Вєдєнєєв Д. В.,
доктор історичних наук, професор,
провідний науковий співробітник навчально-наукового інституту військової історії, права та соціальних наук,
Національний університет оборони України
(м.Київ, Україна)

Левченко С. М.,
кандидат військових наук, провідний науковий співробітник, навчально-науковий інституту військової історії, права та соціальних наук,
Національний університет оборони України
(м.Київ, Україна)

СУТНІСНІ ВЛАСТИВОСТІ СУЧАСНОГО КІБЕПРОТИБОРСТВА ЯК ДЖЕРЕЛО ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Одним із наслідків всеохоплюючої інформатизації буття сучасного суспільства стала прискорена розробка й запровадження в збройні сили та спеціальні служби особливих засобів інформаційного протиборства. На думку спеціалістів, під ними у першу чергу розуміються засоби інформаційного протиборства, зокрема – із несанкціонованого збору даних й порушення функціонування інформаційно-управлінських систем та комп'ютерних мереж різного призначення, з психологічного впливу на збройні сили та населення країн-противників і власної країни.

У збройних конфліктах останніх десятеліть («війнах шостого покоління», «дистанційних війнах»), в яких брали участь армії високотехнологічних держав, бойові (силові) дії починалися із потужного інформаційного впливу та свідомість воєнно-політичного проводу, армій й населення противника, технічних ударів по системах військового й державного управління тощо.

З погляду впливу на людську свідомість, найбільш типовою метою інформаційного протиборства в умовах техногенної цивілізації є модифікація, ушкодження, зміна конфігурації свідомості, що дозволяє противнику у подальшому використовувати на свою користь отриману інформацію, контрольовану громадську думку, уражену інформаційну систему. Нині не треба повністю зомбувати людей та знищувати ворожі інформаційні системи, оскільки їх можна поставити на службу собі. Крім того, поширення соціальних мереж та месенджерів спричинило виникнення атомізованих віртуальних спільнот, існування яких може обраховуватися днями, оскільки стрижнем їхньої єдності є

той чи інший інформаційний привід. Це веде до руйнування фрагментування громадянсько-політичних спільнот (народів, політичних націй тощо) [1, с.296-301].

Назагал, *сучасний етап інформаційної боротьби характеризується застосуванням інформаційних війн другого покоління.* Властиві йому операції спрямовані на досягнення стратегічних цілей без необхідності прямого використання військової сили. Методами сучасної інформаційної агресії є створення атмосфери бездуховності, аморальності та підриву національної ідентичності, маніпулювання суспільною свідомістю з метою загострення політичної напруженості, провокування конфліктів і поширення хаосу, дезінформація населення щодо діяльності державних органів, під-рив їхнього авторитету, дискредитація влади та її міжнародна ізоляція, створення образу ворога для залякування суспільства та мобілізації підтримки агресора [2, с. 91].

На думку провідних дослідників інформаційного протиборства в інформаційно-технічній (віртуальній, цифровій, кібернетичній тощо), управління інформаційними потоками перетворилося у визначальний атрибут владно-управлінських ресурсів та спроможностей XXI столітті. Контроль за інформаційними ресурсами та конфронтаційні дії з ними стали основною мету будь-якого воєнно-політичного протистояння. Відповідно, радикально змінилися і арсенал, і простір інформаційного протистояння, яке усе більше зміщується в сферу дій спеціальних органів з регулювання кіберпростору, застосування складних засобів ведення протистояння [див.: 3].

