МІЖНАРОДНЕ ПРАВО

УДК 341

МАЙСНЕР А.В.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ, ЩО ОБУМОВЛЮЄ ЗДІЙСНЕННЯ АГРЕСІЇ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Стаття присвячена актуальній проблемі сучасного міжнародного права – проблемі розширення кваліфікаційних характеристик агресії за межі його збройного вияву. З погляду на віртуалізацію міжнародної економіки, зростання значущості фактору інформаційно-комунікаційних технологій у міжнародній торгівлі, тенденції до їх монополізації, автор цілком обґрунтовано привертає увагу до тенденції з посилення насильницької конфліктності у міжнародних відносинах. Така тенденція прямо вказує на «перетікання» потенціалу агресії у незбройну сферу міжнародних взаємодій.

Ключові слова: *агресія, інформаційна агресія, глобалізація злочинності.*

Статья посвящена актуальной проблеме современного международного права − проблеме расширения квалификационных характеристик агрессии за пределы его вооруженного проявления. С точки зрения виртуализации международной экономики, возрастания значимости фактора информационно-коммуникационных технологий в международной торговле, тенденции к монополизации, автор вполне обоснованно привлекает внимание к тенденции усиления насильственной конфликтности в международных отношениях. Такая тенденция прямо указывает на «перетекание» потенциала агрессии в невооруженную сферу международных взаимодействий.

Ключевые слова: *агрессия, информационная агрессия, глобализация преступности.*

The article devoted to the issue of international law − the problem of expansion qualification characteristics aggression beyond its armed manifestations. In terms of virtualization international economy, growth factor significance ICT in international trade, tendency to monopolization, author legitimately draws attention to the violent tendencies of strengthening conflict in international relations. This trend clearly indicates on "overflow" capacity aggression in non-armed field of international interactions.

Key words: *aggression, information aggression, globalization of crime.*

Технологія інформаційної агресії багатошарова, багатоаспектна. Вона вбирає цілий набір прийомів і способів, в результаті дії яких утворюється і швидко зростає інформаційна перевага еліт. Ця перевага також досить інтенсивно конвертується в ефективні важелі контролю для світової олігархії над світовою торгівлею, світовою економікою, де сам злочинний феномен інформаційної агресії з її цілевизначенням на світове домінування еліт, знаходить втілення через далеке від справедливої ринкової конкуренції добре закамуфльоване у своїй жорстокості штучне обмеження розвитку більшості країн і народів.

Загострення відносин між сторонами в межах процесу універсальної агресії значною мірою відбувається за рахунок зростання в їхній (сторін) діяльності ролі інформаційно-комунікаційних технологій (ІКТ). Якщо для терористів інформаційно-комунікаційні технології в основному розширюють можливості і поліпшують технології власне терористичної діяльності,

© МАЙСНЕР А.В. – викладач кафедри міжнародного права Навчально-наукового інституту міжнародних відносин (Національний авіаційний університет)

то найвищий їх рівень у практиці розвинутих держав поступово перетворив ІКТ у самостійний різновид агресії щодо країн «третього світу». Це природним чином випливає із логіки технологічного прогресу, який поряд з полегшенням умов існування людини і суспільства, навантажує її тягарями нових проблем.

В цілому слід виходити з того, що західна культура, незважаючи на демонстративний антропоцентризм, сьогодні схильна знижувати роль власне людських факторів, що відносяться до нашого внутрішнього світу, на користь зовнішніх, передовсім техніко-економічних, що загрожує перетворенням людини у маріонетку [7, с.286].

Карл Ясперс, пояснюючи сенс свого терміну «викриття демонічного характеру техніки», вказує, що віра у прогрес ігнорувала той факт, що прогрес обмежений рамками науки і техніки, і що він не може, вийшовши за їх межі, охопити все людське існування у цілому. За цих умов можливою є лише видимість людяності. Мислитель попереджає, що механізм техніки може надавати на людей у часі зовсім іншого тиску, ніж це було можливе раніше: «наприклад, якщо вичерпні відомості спочатку давали людям духовне звільнення, то тепер поширення інформації перетворилось у панування над людьми через контрольованість відомостей» [12, с.137-138].

