міністрами оборони Альянсу в червні 2011 р. й містить скоординований підхід до кіберзахисту з акцентом на запобігання кіберзагрозам через підвищення стійкості до зовнішнього вторгнення й можливостей швидкого відновлення пошкоджених систем. Усі структури НАТО перебуватимуть під централізованим захистом із застосуванням нових вимог. Політика роз'яснює політичні та оперативні механізми реагування на кібератаки, а також інтегрує кіберзахист у процес оборонного планування НАТО. Ця політика

також встановлює принципи військово-технічного співробітництва з країнами-партнерами, міжнародними організаціями, приватним сектором і науковими колами. Паралельно з цією політикою у даній сфері був узгоджений План дій з кібербезпеки (Cyber Defence Action Plan) як інструмент для забезпечення своєчасного й ефективного здійснення політики [8, с. 189-190].

Велику увагу приділяють кібербезпеці США. Особливо активною стала їх політика у цій сфері за часів президентства Б. Обами. Так, ще під час його першої каденції, Адміністрацією Президента США була здійснена низка важливих заходів, а саме:

– 29 травня 2009 року оприлюднено «Огляд кібербезпеки» (Cyber Security Review) – комплексний документ, що визначає пріоритети у сфері кібербезпеки;

– створено посаду Керівника кібербезпеки Ради національної та внутрішньої безпеки;

– створено Кіберкомандування США (U.S. Cyber Command), керівник якого одночасно очолює і Агентство з національної безпеки. Приблизна чисельність структури – 30000 військових;

– оприлюднено нову «Стратегію національної безпеки» (2010 р.), в якій вперше в загальній структурі загроз США окреме місце відведено кіберзагрозам;

– оприлюднено «Міжнародну стратегію для кіберпростору» («International Strategy for Cyberspace») як цілісне бачення урядом США найближчого майбутнього у розвитку кіберпростору (основні положення цього документу будуть більш детально проаналізовані у подальшому тексті даного розділу дисертації);

– оголошено про додаткові заходи з посилення внутрішньої кібербезпеки. З 1 жовтня 2009 року в США оголошено про додатковий набір 1000 співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (Department of Homeland Security), які займатимуться виключно безпекою високотехнологічних систем США. Однак навіть ця кількість співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки. У супровідному документі до спеціально організованих урядом США слухань «Кібервиклик США» (U.S. Cyber Challenge) наводиться думка одного з експертів про те, що реальна потреба уряду в таких фахівцях становить від 10000 до 30000.

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

– створено проекти нормативних документів, спрямовані на покращення взаємодії у сфері кібербезпеки між союзниками США та убезпечення власного інтернет-простору в разі виникнення ситуацій, що загрожують національній безпеці [9, с. 5-6].

Значну увагу розбудові власних сил безпеки у кіберпросторі приділяє Великобританія, потенціал якої у сфері кібербезпеки вважається одним з найпотужніших. Так, нею у 2010 році було розпочато роботу Оперативного центру з кібербезпеки (чисельністю 20 співробітників) з метою координування вже наявних центрів з кібербезпеки різних відомств та створення майданчику для співпраці між урядом та приватним сектором щодо проблем кібербезпеки. Крім того, у Великобританії ефективно працює Командування урядових комунікацій («Government Communications Headquarters»), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

Згідно з відкритими даними активно створюються відповідні підрозділи також у Південній та Північній Кореї, Російській Федерації, Франції. Провідні держави світу активно беруть участь у навчаннях щодо протидії кібератакам, які мають значний ефект для виявлення проблемних зон захисту інфраструктури, моделювання можливих інцидентів і вироблення типових схем реагування, поліпшення міжвідомчої взаємодії.