На думку фахівців, новітнім засобам інформаційного протиборства властиві:

швидкість розповсюдження інформації, адже найголовніше – оперативно донести повідомлення до кінцевого споживача;

зрозумілість і доступність (в умовах інтенсифікації суспільного повідомлення мають бути вкрай короткими, інформативними й невибагливими);

всеохопність за аудиторією й висока частотність, повторюваність (найбільший ефект спостерігається не від звичайного дублювання, а транслювання того ж самого змісту у зміненій формі);

«довіра» до джерела, що формується шляхом подачі відомостей як суто інсайдерської інформації);

створення видимості масовості у мережах;

створення видимості соціальної значущості;

фальсифікація мови шляхом навмисно неправильного використання слів для подальшого викривлення змісту;

хибна ідентифікація через нав’язування реципієнту хибних критеріїв ідентичності, вміщення його у рамки певної уявної спільноти (подвійної реальності, де співіснують взаємовиключні речі, явища та інтереси, насаджується міфологізації свідомості);

нав’язування ірраціоналізму: інформація подається в гіперболізованій та химерній формі [4].

Доведене, що Інтернет створює *сприятливе середовище для сугестивних (навіювальних) технологій*, об'єктом таких технологій часто стають соціальні мережі. Маніпулятивний вплив ефективніший серед інтернет-спільнот, де панують довіра, симпатія, співчуття та взаєморозуміння, що знижує критичність сприйняття інформації. Інтернет відкрив нечувані можливості для організації різноманітних маніпулятивних впливів завдяки своїй глобальності, децентралізації, анонімності та технічним характеристикам.

Нині надзвичайно перспективна роль відводиться *впровадженню штучного інтелекту в інформаційно-пропагандистську діяльність.* Зокрема, Командування спеціальних операцій Збройних сил США (SOCOM) розпочало планомірне творення сучасного інструментарію штучного інтелекту (ШІ) для ведення та масштабування військових операцій з інформаційної підтримки (MISO) та пропагандистських кампаній за кордоном. Ведуться відповідні розробки та практичні заходи, спрямовані на створення «розумних» ШІ-систем з мінімальною участю людського фактору з метою впливу на іноземні цільові аудиторії» та «придушення інакше мислячих наративів», формування суспільної думки на рівні цільових співтовариств. При цьому американська сторона посилається на необхідність реагування на активну розробку подібних засобів в Китаї та Росії.

Що стосується власне кібератак з метою завдання шкоди безпеці і національним інтересам, то, на думку спеціалістів Національного управління кібернетичної та інформаційної безпеки Чеської Республіки, нині вирізняють такі *основні типи атак у кіберпросторі*:

кібероперації з метою шпигунства;

деструктивні атаки у формі диверсійних дій на промислових системах;

атаки програм-вимагачів (вайперів) із видалення корисних даних;

неправомірне використання інформації з чужих повідомлень електронної пошти [5, с.10].

При цьому, проведений Агенством з питань кібербезпеки та безпеки інфраструктури Міністерства національної безпеки США аналіз за тривалий період показав, що основними об'єктами кібершпигунства стають: об'єкти державного управлінського сектору (31% кібератак); промисловий сектор (22%); сфера професійних послуг (11%). Прикметно, що до 85% хакерських груп мали відношення до державного сектору, 8% – до спеціальних державних органів, 4% – до організованих злочинних угруповань [6, с.37-38].

Виходячи із якісного (тотального) зростання можливостей сил і засобів, форм і методів інформаційного протиборства (цілеспрямованого інформаційного впливу як знаряддя реалізації воєнно-політичних спрямувань) науковцями висувається поняття *діджиталізації інформаційної агресії*. Останній в його деструктивному, протиправному вимірі, здатен призвести до створення бажаної інформаційному агресору моделі поведінки з боку тих, на кого намагаються вплинути. При цьому соціальні мережі можуть використовуватися для поширення фейкових новин, вигадок, чуток, пліток, дезінформації та в цілому маніпулювання громадською думкою, поширення

практики кібератак, за допомогою яких доводиться до адресатів «потрібна інформація», насаджується обстановка страху, неконтрольованого розповсюдження дезінформації тощо. Цілеспрямованість діджиталізації інфоагресії полягає в тому, щоб максимально ефективно використати цифрові технології для досягнення конкретних цілей – від політичного маніпулювання до соціальної дестабілізації або економічного тиску. Водночас, джитлізація інфоагресії може бути частиною спеціально спланованих кібернетичних атак на об'єкти критичної інфраструктури (електромережі, транспорт, фінансові установи), що супроводжуються інформаційним тиском і панікою серед населення [7].

