

Научная статья

УДК 323.2

<https://doi.org/10.37493/2307-910X.2025.1.16>

Информационный компонент гибридных войн

Денис Александрович Миргород^{1*}, Лидия Романовна Диденко²

^{1,2} Пятигорский государственный университет, г. Пятигорск, Россия

¹ mirgorod@pgu.ru

² didenkolidia@mail.ru

* Автор, ответственный за переписку: Денис Александрович Миргород, mirgorod@pgu.ru

Аннотация. В настоящее время риски и угрозы безопасности государства становятся все более многосторонними и включают в себя множество аспектов. Традиционные войны с преимущественно милитаристским уклоном дополняются активным привлечением информационных, финансовых, экономических, идеологических и иных компонентов. В этой связи значительную актуальность в научной и экспертной среде приобрело понятие «гибридных войн», основанных на использовании всего доступного инструментария воздействия на противника. Одним из основных механизмов подобного воздействия на современном этапе являются информационные механизмы. Таким образом, информационное противоборство на текущий момент вышло на качественно новый уровень, особенно с учетом развития высоких технологий. Следовательно, исследование данного направления деятельности государств представляет значительный научно-исследовательский интерес и обладает существенной практической значимостью. Особенно заявленную тему настоящей работы актуализируют многочисленные конфликты в современном мире, осуществляемые с привлечением информационного компонента гибридных войн. В частности, наиболее острый характер подобное противодействие носит конфликт России и коллективного Запада. Последний расходует значительные средства на проведение информационных операций против Российской Федерации с целью ее дискредитации на международной арене, а также для дестабилизации внутривнутриполитической обстановки в стране. Реагируя на указанные вызовы, власти РФ в настоящее время привлекают значительное количество ресурсов для выработки и внедрения соответствующих контрмер, направленных на минимизацию и информационных угроз и продвижения собственной повестки. Важность информационной безопасности в рамках гибридных войн также подтвердилась с началом российской специальной военной операции на Украине. События последних нескольких лет наглядно демонстрируют существенную приоритетность развития национальной политики РФ в отношении информационной безопасности и гибридных войн. В статье рассматривается феномен гибридных войн, включающий политическую, экономическую и информационную компоненты. Особое внимание уделяется информационной войне, которая выходит на первый план и включает применение манипуляционных приемов и воздействие на сознание людей. В статье также рассмотрены различные подходы к интерпретации информационной войны. Подчеркивается уязвимость информационной сферы, как в мирное, так и в военное время. Кроме того, в исследовании обозначены разработки новых способов вывода из строя техники противника и овладение информацией, что подчеркивает актуальность исследований в данной области.

Ключевые слова: гибридная война, информационная война, мягкая сила, манипуляция, дестабилизация, политические войны, геополитические задачи, фальсификация общественного сознания, пропаганда, международные связи, дезинформация.

Для цитирования: Миргород Д. А., Диденко Л. Р. Информационный компонент гибридных войн // Современная наука и инновации. 2025. № 1. С. 184-191. <https://doi.org/10.37493/2307-910X.2025.1.16>