З якими ж новими викликами зіткнулося людство, коли мільярди людей, державних і суспільних організацій, а також бізнес-структур отримали можливість спілкуватися у кіберпросторі? Ще актуальнішим є питання чи ці можливості вписуються у природний плин міжнародного життя, плани й наміри учасників міжнародних взаємодій, зважаючи, що участь у кіберпросторі не є суцільною даністю.

Освоєння кіберпростору дедалі більшою мірою пов'язується з набуттям інформацією, яка циркулює в ньому в особливому супероперативному режимі; товарних якостей. Для відповіді на поставлені вище запитання слід усвідомлювати нерівність можливостей використання кіберпростору. Західна культура, спираючись на досягнення технічної цивілізації, отримала колосальні техніко-інформаційні переваги перед іншими культурами, орієнтованими на традиційні способи комунікації. Звідси веде своє походження феномен нееквівалентного інформаційного обміну між розвинутими країнами і країнами, що розвиваються.

Зважаючи на чинне співвідношення сил на світовій арені їх привабливість для меншості (так званого «золотого мільярду») і прагнення до збереження статус-кво, ситуація нееквівалентного інформаційного обміну так само як і у сфері геоекономіки використовується для зміцнення світовими елітами свого домінуючого стану шляхом дій, які несуть ознаки агресії (інформаційної). Інформаційний потік, що йде з Півночі на Південь із Заходу на Схід, виявився в декілька разів потужнішим за зустрічні потоки соціокультурної інформації, що відбивають культурну пам'ять та історичний досвід Заходу і Сходу [7, с.280].

На думку відомого російського соціолога О.С. Панаріна західна культура за цілою низкою критеріїв виявилась більш пристосованою до сучасності і навіть претендує на те, щоб монополізувати сучасність, відокремивши від неї усіх тих, хто не відповідає відомим еталонам епохи модерну [7, с.280].

Освячені метою щонайповнішого підкорення так званих традиціоналістських зон, такі прагнення з очевидністю складають елемент інформаційної агресії, тим більше, що антитрадиціоналізм супроводжується агресивним впровадженням антицінностей.

Але найефективніше використання потенціалу ІКТ для нарощування зверхності у системі чинного світопорядку спостерігається у економічній сфері. При чому на теренах економічного підкорення слаборозвинених країн вони виявляють себе у двох іпостасях: як засіб забезпечення економічної агресії і як самостійна агресорська конструкція, можливість якої зумовлена товарним змістом інформації.

Поява ІКТ, а з ними – нової форми міжнародних відносин на оцифрованій основі, давала міжнародному співтовариству шанс на використання великого позитивного потенціалу глобалізації для втілення принципів рівності у всьому спектрі міжнародних відносин держав і, отже, значного зниження планетарної конфліктності.

Варто нагадати, що логіка глобалізації як об'єктивного явища, вимагає однозначного визнання єдності загальнолюдської перспективи. Взаємозалежність, взаємопов'язаність світу та діючих у його межах акторів стала очевидною. Тому сепаратні стратегії прориву у краще майбутнє, зокрема, прагнення до безподільного панування у цьому майбутньому, створюють небезпеку непередбачуваності, терористичної катастрофогенності.

На жаль такі прогнози дедалі більшою мірою набувають ознак підтвердження, тим більше, що сам процес нехтування глобальними реаліями сучасного єдиного простору-часу

виявляється через діяння і поведінку розвинутої частини міжнародного співтовариства, яка містить очевидні ознаки агресії у її збройних, економічних і, нарешті, інформаційних формах.

