ЛЕКЦІЯ 4. Загрози інформаційній безпеці та інформаційне протиборство

Теоретичні та прикладні аспекти інформаційного протиборства знаходять якісне вираження у класифікації інформаційних конфліктів, яка включає власне інформаційні конфлікти (інформаційно-пропагандистські, інформаційно-психологічні), мережеві конфлікти (кіберконфлікти і конфлікти з використанням соціальних мереж), інтегровані (гібридні) конфлікти та організаційні (конструктивно-впливові) конфлікти. Власне інформаційні конфлікти передбачають як створення системи захисту проти будь-яких видів інформаційної озброєнь, що обумовлює об'єктивні переваги в потенційній інформаційній війні, так і використання системи жорсткого контролю над інформаційними озброєннями супротивника на підставі міжнародно-правових документів з інформаційної безпеки. Теоретичне обґрунтування появи інформаційних конфліктів було представлено у дослідженні Дж.Ная та У.Оуенса «America's Information edge strategy and force planning» (1996р.), в якому підкреслювалася провідна роль США в інформаційній революції, тобто у використанні надважливих засобів комунікації та інформаційних технологій - супутникового спостереження, прямої комунікації, швидкісних комп'ютерів, унікальних можливостей в інтегруванні складних інформаційних систем, - у політиці стримування і нейтралізації традиційних військових загроз та нових видів озброєнь. Саме на основі запропонованої стратегії у військовій доктрині збройних сил США наприкінці XX і на перспективу XXI століття були визначені дві складові театру воєнних дій - традиційний простір і кіберпростір, основними об'єктами якого стали інформаційна інфраструктура і психологічна сфера потенційного супротивника, адже інформаційна війна спрямована на всі можливості і чинники вразливості, що виникають за умови зростаючої залежності від інформаційних ресурсів, а також використання інформації у різноманітних конфліктах[15]. В умовах збільшення масштабів інформаційного протиборства вирізняються такі його форми, як інформаційні

війни та спеціальні інформаційно-психологічні операції. На думку українського дослідника і експерта О.Литвиненка, спеціальні інформаційні операції диференціюються за такими критеріями: операції, що спрямовані проти акторів, які ухвалюють рішення; операції, що спрямовані на компрометацію, заподіяння шкоди для репутації опонентів; операції, що спрямовані на політичну або економічну дестабілізацію, що у сучасній практиці інформаційного протиборства залишається надзвичайно важливим, а іноді й вирішальним засобом досягнення переваги. Проблема інформаційних війн наразі актуалізується, оскільки життєдіяльність сучасного суспільства визначається рівнем технологічного розвитку, якістю функціонування і безпекою його інформаційного середовища. Виробництво і менеджмент, оборона і зв'язок, транспорт й енергетика, економіка і фінанси, наука й освіта, засоби масової інформації тощо у розвинених країнах істотно залежать від інтенсивності інформаційного обігу, повноти, своєчасності і вірогідності інформації[13]. Сучасними прикладами подібних операцій є хакерські дії в мережі Інтернет, коли невідомі зловмисники знищують або спотворюють вебсторінки політичних опонентів, наприклад, замінюють достовірні посилання на вигадані, що виводять, наприклад, на порнографічні сайти. Операції, спрямовані на дестабілізацію політичної чи економічної ситуації, є класичним видом спеціальних інформаційних операцій, які мають на меті дестабілізацію політичної чи економічної ситуації в регіоні, країні, створення умов для приведення до влади дружньо налаштованих урядів або зміни політичного курсу. Як вважають експерти, нинішній конфлікт Росії проти України здійснюється з метою «спрямувати політику України в стратегічно глухий кут, зруйнувати економіку, загальмувати діяльність оборонної промисловості, дискредитувати зростання суспільної самосвідомості, спотворити основи національної культури, створити серед частини населення мотивацію нестабільності та протидії європейському виборові політикуму та громадянського суспільства країни» [16;17]. Метою мережних конфліктів і мережних війн вважають зруйнування фундаментальних уявлень спільноти