Research article

The information component of hybrid wars

Denis A. Mirgorod^{1*}, Lidia R. Didenko²

^{1,2} Pyatigorsk State University, Pyatigorsk, Russia

¹ mirgorod@pgu.ru

² didenkolidia@mail.ru

* **Corresponding author:** Denis A. Mirgorod, mirgorod@pgu.ru

Abstract. *Currently, the risks and threats to state security are becoming increasingly multifaceted and include many aspects. Traditional wars with a predominantly militaristic bias are supplemented by the active involvement of information, financial, economic, ideological and other components. In this regard, the concept of "hybrid wars" based on the use of all available tools to influence the enemy has acquired significant relevance in the scientific and expert community. One of the main mechanisms of such influence at the present stage is information mechanisms. Thus, information confrontation has currently reached a qualitatively new level, especially given the development of high technologies. Consequently, the study of this area of state activity is of significant scientific research interest and has significant practical significance. The declared topic of this work is especially actualized by numerous conflicts in the modern world, carried out with the involvement of the information component of hybrid wars. In particular, the most acute such opposition is the conflict between Russia and the collective West. The latter spends significant funds on information operations against the Russian Federation in order to discredit it in the international arena, as well as to destabilize the domestic political situation in the country. In response to these challenges, the Russian authorities are currently attracting significant resources to develop and implement appropriate countermeasures aimed at minimizing both information threats and promoting their own agenda. The importance of information security in the context of hybrid wars was also confirmed with the start of the Russian special military operation in Ukraine. The events of the past few years clearly demonstrate the significant priority of developing the national policy of the Russian Federation regarding information security and hybrid wars. The article examines the phenomenon of hybrid wars, which includes political, economic and information components. Particular attention is paid to the information war, which comes to the fore and includes the use of manipulation techniques and influence on people's consciousness. The article also examines various approaches to interpreting the information war. The vulnerability of the information sphere is emphasized, both in peacetime and in wartime. In addition, the study outlines the development of new ways to disable enemy equipment and master information, which emphasizes the relevance of research in this area.*

Keywords: hybrid war, information war, soft power, manipulation, destabilization, political wars, geopolitical tasks, falsification of public consciousness, propaganda, international relations, disinformation

For citation: Mirgorod DA, Didenko LR. *The information component of hybrid wars. Modern Science and Innovations. 2025;(1):184-191. (In Russ.).* <https://doi.org/10.37493/2307-910X.2025.1.16>

Введение. Термин «гибридная война» вошел в современный политический лексикон. В военно-политическом дискурсе данный термин понимается как современный способ ведения военных действий, сочетающий классические военные оперативные методы с партизанской войной, терроризмом, биологической и информационной войнами. Политики и ученые признают данный вид войн серьезным вызовом глобальной безопасности. Кроме того, гибридные войны зачастую могут определяться как попытка демонстрации сложности и многогранности тактик и способов ведения современных войн. Они включают в себя большое количество участников, уровней и направлений конфликтов, что в совокупности стирает традиционное понимание различий между типами войн.

Материалы и методы исследований. Использование парадигм из классической стратегической теории и сопоставление их с современными практиками в так называемой гибридной войне позволяет определить, являются ли эти методы действительно новыми и

где такие практики вписываются в более широкую область стратегических исследований. Поэтому в этой статье проводится исследование современного дискурса о гибридной войне в рамках классической стратегической теории [1]. Следовательно, это исследование направлено на создание более полного и обоснованного понимания весьма сложной проблемы, которая стала доминировать в военном дискурсе в течение предыдущего десятилетия. При этом утверждается, что, хотя гибридная война может быть бесполезной как доктринальная концепция, она может оказаться полезной в качестве аналитической основы для исследования природы войны в самом широком смысле, особенно в информационном контексте.

Результаты исследований и их обсуждение. В западной военной политике понятие гибридной военной угрозы длительное время считается уже официально утвержденным термином. Например, на саммите НАТО (сентябрь 2014 года) в итоговом документе прописана необходимость тщательной подготовки Североатлантического альянса к эффективной защите от вызовов, которые возникают в связи с угрозами гибридной войны [9]. Страны-участники Альянса изучают гибридные войны как широкий спектр боевых действий, различных операций с участием граждан и применением пропаганды, кибератак и пр. Отечественные же эксперты отмечают, что «гибридная война предполагает массовые манипулятивные психологические технологии, целенаправленное использование информации для воздействия на общественное сознание с учетом этнопсихологических, гендерных, возрастных и прочих особенностей населения». С помощью широкого распространения информационно-коммуникационных технологий, в частности Интернета, ареной военных действий гибридной войны теоретически может стать вся планета.

В настоящее время информационное противостояние и влияние с помощью «мягкой силы» фактически происходит вне рамок уже существующего международного права. Информационные потоки постоянно вливаются в население, медленно и ненавязчиво меняя его ценности. При этом в зоне риска находится и историческое представление общества, поскольку информационное воздействие изменяет образ мира в умах людей. Именно поэтому одной из главных целей гибридных войн является замена традиционных базовых ценностей общества морально-психологическими установками агрессора.