Потреба до забезпечення кібербезпеки та створення засобів ведення кібервоєн стосуються не лише зовнішніх викликів. Все частіше вони змушують уряди провідних держав переглядати також їхню внутрішню політику у кіберсфері. Зокрема, дедалі активніше застосовується низькотехнологічний (low-tech) рівень контролю, до якого відносять бюрократичні, організаційні та обмежувальні методи захисту власного інформаційного та кіберпростору від латентних загроз безпеці даних та засилля іноземного програмного продукту. Як не парадоксально, але політика країн Заходу у сфері внутрішнього інформаційного простору (зокрема, кіберпростору) дедалі частіше набуває окремих рис політики тих країн, що традиційно відносять до авторитарних. Щоправда, між ними все ж таки залишаються суттєві відмінності. Так, якщо в країнах авторитарного типу передусім здійснюється політика прямого обмеження доступу, то країни Заходу нарощують кількість даних про користувачів, здійснюють моніторинг національного інтернет-трафіку та створюють можливості цільового відключення окремих елементів мережі або її користувачів. Такий акцент на «моніторинговому дискурсі» обумовлений, зокрема, зростанням кількості телекомунікаційних послуг та мереж, контроль за якими є складним для державних правоохоронних служб [Див.: 10, с. 6-7].

Як правило, найчастіше заходи з інтенсивнішого моніторингу контенту мережі та окремих технологічних рішень, що забезпечують доступ до неї, пояснюються наступними причинами:

1) зростання терористичної загрози, використання терористами та міжнародними кримінальними структурами новітніх інформаційних технологій та зростання загрози критичній інфраструктурі держави;

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

3) протидія розповсюдженню дитячої порнографії.

Дедалі активніше застосовуються методи прямого впливу та тиску на власників пошукових інтернет-сервісів, на яких або розміщуються матеріали, що викликають невдоволення з боку державних інституцій, або надають доступ до таких матеріалів. Лідером у застосуванні таких методів цілком обгрунтовано вважається Китай. Так, наприклад, всесвітньовідомим став конфлікт між урядом Китаю та IT-корпорацією

«Google», що виник через небажання останньої обмежувати на вимогу уряду пошукові запити китайських користувачів. Слід зазначити, що активна діяльність «Google» викликала конфліктні ситуації не лише з керівництвом Китаю, а й з урядами європейських країн – Францією (щодо оцифрування культурних надбань та книг), Німеччиною, Грецією, Великобританією, Іспанією (через службу «Google Street View», що не лише фотографувала вулиці, а й збирала персональні дані громадян через незахищені бездротові канали зв'язку), Італією (через безконтрольне розміщення матеріалів, що порушують право на приватне життя) [11, с. 7-9].

Нещодавно корпорацією «Google» був запущений сервіс «Transparency Report», що має висвітлювати частоту звертань держав до корпорації із запитами про усунення того чи іншого контенту або про надання доступу до персональних даних користувачів сервісів корпорації. Він дуже добре ілюструє ситуацію із спробами західних держав впливати на контент та результати пошуку, що здійснюється корпорацією «Google». Адже, згідно з цим звітом, саме країни Заходу та США є лідерами таких запитів.

Слід зауважити, що світовій спільноті вкрай важко дійти згоди та виробити спільні підходи з цілої низки принципово важливих, актуальних питань політико-правового регулювання даної сфери через відмінність ідеологічних, політичних, релігійних, соціокультурних установок та розбіжність національних інтересів щодо них. Про це свідчать різноманітні дискусії (зокрема на найвищому рівні) навіть серед провідних геополітичних акторів сучасності. Під час них обнародуються і досить радикальні (а тому неприйнятні для інших учасників) пропозиції, наприклад: визнати кібернапади «актом війни», кіберзброю прирівняти до зброї масового ураження, а також відповідати на хакерську атаку звичними видами озброєнь (скажімо, ракетним ударом). Додаткові ускладнення викликаються відсутністю єдиного погляду найпотужніших і найбільш просунутих у розробці й використанні новітніх ІКТ світових держав на кіберпростір та кібербезпеку в цілому, а також посиленням загальносвітової дискусії довкола забезпечення авторських та суміжних прав у мережі Інтернет.

Виходячи з зазначених чинників, найбільшого прогресу щодо вирішення проблема кібербезпеки на міжнародному рівні до останнього часу вдалося досягти лише частково – у сфері протидії кіберзлочинності та й то, переважно, лише на національному та регіональному рівні (зокрема, у Європі).

