Ю. С. Размєтаєва[1]

СИСТЕМА МІЖНАРОДНОЇ БЕЗПЕКИ У СВІТЛІ КІБЕРЗАГРОЗ: ПРАВОВІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Система міжнародної безпеки отримує серйозні проблеми в разі кібервійни. Насамперед, неготовність правових інструментів і механізмів. Далі – невизначеність регулювання, оскільки неясно, чи застосовувати в цьому випадку jus ad bellum, jus in bello, право прав людини чи щось інше. Також повинні враховуватися особливості кіберконфліктів, а саме: складність визначення кіберагресії, учасників та наслідків кіберпротистояння, питання доказів, прихований і віддалений характер дій. Все це стає ще більш складним для гібридних конфліктів.

Уразливість системи міжнародної безпеки перед кіберзагрозами в якійсь мірі пояснюється двома речами: стрімким і транскордонним технологічним розвитком та довгим домінуванням підходу, який орієнтувався лише на кримінально-правову складову відповідних загроз. Останні розглядалися як розширення кола способів скоювати злочини за допомогою інформаційно-комунікаційних технологій, включаючи терористичні акти. Тому міжнародна безпека не одразу зорієнтувалася на можливу військову складову та кіберконфлікти, навіть коли стала вимальовуватися серйозна залежність інфраструктури розвинених держав від цифрової складової. Як підкреслює, І. Забара, зараз міжнародно-правове регулювання співробітництва держав з проблематики військової складової застосування технологій «виступає як суттєвий додатковий чинник розвитку міжнародних інформаційних відносин» [1, с. 90].

Однією зі складових у зміні вигляду міжнародних відносин, а також їх правової основи є можливий перегляд системи міжнародної безпеки. Серед нових викликів, які готують кібертехнології, можна виділити використання технологій для здійснення ворожих дій та актів агресії, втручання до цивільної інфраструктури, дестабілізацію суспільно-політичної ситуації, поширення неправдивої інформації та маніпулювання свідомістю, знищення або блокування комп'ютерних систем і мереж.

Перспективи зміни системи міжнародної безпеки досить невизначені. Проте вже можна сказати, що багато інститутів і механізмів неефек-

[1] Кандидат юридичних наук, асистент кафедри теорії держави і права Національного юридичного університету імені Ярослава Мудрого

тивні або недостатньо ефективні. Тому слід розглянути дві площини можливого розвитку цієї системи: іструментальну та ментальну (ідеологічну). Інструментальна площина припускає, що ми повинні відповісти на питання: Чи потрібні нові механізми та інструменти міжнародної безпеки для захисту від кіберзагроз? Чи можна таким чином модернізувати або пристосувати наявні механізми та інструменти міжнародної безпеки, щоб забезпечити успішний захист від кіберзагроз? В рамках тих механізмів безпеки, які вже існують на міжнародному рівні, можна піти шляхом інтерпретації правових актів. У цьому випадку ми зможемо орієнтуватися на застосування існуючих правил до кіберпростору та кіберзагроз, з урахуванням специфіки останніх. Як наголошується, «перенос цих вже існуючих правил і принципів до нової сфери кіберпростору […] піднімає ряд важливих питань. Деякі з цих питань можуть бути вирішені шляхом класичної інтерпретації у поєднанні з певною мірою здорового глузду, розумності, в той час як інші вимагають одноголосного політичного рішення від міжнародного законодавця, міжнародного співтовариства держав» [2]. Ми можемо також піти шляхом розширення повноважень міжнародних інституцій, передусім інститутів ООН. Останні події показали, що ефективне й адекватне кіберзагрозам рішення має бути також продуманим на кілька кроків вперед у будь-якому можливому напрямку. Звідси не виключається необхідність обмеження на створення інформаційної зброї та контролю за нею, попередження інформаційних війн, на кшталт тих, що застосовуються до обмеження й контролю ядерної чи хімічної зброї. Не варто забувати, що виняткові випадки здатні створювати прецеденти, в яких легітимація деяких дій можлива постфактум, особливо там, де запобігання чи своєчасного втручання не відбулося. Проте ефективність наявних інститутів міжнародної безпеки іноді недостатня навіть у традиційних, класичних сферах. Приміром, вето Російської Федерації на резолюцію щодо анексії Криму змушує згадати, що подібне ветування блокує втручання ООН не вперше. Місія ОБСЄ в Україні піддавалася неодноразовій критиці за результати свого моніторингу. Це змушує сумніватися, що в такому маловивченому полі, як кіберпростір і кіберзагрози, відповідні інститути будуть діяти більш успішно.

