УДК:341(045): 004.056

Забара І. М.*

ПРАВОВЕ РЕГУЛЮВАННЯ ВІЙСЬКОВОЇ СКЛАДОВОЇ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стаття присвячена висвітленню поглядів на зміст правового регулювання військової складової міжнародної інформаційної безпеки. Проаналізовано концептуальні підходи до міжнародно-правового регулювання застосування інформаційно-комунікаційних технологій у військових цілях.

Ключові слова: інформація, міжнародно-правове регулювання, міжнародна інформаційна безпека, інформаційна війна.

Article is devoted to the views of the content of the legal regulation of military aspects of international information security. Analysis of conceptual approaches to international legal regulation of information and communication technologies for military purposes.

Key words: information, international legal regulation, international information security, cyberwar.

Статья посвящена рассмотрению взглядов на содержание правового регулирования военной составляющей международной информационной безопасности. Проанализировано концептуальные подходы к международно-правовому регулированию применения информационно-коммуникационных технологий в военных целях.

Ключевые слова: информация, международно-правовое регулирование, международная информационная безопасность, информационная война.

Становлення і розвиток інституту міжнародної інформаційної безпеки було викликано низкою об'єктивних факторів: швидким розвитком інформаційно-комунікаційних технологій, їхнім різноманітним впливом на суб'єктів відносин, а також зростаючою залежністю світового співтовариства від належного функціонування інформаційно-комунікаційних технологій. Різноманіття негативних проявів використання інформаційно-комунікаційних технологій спричинило ситуацію, коли в доктрині міжнародного права почали говорити про кілька складових міжнародної інформаційної безпеки – кримінальну, терористичну, військову.

Історично склалось так, що протягом періоду з другої половини 70-х років і до середини 90-х років XX сторіччя домінував підхід, який ґрунтувався на тому, що основу міжнародної інформаційної безпеки складає тільки один елемент – боротьба із кримінальними злочинами в сфері інформаційно-комунікаційних технологій (ІКТ). Саме з цих позицій були закладені і концептуальні основи правового регулювання інституту міжнародної інформаційної безпеки.

* кандидат юридичних наук, доцент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

Проте, починаючи з другої половини 90-х років XX сторіччя, враховуючи подальший широкомасштабний розвиток ІКТ та зростаючу залежність від них державних інфраструктур, дедалі частіше почали звертати увагу і на іншу сторону їх використання. Мова йде власне про військову складову застосування ІКТ у відносинах між державами. Її почали ототожнювати з можливостями використання ІКТ, які виявились несумісними із задачами підтримки міжнародного миру і безпеки, а також дотриманням принципів міжнародного права – відмови від застосування сили, невтручання у внутрішні справи держав, поваги прав і свобод людини. Особливе занепокоєння викликала можливість ведення інформаційних війн, руйнівні наслідки від яких могли бути прирівняні до наслідків застосування зброї масового знищення.

Поява нових військових можливостей в умовах невизначеності в ідентифікації джерел і суб'єктів ворожих дій, зробили цілком зрозумілим висновок про те, що жодна з держав не зможе боротися покладаючись виключно на власні сили. Як наслідок, з'явилась необхідність у міжнародному співробітництві з проблематики військової складової застосування ІКТ.

Слід зауважити, що весь комплекс проблем, в тому числі і пов'язаних з міжнародно-правовим регулюванням використання ІКТ у військових цілях посилили увагу до цієї тематики як з теоретичної, так і з практичної точок зору: почали з'являтись як окремі наукові дослідження, так і державні військові концепції, доктрини і програми. Окремі питання цієї тематики почали дедалі частіше розглядатися на міжнародних конференціях і у рамках міжнародних організацій.

