УДК 35 DOI https://doi.org/10.35546/kntu2078-4481.2024.4.57

І. В. КУДРЯВСЬКИЙ
кандидат політичних наук, докторант
Міжрегіональна Академія управління персоналом
ORCID: 0009-0009-5167-7648

СТРАТЕГІЇ ЗАХИСТУ ВІД НАПАДУ З АКТИВНИМ ЗАСТОСУВАННЯМ ДІЙ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Дана робота присвячена пошуку напрямків та особливостей формування стратегії захисту в умовах, коли учасники не лише бойових дій та військових конфліктів, але суб'єкти міжнародної політики загалом активно застосовують у просуванні своїх інтересів інформаційні дії, при чому, дотримуючись стратегій, нерідко агресивного експансивного характеру, які простежуються в окремих випадках протягом багатьох десятиліть.

За таких умов інформаційні дії у вигляді виключно реагування на поточну ситуацію, заходи тактичного, чи навіть комплекси заходів оперативного рівня планування самі по собі не можуть належним чином забезпечити зниження та нівелювання деструктивного інформаційно-психологічного впливу різних учасників наповнення інформаційного простору, належної захищеності інформаційної безпеки та безпеки держави.

Оскільки інформаційна політика будь-якої держави, тим більше, коли мова іде про елементи розвідувальної діяльності чи інформаційну діяльність недержавних організацій, має суттєві (іноді ключові) елементи, які не висвітлюються публічно та зберігаються в таємниці, аналізувати довготермінові стратегії інформаційної діяльності нерідко доводиться не лише за декларативними документами, але, перш за все, за їхніми фактичними проявами. При чому, коли мова йде про аналіз стратегії інформаційної діяльності – необхідно досліджувати інформаційні дії суб'єктів протягом тривалого часу.

У роботі проаналізовано виявлені та задокументовані (попри значну латентність окремих елементів таких процесів) комплекси інформаційних дій, тенденції та закономірності, що застосовувалися керівництвом держав, при чому, як тих, у яких державний та політичний режим прийнято вважати демократичним, так і з тоталітарними (авторитарними) режимами, учасниками (керівниками) окремих формально чи фактично неурядових організацій.

Наукова новизна роботи та її практичні результати полягають у застосуванні аналізу історичного досвіду для оцінки особливостей сучасного протистояння в інформаційному просторі з урахуванням поширення сучасних інформаційно-комунікативних технологій, які обумовлюють соціально-психологічні зміни, зокрема, безпосередньо в умовах відбиття Силами оборони України російського широкомасштабного збройного вторгнення, яке на всіх етапах підготовки та реалізації супроводжується масштабною діяльністю, спрямованою на реалізацію деструктивного інформаційно-психологічного впливу.

У висновках роботи запропоновані конкретні заходи, які могли б підвищити ефективність роботи органів державного управління у сфері захисту безпеки інформаційного простору та інформаційної безпеки громадян України від деструктивного інформаційно-психологічного впливу противника та інших учасників наповнення інформаційного простору.

Ключові слова: *державне управління, інформаційний простір, інформаційна війна, стратегічні комунікації, російська агресія, інформаційно-психологічний вплив.*

I. V. KUDRIAVSKY
PhD in Political Science, Doctoral Student
Interregional Academy of Personnel Management
ORCID: 0009-0009-5167-7648

STRATEGIES FOR DEFENSE AGAINST ATTACK WITH ACTIVE USE OF ACTIONS IN THE INFORMATION SPACE

This paper is devoted to the search for directions and peculiarities of forming a defense strategy in conditions when participants not only in hostilities and military conflicts, but also international policy actors in general actively use information actions to promote their interests, and in doing so, adhering to strategies, often of an aggressive expansionary nature, which can be traced in some cases for many decades.

Under such conditions, information actions in the form of solely responding to the current situation, tactical measures, or even complexes of measures of the operational level of planning cannot by themselves properly ensure the reduction and leveling of the destructive information and psychological impact of various participants in filling the information space, proper protection of information security and state security.

Since the information policy of any state, especially when it comes to elements of intelligence activities or information activities of non-governmental organizations, has significant (sometimes key) elements that are not publicly disclosed and

kept secret, long-term information strategies often have to be analyzed not only by declarative documents, but, above all, by their actual manifestations. Moreover, when it comes to analyzing the strategy of information activity, it is necessary to study the information actions of subjects over a long period of time.

The paper analyzes the identified and documented (despite the considerable latency of certain elements of such processes) complexes of information actions, trends and patterns used by the leadership of states, both those in which the state and political regime is considered democratic and those with totalitarian (authoritarian) regimes, and participants (leaders) of certain formally or actually non-governmental organizations.

The scientific novelty of the work and its practical results are the application of the analysis of historical experience to assess the peculiarities of modern confrontation in the information space, taking into account the spread of modern information and communication technologies that cause socio-psychological changes, in particular, directly in the context of repulsion of the Russian large-scale armed invasion by the Ukrainian Defense Forces, which at all stages of preparation and implementation is accompanied by large-scale activities aimed at implementing destructive information and psychological influence of the enemy.

The conclusions of the paper propose specific measures that could increase the efficiency of public administration bodies in the field of protection of information space security and information security of Ukrainian citizens from destructive information and psychological influence of the enemy and other participants in the information space.

Key words: *public administration, information space, information warfare, strategic communications Russian aggression, information and psychological influence.*

Постановка проблеми

Ефективність деструктивного інформаційного та психологічного впливу в історичній ретроспективі значною мірою обумовлена його латентністю та складністю виявлення. Якщо обман противника чи потенційного противника, вплив на цільові аудиторії в його державі (включаючи представників державного управління, армії, поліції, населення) проходив вдало, – це могло змінити ситуацію у когнітивному вимірі інформаційного простору (який історично з'явився значно раніше, ніж віртуальний, і набув розвитку ще до популяризації фізичних носіїв інформації (книг, графічних зображень, тощо)) настільки, що виявлення впливу або ставало уже не актуальним через кардинальну зміну історичних обставин, або ж неможливим, оскільки зміна суспільної думки сприймалася як частина природного соціального процесу.

