DOI: https://doi.org/10.32782/PPSS.2023.1.36

ДО ПИТАННЯ ПЕРЕДУМОВ ВІЙСЬКОВИХ КОНФЛІКТІВ У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇЇ ВПЛИВ НА СВІДОМІСТЬ ГРОМАДЯН

Іван Петрович РУДЯНИН,

канд. іст. наук, доц., доцент кафедри історії України та археології Волинського національного університету імені Лесі Українки
https://orcid.org/0000-0002-9536-4506

BACKGROUNDS OF MILITARY CONFLICTS IN THE CONTEXT OF INFORMATION SECURITY AND ITS IMPACT ON CITIZENS' AWARENESS

The guarantee of national security of any state is its actual security, integrity and inviolability of borders, as well as economic and political independence in modern conditions. At the beginning of the russian military invasion of Ukraine, the world society discovered a new type of external threats in the form of "hybrid" wars that affect key segments of the country's life. A prerequisite for an armed conflict is the detailed preparation of the is mean "groundwork" for the future intervention of foreign armed forces on a certain territory. This is to create a favorable background for the aggressor country in the theater of future hostilities.

***Key words**: "hybrid" wars, national security, information security.*

Запорукою національної безпеки будь-якої держави є її фактична захищеність, цілісність та недоторканість кордонів, а також економічна та політична незалежність в сучасних умовах. З початком російського військового вторгнення в Україну світове суспільство відкрило для себе новий тип зовнішніх загроз у вигляді "гібридних" воєн, які впливають на ключові сегменти життєдіяльності країни [1; 5].

Передумовою до збройного конфлікту є детальна підготовка "підґрунтя" для майбутньої інтервенції чужоземних збройних сил на певну територію. Зазначене полягає у створенні вигідного для країни-агресора фону на театрі майбутніх бойових дій. Так, в довгостроковій та середньостроковій перспективах в країні, яку передбачаю захопити силовим методом, формується потужне політичне лобі, котре покликане створювати різного роду перешкоди на шляху зміцнення обороноздатності об'єкта атаки. В економічному секторі створюються компанії, інвестиційні групи та фінансові установи різних типів власності з відповідним капіталом країни-агресора Паралельно проводяться заходи зі знищення ОПК об'єкта майбутньої атаки на ключових позиціях виробництва ОіВТ та боєприпасів. Проводиться розпродаж або знищення надлишкового військового майна та техніки, скорочення чисельності військових частин та відповідно зменшується особовий склад збройних сил за рахунок переведення з військового штату на план мирного. Згодом здійснюється знищення складів озброєння та боєпостачання під виглядом нещасних випадків, необережного поводження зі зброєю або неналежного зберігання боєприпасів [3]. На цьому фоні значно посилюється кількість кібератак зі сторони відповідних комп'ютерних центрів з метою виведення з ладу автоматизованих

систем управління військового та цивільного, як правило стратегічного призначення.

Одним із показників завершального етапу до здійснення військового вторгнення на ту чи іншу територію, є інтенсивність проведення планових або позапланових військових навчань поблизу кордонів театру майбутніх бойових дій. В даному плані однією із явних ознак військового вторгнення є раптове продовження відповідних маневрів, не передбачене графіками їхнього проведення. Також на завершальному етапі підготовки вторгнення відбувається формування похідних колон з бойовою охороною, а також нанесення відповідних розпізнавальних тактичних знаків на наземний та повітряний транспорт.

Будь яка збройна агресія здійснюється у супроводі інформаційної пропаганди, яка покликана налякати та деморалізувати населення країни яке піддалося атаці, а також виправдати дії держави-агресора на міжнародному та внутрішньому рівнях. Перекручування фактів та подій, неправильне трактування ходу війни, заниження чисельності власних втрат і завищення втрат противника та багато інших механізмів використовуються у сучасних "гібридних" війнах [2].

З метою убезпечити населення від подібного "інформаційного шуму" та його можливого впливу на свідомість населення тієї чи іншої країни слід дотримуватись основних правил "інформаційної гігієни", яка допоможе максимально об'єктивно дати оцінку подіям в умовах війни.

По-перше, подану в ЗМІ новину потрібно перевіряти/порівнювати через інші засоби масової інформації (телеканали, програми, радіоефіри, Інтернет видання, у т. ч. зарубіжні).

По-друге, спробувати співставляти відомі та підтвердженні розвитком подій факти з тими, які подаються суспільству у вигляді "свіжих" новин". У випадку невідповідностей спробувати пов'язати ці відмінності з мотивами та намірами опонентів.

По-третє, брати до уваги коментарі професійних людей, діючих або відставних генералів, учасників бойових дій середньої або вищої ланок управління чи свідків тих подій які описуються (подаються) в ЗМІ.

По-четверте, поступово накопичувати базу знань з актуальних проблем шляхом вивчення ТТХ військової техніки перегляду відео сюжетів в телеграм-каналах, спілкуванні із військовослужбовцями, які беруть або брали участь у бойових діях/подіях війни.

