Национальная безопасность / nota bene
Правильная ссылка на статью:
Тиханычев О.В. История развития «гибридных» действий от войн «под чужим флагом» до «умной силы» // Национальная безопасность / nota bene. 2025. № 1. С.77-102. DOI: 10.7256/2454-0668.2025.1.39475 EDN: ABBZMJ URL: https://nbpublish.com/library_read_article.php?id=39475

История развития «гибридных» действий от войн «под чужим флагом» до «умной силы»

Тиханычев Олег Васильевич

ORCID: 0000-0003-4759-2931

кандидат технических наук

заместитель начальника отдела управления перспективных разработок, ГК "Техносерв"

111395, Россия, г. Москва, ул. Юности, 13

to.technoserv@gmail.com

Статья из рубрики "Глобализация и национальная безопасность"

DOI:

10.7256/2454-0668.2025.1.39475

EDN:

ABBZMJ

Дата направления статьи в редакцию:

22-12-2022

Дата публикации:

03-03-2025

Аннотация: Объектом исследования является «гибридное противоборство», предмет исследования – принципы его организации применительно к новым условиям реализации: глобализации и информатизации современного мира. В статье проанализированы основные составляющие «гибридных» действий и, на основе анализа исторического опыта сделан вывод о том, что данные подходы имеют глубокие исторические корни. Речь, при этом, идёт не о «классическом» использовании наёмников, даже в форме частных военных компаний, не о proxy-конфликтах, а именно о «гибридных» действиях, когда скрывается заказчик и цель привлечения вооруженных формирований, а, главное, военные действия сопровождаются экономическим противоборством и информационно-психологическими операциями. Несмотря на

длительную историю развития, в теории «гибридных войн» имеется достаточно много нерешенных вопросов: по их структуре, относительно границ применения составных компонентов «гибридных войн», по методам противодействия, что делает проведение анализа их содержания и особенностей своевременным и актуальным. С использованием результатов исторического анализа данного процесса можно утверждать, что соотношение силовых и не силовых компонентов в структуре «гибридных войн» менялось на разных исторических периодах и театрах военных действий, развивая эту форму противоборства от классической proxy-войны к разносторонним и высокоорганизованным «гибридным» действиям. Прототипы подобных действий, реализуемые в форме proxy-конфликтов, как показал исторический анализ, можно найти уже в войнах XV–XVII веков, но по-настоящему они стали вестись именно в последние годы, с объединением принципов proxy-войны на нижнем уровне и «оффшорного балансирования» на глобальном. На основе анализа исторического опыта ведения войн и вооруженных конфликтов сделан вывод о том, что современные «гибридные» действия являются прямым развитием давно известных тактических proxy-конфликтов, и их развития на стратегическом уровне «оффшорного балансирования», а угроза «гибридного» противоборства актуальна в настоящее время и в обозримой перспективе, но противодействовать ей существующими методами вооруженного противоборства неэффективно. Автором сделан вывод о необходимости обеспечить готовность нашей страны к парированию подобных угроз, описаны возможные аспекты организации противодействия

Ключевые слова:

гибридная война, наемничество, прокси-война, гибкая сила, умная сила, частные военные компании, информационное противоборство, экономические войны, санкции и блокады, история гибридных войн

Введение

Как показывает история войн и военного искусства, для достижения цели противоборства, в том числе реализуемого в форме вооруженных конфликтов различной интенсивности, может быть использовано множество различных стратегий, эффективность которых зависит от условий ведения конфликта. По мере развития военного искусства, разнообразие применяемых форм и способов увеличивалось, обеспечивая общую цель любого конфликта – достижение максимального результата с наименьшими потерями. К одной из наиболее эффективных стратегий для достижения данной цели относится «непрямое» противоборство (*indirect action*), впервые описанное английским военным теоретиком Бэзил Лиддел Гартом (*Basil Henry Liddell Hart*), который в работе «Стратегия непрямых действий» (*Strategy: The Indirect*) сформулировал и тезис, что цель войны, вполне соответствующая принципам организации «гибридных» действий – добиться лучшего, хотя бы только с вашей точки зрения, состояния мира после войны [1].

Исторически, к одной из форм «непрямых» действий можно отнести так называемую proxy-войну, обеспечивающую ведение военных действий опосредованно, чужими руками. Но, в отличие от proxy-действий, ставшая её дальнейшим развитием так называемая «гибридная война», до сих пор не признана в официальных оборонных концепциях большинства современных государств, хотя её, как показывает исторический анализ, неоднократно применяли и применяют для решения задач как вооруженного

противоборства, так и глобального цивилизационного противостояния [2].

Считается, что само определение «гибридная война» (*Hybrid Warfare, HW*) введено в 2005 году Джеймсом Мэттисом (*James N. Mattis*) и Френком Хоффманом (*Frank Hoffman*), как обозначение этого давно используемого, но до того времени не поименованного явления [3]. В настоящее время специалистами используется несколько вариантов определения «гибридного» противоборства. Содержание этих определений относительно структуры действий (*modus operandi*) можно свести к общему посылу в том, что «гибридная» или, по как иногда говорят, «интегральная» (*integral war*) война – это непрямые действия со скрытым использованием военной силы, сопровождающимся активным информационным и экономическим давлением на противника, обеспечивающими синергетический эффект воздействия [4-8]. По цели (*metam*), основные определения «гибридных» действий сходятся в следующем – ослабить противника, не понеся ущерба, который был бы неизбежен в ходе открытого противостояния [9,10,11].