Однако в данном контексте следует также признать, что гибридная война не является изобретением XXI века. На протяжении всей истории человечества возможности, не связанные напрямую с применением военной силы, часто использовались для принуждения или ослабления противника. Подобные методы разрабатывались для того, чтобы отсрочить осознание факта нападения, парализовать процесс принятия решений и удержать государство-жертву от принятия решительных мер по самозащите. Целью таких «гибридных» действий является дестабилизация экономических сил, подрыв легитимности ключевых государственных институтов, разжигание социальной, расовой и религиозной розни, подрыв международного престижа и международных связей, а также систематическая дискредитация противника. Таким образом, желаемой целью агрессора и важнейшим этапом его конечной победы часто становится ослабление экономической мощи страны, в особенности ее финансовой системы. Для восстановления утраченных позиций захваченные страны тратили большое количество времени и ресурсов, поскольку предотвращение экономических разрушений – сложный процесс.

Согласно общепринятому в настоящее время определению феномена гибридных войн, данное явление включает в себя три основных элемента: политическую войну, экономическую войну и информационную войну [5]. Известно, что гибридная война возникла из вооруженного столкновения двух европейских держав. Их компоненты находились в тесной взаимосвязи и сосуществовали, действуя в зависимости от событий по всем направлениям. Становится очевидным тот факт, что гибридизация – это совокупность признаков различных объектов и явлений.

Из всех вышеперечисленных компонентов гибридной войны информационный выходит на первое место. Российские исследователи отмечают, что такой тип

противоборства закономерно сопровождается применением большого количества манипуляционных приемов, а также воздействием направляемой информации на сознание людей. При этом учитываются их психологические, половые, возрастные и прочие особенности. В силу отсутствия контроля Интернета конкретным государством, информационные войны не происходят в определенном регионе, а распространяются по всему миру. В целом, феномен гибридной войны стал естественным событием со времен холодной войны. Термины «гибрид» и «информационная война» стали более распространенными в связи с нынешней ситуацией в мире. Стратегия национальной безопасности отмечает, что в современных условиях «возрастающий конфликт в глобальном информационном пространстве все больше влияет на характер международной обстановки из-за стремления ряда стран применять информационно-коммуникационные технологии с целью решения геополитических задач. В списке данных целей – манипулирование и фальсификация общественного сознания.

В современной науке существует множество различных подходов к интерпретации информационной войны. Впервые термин «информационная война» употребил Томас Рона в 1976 году в своем аналитическом отчете под названием «Оружейные системы и информационная война» [6]. После данного события в мире укрепилось понимание того, что информацию можно использовать как оружие. При учете постоянного развития западной экономики на почве открытий в области информационных и коммуникационных технологий, можем сделать вывод о том, что данная сфера находится в зоне уязвимости и в мирное, и в военное время. Следует подчеркнуть неизбежность воздействия информационного оружия, состоящего из двух аспектов: влияние на уровень и качество информированности населения и на коммуникационные системы и средства противника. Первый аспект в совокупности состоит из традиционных методов пропаганды и контрпропаганды, которые в современных условиях совершенствуются и становятся более изощренными. Благодаря такому стремительному развитию подстрекательские средства достигли точки наивысшего влияния на умы населения. Второй аспект – специализируется на атаке технических средств и их программных систем. В многих странах мира существуют различные исследовательские и научные организации. Их основная деятельность – разработка новых компьютерных вирусов, зараженных программ и прочих средств, способствующих выводу из строя компьютеров и овладения информацией.

Российский политолог И.Н. Панарин, в свою очередь, дает следующее определение: «Информационная война – это комплексное воздействие на противоборствующую государственную систему и военно-политическое руководство военного режима, которое приведет к принятию решений уже в мирное время и в пользу инициатора воздействия на информацию. Конфликт полностью парализует работу инфраструктуры управления политика» [2].

В рамках изучения информационных войн и анализа обоснования можем определить следующие ее типы: кибервойны, сетевые войны и медиа войны. Говоря о кибервойне, следует отметить, что их главная цель заключается в выполнении поставленных задач. Субъектом в данном случае являются негосударственные структуры. Они осуществляют хищение конфиденциальной информации для дальнейшего ее использования. Основными методами борьбы в данном случае можем считать распространение вирусов и дезинформации, а также манипулирование общественным мнением и СМИ. Медиа войны ставят для себя главной задачей создание конкретной картины мира. Это необходимо для непосредственного воздействия на сознание граждан. В данном случае говорим о СМИ и новостных корпораций. Сетевые войны – смешанный тип медиа и кибервойны. Данный вид активно используется в рамках использования социальных сетей, поскольку это – наиболее удобный способ передачи информации. Сюда входит и воздействие на общественное

мнение, а также осуществление несанкционированного получения конфиденциальной информации.