Перша світова війна стала першою тотальною війною, у якій цілі нації, а не лише професійні армії, були "замкнені" в бою, тобто перебували, висловлюючись сучасною популярною термінологією, "в інформаційній бульбашці". Пропаганда війни в той період почала глобально застосовуватися. Уряди держав виділили величезні ресурси та величезні зусилля для створення матеріалу, покликаного формувати думку та дії на міжнародному рівні. Зусилля держав виправдати свої дії та заручитися міжнародною підтримкою призвели до найпотужнішої пропаганди, яку будь-коли створювали на той час [1, С. 99]. Саме пропаганда при застосуванні різноманітних ідеологій стала ключовим інструментом створення низки державних та політичних тоталітарних режимів, включаючи СРСР. Наслідки цих подій у геополітичних масштабах даються взнаки і сьогодні.

Під час Другої світової війни успішність маніпулювання масовою свідомістю продемонстрував військовий злочинець, "майстер пропаганди" Йозеф Геббельс, а його послідовники, російські військові злочинці, сьогодні розв'язали найбільш криваву війну в Європі у XXI столітті та повторний геноцид українського народу [2, С. 93]. Що ж до російських військових злочинців часів Другої світової війни, то вони з метою дискредитації воїнів Української повстанської армії розгорнули масштабну мережу провокаторів, які вдавали із себе повстанців. У західних областях України в цілому, станом на 20 червня 1945 року, діяло 156 спецгруп НКВС із загальною кількістю учасників в них 1783 особи [3, С. 7]. Перевдягнуті чекісти убивали українців до 1950-х років, створюючи криваве підґрунтя кремлівських пропагандистських міфів про "кровожерливих бандерівців". Результативність деструктивного інформаційно-психологічного впливу значною мірою обумовлена тим, що навіть нетривала дія брехні залишає "післясмак" у вигляді емоцій, які слугують або дезорганізуючим фактором для суспільства, або сигналом до активних дій для окремих його членів [2, С. 93]. На жаль, зусилля історичного ворога українського народу не пройшли безслідно, і навіть зараз, коли кожного дня новими військовими злочинами та ударами по цивільній інфраструктурі російські військово-терористичні формування демонструють свою сутність, серед представників українського населення, особливо похилого віку, залишаються ті, хто продовжує вірити російській пропаганді. Це створює додаткові труднощі для процесу розвитку критичного мислення цільових аудиторій, без якого неможливо забезпечити стійкість громадянського суспільства до ворожого деструктивного інформаційно-психологічного впливу та, відповідно, результативний захист інформаційної безпеки держави й особистості.

Складно оцінити, чи у повній мірі уряди і громадянські суспільства демократичних країн світу усвідомлюють небезпечність російської пропаганди та інформаційно-психологічних операцій, але вони однозначно знають про проблему та намагаються їй протидіяти. Європейські країни вже не перший рік системно відбивають атаки кремлівської пропаганди: від навали ботів до сконструйованих медіакампаній. На серйозне ставлення до цієї проблеми вказує те, що у 2015 році держави ЄС створили Оперативну робочу групу зі стратегічних комунікацій

(ESTF – EastStratCom Task Force) з метою протистояння прокремлівським дезінформаційним кампаніям з боку російської федерації. Завданням діяльності профільної структури ЄС став збір та узагальнення таких випадків в єдину базу з метою розробки механізмів протистояння російській пропаганді [4, С. 121]. Тільки за перших п'ять років своєї діяльності Група розвінчала вісім тисяч російських фейків [5] і зараз продовжує роботу.

З метою протидії російській пропаганді та деструктивному інформаційно-психологічному впливу вживалися заходи і в Україні, у тому числі на найвищому – законодавчому рівні. Зокрема, уже після початку широкомасштабного вторгнення прийнято Закон України від 22.05.2022 р. "Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну", Закон України від 23.01.2023 р. "Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії" [6, С. 134]. Щонайменше прийняття нормативно-правових актів парламентом є свідченням уваги до питання.

Попри це, неспівмірно більша кількість ресурсів, передусім фінансових і кадрових, якими володіє противник, а також російські тоталітарні підходи до питань здобуття інформаційної та когнітивної переваги виключають можливість успішно протистояти російському деструктивному інформаційно-психологічному впливу та пропаганді симетричними методами. Система стратегічних комунікацій, прийнята за основу інформаційної політики України, перебуває на стадії становлення та реформування. Механізми державного управління у сфері захисту безпеки інформаційного простору для належного забезпечення інформаційної безпеки держави та громадянина потребують подальших наукових досліджень, практичних заходів, і в кінцевому результаті – значного підвищення ефективності, для набуття спроможності нашої держави та громадянського суспільства отримати когнітивну перевагу над ворогом, що уможливить виконання завдань на оперативному та стратегічному рівні Силами оборони України і, зрештою, перемогу у війні як єдину умову фізичного виживання українського народу.

Враховуючи безпрецедентний масштаб інформаційної складової російської збройної агресії проти України, для досягнення такого результату необхідний не лише ретельний аналіз методик зниження ефективності (нівелювання) деструктивного інформаційно-психологічного впливу провідних світових держав, але, передусім, розуміння логіки дій противника та реалізація потенціалу власного досвіду, оскільки саме Україна першою в світі зустрілася безпосередньо з інформаційними загрозами такого характеру й масштабу.

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення при інтенсивному застосуванні учасниками наповнення інформаційного простору стратегій захисту від нападу (нівелювання або зниження ефективності деструктивного інформаційно-психологічного впливу противника).

Методологія. В ході роботи застосовано такі методи наукового дослідження: історичний, порівняльного аналізу, ретроспективного аналізу, аналізу та синтезу, дедукції, індукції, системно-структурний, лінгвістичний, формально-логічний.

