

DOI 10.35775/PSI.2025.115.3.020

УДК 32.327

А.Д. ЕРМИЛОВ

аспирант кафедры международных отношений,
мировой политики и дипломатии института международных
отношений Казанского Федерального (Приволжского)

Университета, Россия, г. Казань

E-mail: gridinpetrok@ya.ru

ORCID: 0009-0000-0659-7715

ФЕНОМЕН КОГНИТИВНОЙ ВОЙНЫ И ЕГО МЕСТО СРЕДИ ИНЫХ ФОРМ НЕИНТЕРВЕНЦИОНАЛЬНОЙ АГРЕССИИ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Статья исследует феномен когнитивной войны как инструмента манипуляции общественным мнением в цифровую эпоху. Автор рассматривает исторические предпосылки, начиная с холодной войны, когда некинетические методы воздействия на сознание стали альтернативой традиционным конфликтам. Особое внимание уделяется эволюции технологий манипуляции, таких как психологические операции (PsyOps), радиоэлектронная борьба и кибервойна и анализу их сходств и различий с когнитивной войной. Когнитивная война отличается от других форм информационного воздействия своей направленностью на изменение мышления и поведения через дезинформацию и манипулятивные нарративы. Автор анализирует роль социальных сетей, искусственного интеллекта и больших данных в усилении влияния когнитивной войны, а также обсуждает угрозы для национальной безопасности и культурной идентичности. В условиях глобальной цифровизации когнитивная война становится эффективным инструментом воздействия, что требует новых стратегий противодействия.

Ключевые слова: когнитивная война, неклассические войны, современные международные конфликты, психологические операции, кибервойна.

Общественное мнение является неотъемлемой частью политических структур, в рамках которых мы существуем, и с момента возникновения первых человеческих сообществ представители нобилитета стремились воздействовать на него в своих личных или, гораздо позднее, государственных интересах. В стремлении элит оказывать прямое или косвенное влияние на мышление и идеи широких масс нет ничего принципиально нового. Однако превращение общественного мнения в инструмент манипулирования со своей спецификой, систематичностью, доктринальностью представляет собой новую и угрожающую тенденцию в современных международных отношениях. Появление сети

Интернет и средств массовой информации открыло возможности для масштабного манипулирования сознанием людей с помощью целого спектра различных целенаправленных, легкодоступных и мультимодальных сообщений, которые к тому же могут распространяться при сохранении анонимности.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 4; 5; 6; 7; 8; 9; 11; 12; 13; 14; 15].

Однако проблему всестороннего междисциплинарного исследования когнитивных войн нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Известный американский писатель, социолог и журналист Уолтер Липпман еще в 1921 году, основываясь на глубоком анализе американской прессы в период Первой мировой войны, в своей работе «Общественное мнение» отмечал, что: «Между человеком и объективной реальностью или объективной окружающей средой образуется определенная вставка – псевдосреда. На эту псевдосреду и реагирует человек своим поведением. Однако последствия его поведения, если это какие-то действия, проистекают не в псевдосреде, в которой стимулируется подобное поведение, а в реальной среде, где у каждого действия есть результат и последствия» [10]. Образуется некий треугольник восприятия (субъективного отражения объективной реальности), где углы представляют собой объективную реальность, человеческое представление или восприятие этой реальности и человеческую реакцию. В век информационных технологий, искусственного интеллекта, нейронных сетей и бесконечных потоках информации проблема того, что человеческие поступки, реакции и действия основаны не на непосредственном и объективном знании, а на картинках и образах, нарисованных навязанными извне нарративами, является чрезвычайно актуальной. Кроме того, важно отметить, что в море из миллиардов голосов, которым являются современные социальные сети и прочие источники, становится невероятно сложно определить конкретные источники информации [23]. Касательно сетевой анонимности мнение экспертов разделилось. Некоторые заявляют, что анонимность – это ключевой элемент глобальной интернет-коммуникации, она необходима для функционирования и реализации ресурсов, предоставляемых интернетом. Другие же, напротив, беспокоятся о возможных последствиях, которые могут последовать из-за отсутствия гарантий ответственности обусловленной анонимностью [34].