Кроме указанных определений, «гибридные» войны обозначаются как «ассиметричные» (*asymmetrical warfare*) или «комбинированные» войны (*compound war*), что, впрочем, спорно, но не меняет сущности данного вида противоборства [2,4]. В рамках исследования «гибридных» войн, также иногда упоминаются так называемые «нелигитимные» войны (*illegal war*). Отметим, что это не тождественные понятия: хоть «гибридные» войны, в большинстве своём, являются не легитимными, то есть ведущимися без объявления войны и с отступлением от международных законов её ведения, а «нелигитимные» войны часто не являются «гибридными» и ведутся в явной форме.

Анализ сущности определений «гибридной войны», самого содержания «гибридных» действий подтверждает, что они являются естественным продолжением proxy-войн, которые велись и раньше, буквально со времён появления более или менее массового вооруженного противоборства. Просто с развитием технологий, масштабности военных действий и появления теории «тотальной войны» (нем. *Total Krieg*), эти proxy-действия были дополнены информационными и экономическими составляющими, приобретающими всё большую значимость по мере информатизации общества и глобализации экономики.

Более того, учитывая возросшее влияние информационных и экономических действий, некоторые специалисты склонны исключать из определения «гибридного» противоборства вооруженную составляющую [12]. Впрочем, как показывает обзор современных конфликтов, наличие последней, хотя и в разной степени интенсивности и вовлечённости участников, пока является необходимым условием достижения победы в любой форме противоборства.

Ещё одним важным фактором является то, что применение в отдельности каждой из этих составляющих, как правило, не является «гибридной» войной, для перехода их в военные действия требуется, в подавляющем большинстве случаев, наличие совокупности составляющих, осуществляемых с достаточным уровнем активности.

Впрочем, несмотря на длительную историю развития, в теории «гибридных войн» имеется достаточно много нерешенных вопросов: по их структуре, относительно границ применения составных компонентов «гибридных войн», по методам противодействия, что делает проведение анализа их содержания и особенностей своевременным и актуальным. Решение обозначенной проблемы предлагается обеспечить за счёт

критического анализа истории развития основных компонентов сначала proxy-войн и методов «гибридного балансирования», а потом и составляющих «гибридных войн»: силовой, информационной, экономической и политико-дипломатической. Последнюю, объединив с правовыми (юридическими) мерами воздействия, можно определить, как «организационная» составляющая противоборства.

С использованием результатов исторического анализа данного процесса можно утверждать, что на длительном историческом периоде, основной (а сначала и единственной) составляющей «гибридных» действий являлось скрытое привлечение вооруженных группировок и организаций для решения задач межгосударственного противоборства, как правило, в форме proxy-войн [13]. В то же время, как показывает опыт, соотношение силовых и не силовых компонентов в структуре «гибридных войн» менялось на разных исторических периодах и театрах военных действий, развивая эту форму противоборства от классической proxy-войны к разносторонним и высокоорганизованным «гибридным» действиям. В статье предлагается, на основе анализа этого процесса, оценить современное состояние и перспективы развития «гибридного противоборства», структурировать существующие проблемы и обозначить возможные пути их решения.

1. Структура «гибридных войн» и взгляды на её содержание в разные исторические периоды

Многие специалисты считают, что основой и историческим началом появления proxy, а потом и «гибридных» войн можно считать наёмничество. И действительно, упоминание о привлечении наёмников к войнам между греческими государствами-полисами приводится ещё в «Анабасисе» (греч. Ἀνάβασις) Ксенофонта.

И в дальнейшем, в период с XV по XVII век, значимую роль в разрешении европейских конфликтов играли отряды наёмников – немецких и швейцарских ландскнехтов (нем. *Landsknecht*), ирландских «диких гусей» (англ. *Wild Geese*). Использование наёмничества в эту эпоху связано, в первую очередь, с экономическими причинами: во-первых, обращение с холодным оружием требовало определённых навыков, которым нужно было долго обучаться, во-вторых, содержать постоянную боеготовую армию было слишком дорого для небольших государств, из которых в тот период преимущественно состояла Европа. Для решения задач вооруженной защиты или нападения дешевле было нанять стороннюю силу на определённый срок.

Но, в аспекте анализа содержания «гибридных войн», стоит отметить, что наёмничество того времени было ещё даже не прообразом proxy-войн, а вполне легальным способом разрешения конфликтов. И только с началом становления системы межгосударственных отношений, действия наёмных воинских формирований пришлось каким-либо образом регулировать или скрывать, по крайней мере, в «цивилизованной» Европе.

Впрочем, можно отметить, что близкие к современным proxy-составляющие конфликтов проявлялись и в достаточно отдалённое на историческом периоде время. Специалисты в области военной истории относят к ранним «гибридным» действия по подкупу рабов-илотов во время Пелопонесской войны 431-404 годов до н.э., римско-германские войны 12 года до н.э. - 12 года н.э, сопровождающиеся подкупом врагов и союзников, а также активными дипломатическими действиями, ряд других конфликтов той эпохи.

