УДК 343.33

Марценко Н. С.
к.ю.н., доцент кафедри міжнародного права
та міграційної політики
Західноукраїнський національний університет

ПОНЯТТЯ ТА ВИДИ ІНФОРМАЦІЙНИХ ВІЙН

У сучасному світі надзвичайно широких технологічних можливостей ми практично щодня стаємо свідками різних аспектів системи управління інформацією та їх наслідків. Тому поняття «інформаційна війна» стало звичним як для державних чиновників різних рівнів та різних країн, так і для звичайних громадян. М. Маклуен вдало відмітив, що у сучасному світі економічні відносини все більше приймають форму обміну знаннями, а не обміну товарами, тому боротьба за капітал, простори збуту та інше відходять на другий план, а головним постає доступ до інформаційних ресурсів. Саме М. Маклуен говорив про нищівні наслідки інформаційних війн, наголошуючи, що «істинно тотальна війна – це війна за допомогою інформації» [1]. З огляду на величезний потенціал у розподілі сфер впливу, інформаційна війна має чималі політичні, технічні, оперативні та правові наслідки, тому надзвичайно затребуваними є дослідження сутності та видів інформаційних війн у їх взаємодії та взаємозв'язку. Дані знання будуть корисними у боротьбі з негативними наслідками даного явища у майбутньому.

Загалом, інформаційна війна розуміється як цілеспрямована спроба підірвати і нейтралізувати систему управління противника з метою координації діяльності органів управління [2]. Фактично, інформаційна війна передбачає подання інформації у спосіб, який формує у суспільстві чи групі людей потрібну точку зору та громадську думку щодо окремих питань на користь організатора інформаційної пропаганди. Це сприяє усвідомленню окремих фактів чи подій у потрібному для маніпулятора світлі.

Інформаційна війна може включати: збір тактичної інформації, перевірка достовірності інформації, поширення пропаганди та дезінформації для деморалізації або маніпуляції опонентом і громадськістю, підрив якості інформації опонента, позбавлення опонента можливості збирати інформацію [3]. Тому, володіючи необхідною інформацією, очевидно, держава володіє стратегічними перевагами в першу чергу для забезпечення власної безпеки, а не тільки задля завдання шкоди противнику.

У літературі є багато класифікацій інформаційних війн, однак варто звернути увагу саме на класифікацію, запропоновану Мартіном Лібіцьким, який виділяє такі форми інформаційної війни: 1) ведення війни у сфері

управління; 2) розвідувальна війна; 3) радіоелектронна боротьба; 4) психологічна війна; 5) хакерська війна; 6) економіко-інформаційна війна; 7) кібервійна [5]. Усі вони тісно пов'язані між собою та часто ведуться у комплексі (наприклад, задля ширшого охоплення цілей, інформаційні війни супроводжуються кібервійною та психологічною війною із залученням радіоелектронної боротьби та мережевих технологій).

Однією із найбільш поширених є електронна війна, у якій електронні та інші засоби безпосередньо впливають на електронні засоби та системи противника, а також на бойові системи та озброєння, які функціонують на основі використання в них електроніки. Електронна війна також визначається як сукупність військових дій, основною метою яких є контроль над електромагнітним простором. Електронна атака є частиною радіоелектронної боротьби, що передбачає використання електромагнітної енергії або цільової енергії для атаки з метою деградувати, нейтралізувати або знищити бойові можливості супротивника. Електронний захист є частиною радіоелектронної боротьби і охоплює діяльність, спрямовану на захист власного народу від засобів впливу радіоелектронної боротьби противника [6].

Інформація про противника, зібрана за допомогою радіоелектронної боротьби, має значний інтелектуальний вимір, і тоді радіоелектронну війну можна розглядати як розвідувальну війну [5]. Однак розвідувальна війна перебуває у функції планування і ведення радіоелектронної боротьби і, зокрема, формування електронної картинки поля бою. Тому відношення між електронною та розвідувальною війною найкраще описує термін координація, що також характерно для деяких інших форм інформаційної війни.

Більш складнішою є психологічна війна, яка передбачає використання інформації проти людського розуму [6]. Психологічна війна є невід'ємною частиною будь-якого збройного конфлікту. Загалом, психологічні операції мають на меті передати вибрану інформацію, призначену для слухачів і глядачів таким чином, щоб впливати на їхні емоції, мотиви та об'єктивні міркування та, зрештою, на поведінку іноземних урядів, організацій, груп і осіб для досягнення власних інтересів і цілей. Фактично, головна мета психологічних операцій із захисту власних систем управління полягає в мінімізації наслідків пропаганди та діяльності опонента задля «інформаційної гігієни» органів влади та населення.