Независимо от того, какая точка зрения является правильной экспертные аналитики НАТО полагают, что Альянс должен быть максимально осведомлен и подготовлен к возможной опасности, которую потенциально несет в себе все большая информационная взаимосвязанность. Различные стратегии, ориентированные на взаимодействие с обществом, например такие как стратегии медиаманипулирования, со временем будут становиться все более действенными, охватывать большую аудиторию и быть более убедительными. Отечественное

экспертное сообщество также считает, что инструменты воздействия на общественное мнение в современных реалиях представляют собой серьезную угрозу для интересов и безопасности Российской Федерации. Евромайдан на Украине и попытка государственного переворота в Белоруссии в 2020-2021 гг. ярко продемонстрировали, как информация собирается и распространяется в геополитических и геоэкономических интересах соперников России.

Очевидно, что в ближайшем будущем ожидается стремительное развитие социальных сетей, новостных каналов, алгоритмов автоматизации, искусственного интеллекта, нейронных сетей, новых способов передачи данных. Это делает общество еще более связанным и ориентированным на большие данные. Несомненно, подобные тенденции имеют положительные характеристики, но важно понимать, что, во-первых, в условиях интенсивного использования глобальных сетей возникают новые формы культурной экспансии со стороны наиболее развитых стран в отношении менее развитых. Перед целыми сообществами появилась реальная угроза лишиться своей культурной и национальной самобытности, что демонстрирует активно продвигаемый Соединенными Штатами так называемый «миропорядок, основанный на правилах». Во-вторых, люди склонны не только к получению информации, но и к активному ее распространению и созданию. Генерация контента более не является сугубо прерогативой крупных информационно-новостных гигантов, мировых СМИ. Теоретически создать инфоповод под силу каждому, кто обладает стабильным интернет-соединением и смартфоном. Люди активно делятся своими привычками, религиозными, общественными и политическими убеждениями и мировоззрением, своими предпочтениями, что создает благоприятную среду для реализации технологий информационной войны и смежных концепций. В век, когда противостояние между государствами все больше приобретает некинетический характер, когда классическая полномасштабная военная интервенция уступает место технологиям «цветных революций» и технологиям, основанным на сетевых группах, война имеет дело не с обнаженной плотью, но с обнаженными умами. И одним из новейших направлений подобных технологий «неклассической войны» можно считать концепт когнитивной войны.

Как и многие другие явления, связанные с современной войной, различные технологии неклассической войны берут свое начало в период «холодной войны». Концепция взаимного гарантированного уничтожения стала общепринятой глобальной стратегией, что сделало тотальную войну в масштабах Второй мировой войны маловероятной. Подрывная деятельность и шпионаж стали частью повседневной международной деятельности, а «правдивое отрицание» стало одним из ключевых терминов периода. Таким образом, в США ЦРУ и ФБР расширяли свои полномочия, а различного рода тайные операции стали обыденностью [32]. Эти методы, возникшие ввиду ядерного паритета между двумя полюсами силы в биполярной системе международных отношений, стали альтернативой военному способу реализации своих внешнеполитических интересов. В полной мере стала проявляться сила слов и идей, некинетические инструменты

влияния. Как принято считать на Западе: миллионы людей по всему миру стали свидетелями того, как Советский Союз наблюдал за падением железного занавеса, не сумев противостоять силе «джинсов и рок-н-ролла» [27].

Одной из первых технологий неклассической войны можно считать концепцию психологических операций («PsyOps»). В США термин «PsyOps» используется для обозначения деятельности, связанной с использованием так называемой «белой, серой и черной продукции», которая реализуется различными подразделениями вооруженных сил и Центрального разведывательного управления. Белая пропаганда («white propaganda») – это пропаганда, которая распространяется и признается источником или его официальными представителями [25. С. 42]; Серая пропаганда («gray propaganda») – это пропаганда, которая не идентифицирует специально свой источник [25. С. 178]; Черная пропаганда («black propaganda») – это пропаганда, которая выдается за исходящую из иного источника, чем подлинный [25. С. 54.]. Деятельность включает в себя пропагандистское радиовещание, предоставление инструкций ополченцам или иным сетевым группам и поощрение к дезертирству [28; 31]. Психологические операции имеют несколько ключевых отличий от когнитивной войны. Во-первых, когнитивная война в основном имеет дело с «серой» пропагандой. «Белая» и «черная» пропаганда слишком рискованны, чтобы быть надежными методами воздействия на общественное мнение. Во-вторых, когнитивной войне присущ определенный элемент отрицания, который теряется в случае с «белой» пропагандой и попадает под угрозу в случае с «черной» пропагандой. Более того, в прошлом психологические операции редко работали с широкими слоями населения. «PsyOps» особое внимание уделяет военной или подрывной деятельности, которая обычно не является целью тактических приемов когнитивной войны, нацеленных на гражданскую социальную инфраструктуру и правительство [28].