Кроме того, пусть и с некоторыми допущениями, proxy-действиями можно считать привлечение пиратов, нападавших на испанские суда, осуществляющие перевозки в Америку и за плату принятых в подчинение Британией. Известный пример действий таких

пиратов – периодические рейды кораблей Фрэнсиса Дрейка (*Francis Drake*) против испанского флота и побережья в период 1572-1596 годов, действия берберских пиратов в интересах Османской империи в XVI-XIX веках. Впрочем, на достаточно долгом историческом периоде такие действия являлись типичными и даже общепринятыми для proxy-действий на море. И применялись повсеместно, в том числе, в нашей стране. Достаточно вспомнить действия каперов на Балтике в период правления Ивана IV или отряда греческих пиратов Ламброса Кациониса (греч. Λάμπρος Κατσώνης) на Черном море в 1787-1792 годах.

Впрочем, всё это были отдельные слабосвязанные действия, имевшие общую цель при отсутствии координации. По мнению военных историков, первым вооруженным конфликтом, содержащим в себе признаки современных «гибридных» действий, явилась «Тридцатилетняя война» (*Guerre de Trente Ans*), проходившая в период 1618-1648 годов. Данная война, кроме того, что являлась последним крупным конфликтом с использованием наёмников, включала активное использование, пусть и на примитивном уровне, информационных и даже экономических методов противоборства.

В новейшей истории наиболее ранним из классических примеров proxy-войны с элементами «гибридных» действий, близких к современному пониманию этого явления, может служить гражданская война в Испании (исп. *Guerra Civil Española*), проходившая с июля 1936 по апрель 1939 года. Конфликт вёлся с привлечения сторонних вооруженных формирований и добровольцев, при внешнем соблюдении соглашения о «невмешательстве», подписанного большинством европейских держав. В отличие от ранее реализуемых proxy-войн, боевые действия сопровождались интенсивным информационным противоборством между мировыми социальными системами и масштабным набором экономических мер.

Начиная с того периода, любая война нового времени, в принципе, в той или иной степени является «proxy». Принятие этой гипотезы, позволяет сделать ряд значимых выводов. Например, «гибридным» можно считать начальный этап Второй Мировой войны. Приняв такое допущение, вполне обоснованное, дату её начала, в рамках восстановления исторической справедливости, вполне логично отсчитывать не с установленного сейчас 1 сентября 1939 года, а с 30 сентября 1938-го, когда, подписанием Мюнхенского соглашения, Великобритания и Франция, совместно с Польшей, приняли организационные меры «гибридного» воздействия, направив Германию на войну с СССР. Польша, при этом, не только дипломатическими мерами препятствовала проходу советских войск для помощи Чехословакии, но и сама поучаствовала в её разделе. В дальнейшем, рамках «гибридных» действий странам коллективного Запада пришлось, для формирования общей границы СССР и Германии, пожертвовать сначала целостностью Чехословакии, а потом существованием Польши, государства, которое от статуса участника так называемого «санитарного кордона» (фр. *cordon sanitaire*), созданного против СССР, на тот момент перешло в статус, в современной терминологии относящийся к категории «стран-брандеров». А можно, в развитие указанного вывода, отойти от «европоцентрического» взгляда на историю и начать отсчёт Второй мировой, начальный этап которой имел явно выраженный «гибридный» характер, с «инцидента на мосту Лугоуцяо» (кит. 卢沟桥) 7 июля 1937 года или даже с Мукденского инцидента 18 сентября 1931 года (кит. 九•一八事变), учитывая характер начальной стадии агрессии Японии против Китая с proxy-участием нескольких государств с каждой стороны. Правда, такой подход заставит пересмотреть взгляды на историю того времени, но он сделает её логичнее, включив, например, в структуру Второй Мировой войны боевые действия в Испании.

После Второй Мировой войны, масштаб proxy-войн как силового выражения «гибридных» действий не уменьшился, а силовая компонента по-прежнему составляла существенную роль в их структуре. Наёмничество было запрещено законами ведения войны [14], но и сейчас можно отметить факты использования наёмников, уже преимущественно в форме частных военных компаний (ЧВК), всё более активно используемых в современных «гибридных» конфликтах. Фактически, можно говорить о новом этапе наёмничества, легализованном в современных реалиях «гибридных» действий, коммерциализации права на насилие.

Напомним, что ЧВК на начальном этапе их использования представляли собой небольшие группы наёмников с лёгким вооружением, действующие на свой страх и риск. Существенные изменения в масштабах и правовых аспектах применения ЧВК произошли с появлением в 1989 году в ЮАР компании *Executive Outcomes*, потом её более эффективной преемницы, компании *Sterling Corporate Services*. ЧВК доказали свою эффективность и преимущество над «обычными» группами наёмников при решении задач в proxy-конфликтах, большую гибкость и универсальность применения. Существенную роль в этом сыграл целый ряд факторов:

- персонал ЧВК оказался более опытным в военном отношении, более подготовлен к работе с высокотехнологичным оружием, современными средствами разведки и управления, чем повстанческие или партизанские отряды. А учитывая резкий рост доли высокотехнологичного и высокоточного оружия в современных конфликтах [15], переход от просто высокоточных к боеприпасам, которые можно классифицировать как «избирательные» или «прецизионные», попадающие не просто в объект, а в конкретный его элемент с возможностью выбора траектории захода на цель, подготовленность и техническая грамотность персонала часто становится решающим фактором успеха боевых действий;

- ЧВК более организованы, мотивированы и управляемы, чем «обычные» наёмники;

- применяемые в настоящее время методы информационно-правового обеспечения действий ЧВК обеспечивают снижение сложившегося ранее негативного отношения к «гибридным» действиям, а также повышают правовую защищённость самих сотрудников ЧВК;

- финансирование ЧВК может осуществляться частными компаниями, снижая вероятность скрытия их действий в интересах того или иного государства;

- относительно ЧВК, в том числе с учётом предыдущего фактора, современное общество обладает более низкой чувствительностью к потерям, они не обычные военнослужащие, а «работники войны», их потери не так активно освещаются в прессе, на них не так активно реагирую обычные граждане.