про сутність культури, суспільства і держави для того, щоб дезорієнтувати і внести хаос у масову свідомість, призвести до підриву довіри або розколу у суспільстві. Практичне втілення мережевих конфліктів реалізується через інформаційні операції проти інфраструктури, електронних мас-медіа, систем формування громадської думки, жорсткий контроль національного інформаційного поля, заміну або винесення інформаційного простору за допомогою інтернету за межі національної території і створення нової інформаційної реальності для національної спільноти. Зокрема, під час операції «Союзницька сила» у відповідь на бомбардування інфраструктури сербські хакери заблокували за допомогою атаки «ping of death» офіційний сервер НАТО, а також військові і урядові сайти країн-членів альянсу повідомленнями з макровірусами, що підтвердило прогнози про перенесення військових операцій в кіберпростір на рівень інформаційного протиборства. До мережевих конфліктів відносять і протиборство світової спільноти с міжнародною організованою злочинністю та терористичними угрупованнями, здатними контролювати перебіг політичних, економічних, суспільних і навіть цивілізаційних процесів. Можливість такого конфлікту передбачена в аналітичному дослідженні Національної розвідувальної ради США «Mapping the global future» – 2020 в рамках сценарію «Цикл страху», який є найбільш песимістичними сценарієм майбутнього для світової спільноти. До такого типу конфлікту можна віднести акції секти «Аум Сінрікьо», яка працювала над створенням електромагнітних імпульсних «гармат», здатних вивести з ладу комп'ютерні системи, проводила експерименти зі створення нових небезпечних мережевих вірусів, а також залучала нових прихильників своєї секти з використанням інтернету. Наразі активісти організації «Хамас» координують діяльність бойових угруповань в секторі Газа і на західному березі річки Йордан, підтримуючи з ними зв'язок електронною поштою або в інтернет-чатах, що суттєво ускладнює боротьбу з кібертероризмом. Для мережевих конфліктів XXI століття «Арабська весна» (2011 р.), «WikiLeaks» (2011- 2012 рр.), «Едвард Сноуден» (2013-2014 рр.), «Фейки» (2014-2017 рр.)

характерне використання соціальних медіаплатформ для формування мотивації поведінки і спонукання до деструктивних дій, спрямованих на виправдання протиправних збройних конфліктів. Сучасні конфлікти і злочинна діяльність, що ґрунтуються на мережному принципі, у видимій перспективі можуть стати, як зазначають фахівці, поширеним явищем. Усвідомлюючи перспективи мережних війн, міжнародні терористичні групи, злочинні угруповання та синдикати, фундаменталістські та етнонаціональні рухи наразі модифікують свої структури і стратегії, щоб скористатися перевагами мережного принципу [18-20]. Мережево-центровані війни слугують для перетворення військової структури в таку конфігурацію, яка зробить війська найбільш ефективними: вони будуть діяти швидше; складатися з більш розосереджених сил; знизять коефіцієнт смертності, водночас зменшуючи залежність від застосування зброї; матимуть можливість передбачити (в порівнянні з реактивними діями), а також інтегрувати нові технології в мережу для вироблення інформації і отримання переваги в швидкості у порівнянні з майбутніми опонентами. Так, у дослідженні «Мережевоцентровані війни: витоки та майбутнє» наголошується, що в умовах бурхливих технологічних зрушень, які призводять до трансформації суспільства, важливим є усвідомлення можливостей інформаційної переваги, а саме: у глобальному протиборстві виграють ті актори, які першими почнуть активно використовувати можливості інформаційних технологій та мережево-центровані операційні архітектури. Відповідно впровадження концепції мережево-центрованих війн дозволяє перейти до більш швидкого й ефективного способу ведення бойових дій, що характеризується новими поняттями швидкості командування і самосинхронізації. Тобто, мережево-центричні війни розуміються як військово-технічна революція зверху, тоді як мережна війна вважається соціально-політичними інноваціями знизу, що застосовуються для досягнення цілей певними групами, спрямованими на широку демократизацію суспільства, і разом з політичною боротьбою передбачають контроль за діяльністю владних структур з боку суспільства, а