Аналіз останніх досліджень і публікацій

Інформаційний матеріал, необхідний для аналізу, міститься в наукових працях: українських дослідників, серед яких: Косторнова Є., Когут Я., Мустеца В., Горун О., Озель В., Пашинська Д., Канарський В., Шипілова Л., Максимець В., Вівсяна В., Ковальський С., Гуржій С., Лавров В., Дудатьєв А. [1, 2, 3, 4, 5, 6, 12, 13, 14, 15, 16]; іноземних дослідників, серед яких: Bernard Claverie, François du Cluzel, Tzu-Chieh Hung, Tzu-Wei Hung [17, 18]; публікаціях у медіа, зокрема комерційних пропозиціях, пов'язаних з інформаційною діяльністю [7, 8, 9, 10, 11].

Формулювання мети дослідження

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних стратегій захисту від нападу із застосуванням інформаційних дій (нівелювання або зниження ефективності деструктивного інформаційно-психологічного впливу противника).

Викладення основного матеріалу дослідження

При формуванні стратегії захисту безпеки інформаційного простору не викликає сумнівів необхідність налагодження роботи механізмів ідентифікації та реєстрації інформаційних атак. Державні та міжнародні безпекові організації намагаються налагодити систему моніторингу інформаційного простору. Більше того, зараз багато комерційних кампаній пропонують системи автоматичного моніторингу інформаційного простору на базі штучного інтелекту для приватних клієнтів. Такі послуги можуть допомогти не лише своєчасно виявити й зафіксувати факт інформаційної атаки опонентів (конкурентів, противника), але й визначити ефективність роботи власних фахівців у сфері просування іміджу, маркетингу. Прикладами таких систем можуть слугувати: Semantic Force [7], Ecosap [8], Looqme [9], You scane [10], серед вітчизняних Attack index [11] та багато інших. Такі системи зазвичай мають досить потужний аналітичний блок, зокрема семантичного аналізу, можуть похвалитися непоганою здатністю збору інформації, а при правильних налаштуваннях – і її систематизації. Вони застосовуються як

комерційними, так і державними організаціями. Результати машинного аналізу можуть дати достатньо інформативні зведення та висновки для вузьких спеціалістів, та ці матеріали переважно потребують інтерпретації з метою підтримки діяльності осіб, які приймають рішення. Розробники більшості автоматичних систем моніторингу інформаційного простору прагнуть зробити їх придатними до відстежування когнітивних мін, як індивідуальних так і колективних, що безумовно було б безцінною допомогою у роботі з цільовими аудиторіями, але на даний момент у цьому процесі можна констатувати швидше частковий успіх, передусім у сфері маркетингу й таргетованої реклами. Однозначно позитивним у питаннях моніторингу інформаційного простору і виявлення інформаційних загроз можна назвати те, що важливість цієї діяльності в контексті захисту інформаційної безпеки розуміє керівництво більшості країн та міжнародних організацій.

Поняття реєстрації окремих акцій деструктивного інформаційно-психологічного впливу не є тотожним моніторингу інформаційного простору, хоча ці напрямки діяльності тісно пов'язані. Найбільш потужними союзниками України у протидії російській агресії, зокрема й інформаційній, безумовно залишаються США, ЄС та НАТО. Вище згадувалася діяльність Оперативної робочої групи ЄС із стратегічних комунікацій (ESTF – EastStratCom Task Force). Крім того, ЄС запустив щотижневий інформаційний бюлетень для протидії дезінформаційним атакам російських медіа. Мета щотижневого огляду – показати громадянам ЄС величезну кількість дезінформаційних атак, націлених щодня на європейську аудиторію. Дезінформація, яка міститься в російських новинних програмах, фіксується, наводяться факти, які її спростовують. Більшість новинних матеріалів взято з державних російських ЗМІ, орієнтованих на закордонного глядача, зокрема, телеканалу Russia Today [12, С. 33]. Така активність, безумовно, сприяє підвищенню рівня критичного мислення аудиторій, захисту інформаційної безпеки як на державному рівні, так і на рівні громадян і ЄС, і України, і, враховуючи екстериторіальність сучасного інформаційного простору, світу загалом.

Російська агресія проти України починаючи з окупації Криму, а зараз вже і повномасштабна війна, весь час супроводжується інформаційними операціями на всіх етапах. Саме тому ще у 2014 році Північноатлантичний альянс почав свою діяльність з протидії таким явищам зі створення Центру передового досвіду в галузі стратегічних комунікацій НАТО у Ризі (StratCom Centre of Excellence). StratCom сприяє покращенню можливостей стратегічного зв'язку в Альянсі та країнах-членах. Стратегічне спілкування є невід'ємною частиною зусиль, спрямованих на досягнення політичних і військових цілей Альянсу, тому стає все більш важливим, щоб Альянс належним, своєчасним, точним і відповідальним чином повідомляв про свої цілі та місії. Основними напрямками діяльності за 2021 рік були: 1) експеримент багатонаціональних інформаційних операцій; 2) розробка концепції моделювання інформаційного середовища; 3) розробка концепції навчального модуля моделювання дезінформаційної атаки; 4) курс та конференція в соціальних мережах. Діяльність NATO StratCom Centre of Excellence спрямована не лише на захист держав-членів, але й на партнерів, оскільки цей орган можна вважати таким, що надає підтримку державам-членам, кожна з яких має можливість розбудовувати власну систему інформаційного захисту. У 2015 році було ухвалено стратегію щодо протидії гібридній війні і після цього країни-члени розпочали розширювати набір інструментів НАТО для реагування на ці загрози, які включають в себе дезінформацію та кібератаки [13, С. 76]. Таким чином, і цивільні (Європейський союз) і військові (Північноатлантичний альянс) міжнародні організації з перших днів збройних проявів російської агресії проти України оцінили небезпечність ситуації в інформаційному просторі та почали розгортати механізми, які забезпечують принаймні ефективне відстеження і реєстрацію деструктивного інформаційно-психологічного впливу агресора у формах дезінформації та кібератак. Це далеко не повний спектр необхідних дій, але, безумовно, логічні та ефективні за своїм напрямком заходи.

