Сергей Соловьев
Кандидат наук по социальным коммуникациям, доцент,
Киевский национальный университет имени Тараса Шевченко. (Украина)

Задачи информационной обороны

DOI: https://doi.org/10.52340/isj.2022.24.03

Аннотация В статье продолжен анализ понятия информационной обороны, предложенного автором в ранее опубликованных работах. С целью обеспечения национальной безопасности доказывается необходимость восприятия информационной агрессии на одном уровне с территориальной агрессией. Рассмотрены задачи информационной обороны, наводятся примеры информационной агрессии, фокусируется внимание на проблеме разработки форм реакции государства на информационную агрессию.

Ключевые слова: информационная оборона, информационная агрессия, национальная безопасность, информационное пространство, физическое пространство, кибератака.

Вступление. В информационном обществе, инициаторами и участниками развития которого мы являемся, понятие национальной и международной безопасности расширилось за счет именно информационной составляющей. Известно, что информационное оружие еще в давние времена было компонентом войн – сначала в форме слухов, манипуляций, запугиваний, позже – пропаганды, психологических операций, фейков. Показательны, в первую очередь, стратагемы влияния, описанные Сунь-цзы [1]. Но только в XXI веке, когда эффективность создания и распространения нарративов кардинально возросла, это оружие может претендовать на особую силу и использоваться вне сферы собственно военного инструментария.

Целью статьи является обоснование понятия информационной обороны как восприятия государством информационной агрессии на одном уровне с территориальной агрессией, а также характеристика задач информационной обороны.

Результаты. В украинском законодательстве мероприятия в сфере национальной обороны предусматривают в числе прочего защиту информационного пространства, создание развитой инфраструктуры в информационной сфере. В то же время, информационное влияние других государств не трактуется как агрессия: согласно Закону «Об обороне Украины» принятие мер предусматривается только в случае вооруженного нападения или подготовки к защите от нападения [2]. Таким образом, захват территории или попытка такого захвата трактуется как акт агрессии. В то же время посягательство на информационное, виртуальное, когнитивное, киберпространство не имеют четкого определения – возможно, по причине трудностей описания пересечения воображаемой государственной «границы».

Об опасности восприятия угрозы только лишь в физической сфере еще в 50-е годы размышлял Г. фон Дах, уже тогда определяя современные для него войны как войны мировоззрений, целью которых есть полная интеграция в идеологическую сферу [3]. А область идеологии – это использование информационного инструментария. Эту мысль подтверждает современный украинский академик, государственный деятель В. Горбулин. Он пишет, что в глобальных цивилизационных противостояниях, к которым относится российско-украинская война, военный способ становиться дополнительным, а не главным [4, с. 84].

Иными словами, нападение может быть предпринято в информационном выражении, но защита предусмотрена при физической агрессии. Институционально, технически

государство не выработало действенной реакции именно на информационную агрессию. Подобная неготовность (плюс гибридный характер угроз) привела, например, к оккупации Крыма и части Донецкой и Луганской областей. Интенсивное информационное влияние России на жителей наших территорий позволило агрессору заручиться поддержкой действий РФ и неприятием действий Украины.

Возможности гибридных методов войны, ассиметричных действиях описал начальник Генерального Штаба ВС РФ в своей хорошо известной публикации еще накануне оккупации Украины [5]. Он отводит большую роль невоенным методам, которые, однако, всячески способствуют выполнению военных задач.

Подтверждение эффективности таких методов иллюстрирует один из преподавателей Военного университета Министерства обороны РФ, написав следующее: «События на юго-востоке Украины… являются хорошим примером ведения гибридной войны. …Россия… быстро и без лишнего шума сработала в скрытой области спектра гибридной войны. Пророссийские силы нейтрализовали деятельность украинской администрации Крыма и установили контроль над полуостровом. Демография Крыма… дала возможность провести операцию практически без применения военной силы и человеческих жертв» [6, с.27].