також залучення громадян до процесу прийняття рішень через проекти «електронної демократії» [18]. Інтегровані (гібридні) конфлікти/війни передбачають створення значної переваги в наступальних видах озброєнь, в знешкодженні систем захисту держави-супротивника засобами інформаційного впливу. Разом з гібридизацією засобів і шляхів ведення війн спостерігається зміна ключових політичних цілей, оскільки воєнні дії спрямовуються насамперед на дестабілізацію альянсів та окремих держав, для чого використовуються пропаганда, розбалансування, повстання, заморожені конфлікти «зі швидким розігрівом», тероризм, громадянські війни та інші внутрішні загрози, загострення політичних конфліктів і розширення внутрішніх ліній фронту для перевантаження організаційних потужностей держави і суспільства та зменшення можливостей застосування військових потуг. Тобто, йдеться про те, щоб обмежити дієздатність урядів і парламентів як слабких країн у кризових регіонах, так і стійких демократичних держав, унеможливити гуманітарну інтервенцію або введення санкцій з боку західних держав. Тому спільним завданням альянсів, урядів, громадянського суспільства і військового сектору стає посилення власної стійкості до гібридних методів війни як передумови внутрішньо - і зовнішньополітичної дієздатності [21-28]. Більшість експертів вважають, що інтегровані (гібридні) конфлікти характеризуються наявністю безпрецедентної за масштабами системи управління інформаційними потоками для проведення військових операцій, здійсненням масованих пропагандистських кампаній з широким спектром інформаційних методик - від технологій PR для формування сприятливої світової громадської думки, вибіркового інформування з заданим ефектом сприйняття медіа та інтернет-контенту до всебічної дискредитації політики противника, а також відвертої дезінформації світової громадськості; спрямованого інформаційно-психологічного впливу, потужного використання мережі Інтернет для модифікації національного інформаційного простору і контролю за інформаційною інфраструктурою. Нові стратегії і тактика проведення інформаційних операцій, продемонстровані на під час

Балканського конфлікту, були застосовані різними міжнародними акторами на Близькому Сході, в Афганістані, на пострадянському просторі, зокрема у Молдові, Грузії, в Україні [23;26;27]. Українські дослідники розглядають гібридні війни у контексті системної кризи світової безпеки як новітній вид глобального протистояння, що потребує реформування міжнародних безпекових інститутів та пошуку балансу сил у новій гібридній реальності. При цьому зазначається, що «західні медіа у «гібридному» світі стають заручниками нової реальності, яка не відповідає їх ліберально-демократичним світоглядним переконанням, оскільки мас-медіа намагаються підходити до інформаційно-політичного простору з «демократичними стандартами» мирного і раціонального існування, стандартами «виваженості, об'єктивності та плюралізму думок» [29]. Основними ознаками гібридної війни вважаються: інноваційна агресія (кібервійна, економічний тиск, інформаційно-психологічні атаки тощо); застосування нерегулярних збройних формувань або приватних армій (повстанський, партизанський рух, ПВК, тероризм); офіційні військові дії або демонстрація сили (ідентифікована уніформа, зброя, офіційне визнання участі у конфлікті). Крім того, гібридні війни, можна відзначаються такими особливостями, як нестандартне, складне та багаторівневе протистояння, оскільки гібридна війна може здійснюватися як державними, так і недержавними акторами. Так, у війні в Нікарагуа 1962-1990 рр. альянс антиурядових угруповань у формі «Сандиністського фронту національного визволення» воював проти сил уряду А.С.Гарсії, при цьому отримуючи підтримку з боку США та американських військових, які перевдягалися у форму «сандиністів»; під час війни в Лівані 2006 р. між Ізраїлем та загонами радикального шиїтського руху «Хезболла» Іран через недержавне утворення фактично здійснював війну проти Ізраїлю; агресія РФ проти України на Донбасі стала прикладом того, як традиційний державний актор здійснює «гібридну війну» проти іншої держав[22;24;25]. До особливостей гібридної війни відносять також поєднання звичайних та нетрадиційних засобів ведення війни, оскільки сторона конфлікту може