В настоящее время информационный компонент гибридных войн может интерпретироваться как:

- информационные военные действия, способ получения односторонних преимуществ в сборе, обработке и использовании информации в противоборстве;
- маркировка противоборства в информационной среде и СМИ для достижения поставленных целей, и задач.

Специальная роль в политике ряда государств в современных реалиях отводится проведению информационных операций. Все это имеет прямую связь с нежеланием сторон развязывать крупномасштабные войны с санкциями на использование вооруженных ударов для предотвращения появления противоречий между государствами (ст. 2 Устава ООН) [3].

Глобализация информационного пространства – одна из причин ненасильственного конфликта государств. Появление и развитие новых технологий и источников привело к понижению стоимости средств, которые активно используются в ходе информационных войн. Например, разница между покупкой и использованием истребителей и танков и покупкой компьютерного оборудования для создания сети, которая будет ориентироваться на информационное воздействие, очевидна.

Возрастающая роль информации в современном мире увеличивает потенциал конфликтов данной сферы. Современное общество напрямую зависит от информационно-коммуникационных систем. Данный факт не рекомендуется игнорировать в процессе разработки технологий, которые оказывают влияние на отношение людей к острым ситуациям с помощью манипуляций. Информационные войны зачастую используются в войнах государств с помощью дезинформации и пропаганды, разведки и контрразведки.

Отсутствие постоянной армии указывает на то, что война в настоящее время приняла более гуманное состояние. При этом, относительно короткая история гибридных войн демонстрирует тот факт, что данный тип ведения атак исключает использование моральных норм и следование законам в данном случае становится необязательным. В сравнении с классической тактикой ведения войн, начало гибридной отследить практически невозможно, и официально они не объявляются. Для страны-агрессора здесь главное – достичь поставленной цели, а средства ее достижения могут сильно различаться. В попытках скрыть свою причастность к тем или иным конфликтам, противник может выступать в роли третьей силы. В таком случае сложится впечатление, что агрессор не заинтересован в столкновениях на территории оккупированной страны. Минимизация риска открытой враждебности приводит к использованию разнообразных элементов, которые не всегда являются вооруженными. Главными поражающими силами в данном контексте выступают протестные организации, подрывная оппозиция, экстремистские и преступные группировки. Как правило, они используются тайно и получают финансовую, информационную и прочую поддержку со стороны внешних правящих сил [10]. В этой связи целесообразно отметить способность третьей силы достигать поставленных военно-политических задач, при этом не раскрывая себя.

Целесообразно отметить, что в конце 1970-х годов, когда мир из информационного трансформировался в постинформационный, решение ряда различных задач пришлось на информационные войны. Стала очевидной прямая зависимость современного общества от информационно-коммуникационных систем. Данная закономерность выявлена благодаря политическому и военному руководству крупных стран мира и в обязательном порядке учитывалась в процессе разработки новых технологий, оказывающих влияние на общественное сознание.

Использование информации для различных целей – давно существующая черта, проходящая через всю историю человечества. Отчасти подобное оперирование информацией объясняется тем, что общество восприимчиво к идеям других из-за общей уязвимости населения к принудительному убеждению. Люди, как правило, привыкли

полагаться на мнение окружающих, чтобы понимать информацию из различных сфер. «Даже в высокоразвитых странах отдельный гражданин плохо подготовлен к тому, чтобы формулировать разнообразные суждения, а также предпринимать действия, которые основаны на опыте в отношении общественных проблем» [8]. Подобного набора знаний из первых рук может оказаться достаточно для того, чтобы позволить большинству самостоятельно выбирать свои правительства, решать важные вопросы в рамках государственной политики, а также разумно применять свои знания.