Міжнародно-кримінологічний інтерес проблеми ІКТ та агресії, що базується на їх використанні, представляє тим, що вона (агресія) відбувається в умовах інформаційного суспільства з його феноменом «цифрової нерівності». Саме міжнародно-кримінологічна методологія допомагає з'ясувати суть «цифрової нерівності» − висхідну рушійну силу інформаційної агресії, а саме, володарів реальної глобальної влади − світову фінансово-промислову олігархію, яка за логікою (від М.Вебера, Б. де Жувенеля та ін.) первісності влади по відношенню до соціуму, найінтенсивніше використовує можливості ІКТ. Тим самим глобальна влада значно посилила свою потугу і, отже, світоуправлінський потенціал. Пріоритетний доступ до ІКТ також розширив можливості геополітичних та геоекономічних інститутів (МВФ, СОТ, НАТО), що виявили себе як фактичні інструменти глобальної влади. На думку відомого американського соціолога Джозефа Ная, «новий світ залежить від традиційного світового порядку, у якому влада ґрунтується на регіональних та геополітичних інститутах» [5, с.128].

Інформаційну агресію значною мірою формує «елітарність», обраність «приватної волі». Така обраність виражається знову таки у можливостях володіння інформацією в умовах використання ІКТ. Той, у кого не дістає грошей на організацію захисту своїх економічних секретів та на конкурентне добування інформації, неминуче приречений на розорення незалежно від дійсного (навіть блискучого) стану свого бізнесу. Умови ІКТ гіперболізують впливовість дій, що можуть утворювати інформаційну агресію, оскільки інформаційно незахищений бізнес є завідомо не конкурентоздатним. У торгівельних відносинах держав гіперболізація агресивної складової полягає в тому, що для розвинутих країн самі партнери та суть оборудок з ними постають у максимально прозорому вигляді і навпаки, економічно слаборозвинені країни, в силу інформаційного дефіциту, не мають можливості вибудовувати свої дії з гарантією елементарної вигоди. Фігурально висловлюючись, ефективність інформаційної агресії гіперболізується майже у критеріях геометричної прогресії.

При цьому грабіжницька сутність інформаційної агресії так само як і у випадках збройної і економічної агресії маскується у різноманітні способи і прийоми, основними з яких виражаються через декілька фікцій. Перша фікція полягає в ілюзії сприйняття держави як політичного інструменту з організації суспільного життя певного соціуму, вираження волі народу. Вона запрограмована на те, що дії держав з реалізації своїх переваг у сфері ІКТ у тому числі й ті, що складають відхилення від основоположних норм моралі та права, зумовлюються інтересами суспільства або, щонайменше, вчиняються за формальною санкцією суспільства. У такий спосіб вдається розчинити відповідальність за наслідки злочинності, у витоках якої стоять інтереси і воля конкретних впливових осіб або груп таких осіб.

Друга фікція, якою камуфлюється інформаційна агресія – це фікція, що пов'язана з абсолютизацією вільного ринкового середовища, у межах якого переваги і здобутки учасників міжнародних економічних відносин визначаються об'єктивними законами конкурентної боротьби, яка (нехтуючи фактор єдності світового суспільства та світогосподарчої системи) неухильно результує переваги для найпередовіших, найпросунутіших суспільств.

Що стосується фікції визначальної ролі народного волевиявлення у діяльності держави, в тому числі й у міжнародних економічних процесах, які дедалі більшою мірою наповнюються фактором впливу ІКТ, то тут слід звернутися до праць В.Ф.Антипенка. Посилаючись на авторитетну думку М.Вебера, Бертрана де Жувенеля та інших відомих у світі мислителів, вчений творчо втілює у міжнародно-правову науку їхню концептуальну думку про первісність влади відносно соціуму, а не навпаки, як це прийнято вважати у доктрині та політичній і юридичній практиці. На цій основі побудована концепція кримінальної відповідальності держави, в основі якої лежить оцінка кримінальності реальної влади [1, с.53-68].

При здійсненні оцінки системи маскування інформаційної агресії та її специфіки слід зважити на те, що ІКТ як джерело міжнародної кримінальності є предметом уваги міжнародного права не випадково. Як вже зазначалося, використання ІКТ, попри позасумнівне свідчення прогресивного розвитку людського універсуму, надає загрозливу кумулятивну дію на наявну криміналізацію міжнародних економічних процесів. Звідси особливо небезпечний потенціал агресії, яку несе ІКТ, потребує ретельних і системних заходів з його маскування. При всій багатоаспектності виявів інформаційної агресії у якості її основи слід відмітити механізм так званих «покерних» умов функціонування міжнародної економіки [6, с.169]. Він представляє собою нерівне за-