Под радиоэлектронной борьбой понимается использование электромагнитного спектра для нападения на противника, препятствования его атакам или выявления и разведки конкретных объектов. В некотором смысле радиоэлектронная борьба была предшественницей кибервойны. Ее истоки восходят к началу XX в., когда была изобретена первая беспроводная связь. Инфракрасное самонаведение, радиосвязь и растущее использование беспроводных технологий делают эту область важным подразделением вооруженных сил государств по всему миру. Однако эта область в значительной степени связана с приборами и тактическими преимуществами, т.е. речь идет о информационно-техническом превосходстве над противником. Это не связано с общественным мнением и даже не влияет на гражданское пространство, за исключением отключения электричества или радио с целью установления целенаправленной информационной блокады [29; 21].

Кибервойна определяется как использование кибератак с целью нанесения ущерба национальным активам. Важно отметить, что кибервойна и ее военная классификация до сих пор вызывают много споров [20]. Тем не менее, многие государства-члены НАТО и другие страны инвестировали в развитие различных

инструментов кибервойны, как наступательных, так и оборонительных [24; 33]. Существует обеспокоенность классификацией с точки зрения международного права акта кибератаки, так как она направлена на цифровые активы государства, на компьютерные сети или виртуальные пространства. Однако глобальная тенденция к цифровизации и так называемому «Интернету вещей» привела к тому, что компьютеры теперь контролируют больше функций, чем можно представить. Все, от строительного оборудования до финансовых учреждений, гражданской инфраструктуры и даже военных объектов, теперь зависит от сложной компьютерной сети [26]. Потеря таких компьютерных ресурсов может привести и уже приводила к огромным убыткам не только в плане времени и потери данных, но и к физическому ущербу, который можно измерить в долларах и жизнях людей [17]. В 2009 Пентагон и Израиль подтвердили данный тезис, проведя совместную операцию под кодовым названием «Nitro Zeus», которая включала в себя наступательную кибератаку с использованием вируса Stuxnet против иранской ядерной программы. В результате кибератаки было выведено из строя более тысячи центрифуг на заводе по обогащению урана в Натанзе [30].

Связь кибервойны с когнитивной войной в основном заключается в том, что у них есть общие методы ведения операций. Были случаи, когда компьютерные вирусы распространялись через социальные сети, нацеливаясь на друзей и/или контакты зараженного человека. Однако эти случаи лучше назвать киберпреступлениями, а не целенаправленными попытками ведения кибервойны. В когнитивной войне социальные сети используются совершенно по-другому. Вместо распространения вредоносного программного обеспечения агенты когнитивной войны распространяют вредоносную информацию. Используя те же тактики, что и при DDoS-атаках, а именно ботнеты, агенты когнитивной войны могут распространять огромное количество ложной или вводящей в заблуждение информации через аккаунты, которые выглядят и ведут себя как человеческие [19]. Однако это лишь одна из тактик, используемых в когнитивной войне, и на этом сходство с кибервойной в основном заканчивается.

Наиболее родственным к когнитивной войне является концепт информационной войны. Однако существуют ключевые различия, которые делают когнитивную войну достаточно уникальной, чтобы рассматривать ее как отдельную категорию. Как описал ее бывший командующий ВМС США Стюарт Грин: «Информационные операции, наиболее близкая к когнитивной войне американская доктрина, состоят из пяти элементов. К ним относятся радиоэлектронная борьба, операции в компьютерных сетях, психологические операции, «военная хитрость» и оперативная безопасность» [22]. Суммируя, можно сказать, что концепт информационной войны является обобщающей стратегией, направленной на то, чтобы контролировать информацию в ее широком смысле.

Основное различие между информационной войной и когнитивной войной заключается в том, что в первом случае не проводится различие между тактической информацией на поле боя и информацией, предназначенной для общественности. Например, информационная война связана с DDoS-атаками

и «призрачными армиями», в то время как ни то, ни другое не относится к сфере когнитивной войны. Возможно, более четкое разграничение заключается в том, что информационная война направлена на контроль над чистой информацией во всех ее формах, а когнитивная война направлена на контроль над тем, как отдельные люди и группы людей реагируют на представленную информацию [18].

В определении, опубликованном в декабре 2019 года Оливером Бэkesом и Эндрю Свабом из Гарвардского центра Белфера, когнитивная война определяется следующим образом: «Когнитивная война – это стратегия, направленная на изменение мышления целевой аудитории и, как следствие, ее действий» [16]. Несмотря на намеренную расплывчатость этого определения, оно служит более чем подходящей основой для дальнейшего изучения когнитивной войны.