Обратим внимание на слова «установили контроль на полуостровом без применения военной силы». В принципе, в них выражено потенциал информационного воздействия одной страны на другую, что само по себе свидетельствует о признании информации как инструмента государственной политики экспансии и о имеющейся необходимой базе (законодательной, институциональной, экономической, технической, кадровой) для использования соответствующих технологий.

Необходимость признания угрозы для государства в информационном пространстве наравне с угрозой в физическом пространстве нами было предложено назвать информационной обороной [7]. В частности ее можно рассматривать как конструкт стратегических коммуникаций в сфере национальной безопасности.

Информационная оборона – это готовность к информационному нападению, предвидение его основных характеристик, целей. Мы считаем, что технологии информационной обороны должны обеспечивать как минимум уменьшение последствий нападения, как максимум – недопущение такой агрессии, уменьшение ее интенсивности или использования сил противника для причинения вреда ему самому.

В задачи информационной обороны мы, в частности, включаем:

– подготовку социума к критическому восприятию информации со стороны противника. Под такой информацией будем иметь ввиду официальные сообщения органов власти, СМИ всех форм собственности, сообщения в соцсетях, ролики на видеохостингах, а также продукцию сферы культуры и образования (книги, фильмы, выставки, концерты и др.).

– изучение слабых мест противника в информационной, виртуальной сферах с целью использования в своих интересах. Такими слабыми местами могут быть ошибки СМИ, ненадлежащая подготовка материалов, неэтическое поведение, коррупция субъектов информационных отношений, позволяющие широко интерпретировать деятельность и продукцию таких субъектов;

– информационное влияние на население страны-агрессора для возможного давления общественных институтов на руководство государства. Например, распространение гражданами страны-агрессора информации в соцсетях о передвижении своих войск и настроениях военнослужащих; обсуждение проблем в социальной сфере и т.д. нужно использовать для формирования атмосферы недоверия к властям с целью переключения ее внимания к внутренним проблемам;

– развитие украинской системы международного информационного вещания. Имеется в виду создание, деятельность информационных площадок для транслирования объективной, оперативной информации об Украине за пределы страны, расширение корреспондентской сети за рубежом для противостояния российской пропаганде;

– создание качественных информационных и виртуальных продуктов-носителей стратегических нарративов. Такими продуктами могут быть журналы, фильмы, выставки, фестивали, видеоигры с нарративами демократической, свободолюбивой, успешной,

экономически и технологически развитой Украины для создания атмосферы неприятия менталитета агрессора;

– патриотическое воспитание молодежи в системе образования. Мотивация подрастающего поколения к защите родины формируется постепенно, с учетом интересов учащихся. Полезными инструментами могут быть викторины, олимпиады на исторические, краеведческие темы, поездки по памятным местам, встречи с интересными людьми, съемки видеофильмов, деятельность в учебном интернет-издании, а также освоение азов военного дела, навыков смежных профессий.

Эти и другие задачи нацелены на создание своеобразного иммунитета к информационному воздействию противника и формирование своих смыслов, объясняющих и упорядочивающих факты соответственно целям национальной безопасности.

На уровне системы коллективной международной безопасности зафиксированы шаги в восприятии агрессии в информационном пространстве как агрессии в физическом пространстве. Например, на встрече с министрами обороны стран-членов НАТО в ноябре 2017 г. Генеральный секретарь НАТО Е. Столтенберг заявил, что блок рассматривает кибербезопасность как военный вопрос, а также, что кибератаки могут служить поводом для применения статьи 5 Североатлантического договора [8].

Исходя из заявления Генерального секретаря НАТО, возглавляемая им структура готовится к такой форме противостояния, когда ответ на информационную (кибернетическую) угрозу может воплощаться в физическом измерении. Вполне понятно, что в этом случае будет наблюдаться усиление взаимовлияния информационного, виртуального и физического пространств на государственном и межгосударственном уровнях, т.е., теоретические основы информационной обороны будут воплощены.

Все чаще в среде госуправления звучат мысли о важности информационной компоненты в противостоянии государств. Например в официальном сообщении МВД Украины говорится, что кибератаки на органы государственной власти Украины 14.01.2022 спланировали и провели спецслужбы РФ [9]. Эксперты подчеркивают, что основной фронт в современных гибридных войнах – информация и интерпретация событий [10].