стосування спеціальних ІКТ, (для яких практично не існує моральних та правових бар'єрів), коли стрімке зростання попиту на інформацію забезпечує комерційний результат, який досягається лише тими, хто в змозі застосовувати найдорожчі найпродуктивніші інформаційно-комунікаційні технології переважно для здійснення оборудок підступного шулерського ґатунку. Йдеться про створення фальшивого іміджу насправді неблагополучних компаній, завищення кредитних рейтингів, примітивний шантаж та под. Збільшення обсягів капіталу, що задіюється у електронній торгівлі, тягне збільшений попит на спеціальні ІКТ [2, с.122].

В результаті позначеного владного впливу юридичні заходи з супроводження такого роду міжнародного бізнесу в умовах ІКТ попри його кримінальний зміст по суті зміцнюють його прийнятність, сприяють його характеристиці як поточного процесу. Між тим саме ошукувальна система застосування спеціальних ІКТ з очевидністю складає зміст агресії, утворює загрозу міжнародній безпеці, оскільки інтенсивно поповнює глобальний соціальний конфлікт новими протестними силами, так званими (за І.Валлерстайном) «небезпечними класами» або «антисистемними силами», готовими до боротьби проти свого відчуження [4, с.65, 90, 227].

Небезпечність інформаційної агресії для міжнародного миру зумовлена специфічним характером її злочинного за міжнародним правом механізму. Адже перевага внаслідок використання спеціальних ІКТ одних учасників ринку над іншими, неуклінно зростає, продукуючи соціально-економічну поляризацію і поглиблюючи інформаційну асиметрію, а з нею – і конкурентні можливості, що означає нищівну дію на сектор міжнародної економіки. Соціально-економічна поляризація, що супроводжується прискореним зубожінням великих людських мас, є питомим середовищем для ескалації тероризму на глобальному рівні. Втім криміногенність інформаційної агресії полягає не лише у цьому, у цілому традиційному для капіталістичної світоекономіки, механізмі. [6, с.231].

Виглядаючи зовні як банальне використання переваги у ІКТ, наведений механізм за своєю криміногенною сутністю є злочинним. Він з очевидністю потребує міжнародної кримінально-правової кваліфікації за ознаками агресії в умовах використання ІКТ або інформаційної агресії. Адже по суті поза кримінально-правовим реагуванням і регулюванням залишилось формування і розвиток економіки, основу якої складає кримінальним чином утворювана прибутковість за рахунок інформаційного ошукування покупців і інвесторів. Вдосконалення безпосередньо самих технологій цієї економіки здійснюється у напрямі пошуку і вилучення недостатньо захищеної власності.

Розглянутої вище загальної схеми виникнення і дії інформаційної агресії недостатньо для формування конкретних норм міжнародного права з протидії цьому міжнародному злочину. Останні за своїм смислом покликані створювати перешкоди конкретним прийомам і способам реалізації агресивної діяльності певної держави з використання можливостей ІКТ. Отже постає завдання аналізу і правової оцінки конкретних способів дій, що складають зміст інформаційної агресії, причин неохоплюваності їх дією міжнародного права.

Нерівне використання можливостей спеціальних ІКТ переповнює економіку такою інформацією, яка підмінює норми права, покликані забезпечувати справедливу конкуренцію та «розкладає фундаментальні ринкові принципи економіки, істотно модифікує мотивацію бізнесу, охоплюючи при цьому інші сфери економіки (ділової активності). Ринковий механізм, таким чином, стає несправедливим, конкуренція здійснюється жорсткими, практично воєнними методами, що забезпечується лобіюванням і державною підтримкою такої неринкової поведінки еліт» [6, с.231]. При очевидній міжнародній криміногенності такого перекручення об'єктивних правил ринку, намірів або спроб надати йому (перекрученню) міжнародно-правову кваліфікацію не спостерігається.