В Україні дещо запізнілим, але, безумовно, важливим кроком для реалізації стратегій національної та інформаційної безпеки стало створення 19 березня 2021 року Центру протидії дезінформації. Це робочий орган Ради національної безпеки і оборони України, у завдання якого входить дослідження російської дезінформації, виявлення її в інформаційному полі України й розробка стратегії та заходів боротьби з нею. Публікації Центру на спеціалізованому ресурсі містять контент українською та англійською мовою, що значно розширює охоплення аудиторій. Статут Центру протидії дезінформації визначає наступні цілі: проведення аналізу та моніторингу подій і явищ в інформаційному просторі, виявлення та вивчення поточних та прогнозованих загроз інформаційній безпеці, забезпечення РНБО інформаційно-аналітичними матеріалами з питань інформаційної безпеки України. Серед пріоритетів називаються зокрема розкриття дезінформації та маніпуляції, боротьба з інформаційним тероризмом тощо [14, С. 99]. Безумовно, створення Центру протидії дезінформації при РНБО стало важливим кроком у розвитку механізмів державного управління, спрямованих на захист безпеки інформаційного простору, хоча і не може задовольнити усіх потреб такої діяльності, але навіть такі дії на цьому етапі війни противник не залишив без уваги та реакції. Попри автоматизацію процесів виявлення дезінформації та застосування спеціалізованого програмного забезпечення, робота зі спростуванням фейків вимагає людського ресурсу, значних витрат часу та фінансів. У той же час результативність такої роботи більше помітна у контексті розвитку критичного мислення аудиторій та "кондиціонування" суспільної думки (своєчасне й системне інформування суспільства про те, що

противник регулярно бреше), аніж у контексті зниження ефективності конкретних інформаційно-психологічних акцій, які безумовно сприйме значна частина аудиторій раніше, аніж дізнається про спростування таких акцій. За таких умов правильним рішенням з боку противника була, зокрема, активізація застосування технологій автоматичного поширення дезінформації, більш активне використання ботів та інших програмних засобів, оскільки використання технічного ресурсу у цьому випадку більш економічно виправдане, аніж людського.

Противник прагне маніпулювати свідомістю українців у соціальних мережах і пошукових системах, поширюючи брехню про Збройні Сили України та нагнітання істерії через соціально-економічні проблеми завдяки постам та коментарям у соціальних мережах від сотень тисяч ботів уже давно. Така тенденція зберігається і зараз. Також росія технологічно намагається використовувати боти щодо української та європейської аудиторії з метою поширення своїх наративів та масштабного збору інформації. Російські боти в соцмережах видають себе за справжніх українців та активно просувають наративи московії. Основні зусилля у поширенні інформації російськими ботами покладаються на головний науково-дослідний обчислювальний центр рф (ГОЛОВНІВЦ) – установу, яка виконує завдання ФСБ та підпорядковується безпосередньо адміністрації президента рф [15, С. 109–110]. Втім, враховуючи, що противник застосовує найрізноманітніші засоби деструктивного інформаційно-психологічного впливу, а методика його роботи може різко відрізнятися за шаблонами (аж до відсутності шаблонності взагалі), рівнем редакційної пропрацьованості інформаційного контенту, залученістю спеціалістів художньої творчості, формами, жанрами та каналами донесення інформації до аудиторій, було б наївно думати, що програмному забезпеченню, хай і сучасному, із застосуванням штучного інтелекту, противник виділяє роль стати переможцем у боротьбі за інформаційну та когнітивну перевагу. Роль таких технологій зводиться до деструктивного впливу на частину цільових аудиторій з порівняно невисоким рівнем критичного мислення, яка легко піддається низькопробній пропаганді й масовій дезінформації, а також у тому, щоби втягнути персонал відповідних інституцій демократичних країн в апріорі програшну і запізнілу протидію публікаціям дезінформуючого контенту противника, що вже відбулися, відпрацювали та втратили актуальність у той час, коли готуються до реалізації нові небезпечні атаки високого рівня пропрацьованості з перспективою ефективного впливу в когнітивній сфері.

У боротьбі за інформаційну та когнітивну перевагу має значення розуміння і правильна класифікація контенту. Це питання не залишилося поза увагою науковців і практиків. Не так швидко, як необхідно, але воно розробляється. Наведемо одну з класифікацій з відповідним обґрунтуванням. Контент у сучасному інформаційному просторі відіграє важливу роль, оскільки він стає основним засобом комунікації, маніпуляції та впливу на цільову аудиторію. Ключові аспекти контенту такі: 1. Тип контенту. Інформаційний контент може бути представлений у різних формах: текстові новини, відеоролики, аудіо, інфографіка, меми тощо. Кожен тип має свої особливості перекладу інформації та впливу на отримувача. Наприклад, відеоматеріали зазвичай мають більший емоційний вплив на глядача порівняно з текстом. 2. Джерела контенту. Джерело, з якого походить контент, суттєво впливає на сприйняття його цільовою аудиторією, оскільки враховується так звана “довіра” до тих чи інших джерел. Офіційні джерела, такі як урядові сайти чи авторитетні медіа, можуть надавати контенту більшої ваги, ніж невідомі блоги або особисті сторінки у соціальних мережах. 3. Контекст розміщення. Місце, де розміщено контент, також може впливати на його сприйняття. Контент, який відображається поруч з іншими новинами або рекламою, може бути сприйнятий інакше, ніж коли його переглядають окремо. 4. Таргетування та персоналізація. Сучасні технології дозволяють націлювати контент на конкретні групи людей на основі їхніх інтересів, демографічних характеристик та іншої інформації. Це може зробити контент більш ефективним у впливі на цільову аудиторію. 5. Інтерактивність та залученість. Контент, який створює взаємодію з користувачем (наприклад, інтерактивні опитування, тести, ігри) може збільшити його залученість і вплив на сприйняття інформації [16, С. 334–335]. Складність сучасної інформаційної діяльності, пов’язаної з виявленням контенту, який передбачає деструктивний інформаційно-психологічний вплив у когнітивній сфері, полягає зокрема у тому, що когнітивні закладки, які повинні скластися разом і вплинути на прийняття рішення представником цільової аудиторії, можуть бути достатньо адресними і добре замаскованими, розкиданими у декількох різнорідних елементах інформаційного контенту частинами, кожна з яких сама по собі не викликає підозр профільного спеціаліста, який займається моніторингом інформаційного простору на предмет виявлення інформаційних загроз. Наведена класифікація досить добре може задовольняти потреби аналізу окремого матеріалу, виданого в один час, але інформаційно-психологічні акції зазвичай передбачають серію новинних публікацій, творів мистецтва, мемів, інтерв’ю, синхронізованих “зливів” інформації протягом певного періоду. В окремих випадках на етапах глибокої підготовки можуть навіть заздалегідь створюватися та поширюватися окремі твори мистецтва, які для певних аудиторій надають контекстного значення певним поняттям чи словосполученням, залишаючись непомітними для інших аудиторій чи спеціалістів противника. При цьому окремі “когнітивні закладки”, залишаючи певний “післясмак”, який має спрацювати при отриманні представником цільової аудиторії певної інформації, можуть спрацьовувати не з одним, а з декількома інформаційними приводами на однорідні чи різні результати. Це дозволяє “дотиснути” реалізацію деструктивного інформаційно-психологічного впливу наступними акціями, навіть якщо його не вдалося досягнути з першого разу, у повній мірі застосовуючи результати хоча б часткового успіху. Чим ретельніше