використовувати інструментарій, який не застосовується в умовах традиційної війни, зокрема іррегулярні військові тактики, партизанські способи ведення бойових дій, терористичні акти, використання насилля, інформаційно-психологічні операції тощо. Такі тактики гібридної війни - насилля як засіб деморалізації суспільства, скоєння терактів закордоном та змішані партизанські тактичні маневри - використовуються міжнародною терористичною мережею «Ісламська держава». Відзначають також мобільність та високий рівень гнучкості інструментарію гібридної війни, що завжди пристосовується до нових умов та обставин. Так, терористи «Ісламської держави» врахували дії військово-повітряної кампанії сил Міжнародної коаліції, забрали великі блокпости з доріг, припинили користуватися мобільними телефонами та пересуватися великим автоколонами. І водночас учасники терористичного угруповання завжди перебувають поряд із цивільними об'єктами, ховаються в будівлях та використовують авіаудари проти цивільного населення як засіб вербування нових членів та мобілізації прихильників. Використання новітніх нетрадиційних озброєнь, до яких відносять широко доступні технології такі, як смартфони для комунікації, Інтернет для здійснення кібератак, звичайні автомобілі, посилені броньованим покриттям для здійснення терактів, підземні тунелі для швидкого пересування спостерігалися під час війни в Лівані 2006 р., коли радикальний рух «Хезболла» мав на озброєнні протиповітряні комплекси, протитанкові ракети та гранатомети, безпілотні літальні апарати, тепловізори та користувався зашифрованими повідомленнями [21;25;27;28]. Під час гібридної війни також активно використовуються інформаційні технології, маніпуляції масовою свідомістю та медіапропаганда, значимість якої вважається значною, оскільки йдеться про гібридно-інформаційну війну з огляду на те, що військові дії в ній приглушені, а інформаційні - суттєво посилені. Експансія в інформаційному просторі, на погляд фахівців, стала «ключовою і найнебезпечнішою складовою гібридної війни Росії проти України», враховуючи, що такий медіа-вплив здійснюється

упродовж усієї новітньої історії українсько-російських відносин [30-34]. Важливою ознакою сучасних гібридних війн є використання приватних армій або приватних воєнних корпорацій, які беруть участь у військових конфліктах, а також здійснюють збирання розвідувальних даних, надають послуги зі стратегічного планування, логістики та консалтингу. Приватні воєнні корпорації також надають послуги щодо набору особового складу для контингенту міжнародних поліцейських місій та управління ними; охорони об'єктів, у тому числі таких, що мають важливе і стратегічне значення; охорони нафтових родовищ і трубопроводів, енергетичної системи; посольств та керівників держави; супроводження конвоїв ООН; навчання особового складу урядових збройних сил, поліції та інших сил безпеки; надання послуг військових перекладачів; охорони в'язниць; розмінування мінних полів і знищення боєприпасів; послуг протипожежного захисту; тилового постачання військ; авіарозвідки; збройного супроводу і захисту морських суден від піратів[35- 36]. Залежно від типу послуг приватні воєнні корпорації поділяються на компанії бойового забезпечення, які надають послуги з підтримання бойових дій їхніх сил безпеки та оборони, включно з безпосередньою участю в бойових операціях (остання послуга сучасними приватними воєнними компаніями офіційно не надається); воєнні консалтингові компанії, що спеціалізуються на наданні послуг з планування, створення, реформування й розвитку сил безпеки та оборони, зокрема органів розвідки і контррозвідки, бойової та спеціальної підготовки тощо; воєнні логістичні компанії, сфера діяльності яких охоплює обслуговування й експлуатацію складних систем озброєння, військової техніки та комп'ютерних систем, матеріально-технічне забезпечення військ; будівництво військових об'єктів; приватні охоронні компанії, які працюють в умовах воєнного конфлікту або в зоні підвищеного ризику, зокрема на території країн з нестабільною обстановкою і здійснюють захист об'єктів та фізичних осіб, а не бойові дії, однак у зоні воєнного конфлікту чітке розмежування між цими видами діяльності відсутнє, зокрема під час захисту аеродромів,

нафтопроводів та інших об’єктів інфраструктури охоронні компанії можуть проводити бойові операції проти незаконних військових формувань, терористів тощо; приватні воєнні компанії, які спеціалізуються на розвідувальній та контррозвідувальній діяльності, мережа яких є практично закритою. В армії США ставлення до використання приватних воєнних компаній неоднозначне: в Операційній концепції армії США на 2016-2028 рр. (Operational Adaptability) використання приватних військових компаній представляється проблематичним через потенційно більш високу ціну, меншу стійкість до ризику і питань, пов’язаних з ефективним інтегруванням військових і урядових операцій з діяльністю компанії. Проблеми з підтримкою військових операцій приватними учасниками часто включають непрозорі відносини командування-підпорядкування, залежність від можливостей, які несподівано можуть опинитися недоступними, зменшений контроль за ключовими функціями, етичні міркування і юридичні питання [37]. Організаційні конфлікти передбачають використання можливостей інформаційних озброєнь на окремих територіях з метою провокування внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) і зміни системи національного управління. Найбільш вірогідними національними об’єктами для організаційної агресії вважаються системи управління і прийняття рішень; цивільна інформаційна інфраструктура, у тому числі критично важлива (підприємства безперервного циклу, провідні економічні та фінансові організації, енергетичні об’єкти, ключові виробничі об’єкти); військова інформаційна інфраструктура, яка забезпечує оборону і безпеку країни; засоби масової інформації; масова свідомість населення країни. Вплив на ці системи може мати за мету руйнування або модифікацію інформації, знищення національних інформаційних ресурсів, порушення роботи систем моніторингу комунікації, дезінформацію суспільства. Практичне втілення організаційного конфлікту, підкреслюється у дослідженнях, простежується в операції «Perestroika» (1980-1990 рр.), яка вплинула на ідеологічні та управлінські основи колишнього