Поширення ІКТ і, зокрема, комп'ютерного моніторингу привели до виникнення й розвитку специфічного бізнесу, суть якого полягає у доступі до персональних даних користувачів Інтернету. Міжнародно-кримінальний аспект такої тенденції зумовлюється перетворенням моніторингу на тотальний контрольний, що кінець кінцем результує припинення існування неконтрольованого комп'ютерного інформаційного простору. Реальність тотального контролю підтверджується також і безрезультатністю вживаних після подій 11 вересня 2001 року спроб створити систему захисту особистої інформації. Законодавчі обмеження, що введені у країнах, у своїй більшості не знаходять відповідного втілення передусім приватними компаніями, оскільки серйозно зашкоджують їхнім прибутковим (корпоративним) інтересам. У підсумку формується відчутний глобальний інформаційно-технологічний удар по правах людини, реагування на який навряд чи утримається в межах чинних норм міжнародного права.

Таким чином, інформаційна агресія супроводжується формуванням криміногенних факторів, пов'язаних з тоталітаризацією глобального управління, різного роду маніпуляціями, що тягнуть соціально-економічні катаклізми країн, народів, цивілізацій. Державі при цьому відводиться роль лобіювача приватних корпоративістських інтересів впливових гравців світового фінансово-економічного ринку. Але все це вбирається у форму об'єктивного реагування на об'єктивний запити користувачів і регламентації з боку держави як політичного інструменту втілення волі народу. У дійсності такий механізм надає лише видимість наведених процесів, їх об'єктивного походження.

Наступним явищем, яке має виключно негативні наслідки, і яке необхідно кваліфікувати як форму здійснення злочину агресії є кібер-атака. Кібер-атаки, які можуть стати причиною порушення внутрішніх систем безпеки держави являють собою загрозу для суверенітету незалежної держави, що є прямим порушенням загальновизнаних принципів міжнародного права і являє собою особливу форму агресії [11, с.63].

Як наголошує професор Д. Вентре, кібер-атака є сучасною формою агресії, що чиниться окремими особами або групою осіб, метою яких є підрив комп'ютерної інформаційної системи безпеки, підрив роботи будь-якої інфраструктури, комп'ютерної мережі та/або підрив роботи персональних комп'ютерів та інших пристроїв, здійснений у будь-який спосіб. Кібер-атаки здійснюються зловмисниками, анонімно, що не звільняє осіб, їх учинивших від відповідальності; кібер-атаки є нелегальним проникненням до чужої комп'ютерної системи, що може бути підривом національної системи безпеки. У хакерській (кібер-атаці) атаці можуть брати участь один або декілька висококласних фахівців (хакерів) [10, с.165].

Як різновид або вияв ІКТ кібер-атаки бувають різних видів. Одним з найпоширеніших видів є кібер-шпигунство – діяльність, спрямована на отримання таємної службової інформації з особистих даних, від груп осіб, через злам систем ворожої урядової служби у воєнних, політичних або економічних цілях, використовуючи незаконні методи експлуатації Інтернету, комп'ютерних мереж програмного забезпечення. Дана інформація, потрапивши до рук потенційного агресора , може бути використана у протиправній діяльності проти інших держав, підриваючи їхній державний і суспільний устрій, що є безпосереднім виявом агресії та порушенням міжнародних принципів права [3, с.167].

Наступною загрозою, яку утворює кібер-атака − це саботаж, підрив роботи комп'ютерної мережі або системи супутників, що виконують завдання з підтримання національної безпеки держав [3, с.170]. Загрозі піддаються супутникові, комп'ютерні системи безпеки та життєзабезпечення цілої держави: електростанції, системи водопостачання, топливна система, транспортна інфраструктура. Окрім цивільної сфери, може бути здійснено підрив роботи системи забезпечення діяльності збройних сил, аби утворити «обеззброєння» цілої держави [10, с.152].

Гостроти проблемі додає складність пізнання злочинного механізму кіберзлочинності, кримінально-правових за міжнародним правом актів кібер-атак, а також їх розслідування. Як наголошує Т. Рід , «різнобічний характер кібер-атак означає, що важко визначити мотивацію сторони що нападає, а це означає, що неясно, коли конкретний акт слід розглядати як акт агресії» [9, с.10].