спланований деструктивний інформаційно-психологічний вплив противника, чим вище редакційне пропрацювання інформаційного контенту та більш орієнтоване на цільові аудиторії його розповсюдження, чим краще здійснено розподіл за етапами впливу окремих інформаційних матеріалів в рамках акції – тим складніша реалізація таких акцій, але тим ефективніший вплив вони мають у когнітивній сфері і тим важче виявити подібну інформаційну активність, не кажучи вже про те, щоб на доказовому рівні зафіксувати факт її реалізації.

Не відстежуючи активності противника (саме в питаннях боротьби за когнітивну перевагу, а не лише інформаційну в більш широкому значенні), не можливо обґрунтовано говорити про адекватну протидію таким загрозам. Крім того, навіть при ідеальній реалізації завдань відстеження та фіксації активності противника – самих по собі цих дій недостатньо для отримання когнітивної переваги, та зрештою – перемоги, як у питаннях когнітивної війни, так і в широкому значенні – військової перемоги над ворогом.

До схожих висновків у своїх дослідженнях доходять і вчені – представники країн НАТО. Кібернетичний світ зараз є всеосяжним, постійно присутнім, і жодне рішення чи дія не можуть бути виконані без інструментів, які він надає. Очевидно, що це впливає на пізнання тих, хто ними користується, і буде впливати на окремих людей і групи на всіх рівнях, як психологічно, з наслідками для людей, так і технічно, коли людські помилки впливають на системи. Це сфера, що швидко розвивається, і нові шляхи постійно розсувають межі наших знань і потенційних можливостей використання. Вкрай важливо намагатися передбачити загрози, породжені майбутніми технологіями, і дізнаватися більше про ті, що розробляються сьогодні. Ці загрози стають дедалі поширенішими, а їх функціонування, найчастіше, матиме глобальні наслідки, що вимагає від НАТО і країн-членів замислитись над різноманітними вимірами когнітивної війни. Передбачити їх означає набути засобів, які дозволять вийти за межі реактивної позиції. Якщо збройні сили залишатимуться реактивними, це призведе до втрати технологічної ініціативи, яка сьогодні так важлива для військової стратегії [17, С. 10]. Як бачимо, висновки, щодо того, що час реагування та “війни з тінями минулого” давно пройшов, абсолютно однозначні.

Когнітивна війна стала не просто трендом, а формою ведення бойових дій не тільки для відомих нам гравців – російського агресора, НАТО, США, країн-членів НАТО. Її дію відчувають на собі й інші країни, зазвичай демократичні (оскільки суспільства в антидемократичних режимах часто навіть не усвідомлюють факту когнітивної війни через спотворене сприйняття навколишньої дійсності). У цьому аспекті цікаве резюме тайванських вчених, які оцінюють реалізовану гібридну агресію та потенційні можливості збройного вторгнення Китаю у контексті застосування технологій когнітивної війни. На їх погляд, когнітивна війна повинна розглядатися як воєнний злочин у рамках міжнародного права через страх, залякування та психологічне насильство, яке вона спричиняє людству. Насправді, у цій війні немає переможця, оскільки когнітивна війна також шкодить нападнику; Китай може врешті-решт повірити у вибраний ним факт і бути сліпим до реальності, повторюючи прорахунки, зроблені Росією під час вторгнення в Україну. Тайвань може пережити напад, якщо вжити належних контрзаходів; однак для сприяння демократизації Китаю в майбутньому спільні зусилля всіх демократичних країн є справді необхідними [18, С. 15]. Загалом у матеріалі, датованому 2020-м роком досить розгорнуто дається характеристика когнітивній війні, яку на той період вів Китай проти Тайваню. Причому, представлена досить цікава концепція, відповідно до якої поняття когнітивної війни є значно ширшим, аніж питання інформаційної війни. За результатами аналізу інформаційної діяльності російських окупантів, особливо тих їхніх заходів, які, на перший погляд, часто можуть здаватися нелогічними, також проглядається тенденція підпорядковувати інформаційні дії, як і дії у кіберпросторі, меті отримання саме когнітивної переваги, тобто вести інформаційну (медійну) та кібервійну в інтересах когнітивної війни.