СРСР, сприяла утвердженню незалежності пострадянських держав і встановленню західної моделі демократії в нових суверенних державах Центральної та Східної Європи. Відомі також інформаційні впливи в організаційних конфліктах на Гаїті, в Афганістані, Індії, Індонезії, Африці, на Близькому Сході, в Грузії, Молдові, наразі - в Україні. У рамках міжнародної антитерористичної операції «Відплата» (Афганістан, 2001 р.) США мали намір нейтралізувати і знищити всю терористичну мережу, яка загрожувала Америці й іншим країнам цивілізованого світу, та переконати певні режими, які підтримують політику тероризму, в тому, що така стратегія не відповідає їх власним національним інтересам. Інформаційна війна проти режиму Талібан включала проведення психологічної операції в інформаційному просторі Афганістану з одночасним блокуванням національних радіостанцій, поширенням пропагандистських матеріалів з уривками з Корану, розрахованих на протидію закликам до джихаду, формування в суспільній свідомості відчуття невідворотної перемоги антитерористичного альянсу і необхідності зміни системи управління в країні [16-17]. Розповсюдженим способом організаційної боротьби є створення «п’ятої колони» у владних інституціях зарубіжних держав, оскільки використання такого прихованого гібридного засобу впливу має потужну деструктивну дію, що складно піддається доведенню. На сьогодні у західних країнах висуваються аргументи, що Росія фінансує велику кількість євроскептичних і екстремістських партій та європейських політиків-популістів, щоб забезпечити підтримку власних агресивних дій і отримати нові ресурси для реалізації російських інтересів в Європі, втручається у виборчі системи для зміни результатів волевиявлення за допомогою хакерських атак тощо. Проте прямих доказів такого втручання у внутрішню політику зарубіжних держав недостатньо, тому поле для подальших маніпуляцій щодо здійснення організаційного впливу є практично необмеженим. Фахівці стверджують, що для убезпечення інституційних структур від подібних загроз необхідно збільшувати їх вагу і репутацію у суспільстві, формувати у суспільстві довіру до кожного з органів влади як

відповідними рішеннями, так і діями. Водночас, як йдеться в експертних дослідженнях, застосування організаційної зброї не завжди призводить до деструкції держави і соціуму, що свідчить про адаптаційні властивості конкретного соціуму та можливості нейтралізації негативних впливів. Фахівці підкреслюють, що виражена стійкість до негативних інформаційних впливів спостерігається у всіх державах, які втілювали в своєму управлінні реальні принципи соціальної справедливості і які мають колективний досвід протистояння зовнішнім і внутрішнім деструктивним силам[17;34]. Що стосується України, то держава стала суб'єктом комплексних атак з боку РФ, оскільки інструментарій впливу охоплює всі елементи видів воєнних дій - гібридні, мережеві та організаційні, що здійснюються з різних фронтів, а саме: незаконні збройні формування та підтримка сепаратистів; маніпуляція інформаційним простором; економічний тиск; застосування соціальних мереж для дезінформації не лише громадян України, але й інших країн світу; численні кібератаки з метою оприлюднення деструктивної інформації; пропаганда, психологічний та інформаційний тиск та насадження власних поглядів та переконань. Такий інструментарій становить загрозу для безпеки, територіальної цілісності України, а також для її репутації всередині країни та за її межами [39-41]. Висновки. Інформаційний вимір конфліктів XXI століття обумовлюється стратегічною спрямованістю інформаційних озброєнь проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства, визнанням інформаційних озброєнь як нового глобального виду зброї масового ураження, катастрофічного за результатами свого застосування, необхідністю створення міжнародного механізму протидії та попередження глобальних інформаційних воєн в рамках політичної компетенції міжнародних інституцій з проблем безпеки і оборони, політичних рішень на національному рівні.