Російський дослідник І.М. Рассолов доходить висновку, що «серед великої кількості проблем судової практики по цих справах, можна виділити дві ключові: 1) складність визначення кола осіб, що мусять притягатися до кримінальної відповідальності; 2) фіксація (збирання, надання) доказів, їхня припустимість та достовірність» [8, с.21].

Не заперечуючи небезпечності кібер-атак, у тому числі й для міжнародних відносин, слід все ж взяти до уваги, що агресія – це тривалий злочин, що ґрунтується на системній організаційній основі і геостратегічній мотивації на економічну зверхність і світове домінування. Тому кібер-атаки складають скоріше елементи інформаційної агресії, розглядаються як акти такої агресії за умовою їх державницького походження або ж вияву системної боротьбі радикальних (терористичних) збройних формувань. Кіберзлочинність корисливої природи, що йде від фізичних осіб або груп осіб, звісно не може кваліфікуватися як акти агресії, хоча вони побічно насичують інформаційну агресію додатковою кримінальністю.

Шкідливість даного підходу для організації цілеспрямованої міжнародно-правової протидії інформаційній а, отже, всеохоплюючій «універсальній» агресії полягає у тому, що він відволікає увагу міжнародного співтовариства від глобальної небезпеки дійсної тотальної агресії, в основі якої лежать амбіції світового володарювання світової фінансово-промисловою олігархією. Остання інструментом і прикриттям своєї агресивної геостратегії обрали невелику групу найроз-

винутіших держав, через які у межах контролю над світовими процесами реалізуються спеціальні ІКТ, що складають сутність інформаційної агресії.

У цілому ж здійснений аналіз зі всією очевидністю свідчить про наявність у міжнародних взаємодіях інформаційної агресії, сутність якої в умовах нееквівалентного глобального інформаційного обміну складає використання спеціальних інформаційно-комунікаційних технологій на основі монополізації володіння ними розвинутою меншістю міжнародного співтовариства. Кваліфікованих ознак агресії така інформаційно-комунікаційна перевага набуває внаслідок своєї спрямованості на порушення суверенітету, територіальної недоторканості та політичної незалежності країн. Зростаюча інтенсивність інформаційної агресії зумовлена цілями світової фінансово-промислової олігархії на світове управління через геоекономічне домінування.

Список використаних джерел:

1. Антипенко В.Ф. Криминогенность государственной власти/Теория уголовной ответственности государства. – Одесса: Феникс, . – С. 53 – 68.

2. Brown A. The Poker Face of Wall Street/A.Brown. – Wiley, 2007. – 368 p.

3. Brenner S. Cyber Threats: The Emerging Fault Lines of the Nation State. Oxford University Press, 2009. – 320 p.

4. Валлерстайн И. После либерализма: Пер.с анг./Под ред. БКО Кагарлицкого М.: Едиториал УРСС, 2003. – 256 с.

5. For the People: Can We Fix Public Service? John D.Donabwe//Governance: democracy in the formation age. Edited by Elina Ciulla Kamarck, Joseph S. Nye Tr. Bision of gobernance in the 21th century. – Cambridge Massachussets: Brooking institution press Washington.2002. − 282 p.

6. Крутских А. О чем эта книга. Предисловие/Андрей Крутских//Роговский Е.А. Кибер – Вашингтон: глобальные амбиции. – М.: Международные отношения, 2014. – 848 с.

7. Панарин А.С. Россия в циклах мировой истории. – М.: Изд-во МГУ, 1999. – 288 с.

8. Рассолов И.М. Правовые проблемы обеспечения кибербезопасности в России и зарубежных странах //М: журнал «Содружество», 2008. – С. 21-35.

9. Rid Thomas «Cyber War will not take place», Journal of Strategic Studies, 2011. – P. 5-32.

10. Ventre D. Cyberspace et acteurs du ciberconflict. Hermes-Lavoisier. 2011. − 288 p.

11. Тимошков С.Г. Агрессия как международное преступление//диссертация на соискание степени к.ю.н. – М. – 2016. – 195 с.

12. Ясперс К. Смысл и назначение истории: Пер.с нем. 2-е изд – М.: Республика, 1994. – 527 с.