Що стосується можливої розробки та впровадження нових механізмів або появи спеціальних інститутів міжнародної безпеки, то на користь цього рішення схиляє їх потенційна ефективність як спеціально призначених для відповіді на кіберзагрози та кожен випадок, коли не спрацьо-

вують наявні механізми. Але, можливо, це має бути поєднання двох інструментів – створення нових міжнародних інститутів і розширення повноважень старих. Так, Г. Шаффер, наводить приклад того, як Рада Безпеки ООН «розширила свій мандат за контролем міжнародного миру та безпеки, щоб дозволити «гуманітарну інтервенцію»» [3, с. 670].

Ментальна площина розгляду можливого розвитку системи міжнародної безпеки передбачає вибір між «відкритим» та «закритим» рішенням. Чи слід державам зосередитися на вдосконаленні системи національної безпеки, створенні щита і меча для себе? Або держави повинні виходити з глобального інформаційного порядку та взаємозалежності? Це саме ментальний, ідеологічний, а не просторовий вибір, тому що кіберпростір транснаціональний. Комунікацію та інформаційний обмін дуже складно утримати в певних межах, особливо при нинішньому розвитку інформаційних технологій. Ви можете, звичайно, спробувати створити «залізну завісу» для інформації, але якщо люди вже відчули смак свободи, всі вони (або, принаймні, значна частина) будуть прагнути до неї знову і знову.

Отже, закритий шлях передбачає зосередження на сфері національної безпеки, розробку окремих стратегій кіберзахисту та протидії кібервійні. Він веде до нарощування інформаційно-технологічних потужностей і можливого замикання усередині системи. Але проблема тут не тільки в неможливості запобігти будь-якому невигідному державі витоку інформації чи суперечності вигідної для безпеки тотального кіберспостереження правам людини. Проблема ще й у тому, що окрема держава не зможе протистояти можливим кіберзагрозам, якщо буде покладатися тільки на свої розробки та виключить з метою безпеки деякі аспекти інформаційного обміну з іншими. Слід також звернути увагу на те, що доктрини національної кібербезпеки не завжди встигають змінитися так швидко, як технології.

Як наголошується, прийняті в останні роки національні концепції, що передбачають використання інформаційного простору у військових цілях, «фактично тільки склали уявлення про можливості кожної з держав, залежно від їх науково-технічного та технологічного розвитку» [1, с. 86]. Відставання також спостерігається у сфері національного правового регулювання. Як зазначається, «щоб впоратися з новими та зростаючими загрозами, уряди продовжують покладатися на обмежені та фрагментарні правові положення, не призначені для вирішення проблеми кібератак» [4, с. 885]. Не варто забувати, що навіть у технологічно

розвинених, демократичних державах істотним змінам в законодавстві щодо пов'язаних з кіберзагрозами питань передує серйозне громадське обговорення, що збільшує час реакції на просування кібертехнологій. У державах, що прагнуть до демократичного режиму, до цього можуть додаватися інші перешкоди, такі як корупція або олігархічні інтереси.