З функціонального погляду діджиталізації інформаційної агресії спирається на:

новітні інформаційно-комунікаційні технології та створює можливості для їх подальшого використання й удосконалення;

відповідний комунікативний інструментарій (соціальні мережі, чати, пабліки, спеціальні платформи для обговорення тих чи інших проблем, інтернет-ЗМІ, YouTube, мобільна телефонія тощо);

цільові аудиторії, референтні групи, доступ до електронних систем об'єкта критичної інфраструктури, на які здійснюється вплив для досягнення остаточної мети

«інфоагресивний продукт» (дезінформація, фейкові новини, ворожа пропаганда, мова ненависті, хейтспіч, відверті заклики до ведення, наприклад, агресивних загарбницьких війн, кібератаки на електронні системи об'єктів критичної інфраструктури, кібершпигунство і кібершахрайство, будь-який інший небажаний для конкретного суспільства вплив на громадську думку через комунікативні інтернет-платформи тощо) [8].

Для підривного впливу на політичну (владну) систему визначаються «технології конфліктної мобілізації в соціальних мережах», коли відбувається стимулювання негативного ставлення до влади з самих різних приводів, а потім воно каналізується в відкриті антиурядові виступи. При цьому використовуються такі технології впливу на суспільну свідомість як меметичний вплив (демотиватори, комікси, «фотожаби» тощо), неймінг (конструювання відповідним чином змістовно забарвлених назв подій, політичних сил, партій тощо), таргетінг (відповідний відбір для подання, вкидування або конструювання новин), створення кіберсимулякрів (віртуальних осіб, організацій) та вирусний маркетінг [9].

Список використаних джерел:

1. Калініченко Б. М. Новітні засоби інформаційного протиборства в умовах техногенної цивілізації. *Держава і право:* Зб. наук. праць. Сер. Політичні науки. 2019. Вип. 86. С. 296–305.

2. Кириченко Ю. В., Сергієнко Т. І., Сластін В. О. Інформаційні війни як інструмент гібридної агресії: український досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2025. № 1. С.89–95.

3. Даник Ю.Г., Пермяков О.Ю. Сучасні інформаційні технології забезпечення національної безпеки і оборони: реалії та тенденції розвитку. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2018. № 1. С.160–167.

4. Яскевич А. Інтернет як нове середовище сугестивного маніпулятивного впливу. *Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони (27 вересня 2024 року)* : зб. матер. міжвідомч. наук.-практ. конф. : у 2-х ч. Ч. 1. Київ : НА СБ України. 2024. С. 265–267.

5. Інформаційна довідка щодо актуальних кіберзагроз (атак) в мережі Інтернет та дій провідних країн світу у сфері кібербезпеки за травень 2021 року. К.: НУО України, 2021. 40 с.

6. Інформаційна довідка щодо актуальних кіберзагроз (атак) в мережі Інтернет та дій провідних країн світу у сфері кібербезпеки за грудень 2020 року. К.: НУО України, 2020. 40 с.

7. Батиргареєва В. Щодо визначення та ознак діджиталізації інфоагресії. *Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони (27 вересня 2024 року)* : зб. матер. міжвідомч. наук.-практ. конф. : у 2-х ч. Ч. 1. Київ : НА СБ України. 2024. С.11–16

8. Помаза-Пономаренко А., Тарадуда Д. Кібербезпека об’єктів критичної інфраструктури: ґенеза координації дій складових сектору безпеки й оборони. *Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони (27 вересня 2024 року)* : зб. матер. міжвідомч. наук.-практ. конф. : у 2-х ч. Ч. 1. Київ : НА СБ України. 2024. С. 190–194.

9. Нетеса Н.В., Мокляк В.В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право.* 2023. № 3. С. 98–107.