В результате, в конце прошлого века количество ЧВК и масштабы их действий начали непрерывно расти, они стали одной из существенных составляющих всех типов конфликтов, включая «гибридные». Уже в операции «Буря в пустыне» (*Desert Storm*) ВС США начали активно привлекать ЧВК для решения боевых и специальных задач, по данным открытых источников, привлекалось несколько десятков тысяч сотрудников частных компаний. В последующих операциях ВС США в Ираке (*Shock and Awe, Iraqi Freedom*), Ливии (*Unified Protector*), Сирии (*Endurig Freedom*) и Афганистане (*Resolute Support Mission*), количество привлекаемых Департаментом безопасности США сотрудников уже превысило численность военнослужащих в группировках и составило

52% от всех сил. Более того, отмечаются факты привлечения ЧВК к решению несиловых задач, таких как информационное противоборство. Примером может служить привлечение компании *SOS International* к выполнению задач в рамках военно-информационного обеспечения боевых действий (*Military Information Support Information, MISO*) или частной компании *GDIT* (*General Dynamics IT*) для информационных атак на российский и китайские вакцины от ковид. Аналогичные тенденции наблюдаются и в армиях других, ведущих в военном отношении государств.

Исторический опыт показывает, что боевая ценность и статус частных военных формирований может меняться в широком диапазоне: от карательных батальонов с полицейскими функциями, характерных для незаконных формирований южноамериканских наркобаронов и латиноамериканских «эскадронов смерти» (исп. *los escuadrones de la muerte*), до полнофункциональных и самодостаточных крупных ЧВК. способных эффективно вести самостоятельные штурмовые действия с применением всех родов войск и видов вооружений. Впрочем, и те, и другие, как показали события 2014-2023 годов на Украине и 2023 года в России, довольно опасный инструмент, который государство должно держать под постоянным и эффективным контролем, не позволяя ему стать не только военной, но и политической силой.

В этом отношении весьма показателен опыт коммерциализации «гибридных» действий с привлечением повстанцев и ЧВК, отмечаемый в ходе гражданских войн 1990 – 2000-х годов на африканском континенте: в Либерии, Сьерра-Леоне и в Кот-д'Ивуаре. По итогу конфликтов в этих странах, иррегулярные группировки смогли обеспечить не только эффективную вооруженную борьбу, но и целенаправленные экономические и политические действия, приводившие, в результате, к смене власти. Пусть эта смена была временной, важна сама тенденция коммерциализации и расширения действий ЧВК из военной сферы в политическую.

В любом случае, процесс привлечения к ведению «гибридных» действий различных ЧВК активно продолжается и расширяется, меняя тем самым структуру, облик и распределение задач «гибридных» сил.

В то же время, несмотря на всю эффективность, использование ЧВК является не единственным примером трансформации силовых действий «гибридного» характера в наше время. Другим вариантом, например, является поддержка антиправительственных вооруженных формирований внутри страны-противника, многие из которых действуют методами, противоречащими международным законам ведения войны, а то и просто террористическими. Примером может служить создание США для противодействия сначала СССР, а потом просоветскому правительству Афганистана движение Талибан (пушту طالبان — студенты, учащиеся медресе). Другой пример: создание и поддержка Западом сначала ливийской, а потом так называемой «сирийской умеренной оппозиции» (араб. المعارضة السورية), с той или иной степенью успешности противодействующих законно избранным правительствам данных стран, их вооруженным силам, используя террористические методы борьбы. Соответственно, использование подобных методов «гибридной» войны порождает ещё одну проблему – как противодействовать таким действиям, не переходя границ законности и не нарушая гуманитарных принципов ведения войны. С подобной проблемой столкнулась армия Израиля при проведении операции «Железные мечи» (ивр. מבצע חרבות ברזל,الحديدية).

2.Трансформация «гибридных войн» новейшего времени

Обобщая данные исторического анализа, можно сделать вывод, что большинство

конфликтов второй половины XX – начала XXI веков, обладает признаками «гибридности». Даже беглый анализ некоторых из них подтверждает указанный тезис:

- война в Индокитае 1945-1954 годов;

- война в Корее 1950-1953 года;

- война во Вьетнаме 1965-1975 годов;

- война за независимость в Эритрее 1961-1991 годов;

- война в Анголе 1975-2002 года;

- вооруженные конфликты в Афганистане 1979-1989 и 2001-2014 годов;

- война в Ливии 2011 года;

- ряд локальных конфликтов на территории бывших СССР и Югославии в период 1991-2021 годов;

- вооруженный конфликт в Сирии, начавшийся в 2011 году;

- неудачная попытка организовать «гибридные» действия Франции против Нигера силами наёмников и *ECOWAS* и другие конфликты разной степени интенсивности и успешности;

- экономические, информационные и дипломатические действия США против Ирана, осуществляемые в рамках «гибридной» войны с 1979 года, активизировавшиеся в 2023 году после начала силовых действий на территории союзного Ирану Йемена в рамках операции «Страж процветания» (*Operation Prosperity Guardian*);