Дискуссия и выводы. Полноценная защита физического пространства невозможна без применения комплекса мер по защите информационного и виртуального пространств.

Проблемным может быть определение характеристик информационной (виртуальной, кибернетической) агрессии, составляющих угрозу национальной и международной безопасности. Например, следует определиться, в какой мере, и является ли информационным нападением высказывания официальных лиц РФ необъективных и унизительных мнений об истории Украины, манипулятивные публикации в российских медиа, формирование негативного образа Украины в российских фильмах, видеоиграх и т.д. Соответственно, следует определиться и с адекватной формой защиты от информационной агрессии: главным образом – в каком пространстве, в каком виде должна воплощаться защита, какой инструментарий должен использоваться. Это относится к стратегическим коммуникациям.

Целесообразно классифицировать предполагаемые виды информационной агрессии с целью выработки форм реакции государства.

Например, необходимо дать научный ответ, является ли видом информационной агрессии статья за подписью В. Путина «Об историческом единстве русских и украинцев» опубликованная в июле 2021 г. на официальном кремлевском сайте на русском и украинском языках. Также важно исследовать более массовые явления: концерты российских исполнителей в Украине, публикации в антиукраинском сегменте СМИ с призывами «объединиться», «вспомнить, как хорошо было в СССР», трансляцию псевдоисторических видеороликов.

Без четкого научного подхода к определению характеристик подобных явлений невозможно выработать формы реакции государства, направленные на повышение национальной безопасности.

Литература:

[1]. Сунь-дзи. Мистецтво війни. / пер. з кит. та коммент. С. Лесняк. Львів : Видавництво старого Лева, 2015. 105 с.
[2]. Про оборону України : Закон України № 1932-XII від 06.12.91. Дата оновлення: 21.06.2018. URL: http://zakon.rada.gov.ua/laws/show/1932-12 (дата звернення: 15.05.2017).
[3]. Дах Ганс фон. Тотальний опір: Інструкція з ведення малої війни для кожного. Частина 1. / пер. Х. Назаркевич, Львів : Астролябія, 2014.
[4]. Горбулін В. Як пеемогти РОсію у війні майбутнього. Київ : Брайт Букс, 2021.
[5]. Герасимов В. В. Ценность науки в предвидении. *Военно-промышленный курьер*. 2013. № 8(476). 27 февр.
[6]. Карякин В. В. Особенности гибридной войны на юго-востоке Украины. *Информационные войны*. 2019. № 2(50).
[7]. Соловйов С. Г. Теоретичні засади інформаційної оборони. *Державне будівництво*. 2015. № 1. URL: http://www.kbuapa.kharkov.ua/e–book/db/2015–1/doc/1/06.pdf (дата звернення: 15.05.2017)
[8]. Сидоренко С. На землі, на воді та в інтернеті: НАТО підвищує готовність до російської агресії. URL: https://www.eurointegration.com.ua/articles/2017/11/10/7073456/ (дата звернення: 20.06.2018).
[9]. Кібератака на органи державної влади, яка сталася у ніч на 14 січня, була спланована і проведена спецслужбами держави-агресора. URL: https://telegra.ph/file/6d37f06fe9145007ad465.jpg (дата звернення: 24.01.2022).
[10]. Максим Розумний: Як зупинити Путіна? URL: https://espreso.tv/maksim-rozumniy-yak-zupiniti-putina (дата звернення: 24.01.2022).

Serhii Soloviov
Candidate of Sciences in Social Communications, Associate Professor,
Kyiv National Taras Shevchenko University (Ukraine)

TASKS OF INFORMATION DEFENSE

Summary

The article continues the analysis of the concept of information defense proposed by the author in previously published works. The necessity of perception of information aggression on the same level as territorial aggression in order to ensure national security is proved. The tasks of information defense are considered, examples of information aggression are cited, and attention is focused on the problem of developing forms of state response to information aggression.
Key words: information defense, information aggression, national security, information space, physical space, cyber attack.