Проблематика міжнародно-правового регулювання інформаційної безпеки і безпосередньо використання ІКТ у військових цілях знайшла відображення в наукових роботах В.А. Василенка, Р. Даіберта (Deibert), Г. Кеннета (Kenneth) Р. Кларка (Clarke), Р. Кнейка (Knake), С. Комова, С. Короткова, А.В. Крутських, Т. Морта (Morth), Т. Морера (Maurer), Е. Накашими (Nakashima), А. І. Смирнова, А. В. Федорова, С. А. Форда (Ford) та інших. Серед розглянутих авторами були окремі теоретичні питання щодо міжнародно-правових проблем заборони інформаційної зброї та використання інформаційного простору (кіберпростору) у військових цілях, правові питання міждержавного співробітництва забезпечення інформаційної безпеки. Певною мірою була досліджена роль ООН у формуванні засад міжнародно-правового регулювання співробітництва держав у контексті міжнародної інформаційної безпеки. В той же час, залишаються питання щодо розвитку правового регулювання співробітництва держав у питаннях, пов'язаних із військовою складовою міжнародної інформаційної безпеки.

Метою статті є дослідження становлення і розвитку концептуальних засад правового регулювання військової складової міжнародної інформаційної безпеки. У зв'язку з цим вартими розгляду постають питання щодо формування в доктрині міжнародного права поглядів на зміст і міжнародно-правове регулювання відносин, пов'язаних із використанням ІКТ в якості засобів військового впливу.

Проблематика, пов'язана із вірогідною можливістю використання інформаційного простору у військових цілях, а також необхідністю визнання інформаційних війн в якості однієї із основних загроз в тематиці міжнародної безпеки, неодноразово ставала предметом дискусій серед фахівців, в тому числі і серед представників доктрини міжнародного права, ще починаючи з дев'яностих років двадцятого сторіччя.

Досліджуючи можливості застосування ІКТ у військових цілях, ряд фахівців звертав увагу на особливу небезпеку використання інформаційних війн у якості інструмента проведення зовнішньої політики держав [1]. Представники доктрини міжнародного права,

розглядаючи інформаційну війну з позицій Статуту ООН, наголошували на тому, що вона є своєрідним застосуванням сили, носить протиправний характер [2] і пропанували як певні обмеження щодо її ведення [3, с. 344-345], так і її повну заборону [4].

Разом з тим, це був не єдиний підхід, який висловлювався в доктрині міжнародного права. На противагу зазначеному, його представники наголошували на недоцільності виокремлення військової складової (військового аспекту) міжнародної інформаційної безпеки, і, відповідно, наголошували на відсутності потреби у міжнародно-правовому регулюванні. В якості аргументу зазначався той факт, що відповідних норм сучасного міжнародного права і міжнародного гуманітарного права є достатньо, щоб врегулювати використання інформаційного простору у військових цілях.

Ці концептуальні підходи логічно лягли в основу дискусій, що відбувались на міждержавному рівні протягом наступного десятиліття.

В той же час, прийняті протягом 1998-2012 років різноманітні національні концепції, що передбачали використання інформаційного простору у військових цілях, фактично тільки склали уяву про можливості кожної з держав, в залежності від їх науково-технічного і технологічного розвитку.

Виходячи саме з широкого розуміння застосування ІКТ у військових цілях зокрема, як ведення інформаційних війн, проведення інформаційних операцій і застосування інформаційної зброї, вартим є розгляд концептуальних підходів з позицій їх міжнародно-правового регулювання. Незважаючи на різницю між ними, найвищий прояв застосування ІКТ у військових цілях пов'язується із інформаційною війною. Тому, вартими розгляду в першу чергу, є саме доктринальні погляди, пов'язані саме з нею.

Слід зазначити, що поняття «інформаційної війни» виявилось одним із самих дискусійних у правових дослідженнях. Єдність в думках щодо того, що саме представляє інформаційна війна і яким чином повинно реагувати міжнародне право відсутня і зараз [5]. Доречним буде зауважити, що в доктрині міжнародного права доволі часто використовуються і різні терміни, які в тій чи іншій мірі відображають застосування ІКТ у військових цілях, в тому числі і з тим, що пов'язується із інформаційною війною [6, с. 337-347].

Незважаючи на значну кількість визначень, що зустрічається в науковій літературі, вартим уваги, на нашу думку, є наступне: «інформаційна війна – протиборство між двома або більше державами в інформаційному просторі з метою нанесення шкоди інформаційним системам, процесам і ресурсам, критично важливим і іншим структурам, підриву політичної, економічної і соціальної систем, масованої психологічної обробки населення для дестабілізації суспільства і держави, а також примушення держави до прийняття рішень в інтересах іншої сторони» [7].