- противоборство Ирана и Израиля, осуществляющееся как на территории третьих стран, так и проецированием силы с применением сторонних вооруженных формирований и религиозно-политических организаций, практически переросшее в «горячую» фазу в 2024 году;

- экономические и информационные действия в рамках «гибридной» кампании против Венесуэлы, сопровождающиеся локальными силовыми акциями (операция «Гедеон») и перешедшие в попытку «цветной» революции в 2024 году;

- масштабные «гибридные» действия, ведущиеся коалицией стран НАТО против России, ведущиеся с начала XXI века, включавшие информационные и экономические действия, попытки разной степени успешности организовать «цветные» революции на постсоветском пространстве и переходившие в фазу активного противоборства на территории Южной Осетии в 2008 году и на территории Украины и новых российских регионов в 2022 году.

По совокупности признаков, определёнными качествами «гибридного» конфликта, хоть и в мягком варианте, растянутом во времени, обладала «холодная война» (*Cold War*) 1948-1991 годов. С учётом этого, многие специалисты объединяют ведущиеся сейчас «гибридные» войны в единый процесс – так называемую «вторую холодную войну» (*Cold War* 2.0).

Опыт всех перечисленных конфликтов напоминает, что в структуре современных «гибридных войн», кроме силовой, существуют и играют существенную роль несиловые составляющие, иногда называемые «некинетическими формами воздействия» и

используемые, как до перехода противоборства в «горячую» фазу, так и после перехода, если его не удалось предотвратить: информационная, экономическая и организационная [16]. Ещё раз напомним, что, как показывает анализ исторической ретроспективы, соотношение между компонентами постепенно меняется в пользу несиловых, которые, впрочем, являются не менее опасными и разрушительными, как показал распад Советского союза и Югославии. Пока известно немного примеров достижения победы в «гибридных» войнах без использования явного силового противоборства, но они есть. Примером может служить уже упомянутый распад СССР.

Первые значимые проявления несиловых составляющих на исторической ретроспективе, как отмечено ранее, представляет история «Тридцатилетней войны», которая, наряду с многими другими изменениями в ведении боевых действий, показала значительное повышение интенсивности информационной составляющей противоборства и существенное расширение влияния военных действий на население и его экономический уклад. Хотя и на более раннем периоде, информационные действия в межгосударственном противоборстве использовались довольно активно. Наиболее известным примером этого считается деятельность ордена иезуитов (лат. *Societas Iesus*), основанного Римско-католической церковью ещё в 1534 году.

Несмотря на то, что ещё Платон утверждал «идеи правят миром» (греч. *Οι ιδέες κυβερνούν τον κόσμο*), с точки зрения технологий войны, информационная составляющая стала значимой частью «гибридных» действий с появлением и распространением печатного дела [17,18].

По мере развития коммуникационных технологий, разнообразие и объём информационных действий, реализуемых, в первую очередь, в форме явной и скрытой пропаганды, росли. Активной информационной составляющей отличалось ведение Наполеоновских войск, достаточно вспомнить попытки агитации казачества с целью убеждения, что казаки не принадлежат к русскому этносу и другие попытки использовать национальную карту в войне против России. Но наиболее яркие примеры этому можно найти в период подготовки и ведения Первой мировой войны: массовая публикация пропагандистских статей во французских и английских периодических изданиях, действия Комитета общественной информации (комитет Крила, *Creel Committee*) в США.

В дальнейшем, в годы Первой мировой войны, появившаяся фотография позволила публиковать в средствах массовой информации изображения с мест боёв. И если сначала этот процесс сдерживался принципами морали, не рекомендующими публиковать, например, фото убитых, то со временем необходимость повышения эффективности пропаганды взяла верх над нравственностью. В 1915 году англичане впервые использовали для пропаганды фото убитых солдат противника, их примеру последовали немцы, а впоследствии – другие участники конфликта. В голы Второй мировой войны к информационным средствам воздействия добавилось кино, как документальное, так и художественное. Война во Вьетнаме стала первым конфликтом эпохи телевидения, «шагнув с экранов почти в каждый дом» (*a living-room war*). В настоящее время, с появлением Интернета, видео с места боёв стало обычным явлением, вооруженная составляющая «гибридных» действий, стала вестись практически в прямом эфире и активно использоваться в информационной составляющей «гибридных» действий.

С появлением Интернета сформировался ещё один значимый фактор, влияющий на информационную составляющую - «гибридные» конфликты последних лет показали, что государственная монополия на информацию постепенно заканчивается и всё большее

влияние на информационное противоборство начинают оказывать интернет-сообщества (такие, как информационный проект *InfoDefense* или хакерская группа *Beregini*) и даже отдельные медийные лица, так называемые «лидеры общественного мнения» («ЛОМы»). Эту особенность необходимо учитывать при оценке информационной составляющей современных «гибридных» конфликтов.