Висновки та перспективи подальших розвідок у даному напрямку

Враховуючи викладене, заходи щодо відстеження і реєстрації актів російської інформаційної агресії, які вживаються в даний час політичним та військовим державним керівництвом України, країн-партнерів та міжурядових організацій, безумовно необхідні і дозволяють щонайменше накопичити досвід, який дає можливість аналізувати принаймні ту частину дій противника, що була виявлена. Поряд з тим, складність та латентність застосування засобів інформаційного нападу, який сучасні технології дозволяють реалізовувати у найрізноманітніших формах, роблять недостатніми самі по собі засоби відстеження і реєстрації актів ворожої інформаційної агресії, а також недостатньо ефективними заходи захисту безпеки інформаційного простору без активних дій наступального характеру, покликаних забезпечити власну ініціативу, управління інформаційним простором, інформаційну перевагу, когнітивну перевагу, вплив на цільові аудиторії противника включно з його державним, військовим керівництвом, особовим складом та населенням. Буде цей вплив деструктивним (деморалізація з метою відмови від підтримки подальшої агресивної війни), конструктивним (інформування про реальну ситуацію, що послабить позиції російської пропаганди й дезінформації, популяризація сучасних загальнолюдських і демократичних цінностей, тощо) чи міститиме поєднання конструктивного і деструктивного впливу, – залежить від того, які форми і методи боротьби за когнітивну перевагу будуть обрані тими, хто прийматиме відповідні рішення, але, однозначно, без такої інформаційної активності система захисту безпеки власного інформаційного простору виявиться неповною та не зможе забезпечити виконання своїх завдань.

Неформальний альянс держав з антидемократичними режимами, який у медіа демократичних країн нерідко називають "віссю зла", на прикладі росії (концепція когнітивної зброї С. Сулакшина) та Китаю ведуть боротьбу в інформаційному просторі саме з метою здобуття когнітивної переваги. Дослідники НАТО, країн-членів НАТО, Тайваню та інших країн інтенсивно займаються вивченням особливостей ведення когнітивної війни як неконвенційної форми бойових дій, пошуком шляхів протидії когнітивній війні і загрозам, які вона несе.

Українська наукова думка, а тим більше – практика, дещо відстає у розробці необхідного наукового підґрунття та організації механізмів державного управління, які могли б реально захистити безпеку інформаційного простору від загроз, пов'язаних із веденням противником когнітивної війни. Навіть вітчизняні вчені, які дійшли до осмислення поняття "когнітивної безпеки" [19, С. 283], часто, на жаль, не виходять за рамки розуміння інформаційного протистояння як реактивного процесу (виявлення, аналіз загроз, протидія загрозам і саме в такому порядку). Подібна ситуація, якщо вона не зміниться у майбутньому, з кожним місяцем забиратиме життя наших співвітчизників та знижуватиме шанси на перемогу.

Враховуючи викладене, пропонується:

Підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору в ході відбиття Силами оборони України російського широкомасштабного вторгнення при середньостроковому та довгостроковому стратегічному плануванні розглядати у контексті отримання когнітивної переваги над противником.

Заходи протидії деструктивному інформаційно-психологічному впливу противника, зокрема й у когнітивній сфері, поєднувати із заходами впливу на затверджені цільові аудиторії противника з досягненням ефекту у когнітивній сфері.

Інформаційну безпеку держави та особисту безпеку її громадян розглядати через призму завоювання інформаційної переваги над противником, завоювання та утримання когнітивної переваги над противником, уможливлення управління інформаційним простором, причому не лише своїм, але й ворожим, уникаючи грубих порушень демократичних принципів розвитку громадянського суспільства і держави.

В рамках структурних підрозділів, які беруть участь у реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору створити нечисленні, але укомплектовані висококваліфікованими спеціалістами відділи, відповідальні за виявлення ворожого впливу, орієнтованого на ефекти у когнітивному вимірі інформаційного простору та аналіз таких дій з формуванням заходів адекватного реагування, прогнозування майбутніх акцій противника та підготовку пропозицій в ході планування впливу на затверджені цільові аудиторії противника.

Список використаної літератури

1. Косторнова Є. Пропагандистські технології Першої світової війни, Другої світової війни й російсько-української війни 2014–2023 років: порівняльний аналіз. Соціальні комунікації: теорія і практика. 2023, № 1 (том 15). С. 96 – 114. DOI: https://doi.org/10.51423/2524-0471-2023-15-1-8. (дата звернення 23.07.2024).

2. Когут Я. Методи протидії інформаційно-психологічним операціям. Збірник тез доповідей учасників VIII Всеукраїнського круглого столу 08 грудня 2022 року "Державотворення та правотворення в контексті євроінтеграції". 2022. 234 С. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5091/1/08_12_2022.pdf#page=92. (дата звернення 23.07.2024).

3. Мустеца В. Використання каральними органами СРСР агентурно-бойових груп в боротьбі проти повстанців ОУН на Буковині. Вісник центру Буковинознавства. 2019, № 3. С. 30 – 42. URL: https://shron1.chtyvo.org.ua/Mustetsa_Vasyl/Vykorystannia_karalnymy_orhanamy_SRSR_ahenturno-boiovykh_hrup_v_borotbi_proty_povstantsiv_OUN_na_Buk.pdf. (дата звернення 23.07.2024).

4. Горун О. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні. Інформація і право. 2023. № 1 (44). С. 116 – 128. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287772. (дата звернення 23.07.2024).

5. ЄС розвінчав понад вісім тисяч кремлівських фейків. Верховна Рада України. 2020. URL: https://www.rada.gov.ua/print/192178.html. (дата звернення 23.07.2024).

6. Озель В., Пашинська Д. Конституційно-організаційні засади протидії російській пропаганді в умовах війни. Матеріали Міжнародної науково-практичної конференції "Конституційні засади протидії російській пропаганді в умовах війни". 2023. С. 132 – 135. DOI: https://doi.org/10.32782/PPSS.2023.1.34 (дата звернення 23.07.2024).

