

МЕХАНІЗМИ РЕАЛІЗАЦІЇ СУЧАСНИХ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ ІНФОРМАЦІЙНО-ГІБРИДНИХ КОНФЛІКТІВ

Світлана ДОМБРОВСЬКА

*доктор наук державного управління, професор,
Заслужений працівник освіти України,
проректор з наукової роботи НАУ «ХАІ»
м. Харків, Україна*

Розширення інформаційного простору та прискорення обігу інформації на основі нових технологій сприяє накопиченню реальних та штучно створюваних суперечностей у сфері інформаційної політики.

У зв'язку з цим в сучасних умовах все більше поширення отримує таке явище, як інформаційні та гібридні війни, які, у свою чергу, ведуть до загострення суперечностей інформаційного характеру.

Українська держава в останнє десятиліття ХХІ століття зіткнулася з серйозними викликами в сфері національної безпеки (конфлікт на Донбасі, пандемія Covid-19, збройна агресія росії проти України, конфлікт, що розпочався на Близькому Сході) тощо. У зв'язку з цим особливої уваги та докладного вивчення вимагає така форма конфлікту, як інформаційно-гібридні війни.

На наш погляд, ці явища – не однакові за змістом, але досить часто війни, що відбуваються у світі в останнє десятиліття, використовують механізми як з інформаційною складовою, так і є гібридними за формою реалізації. У зв'язку з цим логічним, на наш погляд, було б розглядати механізми реалізації сучасних загроз в інформаційній сфері як інформаційно-гібридні конфлікти (війни), оскільки ці явища перешкоджають не тільки розвитку інформаційного суспільства, але й зачіпають буквально всі сторони соціального життя в масштабі всієї планети.

Зазначаючи в цілому позитивну роль переходу до інформаційного суспільства, що виражається у використанні нових сучасних методів і засобів обробки та передачі інформації з метою підвищення ефективності функціонування багатьох сфер діяльності, необхідно вказати й на важливу обставину в цьому зв'язку.

Насамперед слід мати на увазі, що позитивні властивості інформації та інформаційних технологій, які створюються на благо цивілізації, однаково доступні й часто використовуються в міжнародній політиці як механізми інформаційно-гібридних війн.

Хвиля технічного прогресу внесла суттєві зміни в методи вирішення військових, економічних, торгових та інших конфліктів. Прямі силові методи уступають (або використовуються поряд з інформаційними механізмами) місце інформаційним¹. У сучасних умовах усе частіше ці методи використовуються комплексно. Цифрові технології в сучасних умовах активно проникають в усі сфери соціально-економічної системи. Не є виключенням і публічне управління. Синергетичний потенціал соціальних, мобільних, «хмарних» технологій, а також технологій аналізу даних і «Інтернет речей» сукупно здатні привести до кардинальних трансформаційних змін в публічному управлінні, спрямованих на підвищення його ефективності. Саме тому в умовах становлення «цифрових» ринків і економік, розвитку «електронної держави» потрібні інвестиції в інфокомунікаційні технології. Їх активне впровадження в практику дозволить використати нові моделі взаємодії і обслуговування, підвищити дієвість систем менеджменту і публічного управління².

Перспективи стійкого розвитку України безпосередньо пов'язані із забезпеченням збалансованого і ефективного функціонування механізмів публічного управління на усіх рівнях в умовах цифровізації усіх соціально-економічних процесів, що динамічно змінюються.

У сучасному глобалізованому і одночасно диференційованому суспільстві використання сучасних і адаптивних моделей публічного управління стає найважливішим завданням і способом рішення проблем. Формування публічного управління відповідно до вимог часу є одним з головних інструментів затвердження сучасних моделей управління, тому розуміння сутності трансформаційних процесів сучасних воєн уможливить створення та застосування адекватних важелів впливу на ці процеси, що неминуче позначиться на питаннях національної безпеки. Водночас розуміння руйнівної сили інформаційної війни (війн) потребує глибокого дослідження цього феномена. Інформаційні взаємодії, контакти, конфлікти та різні форми їх вирішення є основою розвитку суспільства.

Основним суб'єктом інформаційних операцій спочатку являлася держава в цілому і її окремі інститути, що розглядають ці інструменти як засіб реалізації зовнішньої політики. З часом сталося розширення числа акторів і можливостей з проведення інформаційних операцій, якими володіють міжнародні організації і недержавні актори, причому

¹ Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // *Державне управління: удосконалення та розвиток*: елек. журнал. 2023. № 9. URL: <https://www.nayka.com.ua/index.php/dy/article/view/2133>

² Олещук П. М. Новітні політичні технології інформаційного впливу : монографія. Київ: Видавець Вадим Карпенко, 2018. 288 с.

частенько їх можливості перевершують здатність окремих країн в проведенні інформаційних і кібератак.

Методи і технології сучасних інформаційних операцій можна розділити на дві основні групи: підготовки інформаційного вкидання; створення і підтримка каналів комунікації технологічної і непрямой дії.