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». Так, наприклад, азіатські країни, на відміну від США, послідовно відстоює позицію, що кібербезпеку не можна розглядати як повністю самостійний напрям, який існує окремо від соціальних, політичних, економічних і військових наслідків застосування сучасних інформаційних технологій. Більше того, за такого підходу (згідно російської позиції) взагалі недоречно казати про абсолютно «вільні потоки інформації», оскільки безпекова тематика охоплює й наслідки їх впливу на державу та її громадян.

Відтак, автор статті вважає, що сумуючи основні міжнародні ініціативи і підходи до розв'язання зазначеної проблеми, доцільно вживати не поняття «кібербезпека» (навіть у міжнародному контексті), а більш адекватну назву даної проблеми – «інформаційна безпека» чи «міжнародна інформаційна безпека». І ретельний аналіз цієї проблеми є першочерговою задачею як науковців, так і практичних діячів.

Список літератури:

1. Дюжев Д. В. Інформаційне суспільство: соціально-правова парадигма суспільного розвитку: Автореф. дис. ... канд. філософ. наук: 09.00.03 / Д. В. Дюжев; Донец. нац. ун-т. – Донецьк, 2004. – 18 с.
2. Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К.: НІСД, 2012. – 32 с.
3. В мире два десятка стран занимаются кибероружием – McAfee [Електронний ресурс]. – Режим доступа: http://www.cybersecurity.ru/armament/86546.html
4. China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogsandstories/2010-01-13/chinas-secret-cyber-terrorism/full/
5. Штайнмюллер К.-Х. «Кривые будущего роста вызывают улыбку». (Разговор с футурологом о его профессии) // Россия в глобальной политике. – 2013. – Т. 11. – № 1. – С. 146-160.
6. Для кибер-войн напишут свою Женевскую конвенцию [Електронний ресурс]. – Режим доступу: http://techno.bigmir.net/net/1503150
7. Гуцало М. Г. Новий профіль міжнародного тероризму / М. Г. Гуцало // Стратегічні пріоритети. – 2012. – № 4 (25). – С. 174–182.
8. Брежнєва Т. В. Політика НАТО з кіберзахисту та співробітництво з партнерами / Т. В. Брежнєва // Стратегічні пріоритети. – 2012. – № 4 (25). – С. 189–195.
9. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України: аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К.: НІСД, 2011. – 30 с.
10. Дубов Д. В. Указ. робота.
11. Дубов Д. В. Указ. робота.

Билоусов А.С.
Одесский национальный политехнический университет

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЩАЯ ЗАДАЧА МИРОВОГО СОДРУЖЕСТВА

В статье рассматриваются проблемы решения правового регулирования последствий развития информационного общества, которые несут серьезную угрозу мировому пространству, создавая опасность на международном, региональном и национальном уровнях. Показано, что потребность к обеспечению кибербезопасности и созданию средств ведения кибервойн касаются не только внешних вызовов. Все чаще они вынуждают правительства ведущих государств пересматривать также их внутреннюю политику в киберсфере. Обосновано, что мировому сообществу крайне сложно прийти к согласию и выработать общие подходы по целому ряду принципиально важных, актуальных вопросов политико-правового регулирования данной сферы, несмотря на наличие различных идеологических, политических, религиозных, социокультурных установок и расхождений национальных интересов относительно них.
Ключевые слова: безопасность, международная безопасность, Интернет, информационное общество, мировое пространство, киберсфера, кибербезопасность.

Bilousov O.S.
Odessa National Polytechnic University

INTERNATIONAL INFORMATION SECURITY AS THE COMMON TASK OF THE WORLD COMMUNITY

Summary
The problems of decision of the legal adjusting of consequences of development of informative society are examined in the article, that carry a serious threat to outer space, creating a danger on international, regional and national levels. It is shown that necessity to providing of of cybernetic safety of and creation of facilities of conduct of cyberwars touch external calls not only. All more often they force the governments of the leading states to look over also their domestic policy in to the cybernetic sphere. It is reasonable, that world community is extremely difficult to come to the consent and produce general approaches on quite a few fundamentally important, actual questions of the political-law adjusting of this sphere, in spite of presence of different ideological, political, religious, sociocultural options and divergences of national interests in relation to them.
Keywords: safety, international safety, Internet, informative society, outer space, cybernetic sphere, cybernetic safety.