7. Semantic Force – це омніканальна платформа моніторингу, аналітики медіа та обслуговування клієнтів, що базується на передовому семантичному та візуальному аналізі. // URL: https://semanticforce.ai/ua?gad_source=1&gclid=CjwKCAjwzIK1BhAuEiwAHQmU3uMdUhPvcVVCx8j7BKnPNYacaYluvSC9wjbowem7lx3JwiOwkkXYRoCz94QAvD_BwE (дата звернення 24.07.2024).

8. Допомагаємо оцінити ваші комунікації. URL: https://ecosap.media. (дата звернення 24.07.2024).

9. Оцінюємо здоров'я бренду з фокусом на ріст бізнес результату. URL: https://uk.looqme.io. (дата звернення 24.07.2024).

10. Моніторинг соцмедіа з візуальними інсайтами. URL: https://youscan.io/ua/. (дата звернення 24.07.2024).

11. Контролюй та коригуй інформацію про себе. URL: https://attackindex.com/uk/golovna-attakindex/. (дата звернення 24.07.2024).

12. Канарський В., Шипілова Л. Публічно-управлінські механізми протидії інформаційним загрозам: європейський досвід. Матеріали щорічної міжнародної науково-практичної конференції "Україна 2030: публічне управління для сталого розвитку". Київ. 2020. С. 32 – 34. URL: https://www.researchgate.net/profile/Tetyana-Syvak/publication/349310794_STRATEGIC_COMMUNICATIONS_AS_THE_BASIS_OF_PUBLIC_ADMINISTRATION_PROCESS/links/602a195ea6fdcc37a829191d/STRATEGIC-COMMUNICATIONS-AS-THE-BASIS-OF-PUBLIC-ADMINISTRATION-PROCESS.pdf#page=32 (дата звернення 24.07.2024).

13. Максимець В., Вівсяна В. Співробітництво України та НАТО у протидії деструктивним інформаційним впливам російської федерації (2022–2023 рр.). Вісник НТУУ "КПІ" Політологія. Соціологія. Право. 2023, № 2 (58). С. 74 – 80. DOI: https://doi.org/10.20535/2308-5053.2023.2(58).285605. (дата звернення 24.07.2024).

14. Ковальський С. Протидія російській дезінформації та пропаганді в українському інформаційному просторі (на прикладі електронного ресурсу центру протидії дезінформації при РНБО України). Діалог: медіастудії. 2023, № 9. С. 96 – 108. DOI: https://doi.org/10.18524/2308-3255.2023.29.300638. (дата звернення 24.07.2024).

15. Гуржій С. Організаційно-технічні та кримінально-правові основи протидії російським ботам в умовах війни. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2023, № 64. DOI: https://doi.org/10.32841/2307-1745.2023.64.21. (дата звернення 24.07.2024).

16. Лавров В., Дудатьєв А. Інформаційна війна та її вплив на контент: методи оцінки ризиків та шляхи протидії. Матеріали VII Міжнародної наукова конференції "Проблемні питання науки та проблеми розвитку". Берлін. 2023 р. С. 333 – 337. URL: https://eu-conf.com/wp-content/uploads/2023/10/PROBLEMATIC-QUESTIONS-OF-SCIENCE-AND-PROBLEMS-OF-DEVELOPMENT.pdf#page=334. (дата звернення 24.07.2024).

17. Bernard Claverie, François du Cluzel. The Cognitive Warfare Concept. // [Електроний ресурс]. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf. (дата звернення 24.07.2024).

18. Tzu-Chieh Hung, Tzu-Wei Hung. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. // [Електроний ресурс]. Journal of Global Security Studies. 2020. № 4 (7). С. 1 – 18. DOI: https://doi.org/10.1093/jogss/ogac016. (дата звернення 24.07.2024).

19. Кобець Т. Основні підходи до розуміння "когнітивна безпека" в сучасній науці: політичний та інформаційний аспект. // [Електронний ресурс] Вісник Львівського університету. Серія філос.-політолог. студії. 2023, № 49. С. 278 – 285. DOI https://doi.org/10.30970/PPS.2023.49.34. (дата звернення 24.07.2024).

References

1. Kostornova Ye. (2023) Propahandystski tekhnolohii Pershoi svitovoi viiny, Druhoi svitovoi viiny y rosiisko-ukrainskoi viiny 2014–2023 rokiv: porivnialnyi analiz. [Propaganda Technologies of the First World War, the Second World War and the Russian-Ukrainian War of 2014-2023: A Comparative Analysis]. Sotsialni komunikatsii: teoriia i praktyka, no. 1, pp. 96 – 114. DOI: https://doi.org/10.51423/2524-0471-2023-15-1-8. [in Ukrainian].

2. Kohut Ya. (2022) Metody protydii informatsiino-psykholohichnym operatsiiam [Methods of countering information and psychological operations]. Zbirnyk tez dopovidei uchasnykiv VIII Vseukrainskoho kruhloho stolu 08 hrudnia 2022 roku "Derzhavotvorennia ta pravotvorennia v konteksti yevrointehratsii". URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5091/1/08_12_2022.pdf#page=92. [in Ukrainian].

3. Mustetsa V. (2019) Vykorystannia karalnymy orhanamy SRSR ahenturno-boiovykh hrup v borotbi proty povstantsiv OUN na Bukovyni [The use of agent-combat groups by the USSR punitive authorities in the fight against the OUN insurgents in Bukovyna]. Visnyk tsentru Bukovynoznavstva, no. 3, pp. 30 – 42. URL: https://shron1.chtyvo.org.ua/Mustetsa_Vasyl/Vykorystannia_karalnymy_orhanamy_SRSR_ahenturno-boiovykh_hrup_v_borotbi_proty_povstantsiv_OUN_na_Buk.pdf. [in Ukrainian].

4. Horun O. (2023) Protydiia vorozhii media-propahandi v umovakh pravovoho rezhymu viiskovoho stanu v Ukraini [Counteracting hostile media propaganda under the legal regime of martial law in Ukraine]. Informatsiia i pravo, no.1 (44), pp. 116 – 128. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287772. [in Ukrainian].