Це визначення було запропоновано представниками російської доктрини міжнародного права і знайшло відображення у проекті Конвенції про забезпечення міжнародної інформаційної безпеки (концепція) (2011 р.) [7].

Розуміння категорії «інформаційна війна» як боротьби, протистояння, конфліктних відносин між державами, за умов яких сторони використовують ІКТ в якості засобів впливу, розкривається в запропонованій концепції через визначення основних загроз, які, на думку авторів, призводять до порушення миру і безпеки в інформаційному просторі. До їх кола включено:

- використання інформаційних технологій і засобів для здійснення ворожих дій і актів агресії;
- цілеспрямований деструктивний вплив у інформаційному просторі на критично важливі структури іншої держави;

• дії в інформаційному просторі з метою підриву політичної, економічної і соціальної систем іншої держави, психологічна обробка населення, що дестабілізує суспільство;

• транскордонне поширення інформації, що протирічить принципам і нормам міжнародного права, а також національним законодавствам держав;

• маніпулюванні інформаційними потоками в інформаційному просторі інших держав, дезінформація та приховування інформації з метою викривлення психологічного та духовного середовища суспільства, (…);

• інформаційна експансія, набуття контролю над національними інформаційними ресурсами іншої держави, (…)» [7].

Варто звернути увагу на те, що серед зазначених загроз є такі, які варто віднести не скільки до військових, скільки до військово-політичних складових міжнародної інформаційної безпеки. Це випливає з того, що серед визначених в концепції загроз, є не тільки такі, які охоплюють випадки коли шкода заподіюється державою за допомогою ІКТ цілісності іноземних державних інфраструктур, але й такі, які за допомогою ІКТ заподіюють впливу на підсвідомість людини, психологічне середовище суспільства. У сукупності вони забезпечують як військове, так і політичне домінування над територією і населенням іншої держави.

Варто додати, що не менш важливими для розуміння такого військово-політичної складової є принципи забезпечення міжнародної інформаційної безпеки, які дають уяву про концептуальні позиції цього підходу. Зокрема, серед основних принципів забезпечення міжнародної інформаційної безпеки, які безпосередньо пов'язані з її військовим (військово-політичним) складовою визначено: принцип неподільності безпеки та принцип відповідальності за власний інформаційний простір.

Так, *принцип неподільності безпеки* означає, що безпека кожної з держав нерозривно пов'язана із безпекою усіх інших держав і світового співтовариства в цілому, передбачається також те, що держави не будуть зміцнювати свою безпеку на шкоду безпеці інших держав;

принцип відповідальності за власний інформаційний простір передбачає відповідальність держави як власне за свій державний інформаційний простір, так і за його безпеку, а також за зміст інформації, що в ньому розміщується [7].

Такий концептуальний підхід припускає також і декілька принципових положень, які недвозначно визначають питання застосування ІКТ у військових цілях. Вони, зокрема, зводяться до наступного:

• агресивна «інформаційна війна» складає злочин проти міжнародного миру і безпеки;

• кожна держава має невід'ємне право на самооборону перед агресивними діями в інформаційному просторі у відношенні до неї, за умов достовірного визначення джерела агресії і адекватних відповідних заходів;

• інформаційний простір держави не повинен бути об'єктом набуття іншою державою в результаті загрози силою або її застосування;

• кожна держава визначатиме свій військовий потенціал в інформаційному просторі на основі національних процедур з урахуванням законних інтересів безпеки інших держав, а також необхідності сприяти міжнародному миру і безпеці. Жодна з держав не буде докладати зусиль до панування в інформаційному просторі над іншими державами;

• держава може розміщувати свої сили і засоби забезпечення інформаційної безпеки на території іншої держави у відповідності з угодами, укладеними на добровільній основі у відповідності з нормами міжнародного права» [7].

Важливим в такому підході, на нашу думку, є і те, що концепція враховує і погоджує різноманітну і широкомасштабну інформаційну діяльність держав з принципами міжнародного права, визначаючи, що «діяльність кожної держави в інформаційному просторі повинна сприяти соціальному і економічному розвитку і здійснюватись таким чином, щоб бути сумісною із задачами підтримки міжнародного миру і безпеки, відповідати загальновизнаним принципам і нормам міжнародного права, включаючи принципи мирного врегулювання спорів і конфліктів, незастосування сили в міжнародних відносинах, невтручання у внутрішні справи інших держав, поваги суверенітету держав, основних прав і свобод людини» [7]. При цьому «кожна держава, враховуючи законні інтереси безпеки інших держав, може вільно і самостійно визначати свої інтереси забезпечення інформаційної безпеки на основі суверенної рівності, а також вільно обирати способи забезпечення власної інформаційної безпеки у відповідності з міжнародним правом» [7].