В условиях современного «цифрового» мира информационное противоборство не просто выделяется в отдельную форму действий, оно подразделяется на составляющие: по объектам воздействия – информационно-техническое противоборство, действующее на технические и программные коммуникационно-управляющие системы и информационно-психологическое, направленное на сознание человека, как индивидуальное, так и общественное. По глубине воздействия, его иногда разделяют на немедленное и когнитивное, направленное на формирование долгосрочных воздействий. Есть и ряд других признаков, показывающих возрастающую сложность данного компонента «гибридных» войн – например, специалисты выделяют в них частные направления информационного противоборства, определяемые уровнем действий и объектами воздействия: психологические операции, война в медиапространстве, информационные операции, кибер-операции (или техносферная война). Для решения задач в рамках указанных форм действий создаются специализированные подразделения информационно-психологического противоборства [19], кибер-командования, такие, как американское *USCYBERCOM*. При этом в странах НАТО психологическая борьба и информационные операции считаются разными формами противоборства с различными целями и регламентируются разными документами. Ведение психологических операций регламентируется Полевым уставом *FM 33-1*, а информационное противоборство регулируется документами более высокого уровня *AJP-3.10* (*NATO Standard: Allied Joint Doctrine for Information Operations*) и *JDN 2/19* (*Joint Doctrine Note 2/19. Defense Strategic Communication: an Approach to Formulating and Executing Strategy*). Впрочем, с учётом влияния информатизации, психологические операции с 2010 года расширены до статуса информационных операций военной поддержки (*Military Information Support Operations, MISO*), а информационные операции разделены на военно-гражданские (*Civil-Military Operations*), операции в киберпространстве (Cyberspace operations), международные операции (*Multinational Information Operations*), оборонительную операцию по защите информационной инфраструктуры (*Information Assurance*) и другие. Выделение информационного противоборства в отдельную форму действий и его детализация подчёркивает возрастание важности этой компоненты, в том числе – в рамках «гибридных» действий.

Этот факт дополнительно подтверждается расширением сил и средств ведения информационного противоборства. Кроме штатных подразделений, возможностей которых не всегда хватает для решения растущего спектра задач информационно-психологических операций, применяется большое количество организаций, используемых скрытно, на коммерческой основе, как для ведения кибер-разведки, так и для выполнения других функций в рамках «гибридных» действий. По оценкам журнала *Newsweek*, только в США численность привлекаемых на такой основе специалистов на 2021 год составляет порядка 60 тысяч человек.

Впрочем, указанные факты меняют структуру привлекаемых к «гибридным» действиям сил, но не меняют сущности информационных действий в «гибридной войне». Отличия от ранее используемых методов заключаются, преимущественно, в применяемых технологиях, обеспечивающих использование современных методов социальной инженерии, повышению динамичности и масштаба воздействия, охвата целевой

аудитории [20].

Ещё один аспект современного информационного противоборства, точнее, как отмечено ранее, его информационно-технической составляющей, заключается в активном применении кибер-оружия. В условиях тотальной информатизации общества, его применением обеспечивается достаточно высокая эффективность воздействия на критические информационные и энергетические системы различных уровней, как военного, так и гражданского назначения. Учитывая критичную зависимость от информационных технологий всех сфер управления и жизнеобеспечения современных государств, программно-аппаратные средсва кибер-воздействия потенциально обладают разрушительными возможностями относительно вывода из строя инфраструктуры и экономики, близкими по последствиям к ядерному оружию. И, при этом, их применение не регулируется практически никакими международными актами, а доступность весьма высока: как для самостоятельной разработки, так и покупки или получения от третьих стран. Таким образом, кибер-оружие, средства программно-аппаратного воздействия на критические элементы инфраструктуры, становятся неким «оружием массового поражения для бедных», что делает эту составляющую «гибридных» войн весьма значимой и опасной.

С наступлением постиндустриальной эпохи, развитием «цифрового» общества, информационное противоборство дополнилось применением деструктивных социально-политических технологий [21]. Их разнообразие позволяет выстроить внутреннюю классификацию подобных воздействий: от простой финансовой и информационной поддержки оппозиционных течений и создания внутри государства-противника «пятой колонны», до операций по распространению влияния, обеспечивающих, в перспективе, так называемую «мягкую оккупацию» (*soft occupation*) страны и переход её под внешнее управление [22,23]. Одним из первых случаев применения подобных технологий на практике считается государственный переворот 1953 года в Иране (операция «Аякс» - *TP-AJAX*). В мягкой форме, например, в виде льготного обучения иностранных студентов, подобные методы использовали и используют все ведущие страны: США, Великобритания, СССР. Это может быть как обучение в ведущих ВУЗах страны, так и создание специальных заведений, таких, как швейцарская «Школа молодых глобальных лидеров» (*Young Global Leaders*). По опыту последнего времени, достаточно эффективной является программа обучения (*Strategic Leadership in Global Societal Security Programme, SLP*), адаптируемая и внедряемая в рамках когнитивной (ментальной) составляющей потенциальных «гибридных» войн в обучающие программы различных государств. В СССР для подобных целей был в 1960 году специально создан Университет дружбы народов (ныне РУДН).

В более интенсивной форме таких действий и сейчас активно развиваются организации, реализующие подобные технологии, такие, как американские «Национальный фонд в поддержку демократии» (англ. *National Endowment for Democracy, NED*), «Агентство международного развития» (англ. *United States Agency for International development, USAID*) и им подобные.

Обратной стороной «мягкой оккупации» можно считать оказание давления, а то и прямое устранение политиков и активистов в странах, с которыми ведётся «гибридное» противоборство. Причём вне зависимости уровня участия этих стран в «гибридных» действиях. Наиболее свежий пример – покушение на премьер-министра Словакии Роберта Фицо в мае 2024 года.