5. (2020) YeS rozvinchav ponad visim tysiach kremlivskykh feikiv [The EU has debunked more than eight thousand Kremlin fakes]. Rada.gov.ua. URL: https://www.rada.gov.ua/print/192178.html. [in Ukrainian].

6. Ozel V., Pashynska D. (2023) Konstytutsiino-orhanizatsiini zasady protydii rosiiskii propahandi v umovakh viiny [Constitutional and Organizational Principles of Countering Russian Propaganda in the Context of War]. Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii "Konstytutsiini zasady protydii rosiiskii propahandi v umovakh viiny", pp. 132 – 135. DOI: https://doi.org/10.32782/PPSS.2023.1.34 [in Ukrainian].

7. Semantic Force – tse omnikanalna platforma monitorynhu, analityky media ta obsluhovuvannia kliientiv, shcho bazuietsia na peredovomu semantychnomu ta vizualnomu analizi [Semantic Force is an omnichannel media monitoring,

analytics, and customer service platform based on advanced semantic and visual analysis]. URL: https://semanticforce.ai/ua?gad_source=1&gclid=CjwKCAjwzIK1BhAuEiwAHQmU3uMdUhPvcVVCx8j7BKnPNYacaYluvSC9wjbowem7lx3JwiOwkkXYRoCz94QAvD_BwE [in Ukrainian].

8. Dopomahaiemo otsinyty vashi komunikatsii [We help you evaluate your communications]. URL: https://ecosap.media. [in Ukrainian].

9. Otsiniuiemo zdorovia brendu z fokusom na rist biznes rezultatu [We assess the health of the brand with a focus on the growth of the business result]. URL: https://uk.looqme.io. [in Ukrainian].

10. Monitorynh sotsmedia z vizualnymy insaitamy [Social media monitoring with visual insights]. URL: https://youscan.io/ua/. [in Ukrainian].

11. Kontroliui ta koryhui informatsiiu pro sebe [Control and correct information about yourself]. URL: https://attackindex.com/uk/golovna-attakindex/. [in Ukrainian].

12. Kanarskyi V., Shypilova L. (2020) Publichno-upravlinski mekhanizmy protydii informatsiinym zahrozam: yevropeiskyi dosvid [Public-management mechanisms for countering information threats: European experience]. Materialy shchorichnoi mizhnarodnoi naukovo-praktychnoi konferentsii "Ukraina 2030: publichne upravlinnia dlia staloho rozvytku", pp. 32 – 34. URL: https://www.researchgate.net/profile/Tetyana-Syvak/publication/349310794_STRATEGIC_COMMUNICATIONS_AS_THE_BASIS_OF_PUBLIC_ADMINISTRATION_PROCESS/links/602a195ea6fdcc37a829191d/STRATEGIC-COMMUNICATIONS-AS-THE-BASIS-OF-PUBLIC-ADMINISTRATION-PROCESS.pdf#page=32 [in Ukrainian].

13. Maksymets V., Vivsiana V. (2023) Spivrobitnytstvo Ukrainy ta NATO u protydii destruktyvnym informatsiinym vplyvam rosiiskoi federatsii (2022–2023 rr.) [NATO-Ukraine Cooperation in Countering Destructive Information Influences of the Russian Federation (2022-2023).]. Visnyk NTUU "KPI" Politolohiia. Sotsiolohiia. Pravo, no. 2 (58), pp. 74 – 80. DOI: https://doi.org/10.20535/2308-5053.2023.2(58).285605. [in Ukrainian].

14. Kovalskyi S. (2023) Protydiia rosiiskii dezinformatsii ta propahandi v ukrainskomu informatsiinomu prostori (na prykladi elektronnoho resursu tsentru protydii dezinformatsii pry RNBO Ukrainy) [Countering Russian disinformation and propaganda in the Ukrainian information space (on the example of the electronic resource of the Center for Countering Disinformation at the NSDC of Ukraine)]. Dialoh: mediastudii, no. 9, pp. 96 – 108. DOI: https://doi.org/10.18524/2308-3255.2023.29.300638. [in Ukrainian].

15. Hurzhii S. (2023) Orhanizatsiino-tekhnichni ta kryminalno-pravovi osnovy protydii rosiiskym botam v umovakh viiny [Organizational, Technical and Criminal Law Bases of Counteracting Russian Bots in the Context of War]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Ser.: Yurysprudentsiia, no. 64. DOI https://doi.org/10.32841/2307-1745.2023.64.21. [in Ukrainian].

16. Lavrov V., Dudatiev A. (2023) Informatsiina viina ta yii vplyv na kontent: metody otsinky ryzykiv ta shliakhy protydii [Information Warfare and its Impact on Content: Risk Assessment Methods and Ways to Counteract]. Materialy VII Mizhnarodnoi naukova konferentsii "Problemni pytannia nauky ta problemy rozvytku", pp. 333 – 337. URL: https://eu-conf.com/wp-content/uploads/2023/10/PROBLEMATIC-QUESTIONS-OF-SCIENCE-AND-PROBLEMS-OF-DEVELOPMENT.pdf#page=334. [in Ukrainian].

17. Bernard Claverie, François du Cluzel. The Cognitive Warfare Concept. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf. [in English].

18. Tzu-Chieh Hung, Tzu-Wei Hung. (2020) How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. Journal of Global Security Studies, no. 4 (7), pp. 1 – 18. DOI: https://doi.org/10.1093/jogss/ogac016. [in English].

19. Kobets T. (2023) Osnovni pidkhody do rozuminnia "kohnityvna bezpeka" v suchasnii nautsi: politychnyi ta informatsiinyi aspekt [The main approaches to understanding "cognitive security" in modern science: political and informational aspects.]. Visnyk Lvivskoho universytetu, no. 49, pp. 278 – 285. DOI: https://doi.org/10.30970/PPS.2023.49.34. [in Ukrainian].