Така концептуальна позиція в цьому питанні досить чітко визначає можливості держав в інформаційній сфері. Тому, зрозумілою є позиція тих держав, які принципово підтримали цю концепцію, висловившись щодо неї в національних доповідях під час роботи Групи урядових експертів ООН (2004-2005 рр. та 2009-2010 рр.) за тематикою «Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» [5].

Аналогічний підхід до проблем забезпечення військової складової міжнародної інформаційної безпеки було закладено і на регіональному рівні. Так, положення *Угоди між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року* [8] виходять саме з таких концептуальних позицій.

Низкою положень, запропонованих в концепції, передбачено можливість зменшення військових інформаційних загроз та реалізацію принципів забезпечення міжнародної інформаційної безпеки. Так, в основу підходу до попередження і розв'язання військових конфліктів в інформаційному просторі покладено обов'язок прийняття державами заходів випереджувального виявлення потенційних конфліктів у інформаційному просторі та мирного врегулювання криз та спорів. При цьому передбачається низка умов, за яких є можливим саме комплексне забезпечення міжнародної інформаційної безпеки. Такі умови полягають у визначенні позицій держав, що «будуть утримуватись від розробки і прийняття планів, доктрин, здатних спровокувати зростання загроз у інформаційному просторі, та спроможних викликати напруження у відносинах між державами і виникнення «інформаційних війн» [7]. Крім того, передбачається, що держави «утримуватимуться від будь-яких дій, спрямованих на повне або часткове порушення цілісності інформаційного простору іншої держави;

- утримуватимуться в міжнародних відносинах від загрози силою або її застосування проти інформаційного простору будь-якої держави для його порушення або в якості засобу розв'язання конфліктів;
- не будуть приймати заходи з обмеження поширення «інформаційної зброї» і технологій її створення;
- будуть приймати усі необхідні заходи для попередження деструктивного інформаційного впливу зі своєї території або з використанням інформаційної інфраструктури, що знаходиться під її юрисдикцією, а також зобов'язуються взаємодіяти для визначення джерела комп'ютерних атак, проведених з використанням її території, протидії цим атакам та ліквідації наслідків;
- зобов'язуються утримуватись від організації або підтримки організації будь-яких іррегулярних сил для здійснення неправомірних дій в інформаційному просторі іншої держави;

• зобов'язуються не використовувати ІКТ для втручання у справи, що відносяться до внутрішньої компетенції іншої держави;

• зобов'язуються утримуватись від наклепницьких тверджень, а також від образливої або ворожої пропаганди для здійснення інтервенції або втручання у внутрішні справи інших держав;

• мають право і зобов'язуються боротися проти поширення недостовірних або перекручених повідомлень, які можуть розглядатись як втручання у внутрішні справи інших держав, або як такі, що заподіюють шкоду міжнародному миру і безпеці;

• зобов'язуються співробітничати одна з одною в сфері забезпечення міжнародної інформаційної безпеки для підтримки міжнародного миру і безпеки і сприяння міжнародній економічній стабільності і прогресу, спільному добробуту народів і міжнародному співробітництву, вільному від дискримінації» [7].

Передбачається, що для розв'язання конфліктів в інформаційному просторі використовуватимуться усі засоби мирного вирішення спорів – переговори, посередництво, примирення, арбітраж, судове розгляд, звернення до регіональних органів та угод тощо. Передбачаються також і заходи зі зміцнення довір'я.

Критика і заперечення такого концептуального підходу зводяться до кількох положень. Вони полягають у наступному.

По-перше, проблема не містить військової складової.

По-друге, реальну загрозу складають тільки кримінальна та терористична складові використання ІКТ. Військова складова міжнародної інформаційної безпеки не є важливою.

По-третє, інформаційна зброя, яка може використовуватись державами, є тільки засобом впливу на системи і мережі.