К квинтэссенции использования деструктивных социальных технологий можно отнести методы организации так называемых «цветных революций» (англ. *color revolution, flower revolution*), достаточное количество примеров которых можно привести за последние несколько десятилетий.

Очень плотно с информационной составляющей связано использование политико-дипломатических (организационных) методов обеспечения «гибридных» действий. Собственно, дипломатические действия всегда являлись составной частью межгосударственного противоборства в любой его фазе, обеспечивая поиск союзников, блокировку союзов противника и другие функции. В настоящее время, эти действия стали более активными и скоординированными с другими составляющими «гибридной войны». Одним из первых примеров нового подхода к ведению подобных действий в рамках «гибридного» противоборства можно считать создание в США Межведомственной рабочей группы в период операции «Буря в пустыне» 1991 года. Данная группа, включающая представителей вооруженных сил и МИД, обеспечивала оперативную координацию действий и информирование в нужном ключе союзников и Совбеза ООН.

Таким образом, информационная и организационная составляющие «гибридных» действий в современных конфликтах становятся всё более влияющими на их ход и исход. В этой связи можно перефразировать известное высказывание Клаузевица (нем. *Der Krieg ist eine bloße Fortsetzung der Politik mit anderen Mitteln*): уже не война становится продолжением политики другими средствами, а политика становится продолжением войны.

Специалистами выделяется ещё один важный аспект «гибридных» войн – их экономическая составляющая. В исторической ретроспективе её использование началось с переходом от обособленных национальных экономик к мировой системе хозяйствования, связанной с международной торговлей, а по мере глобализации экономики – и с межгосударственным разделением труда. На начальном этапе развития «гибридных» действий, экономическая война осуществлялась, преимущественно, в форме запретов на поставку или вывоз определенных товаров.

К ранним формам экономической составляющей «гибридного» противоборства можно отнести различные формы блокад, примеры которых в истории имеются в большом количестве. Впрочем, силовые блокады, это всё же ближе к военным методам противоборства. А вот другие, экономические неконкурентные меры борьбы, связанные с заградительными и протекционными мерами, возникли практически с появлением рыночной экономики. Примерами могут служить официальные выплаты Голландской Вест-Индской компанией в XVII веке дивидендов из выручки от добычи с захваченных иберийских кораблей, или так называемые Навигационные акты (*The Navigation Acts*) от 1651 года, Закон о шляпах (*Hat Act*) 1732 года, ограничивающий производство и экспорт шляп вне метрополии из-за конкуренции с английскими производителями, или британский Закон о железе (*Irton Act*), принятый в 1750 году с аналогичной целью в отношении сталелитейной промышленности в колониях. А суть Навигационных актов заключалась в том, что товары в Англию должны были доставляться исключительно английскими судами, что обеспечивало стимуляцию развития британского судостроения. Навигационные акты были отменены только в 1849 году, когда Британия стала мировым лидером морских перевозок. И перечисленное – лишь небольшая часть примеров: можно вспомнить регулирование английских тарифов на импорт с 1820 по 1876 год для противодействия Франции, или Имперские преференции: систему тарифов, применявшуюся с 1932 по 1947 год и обеспечивающую привилегированное положение Британии в торговле с колониями, другие акты экономического противоборства.

С развитием промышленности и международной торговли, глобализацией мировой экономики, формы экономического противоборства существенно расширились, начали применяться новые меры воздействия: товарные, сырьевые, технологические, финансовые [24]. Экономическое противоборство чаще всего реализуется в невоенной форме, в виде санкций, и продолжает оставаться активным инструментом «гибридного» противоборства. В период с 1971 года до конца XX века можно отметить применение около ста двадцати случаев санкций, в первую очередь в рамках экономической войны коллективного запада против СССР. В XXI веке указанный инструмент используется не менее интенсивно: от заградительных таможенных пошлин, до американских законов «О контроле над экспортом» и «О противодействии противникам Америки посредством санкций» (*Countering America's Adversaries Through Sanctions Act, CAATSA*) 2017 года [25]. Санкционные механизмы активно используются США и их союзниками до сих пор (рисунок 1), несмотря на меняющиеся геополитические условия. На рисунке 1 указано состояние на конец 2023 года, с того времени количество санкций только росло.

