СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

У двох частинах

Частина 1

Суми
Сумський державний університет
2020

certain legal aspects of information society services, in particular electronic commerce, in the Internal Market («Directive on electronic commerce»). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586695311265&uri=CELEX:32000L0031 (last accessed: 11.04.2020).
9. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25
November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586696082406& uri=CELEX:32015L2366 (last accessed: 11.04.2020).
10. Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers` nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586696308055&uri=CELEX: 32018R0302 (last accessed: 11.04.2020).
11. Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586696463390&uri=CELEX:32019L0771 (last accessed: 11.04.2020).
12. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586696534067&uri=
CELEX:32019L0770 (last accessed: 11.04.2020).

КІБЕРВІЙНА ТА ПИТАННЯ ЗАСТОСУВАННЯ ДО НЕЇ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

Рєпін Д. А.
Студент ІІІ курсу ННІ права
Сумського державного університету
Науковий керівник: Денисенко С. І.
к. ю. н., доцент, старший викладач кафедри МЄПЦПД ННІ права
Сумського державного університету

Сьогодні поняття забезпечення міжнародної інформаційної безпеки та підтримання міжнародного миру і стабільності нерозривно пов’язано. Поширення нових інформаційних і комунікаційних технологій призвело до їх широкого використання не

тільки в цивільній, а й у військовій справі. Держави все частіше звертають увагу на розвиток як оборонних, так і наступальних операцій в кіберпросторі. Слід підкреслити, що концепції правової підтримки міжнародної інформаційної безпеки знаходяться тільки на етапі формування і регулювання як на міжнародній арені, так і в національнихпрограмах окремих, тому загроза кіберпростору для ведення війни цілком реальна і вимагає негайного юридичного врегулювання.

Проблемам, пов'язаним з кібервійною, приділяють чималу увагу серед міжнародної спільноти. Нові підрозділи та органи по забезпеченню кібербезпеки створюються на різних рівнях державної влади, у тому числі і в збройних силах. Але операції в кіберпросторі, а тим паче в ситуаціях збройних конфліктів можуть мати дуже серйозні наслідки, особливо коли їх дія направлена не тільки на конкретну комп'ютерну систему або комп'ютер, які визначені як об'єкт нападу. Дійсно, мета операцій в кіберпросторі зазвичай полягає у впливі на «фізичний світ». Вплив на цивільне населення деяких операцій в кіберпросторі може бути величезним. Тому важливо обговорити норми міжнародного гуманітарного права (далі – МГП), які можуть урегулювати такі операції, оскільки одним із завдань цієї галузі права є захист цивільного населення від впливу військових дій.

По-перше, через все більше розширення використання комп'ютерних систем цивільна інфраструктура вкрай вразлива перед нападами на комп'ютерні мережі. Зокрема, цілий ряд найважливіших об'єктів, таких як електростанції, атомні станції, системи очищення і розподілу води, нафтопереробні підприємства, газові та нафтові трубопроводи, банківські системи, системи лікарень, залізні дороги і авіалінії тощо, покладаються на так звані системи інформаційного або телеуправління та збору даних. Ці системи є сполучною ланкою між цифровим і фізичним світами, і вони вкрай вразливі перед зовнішнім втручанням, яке може бути здійснено будь-яким агресором.

По-друге, цілісність мережі Інтернет, тому, дійсно, більшість військових мереж покладаються на цивільну, головним чином комерційну, інфраструктуру, наприклад, супутники, інформаційні, телекомунікаційнімережі, цивільні транспортні засоби, контроль над морським та авіа суднами, які обладнані навігаційними системами, що залежать від глобальної навігаційної супутникової системи (система GPS навігації), яка використовується і військовими.

Таким чином, в значній мірі неможливо провести відмінність між цивільною і суто військовою комп'ютерною інфраструктурою, а це кидає серйозний виклик одному з основоположних принципів міжнародного гуманітарного права, а саме принципу проведення відмінності між військовими і цивільними об'єктами, який визначено статтею

48 Додаткового протоколу Ідо Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів. Більш того, міжмережева взаємодія військових та цивільних комп'ютерних систем означає, що наслідки нападу на військовий об'єкт не будуть обмежені тільки цією ціллю [3].

Дійсно, кібератаки можуть торкнутися різних інших систем, включаючи цивільні системи і мережі, наприклад шляхом поширення шкідливих програмних засобів. Це означає, що напад на військову комп'ютерну систему здатний зашкодити цивільним комп'ютерним системам, що у свою чергу може виявитися вкрай згубним для цивільного населення, оскільки наслідки від такого втручання можуть бути непередбачуваними: можливість катастрофічних сценаріїв, наприклад, зіткнення літаків, витік радіації з ядерних установок, вивільнення токсичних хімікатів на хімічних підприємствах або порушення роботи найважливіших інфраструктур і служб: електросистем, водопостачання тощо [1, ст. 10-13]. Також маємо зазначити, що такі дії також можутьмати жорстокі наслідки через відсутність якісних засобів життєдіяльності кожної людини, починаючи від їжі та води, закінчуючи відсутності дієвого регулювання таких проблем, що може потягти за собою поширення злочинності серед цивільного населення тощо. Тому необхідно прояснити основоположні норми, що стосуються ведення військових дій, які сторони в конфлікті зобов'язані дотримуватися.