По-четверте, відсутність можливості відслідковувати і фіксувати суб'єктів інформаційного впливу.

По-п'яте, відсутність єдиної термінології щодо розуміння різних складових міжнародної інформаційної безпеки.

По-шосте, відсутність гармонізації національного законодавства.

По-сьоме, недостатній рівень осмислення і розробки проблеми [9, с. 90-91].

Останні десятиліття показали, що ці положення вже не є достатньо обґрунтованими і можливим рішенням, адекватним вищезазначеним військовим загрозам, є створення міжнародного механізму обмеження гонки інформаційної зброї і попередження інформаційних війн. Організацією, яка здатна здійснити таку роботу є ООН, яка вже доказала свої можливості в координації діяльності з обмеження інших видів зброї.

Варто, на нашу думку, звернути увагу на те, що такий підхід, запропонований цією концепцією, передбачає комплексне розв'язання проблеми використання ІКТ (інший термін – «використання кіберпростору») у військових цілях і нагадує вже відомі схожі концептуальні підходи до проблем обмеження і контролю ядерної, хімічної і бактеріологічної зброї.

Другий підхід, як вже зазначалось, базується на тому факті, що відповідних норм сучасного міжнародного права і міжнародного гуманітарного права є достатньо, щоб врегулювати використання інформаційного простору у військових цілях. Такий підхід підтримується представниками доктрини розвинутих у технологічному плані держав. Разом з тим, наполягаючи на своїй позиції, представники цієї концепції зауважують, що хоча вищезазначені принципи і є загальновизнаними і застосовуються в контексті до кіберпростору, правильним є також і те, що тлумачення цих нормативно-правових основ в

контексті діяльності в кіберпросторі може представляти собою нові і унікальні виклики, які потребуватимуть консультацій і співробітництва між державами. Отже, мова може йти про можливість міжнародного співробітництва і з проблематики військової (військово-політичної) складової застосування ІКТ.

Таким чином, розглянувши питання, пов'язані із правовим регулюванням військової складової міжнародної інформаційної безпеки, можна зазначити наступне:

формування концептуальних засад правового регулювання військової складової міжнародної інформаційної безпеки розпочалось з 90-х років XX сторіччя:

- в доктрині міжнародного права склалось два концептуальних підходи до міжнародно-правового регулювання використання ІКТ у військових цілях;
- військова складова використання ІКТ, разом із кримінальною і терористичною, у сукупності утворюють комплекс правової проблематики інституту міжнародної інформаційної безпеки;
- міжнародно-правове регулювання співробітництва держав з проблематики військової складової застосування ІКТ виступає в якості суттєвого додаткового фактору розвитку міжнародних інформаційних відносин.

Список використаних джерел

1. The Information Revolution and National Security. – Washington. – CSIS. 1996; The Information Revolution and International Security. – Washington. – CSIS. 1998; Char A. La guerre mondiale de l'information. / A. Char. – Sainte-Foy, 1999.
2. Morth T. Considering our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter / T. Morth // Case Western Reserve Journal of International Law – 1998. – P. 567-600.
3. Лукашук И. И. Международное право. Особенная часть: учеб. для студентов юрид. фак. и вузов / И. И. Лукашук. – Изд. 3-е, перераб. и доп. – М. : Волтерс Клувер, 2007. – 544 с.
4. Мережко А. А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). Проект А. А. Мережко [Електронний ресурс] / А. А. Мережко // Український центр політичного менеджменту – Режим доступу: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
5. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. ООН, Нью-Йорк, 2012. [Електронний ресурс] – Режим доступу: http://disarmament.un.org/DDApublications/index.html.
6. Козик А. Л. Сетевые компьютерные нападения с точки зрения современного международного права / А. Л. Козик // Российский ежегодник международного права. – 2011. Специальный выпуск. СпБ. 2012. – 376 с.
7. Конвенция об обеспечении международной информационной безопасности (концепция). [Електронний ресурс] – Режим доступу: http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument.

8. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года. [Електронний ресурс] – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=28340.
9. Федоров А. Ф. Семь тезисов противников «международной информационной безопасности» / А. Ф. Федоров // Международная жизнь. – 2001. – №2. – С. 89-92.