Хакерська війна є однією з форм інформаційної війни та найчастіше виконується окремими особами. Зазвичай хакерська атака націлена на перевантаження та зміну вмісту атакованого веб-сайту або інформаційного ресурсу. Використання хакерської війни значною мірою залежить від кількості використовуваних комп'ютерів та кількість користувачів Інтернету, тому

ступінь інтеграції комп'ютерних мереж обернено пропорційний наслідкам хакерської війни.

Економіко-інформаційна війна керується інформацією про економічне значення для конфліктуючих сторін. Тут важливе значення може мати інформація про різні договори, розробки, стратегію компанії, внутрішню структуру та організацію, виробничі плани, інвестиції тощо. Даний тип війни присутній навколо конфіденційної інформації, яка буде використана проти конкурентів в інтересах своїх компаній. Даний конфлікт по суті є економічним шпигунством.

Кіберпростір є сферою, яка надає нові можливості для ведення кібервійни, а постійно зростаюча залежність суспільства від інформації та комунікаційних технологій створюють численні слабкі місця та підґрунтя для інформаційних війн. Зважаючи на те, що кібервійни є не тільки оборонними, але і наступальними, та мають за мету зламати або знищити інформаційно-комунікаційні системи супротивника, важливо упорядкувати та надійно захистити національну інформаційну інфраструктуру як основу для захисту життєво важливих суспільних та державних об'єктів [7].

Отже, інформаційні війни є не менш небезпечними ніж класичні війни, а інколи навпаки – є більш непередбачуваними та масштабними. Інформаційні війни можуть набувати різних форм та протікати з різною інтенсивністю, позначаючись при цьому на економічному, політичному, соціальному житті однієї або і більше держав. Тому, боротьба із цим негативним явищем потребує зваженого міжнародно-правового підходу та формування міцної міжнародної інформаційної безпекової доктрини, яка б враховувала усю небезпеку інформаційних війн та пропонувала б дієві методи стримування і покарання інформаційних агресорів.

ЛІТЕРАТУРА:

1. McLuhan, M., & Fiore, Q. (1968). War and Peace in the Global Village: An Inventory of Some of the Current Spastic Situations That Could Be Eliminated by More Feedforward. New York: Bantam.

2. Blair, B.G., 2001. Strategic Command and Control. Washington, D.C., The Brookings Institution

3. Reisman, W.M. & Antoniou, C.T., 1994. The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict. New York, Vintage Books

4. Petrović, S., 2001. Kompjuterski kriminal. Beograd, Ministarstvo unutrašnjih poslova Republike Srbije

5. Libicki, M.,1995. What Is Information Warfare? [e-book]. Washington, National Defense University. Available at: http://www.dtic.mil/get-tr doc/pdf?AD=ADA367662

6. Damjanović, D., Types of information warfare and examples of malicious programs of information warfare, pp.1044-1059

7. Arquilla, J. & Ronfeldt, D., 1995. Network war and cyberwar, a copy of the study publication in «Comparative Strategy». RAND Corporation

УДК 347.23

Москалюк Н. Б.
д.ю.н., доцент, в.о. завідувача кафедри
безпеки та правоохоронної діяльності,
Західноукраїнський національний університет

ПРАВОВІ ЗАСАДИ НАЦІОНАЛІЗАЦІЇ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Російсько-українська війна внесла свої корективи не лише у питання реалізації та захисту прав власності національних фізичних та юридичних осіб, а й у питання особливих способів набуття прав державної власності Україною. Йдеться про можливості, які надаються IV Гаазькою конвенцію про закони і звичаї війни на суходолі та додатка до неї: Положення про закони і звичаї війни на суходолі [1]. Саме на основі положень конвенції 3 березня 2022 року Верховна Рада України прийняла Закон України «Про основні засади примусового вилучення в Україні об'єктів права власності Російської Федерації та її резидентів»**,** де визначила, що **«**З метою захисту суверенітету і територіальної цілісності України, національних інтересів, національної безпеки, забезпечення її економічної самостійності, прав, свобод та законних інтересів громадян України, суспільства та держави, враховуючи повномасштабну агресивну війну, яку Російська Федерація розв’язала і веде проти України та Українського народу з порушенням норм міжнародного права, вчиняючи злочини проти людства, виходячи з положень Конституції України, Декларації про державний суверенітет України та загальновизнаних міжнародних норм і правил, зокрема щодо суверенного права України на захист, враховуючи Указ Президента України "Про введення воєнного стану в Україні" від 24 лютого 2022 року № 64/2022, затверджений Законом України "Про затвердження Указу Президента України "Про введення воєнного стану в