Длительное время серое вещество человеческого мозга являлось мишенью тех, кто стремился изменить общественное сознание посредством информации. С точки зрения того, как это концептуализировать, в научной литературе существует большое количество определений. Например, данный процесс могут описывать как «организованную попытку посредством коммуникации повлиять на веру или действие, или внушить отношение большой аудитории способами, обходящими или подавляющими адекватно информированное, рациональное, рефлексивное суждение индивида» [7]. Другое определение, которое касается политической пропаганды, гласит, что она «включает методы влияния, используемые правительством, партией, администрацией, группой давления с целью изменения поведения общественности». Данное определение сопряжено с социологической пропагандой. Ключевая особенность пропаганды заключается в том, что люди и идеи находятся в диалектической связи. Граждане – коллективно или индивидуально – являются объектами информации, но также они являются источником и хранилищем информации. Джейсон Стэнли (американский философ), описывает политическую пропаганду как «разновидность речи, которая фундаментально включает политические, экономические, эстетические или рациональные идеалы, мобилизованные для политической цели» [2]. В подобных ситуациях коммуникативный акт осуществляется для достижения поставленных целей и задач.

В своем исследовании Джейсон Стэнли также отмечает, что в пропаганде может использоваться не только ложная информация. «Правдивое утверждение, произнесенное с искренностью, может оказаться пропагандой», – отмечает Стэнли. В ряде случаев происходит так, что, чем ближе пропаганда к истине, тем более эффективной она, вероятно, будет. Например, в ходе избирательной кампании 2016 года в США некоторые из наиболее разрушительных пропагандистских действий связывались с утечками электронных писем руководства Демократической партии, которые оказались признаны правдивыми. Кроме того, Стэнли признает, что пропаганда может включать – и действительно часто включает – передачу эмоций. Эффективная пропаганда зачастую питается эмоциями людей и их нормативными суждениями о мире.

Заключение. Таким образом, в настоящее время информационные войны являются наиболее известным методом конфронтации среди государств. Международное сообщество сегодня применяет информацию с целью недопущения большого количества жертв, военных потерь и разрушений инфраструктуры. В данном случае информационные войны – это метод влияния и достижения целей государств. В рамках гибридных войн, комплекс инструментов для ведения информационных войн достаточно широк. Как отмечалось, сюда входят кибератаки, медиа войны, распространение дезинформации, сетевые войны и пр. Данные инструменты также носят деструктивный характер и оказывают серьезное влияние на государственный имидж и на тех, на кого направлены атаки, и являются новым видом оружия XXI века.

ЛИТЕРАТУРА

1. Giacomello G., Ruzza S. Regardless of Clausewitz? Classical strategic theory in a hybrid world // Non-State Challenges in a Re-Ordered World. 2015. No. 1. P. 191–208.

2. Sokolova S. N. Information warfare in the multipolar world // Bulletin of Polessky State University. Series in Social Sciences and Humanities. 2023. No. 2. P. 61–68.
3. Власенко И. В., Лидовская К. С. Перспективы развития информационной безопасности в условиях гибридной войны // Актуальные проблемы правового, экономического и социально-психологического знания: теория и практика: Материалы VII Международной научно-практической конференции. В 3-х томах, Донецк, 27 апреля 2023 года. Донецк: Цифровая типография, 2023. С. 263–268.
4. Власов М. С. Особенности информационного противостояния России и США в гибридной войне // Вопросы национальных и федеративных отношений. 2024. Т. 14. № 3 (108). С. 968–975.
5. Гафурова В. М. История развития компонентов «гибридных войн» // Актуальные проблемы современной науки, техники и образования: Тезисы докладов 82-й международной научно-технической конференции, Магнитогорск, 22–26 апреля 2024 года. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2024. С. 5.
6. Евстафьев Д. Г., Манойло А. В. Информационные войны и психологические операции как базис гибридных войн нового поколения // История. 2021. Т. 12. № 6 (104).
7. Руднев Н. О. Некоторые методы и тактики информационной войны // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 года. Уфа: Башкирский государственный университет, 2022. С. 246–249.
8. Рябов Д. А. Информационная составляющая гибридной войны // Обозреватель. 2024. № 5 (406). С. 19–35.
9. Шагов А. Е. Феномен информационных войн и вопросы военной истории: к осмыслению проблемы // Современная научная мысль. 2022. № 3. С. 143–147.
10. Швец А. Д., Соколов С. С. Противодействие кибернетическим атакам как компоненту информационных операций во время «гибридных» войн // Информационные управляющие системы и технологии: Материалы IX Международной научно-практической конференции, Одесса, 24–26 сентября 2020 года. Одесса: Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С.О. Макарова, 2020. С. 150–153.