До першої групи відносяться: методи вкидання офіційної інформації (озвученою першими особами, відомствами або розміщеною від імені анонімного спікера), технології, методи підготовки «журналістських» розслідувань, технології хакерських «зливів», організація «інформаційної лавини».

До другої групи входять технології і методи створення власної мережі ЗМІ, способи і методи створення і просування каналів комунікації в інтернеті, технології організації лояльного бізнесу, а також способи використання нейтральних ЗМІ і прямої комунікації³.

На сьогодні використання інструментарію інформаційних операцій створює цілий ряд викликів і загроз, до числа яких можна віднести загрози системі стратегічної стабільності. Наприклад, проведення кібератак здатне ускладнювати роботу системи військового і публічного управління, створити загострене відчуття поспіху у тих, хто відповідальний за вироблення рішень на удар або удар у відповідь; масштабний напад в кіберпросторі при неясності задумки того, хто атакує і складнощах в атрибуції кібератак здатних спровокувати масштабну воєнно-політичну кризу.

Сучасні держави багато в чому успішно інтегрували інформаційно-комунікаційні технології в інструментарій зовнішньої політики. Прикладами цього можна вважати щонайширше використання можливостей соціальних мереж в офіційній комунікації (навіть Китай, незважаючи на заборону на роботу ряду майданчиків в країні, використовує їх для комунікації із зарубіжною аудиторією), використання можливостей інформаційно-психологічної дії в силових методах зовнішньої політики. Усіма провідними державами світу усвідомлюються небезпеки, витікаючі від іноземної інформаційної дії, підтвердженням чому являються як законодавчі зусилля із регулювання і захисту власного інформпростору, так і створення нових органів влади або військових підрозділів для дій в інформаційному і кіберпросторі.

Наведені та інші небезпеки, виклики інформаційного розвитку сучасного світу спричинили постановку на порядок денний, як уже наголошувалось, проблеми так званої інформаційно-гібридної війни, яка визначається сьогодні як прихована діяльність з метою забезпечення інформаційного домінування, що набуває значення не менше

³ Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві. ЮСТІНІАН. 2009. URL: <http://www.justinian.com.ua/article.php?id=3233>

важливіше, ніж традиційне військове домінування. Воно спрямоване на формування інформаційно-залежних відносин від суб'єкта впливу як на технологічному, так і на соціально-психологічному та державно-управлінському рівнях.

Одним із головних досягнень сучасної цивілізації в умовах глобалізації, яка на даний момент вважається основною тенденцією історичного розвитку, є Інтернет-революція⁴.

Процес поширення інформаційних технологій пов'язаний як з новими досягненнями, так і з появою цілої низки нових проблем. Користь від цієї Інтернет-революції може позначитись у політичній, економічній та соціальній сферах

Таким чином, підбиваючи підсумки можливості використання мережевих технологій в інформаційному протиборстві, слід зазначити наступне.

Інформаційна війна – вища форма міждержавного інформаційного протистояння, конфлікт інтересів суб'єктів геополітичної конкуренції (протиборства) в інформаційному просторі з метою вирішення протиріч щодо влади та здійснення політичного керівництва, а також щодо перерозподілу їх ролі, місця та функцій у політико-управлінській системі сучасного суспільства, в якому зіткнення конфліктуючих сторін відбувається у формі інформаційних та інформаційно-психологічних операцій із застосуванням інформаційної зброї.

Сутність такої інформаційної війни полягає у завданні військової поразки противнику шляхом досягнення та використання інформаційної переваги над ним.

Інформаційно-гібридна війна може здійснюватися і в умовах відсутності силового конфлікту, що виводить цей різновид до числа найбільш застосовних та універсальних засобів забезпечення реалізації зовнішніх інтересів. У відносно мирних умовах інформаційні війни цього типу можуть застосовуватися як спеціальні механізми управління кризами та провокування варварства на території противника.

Ця обставина визначає асиметричний характер інформаційних воєн і наявність потенційних можливостей у свідомо слабшої сторони щодо завдання цілеспрямованими точковими ударами серйозної шкоди технологічно розвиненому противнику.

У постіндустріальному і очевидно інформаційному світі, що формується, найважливішим ресурсом виявляється не традиційний географічний простір із закріпленими в ньому фізичними людьми та виробничими потужностями, а інтелект, інформація та фінанси.

⁴ Почепцов Г. Смыслові та інформаційні війни: пошук відмінностей. Media Sapiens. URL: http://osvita.mediasapiens.ua/ethics/manipulation/smislovi_ta_informatsiyni_viyini_poshuk_vidminnostey/.

При цьому за допомогою високих технологій інформація, що містить дані про результати інтелектуальної діяльності, легше переміщується у просторі. Відсутність територіальної «прив'язки» ключових ресурсів дозволяє інформаційно-комунікаційним лідерам опановувати їх і використовувати у своїх цілях без будь-якого фізичного втручання.

Ефективне освоєння чужих територій стає можливим без урахування стану кадрового потенціалу та добробуту основної частини населення країни, що освоюється шляхом використання для досягнення поставлених цілей інформаційно-технологічної локалізації та фактичного вилучення із соціально-економічного простору носіїв інтелекту та розпорядників фінансових ресурсів.