Потрібно сказати про те, що закритий шлях для системи безпеки може призвести до однієї серйозної суперечності – між інтересами окремої держави та логікою глобального інформаційного розвитку. Існуюча на глобальному рівні інформаційна інфраструктура не може обмежуватися територіальними кордонами. Сучасний кіберпростір пронизаний системою взаємопов'язаних елементів на транснаціональному рівні, – і це один з визначальних чинників у розвитку міжнародно-правових інформаційних відносин. Тому відкритий, глобалізаційний шлях для системи міжнародної безпеки у світлі кіберзагроз видається більш обґрунтованим і ймовірним. Важливо, що інформаційні відносини між приватними акторами практично безповоротно прийняли транскордонний характер. Це стосується і комунікації між окремими людьми, індивідуальних інформаційних обмінів. У такому відкритому, глобальному інформаційному суспільстві та кіберпросторі можливе спільне підтримання балансу у сфері міжнародної безпеки.

Поєднання національної та міжнародної стратегій кіберзахисту, опора на приватних і державних акторів та динамізм – ось приблизний рецепт для безпеки кіберпростору. Як справедливо зазначається, «і захист устаткування, і захист програмного забезпечення є головним пунктом кібербезпеки […] Тим не менш, обидва види захисту повинні бути реалізовані та вбудовані до національної та міжнародної стратегії (регулювання), щоб досягти своїх цілей» [5, с. 22].

На закінчення, необхідно відзначити тенденцію, яка справедлива для будь-яких загроз безпеки, у тому числі кіберзагроз – підвищення транснаціональної взаємозалежності. Як вказує Г. Шаффер, «Збільшення транснаціональної взаємозалежності перетворює внутрішні проблеми на глобальні» [3, с. 670]. Так що навіть якщо в якійсь сучасній державі відбувається виключно громадянський конфлікт, він впливає на міжнародні відносини, у тому числі на систему міжнародної безпеки.

Література:

1. Забара І. М. Правове регулювання військової складової міжнародної інформаційної безпеки / І. М. Забара // Актуальні проблеми міжнародних

відносин : зб. наук. праць. – К. : Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – 2013. – Вип. 117 (II). – С. 84–91.

2. Melzer N. Cyberwarfare and International Law [Electronic resource] / N. Melzer // UNIDIR. – 2011. – Available at http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

3. Shaffer G. International Law and Global Public Goods in a Legal Pluralist World / G. Shaffer // The European Journal of International Law. – 2012. – Vol. 23. – No. 3. – C. 669–693.

4. Hathaway Oona A., et al. The Law Of Cyber-Attack / Oona A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel // California Law Review. – 2012. – Vol. 100. – No. 4. – P. 817–885.

5. Maskun S. H. LL.M Cyber Security: Rule of Use Internet Safely / S. H. LL.M. Maskun // Journal of Law, Policy and Globalization. – 2013. – Vol.15. – P

О. М. Сіваш[1]

ДИПЛОМАТИЧНИЙ ЗАХИСТ ЯК ФОРМА ЗАХИСТУ ПРАВ ГРОМАДЯН ЗА КОРДОНОМ

Історія міжнародних відносин свідчить, що захист прав і законних інтересів громадян за кордоном здійснюється в різних формах і різними способами. Однією з визнаних форм такого захисту є дипломатичний захист. Інститут дипломатичного захисту здавна відомий міжнародному праву, саме він був єдиним засобом захисту осіб (фізичних і юридичних) в міжнародних відносинах за умови відсутності міжнародного захисту прав людини[2].

Однак, незважаючи на те, що в сучасному міжнародному праві закріплений принцип поваги до прав людини[3], на основі якого активно

[1] Кандидат юридичних наук, доцент, доцент кафедри міжнародного права Національного юридичного університету імені Ярослава Мудрого

[2] Содіков, Ш. Д. в своєму дисертаційному дослідженні пише: «Саме міжнародно-правові норми про дипломатичний захист, на фоні тотального заперечення будь-якої міжнародної правосуб'єктності фізичних і юридичних осіб, створював юридичну основу для захисту державою своїх осіб на території іноземної держави»[1, С. 8].

[3] Статут ООН;Заключний акт НБСЄ 1975 р.; Декларація про принципи міжнародного права, що стосуються дружніх відносин і співробітництва держав відповідно до Статуту ООН 1970 р.