Роль пропаганди в епоху швидкісних інформаційних технологій переоцінити важко, особливо тепер, коли павутина Інтернету охопила майже усі куточки нашої планети.

Для збереження порядку та системної роботи органів державної влади та об'єктів промисловості різних рівнів та призначення в умовах воєнного стану, суспільство створило спеціальні правила запобігання витоку секретної та службової інформації і впровадило в дію норми, які покликані їх захищати, у т. ч. в умовах війни [6].

Поняття інформаційної безпеки є неоднорідним і включає в себе комплекс заходів, покликаних запобігти навмисному або випадковому впливу на зміст тієї чи іншої інформації, яка є складовою національної безпеки країни,

розкриття або зміна якої можуть нашкодити окремому, або групі суб'єктів міжнародних відносин.

В даному плані слід відзначити, що поняття Інформаційної безпеки містить в собі наступні складові:

– цілісність інформації, яка полягає у повноті даних або відомостей та неможливості їхнього часткового використання з тією або іншою метою;

– конфіденційність інформації яка визначає її форму та спосіб доступності до неї для конкретної особи або групи осіб;

– достовірність інформації визначається її авторством або походженням.

В епоху стрімкого розвитку комп'ютерних технологій, більшість інформаційних систем залишаються вразливими до хакерських атак. Їхню діяльність визначає алгоритм кроків спрямованих на розшифровку відповідного тексту або зображень, звукового запису та інших видів накопичення та передачі інформації. Сучасні антивірусні системи не справляються з кібератаками центрів, які діють майже у всіх розвинених країнах. Робота відповідних осередків підвищується напередодні військового вторгнення в країну, яка має стати об'єктом збройної інтервенції. Саме через комп'ютерні мережі поширюють неправдиву, так звану "фейкову" інформацію суспільству. При цьому, найбільше ефективними засобами впливу виявляються дані які важко перевірити та спростувати, або котрі дуже виглядають правдоподібно. Відповідна інформація подається населенню у вигляді точок зору експертів, реальних або "новостворених" фахівців тієї чи іншої галузі, аналітиків та відомих громадських діячів, політиків, які мають авторитет, популярність та суттєву електоральну підтримку. Так формується потрібка точка зору у суспільстві, свого роду громадська думка, яка через заангажовані ЗМІ стрімко поширюється на інші інформаційні ресурси і розповсюджується по всій країні.

В даному випадку слід зауважити, що найважче для будь якої групи людей, змінити точку зору великої кількості громадян. Даний феномен полягає у тому, що левова частина населення будь якої держави не бажає змінювати сформовані роками і навіть десятиліттями стереотипи, перш за все через відсутність вільного часу на відповідні роздуми або осмислення запропонованих кимось нових реалій (точок зору). Звикати до нового завжди важче через небажання більшості людей виходити із власної "зони комфорту". Відповідними умовами користуються нейролінгвісти, політологи, соціологи та інші висококваліфіковані фахівці які допомагають певним групам в суспільстві формувати "правильний" світогляд у більшості населення тієї чи іншої держави, виховувати та підтримувати стереотипи у формах поведінки в тій чи іншій ситуаціях, тощо.

Загалом, інформаційна безпека держави та суспільства в умовах війни є поняттям комплексним і передбачає здійснення заходів з чіткого контролю за публікаціями та розповсюдженням відомостей в сучасних засобах масової інформації, в комунікаційних системах, вивчення її походження, правильної оцінки та законності циркуляції серед населення країни, по суті введення в дію жорсткої цензури на публікації відповідного змісту. Правоохоронні органи держави та компетентні служби уповноважені забезпечувати інформаційну, а відтак національну безпеку України під час бойових дій та після їхнього завершення.

Список використаних джерел:

1. Komarchuk O. Гібридна війна: сутність та структура феномену. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2018. № 1 (3). С. 48–54. URL: https://doi.org/10.29038/2524-2679-2018-01-48-54 (дата звернення: 4.11.2023).

2. Гібридна війна росії проти України. Як перемогти на інформаційному фронті. Аналітичний посібник. 2023. 55 с. URL: http://surl.li/ndqvc (дата звернення: 4.11.2023).

3. Де, як і чому вибухали військові склади в Україні останні 15 років. Радіо Свобода. 2018. URL: https://www.radiosvoboda.org/a/29534591.html. (дата звернення: 4.11.2023).

4. Дерев'янко, І.П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти.* Вип. 11, с.6-16. doi:https://doi.org/10.31866/2616-745X.11.2023.278396

5. Кундеус О. М. Теоретичні аспекти гібридної війни РФ проти України. *Регіональні студії.* Ужгород, Видавничий дім "Гельветика". Вип. 20. 2020. С.120-124.

6. Рішення Ради національної безпеки і оборони України від 29.12.2016 року "Про Доктрину інформаційної безпеки України" : Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374. (дата звернення: 4.11.2023).