DOI: https://doi.org/10.32782/PPSS.2023.1.66

ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЛЮДИНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

Єгор Сергійович МІНЕНКО,

аспірант кафедри політичних наук
Навчально-наукового інституту права та
політології Українського державного університету
імені Михайла Драгоманова
https://orcid.org/0000-0001-7169-3252

CHALLENGES TO HUMAN INFORMATION SECURITY IN THE CONTEXT OF HYBRID WARFARE AGAINST UKRAINE

"Until 2014, the term "hybrid warfare" was little known to most Ukrainians, including the media, politicians, and the general public. Basically, only a few researchers in the field of political science and strategic communications, as well as military experts, understood the term. Initially, the concepts of "information warfare," "information confrontation," and "information weapons" were more common, although they were often used with a journalistic connotation. However, today the situation has changed dramatically. Ukraine's state security policy, including information security, is largely based on an understanding of the nature and danger of hybrid warfare as part of full-scale armed aggression. It is important to understand that hybrid warfare involves not only military actions, but also the use of various non-military means and strategies to influence the internal affairs and vulnerabilities of a country. This may include information propaganda, cyberattacks, hybrid influence operations and other means aimed at undermining national security and stability."

До 2014 року термін "гібридна війна" був маловідомим для більшості українців, включаючи ЗМІ, політиків і широку громадськість. В основному лише деякі дослідники в галузі політології та стратегічних комунікацій, а також військові фахівці розуміли цей термін. Спочатку більше поширені були поняття "інформаційна війна", "інформаційне протистояння" та "інформаційна зброя", хоча вони часто вживалися з публіцистичним підтекстом.

Однак, сьогодні ситуація кардинально змінилася. Державна політика України в області безпеки, зокрема в інформаційній, значною мірою базується на розумінні сутності та небезпеці гібридної війни як частини повномасштабної збройної агресії. Важливо розуміти, що гібридна війна включає в себе не лише військові дії, але і використання різноманітних невійськових засобів та стратегій, щоб впливати на внутрішні справи і вразливості країни. Це може включати інформаційну пропаганду, кібератаки, гібридні впливові операції та інші засоби, які спрямовані на підірвання національної безпеки та стабільності.

Сам термін "гібридна війна" не має єдиного визначення і може трактуватися різними спеціалістами по-різному. Його розуміння та вживання змінюється залежно від контексту та актуальних подій. Також важливо відзначити, що в західних наукових дослідженнях та дискусіях термін "гібридна війна" почав використовуватися приблизно з середини 2000-х років і може мати відмінні підходи та інтерпретації від тих, що використовуються сьогодні.

У 2010 році, представники науковців та службовців Міністерства оборони США визначили гібридну війну як "комбінацію державних і недержавних загроз, включаючи атаки з використанням комп'ютерних мереж, супутників, переносних ракет класу "земля-повітря", саморобних вибухових пристроїв, маніпуляцій з інформацією та ЗМІ, а також залучення хімічної, біологічної, радіологічної та ядерної зброї" [6].

Сутність гібридної війни можна усвідомити через розуміння сучасного суспільства та його взаємозв'язків, а також у контексті системної кризи глобальної системи безпеки. У короткому висновку, гібридну війну можна розглядати як новий тип глобального протистояння, спрямований на досягнення політичних цілей агресії шляхом генерації внутрішніх протиріч і конфліктів, а також захоплення стратегічних ресурсів держави-жертви. Цей тип конфлікту реалізується в різних сферах.

Основна мета гібридної війни полягає в захопленні частини стратегічних ресурсів держави-жертви під керівництвом агресора. При цьому еліта держави-жертви "добровільно" допомагає у передачі цих ресурсів. Такий підхід ускладнює визначення методів та засобів гібридної війни, що у свою чергу гальмує швидке та адекватне реагування на агресію.

Відмінності між "традиційними" війнами та гібридними війнами полягають у незмінності наслідків останніх. Це пов'язано з тим, що процес трансформації вимагає зміни менталітету населення, яке втрачає свою основну мету і духовні цінності, замінюючи їх морально-психологічними ілюзіями та міфами, що створює додаткові труднощі для подолання наслідків гібридних конфліктів.

Російська Федерація використовує свій досвід радянської школи безпеки для реалізації цих технологій в інформаційній війні проти України.

Різні дослідники називають такі засоби та методи впливу на інформаційно-психологічний фронт:

– засоби масової інформації та спеціальні інструменти спрямування інформації та пропаганди;

– глобальні комп'ютерні мережі та програмне забезпечення для поширення пропагандистських матеріалів;

– методи незаконної модифікації інформаційного середовища, де приймаються рішення;

– засоби створення віртуальної реальності, поширення чуток та підсвідомого впливу.

Також, вказують на важливість таких методів як:

– пропаганда, напівправда, брехня, дезінформація та маніпуляція;

– диверсифікація громадської думки та психологічний та психотропний тиск;

– міфодизайн.

Ці методи спрямовані на досягнення різних цілей, включаючи підрив міжнародного іміджу України, дестабілізацію внутрішньої ситуації та формування стереотипів про народи та культури. Такий підхід використовується для досягнення політичних та геополітичних цілей в інформаційній війні.

Список використаних джерел:

1. Захаренко К. Засоби масової інформації як чинник розвитку суспільства. *Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія*. 2015. Вип. 38. С. 29-36.

2. Почепцов Г., Чукут С. Інформаційна політика: навч. посіб.: 2-ге вид. К., 2008. 663 с

3. Почепцов Г. Гібридна війна: інформаційна складова. URL: https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/ (дата звернення: 12.11.2023)

4. Золотар О. О. Особливості інформаційної безпеки людини в умовах гібридної війни. *Інформація і право*. 2017. № 3(22). С. 124-131.

5. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3(9). С. 105-114

6. Hybrid Warfare URL: http://www.gao.gov/assets/100/97053.pdf (дата звернення: 12.11.2023).