Феномен когнитивной войны представляет собой новую и серьезную угрозу в современных международных отношениях, где информационные технологии и социальные сети стали мощными инструментами манипуляции общественным мнением. Как показано в статье, когнитивная война отличается от традиционных форм информационного воздействия, таких как психологические операции или кибервойна, своей направленностью на изменение мышления и поведения целевой аудитории через распространение дезинформации, манипулятивных нарративов и искусственно созданных инфоповодов.

Исторически когнитивная война берет свое начало в период холодной войны, когда некинетические методы воздействия на сознание людей стали альтернативой открытым военным конфликтам. Однако в условиях цифровой эпохи, с развитием искусственного интеллекта, нейронных сетей и социальных медиа, масштабы и эффективность таких методов значительно возросли. Современные технологии позволяют не только быстро распространять информацию, но и создавать иллюзию правдивости, что делает когнитивную войну особенно опасной.

Особую угрозу когнитивная война представляет для национальной безопасности и культурной идентичности. Примеры событий на Украине и в Белоруссии демонстрируют, как информационные кампании могут быть использованы для дестабилизации обстановки и достижения геополитических целей. В условиях глобальной цифровизации и возрастающей взаимосвязанности, когнитивная война становится все более изощренной и трудной для обнаружения.

В заключение можно сказать, что когнитивная война требует серьезного внимания со стороны государств и международных организаций. Необходима разработка новых стратегий противодействия, включая усиление кибербезопасности, повышение медиаграмотности населения и создание механизмов для выявления и нейтрализации дезинформации. Только комплексный подход позволит минимизировать риски, связанные с этим новым видом информационного оружия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
2. **Алаудинов А.А.** Цели и задачи России в специальной военной операции на Украине и в гибридной войне с коллективным Западом // Вопросы политологии. 2024. № 5.
3. **Алаудинов А.А., Стригунов К.С., Гончаренко А.Р.** Структура и характеристика субъектов военного конфликта на Украине и его основные отличия от гибридных войн в Сирии и Ливии // Вопросы национальных и федеративных отношений. 2024. № 6.
4. **Апарин С.В., Суховерхова А.А., Григорян Д.К.** Цифровые войны: роль черного пиара // Вопросы национальных и федеративных отношений. 2025. № 1.
5. **Буданцев Э.В.** Информационная безопасность как фактор стратегического суверенитета на пространстве Большой Евразии // Евразийский Союз: вопросы международных отношений. 2024. № 6.
6. **Власов М.С.** Особенности информационного противостояния России и США в гибридной войне // Вопросы национальных и федеративных отношений. 2024. № 3.
7. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
8. **Егорова М.Р.** Информационная война как угроза национальной безопасности страны в современном мире на примере конфликтов XXI века // Евразийский Союз: вопросы международных отношений. 2023. № 7.
9. **Иващенко З.С., Васильченко О.В., Григорян Д.К., Малявина А.Б.** Фейковые новости о ходе проведения Специальной военной операции как угроза национальной безопасности Российской Федерации // Евразийский Союз: вопросы международных отношений. 2024. № 9.
10. **Липпман У.** Общественное мнение. Москва: Издательство АСТ, 2023.
11. **Медведева В.К., Медведев Н.П.** Информационная политика государства: современные вызовы и направления совершенствования (Часть 1) // Вопросы политологии. 2025. № 1.
12. **Скворцов Я.Л., Казарян Г.И., Курилкина Е.А.** Гибридная война: информационные стратегии НАТО и вызовы для России // Вопросы политологии. 2024. № 8.
13. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
14. **Уртаева Э.Б.** Геополитические аспекты информационных войн и их влияние на политические процессы // Вопросы политологии. 2024. № 3.