Положення МГП не згадують конкретно методів та засобів ведення війни у кіберпросторі. Тоді чи може МГП застосовуватися до кібервійни? Відсутність в МГП конкретної згадки щодо діянь в кіберпросторі не означає, що такі операції не регулюються нормами МГП. Нові технології будь-якого роду розробляються постійно, і масштаб МГП досить широкий для того, щоб врахувати і такий розвиток подій. МГП конкретно забороняє або обмежує застосування деяких видів зброї, однак крім цього воно регулює своїми загальними нормами застосування всіх засобів і методів ведення війни, включаючи способи застосування всіх видів зброї. Так, статтею 36 Додаткового протоколу I до Женевських конвенцій передбачено, що при вивченні, розробці, придбанні чи прийнятті на озброєння нових видів зброї, засобів або методів ведення війни Висока Договірна Сторона повинна визначити, чи підпадає їх застосування, за деяких або за всіх обставин, під заборони, що містяться в цьому Протоколі або в яких-небудь інших нормах міжнародного права, застосовуваних до Високої Договірної Сторони [3].

Крім конкретного зобов'язання, яке ця норма накладає на держави - учасників Додаткового протоколу I, вона показує, що норми МГП застосовуються по відношенню до нових технологій. І все-таки кібервійна кидає виклик окремим самим основоположним положенням МГП:

1. МГП виходить з того, що сторони в конфлікті відомі і ідентифіковані. Це не завжди само собою зрозуміло навіть в традиційних збройних конфліктах, особливо неміжнародних збройних конфліктах. У деяких випадках відсутня можливість дізнатися, хто саме є ініціатором конфлікту, і навіть коли це можливо, частіше за все на це потрібно дуже багато часу.

2. Будь-яке право ґрунтується на визначенні суб'єкта відповідальності. Наприклад особа здійснила злочин проти комп'ютерної системи, але при цьому зв'язок такого діяння не може бути встановлений як окрема операція військового конфлікту, або коли відсутня можливість встановлення особи, організації або держави, що стоїть за цим діянням, тодінорми МГП взагалі не можуть застосовуватися, тому що неможливо визначити, чи має взагалі місце збройний конфлікт.

3. Багато операцій в кіберпросторі, швидше за все, будуть мати руйнівний вплив, але вплив, яке відразу ж не буде сприйматися як руйнівна в фізичному сенсі. По-третє, вся структура норм, що стосуються ведення військових дій, і зокрема принцип проведення відмінності.

На сьогоднішній день Талліннське керівництво по міжнародному праву, застосовуваним до кібервійни, є найбільш ґрунтовною спробою витлумачити норми міжнародного правастосовно кібервійни. Воно було складено групою експертів за дорученням Спільного центру передових технологій в області кібероборони НАТО, у Керівництві містяться норми з коментарями, що відображають різні точки зору щодо деяких суперечливих питань, що виникають у зв'язку з інформаційними технологіями [2, ст. 16].

Аналізуючи нормативно-правові акти МГП, можна з впевненістю зазначити, що норми міжнародного гуманітарного права можуть застосовуватися тільки тоді, коли операції в кіберпросторі ведуться в контексті збройного конфлікту або в зв'язку з ним. Таким чином, не повинно викликати заперечень твердження, що якщо операції в кіберпросторі проводяться в контексті збройного конфлікту, вони регулюються тими ж нормами МГП, що і цей конфлікт: наприклад, якщо разом з початком бойових дій, сторона в конфлікті здійснює напад на комп'ютерні системи свого супротивника. Так, відповідно до статті 6 Женевської Конвенції про захист цивільного населення під час війни, ця Конвенція повинна застосовуватися з самого початку будь-якого конфлікту або окупації, а припинятися тільки після загального припинення бойових дій на території сторін конфлікту [4]. Однак цілий ряд операцій, які характеризуються як військові дії у кіберпросторі, можуть здійснюватися і не в контексті збройних конфліктів. Такі терміни, як «кібератаки» або «кібертероризм», можуть бути пов'язані з методами ведення війни,

але не обов'язково проводяться під час збройного конфлікту. Операції в кіберпросторі можуть бути злочинами, що здійснюються в повсякденних ситуаціях, які не мають нічого спільного з війною.

Таким чином, можна прийти висновку, що іноді сторони в збройних конфліктах використовують кіберпростір, якодин із методів ведення війни, при цьому вони повинні дотримуватися всіх чинних міжнародно-правових актів щодо ведення війни, у тому числі і міжнародного гуманітарного права. Але чи надасть сучасне міжнародне гуманітарне право достатній захист цивільному населенню, не зашкодившицивільній інфраструктурі? На нашу думку дане питання буде залежати від розвитку міжнародного гуманітарного права, оцінюючи вплив інформаційних технологій, в умовах науково-технічного прогресу. Сьогодні дане питання є досить спірним, оскільки наявні слабкі сторони принципів проведення відмінності, пропорційності і прийняття запобіжних заходів (коли незрозуміло чи має місце збройний конфлікт, чи є відповідний об'єкт цивільним або військовим тощо). Тому тільки ефективне та оперативне регулювання даної сфери зможе надати захист цивільному населенню від перетворення її в безпосередній об'єкт нападу або від шкоди, яка може стати катастрофічною для цивільного населення.

ЛІТЕРАТУРА:

1. Stefano Mele. Cyberwarfare and its damaging effects on citizens. September 2010. 19 p. URL: http://stefanomele.it/public/documenti/185DOC-937.pdf.

2. Tallinn Manual on the international law applicable to cyber warfare, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. *Cambridge University Press*. 2013. 215 p. URL: http://csef.ru/media/articles/3990/3990.pdf.

3. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_199.

4. Женевська конвенція про захист цивільного населення під час війни від 12 серпня 1949 р. URL: https://zakon.rada.gov.ua/laws/show/995_154.