REFERENCES

1. Giacomello G, Ruzza S. Regardless of Clausewitz? Classical strategic theory in a hybrid world. Non-State Challenges in a Re-Ordered World. 2015;(1):191-208.
2. Sokolova SN. Information warfare in the multipolar world. Bulletin of Polessky State University. Series in Social Sciences and Humanities. 2023;(2):61-68.
3. Vlasenko IV, Lidovskaya KS. Prospects for the development of information security in a hybrid war. In Actual problems of legal, economic and socio-psychological knowledge: theory and practice: Materials of the VII International Scientific and Practical Conference. In 3 volumes, Donetsk, April 27, 2023. Donetsk: Digital Printing House; 2023;263-268. (In Russ.).
4. Vlasov MS. Features of the information confrontation between Russia and the United States in a hybrid war. Issues of National and Federative relations. 2024;14(3(108)):968-975. (In Russ.).
5. Gafurova VM. The history of the development of components of "hybrid wars". In Actual problems of modern science, technology and Education: Abstracts of the 82nd International Scientific and Technical Conference, Magnitogorsk, April 22-26, 2024. Magnitogorsk: Magnitogorsk State Technical University named after G.I. Nosov; 2024. P. 5. (In Russ.).
6. Evstafiev DG, Manoilo AV. Information wars and psychological operations as the basis of hybrid wars of the new generation. Istoriya. 2021;12(6(104)). (In Russ.).
7. Rudnev NO. Some methods and tactics of information warfare. In Information technologies for ensuring integrated security in a digital society: a collection of materials of the V All-Russian Youth Scientific and Practical Conference, Ufa, May 20-21, 2022. Ufa: Bashkir State University; 2022;246-249. (In Russ.).
8. Ryabov DA. The information component of hybrid warfare. Observer. 2024;(5(406)):19-35. (In Russ.).
9. Shagov AE. The phenomenon of information wars and questions of military history: towards understanding the problem. Modern scientific thought. 2022;(3):143-147. (In Russ.).

10. Shvets AD, Sokolov SS. Countering cyber attacks as a component of information operations during "hybrid" wars. In Information control systems and technologies: Proceedings of the IX International Scientific and Practical Conference, Odessa, September 24-26, 2020. Odessa: Federal State Budgetary Educational Institution of Higher Education Admiral S.O. Makarov State University of the Sea and River Fleet; 2020;150-153. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Денис Александрович Миргород – кандидат политических наук, доцент, заведующий кафедрой восточных языков и культур, профессор кафедры международных отношений, политологии и мировой экономики, Пятигорский государственный университет, mirgorod@pgu.ru

Лидия Романовна Диденко – преподаватель кафедры журналистики, медиакоммуникаций и связей с общественностью ИМО, Пятигорский государственный университет, didenkolidia@mail.ru

Вклад авторов: все авторы внесли равный вклад в подготовку публикации.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию: 10.02.2025;
одобрена после рецензирования: 16.04.2025;
принята к публикации: 21.04.2025.

INFORMATION ABOUT THE AUTHORS

Denis A. Mirgorod – PhD in Political Science, Associate Professor, Associate Professor, Head of the Department of Oriental Languages and Cultures, Professor of the Department of International Relations, Political Science and World Economy, Pyatigorsk State University, mirgorod@pgu.ru

Lidia R. Didenko – Lecturer at the Department of Journalism, Media Communications and Public Relations, Pyatigorsk State University, didenkolidia@mail.ru

Contribution of the authors: the authors contributed equally to this article.

Conflict of interest: the authors declare no conflicts of interests.

The article was submitted: 10.02.2025;
approved after reviewing: 16.04.2025;
accepted for publication: 21.04.2025.