15. **Шавлохов А.К., Максименко Д.И.** Актуальные вопросы обеспечения информационной безопасности населения в условиях военных конфликтов: правовые аспекты // Региональное и муниципальное управление: вопросы политики, экономики и права. 2023. № 3.
16. **Backes Oliver and Andrew Swab.** Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019.
17. **Brenner Susan W. and Leo L. Clarke.** Civilians In Cyberwarfare: Casualties. Law. UPenn, University of Pennsylvania Carey Law School, July 2010 // www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/BrennerClarke.pdf.
18. **Burns Megan.** Information Warfare: What and How? CS.CMU, Carnegie Mellon University, 1999 // www.cs.cmu.edu/~burnsm/InfoWarfare.html.
19. **Costa-Roberts Daniel.** Here's How to Spot a Russian Bot. Mother Jones, 1 Aug. 2018 // www.motherjones.com/media/2018/08/how-to-identify-russian-bots-twitter/.
20. Cyberwar – Does It Exist? NATO Review, NATO, 13 June 2013 // www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.
21. Electronic Warfare: Joint Publication 3-13.1. Edited by William E Gortney, FAS, Joint Chiefs of Staff, 8 Feb. 2012 // www.fas.org/irp/doddir/dod/jp3-13-1.pdf.
22. **Green Stuart A.** Cognitive Warfare. The Augean Stables, Joint Military Intelligence College, July 2008 // www.theaugestables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare.pdf.
23. **Greenemeier Larry.** Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers. Scientific American, 11 June 2011 // www.scientificamerican.com/article/tracking-cyber-hackers/.
24. **Grenoble Ryan.** Trump Reverses Obama-Era Rules On Cyberattacks. HuffPost, 17 Aug. 2018 // www.huffpost.com/entry/trump-cyberattack-directive-20_n_5b758f76e4b0df9b093d1b06.
25. Joint Publication 1-02. DoD Dictionary of Military and Associated Term. Washington. 21 April 2001.
26. **Low Vincent.** The Trend Towards Digitisation. Sg.Canon, Canon, 2020 // www.sg.canon/en/campaign/business-insight/ambassador/the-trend-towards-digitisation.
27. **McCarthy Brigid.** How Rock and Roll Brought the Soviet Union Down. Edited by Lisa Mullins, The World from PRX, Public Radio International, 19 May 2011 // www.pri.org/stories/2011-05-19/how-rock-and-roll-brought-soviet-union-down.
28. Psychological Operations: Air Force Doctrine 2-5.3. Edited by Timothy A. Kinnan, Iwar, United States Air Force, 27 Aug. 1999 // www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf.
29. **Rambo.** History of Electronic Warfare. Blogspot, 7 Dec. 2009 // www.ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html.
30. **Sanger David E. and Mark Mazzetti.** U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict // New York Times, Feb. 16, 2016 // <https://www.nytimes>.

com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?r=0&r=0.

31. **Seligman Lara.** The Child Soldier Crisis: 'Kids Are Cheap'. Foreign Policy, 8 Nov. 2019 // www.foreignpolicy.com/2019/11/08/child-soldier-crisis-kids-are-cheap-yemen-isis-my-star-sky/.
32. The Evolution of the U.S. Intelligence Community-An Historical Overview. FAS, Federation of American Scientists, 23 Feb. 1996 // www.fas.org/irp/offdocs/int022.html.
33. The UK Is a Global Cyber Power, Says Director GCHQ. Edited by Jeremy Fleming, GCHQ, 25 Feb. 2019 // www.gchq.gov.uk/news/the-uk-is-a-global-cyber-power--says-director-gchq.
34. **Torbet Georgina.** 3 Undeniable Reasons Why You Need Online Anonymity. MakeUseOf, 3 Apr. 2020 // www.makeuseof.com/tag/3-undeniable-reasons-need-online-anonymity/.

A.D. ERMILOV

Postgraduate student of the Department
of International Relations, World Politics and Diplomacy at the Institute
of International Relations, Kazan Federal University (Volga Region)
University, Kazan, Russia
ORCID: 0009-0000-0659-7715

THE PHENOMENON OF COGNITIVE WARFARE AND ITS PLACE AMONG OTHER FORMS OF NON-INTERVENTIONAL AGGRESSION IN MODERN INTERNATIONAL RELATIONS

The article explores the phenomenon of cognitive warfare as a tool for manipulating public opinion in the digital age. The author examines the historical background, starting with the Cold War, when non-kinetic methods of influencing consciousness became an alternative to traditional conflicts. Special attention is paid to the evolution of manipulation technologies such as psychological operations (PsyOps), electronic warfare, and cyberwarfare, and the analysis of their similarities and differences with cognitive warfare. Cognitive warfare differs from other forms of information influence in its focus on changing thinking and behavior through disinformation and manipulative narratives. The author analyzes the role of social networks, artificial intelligence, and big data in increasing the impact of cognitive warfare, as well as discusses threats to national security and cultural identity. In the context of global digitalization, cognitive warfare is becoming an effective tool of influence, which requires new counteraction strategies.

Key words: cognitive warfare, non-classical wars, modern international conflicts, psychological operations, cyberwar.