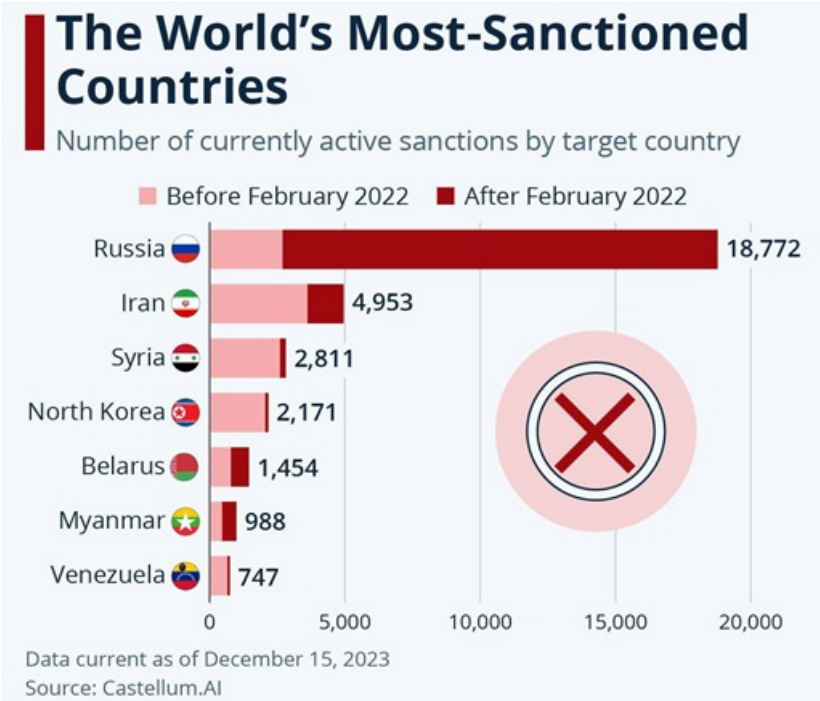

Рис. 1. Объём санкций, возлагаемых на разные страны по состоянию на конец 2023 года (с сайта www.statista.com)

Примером экономических «гибридных» действий в финансовой сфере могут служить блокировки зарубежных счетов Ирака в 2012 году, Венесуэлы в 2019, счетов банков и валютных запасов России в 2022 году, блокировка доступа иранских банков к системе *SWIFT* в 2018 году и российских в 2022 году.

В качестве одной из составляющих экономического противоборства, на которое воздействуют санкциями, можно выделить технологическое. Период снижения международной напряженности в конце XX, начале XXI веков породил иллюзию всеобщей безопасности и запустил процессы глубокого международного разделения труда. Это, с одной стороны, существенно повысило эффективность производства, с другой – породило опасность возникновения экономического коллапса в случае «гибридного» воздействия. Последнее не замедлило проявиться в ходе обострения мировых противоречий в 2014-2023 годах. Усиление запретов по программе *CAATSA* и правил экспортного контроля *(EAR)*, введение запретов на поставку и так называемый

«условный экспорт» (*deemed export*) технологий и готовой высокотехнологичной продукции из США и стран Евросоюза в Россию и Китай, породили достаточно большой пул проблем во всех областях экономики для всех противоборствующих сторон. Всем участниками процесса пришлось принимать срочные меры: введение «параллельного импорта», программ импортозамещения, поиск новых рынков сбыта, «откат» производства к более старым технологиям и т.п. Учитывая, что введение запретов куда как более быстрый процесс, чем их преодоление, технологическая составляющая экономической формы «гибридного» противоборства породила множество проблем и вопросов.

С точки зрения международной безопасности, одной из крупнейших проблем применения экономического противоборства в рамках «гибридных» действий различной интенсивности, является субъективность определения границы, на которой заканчивается конкуренция, добросовестная она или нет, и начинается экономическая война в целях нанесения ущерба государству-противнику или экономический терроризм, примером которого являются диверсии на трубопроводах «Северный поток» в 2022 году, попадающие под действие конвенции ООН «Международная концепция о борьбе с бомбовым терроризмом» № 52/164 от 16 декабря 1997 года (*International Convention for the Suppression of Terrorist Bombings*). Возникающая в результате неопределённость объективно может привести к переходу экономических «гибридных» действий на основе *casus belli* в классическую «горячую» фазу войны, как это уже было после введения нефтяных санкций США против Японии в июне-ноябре 1941 года.

Нельзя ещё раз не отметить ещё одну составляющую экономического противоборства, находящуюся на грани гуманитарно-допустимого – ресурсную.

Военная история позволяет отметить, что подобные действия когда-то относились к вполне легитимным формам вооруженного противоборства: блокады крепостей, запрещающие поставку продовольствия, перекрытие воды. Как и другие формы вооруженного противоборства, блокады до эпохи глобализации применялись в основном, в ходе «классических» военных действий. С момента становления и укрупнения государств, формирования разнообразных межгосударственных отношений, блокада стала одной из форм «гибридного» противоборства. А «классическая» осада, в отличие от экономической блокады, стала применяться намного реже. Хотя, при ведении войны «на уничтожение» (нем. *Totalen Krieg*), и в наше время совершались подобные нарушения общепринятых гуманитарных правил, достаточно вспомнить осаду Ленинграда или водную блокаду Одессы в годы Великой Отечественной войны.

В рамках «гибридного» противоборства подобные осадам городов ресурсные ограничения вновь находят применение, теперь в непрямой форме. Более того, с ростом технических возможностей и разнообразия экономических связей в современном мире, формы ресурсного противоборства меняются, реализуясь в виде транспортной, энергетической и даже как в доисторические времена – продовольственной и водной блокады. Типичные примеры последнего вида действий – попытка отвести воды реки Иордан от Израиля, послужившая одной из причин начала «шестидневной войны» 1967 года, морская блокада Палестины в 2010 году, или полная блокада Сектора Газа, осуществлённая тем же Израилем при проведении операции «Железные мечи». Ещё один современный пример – энергетическая и водная блокада Крыма, продолжавшаяся с 2014 по 2022 год, завершить которую удалось только силовым путём.

Всё это, разумеется, не просто меры экономического противоборства или санкции, это антигуманные действия, осуществляемые в непрямой форме, вкупе с другими

гибридными мерами. И напрямую противоречащие требованиям «Конвенции (IV) о защите гражданского населения во время войны» 1949 года. Как, впрочем, и большинство подобных мер, принимаемых ранее с целью воздействия на мирное население: неприцельные бомбардировки Дрездена и Кенигсберга, ядерные бомбардировки Хиросимы и Нагасаки. Как и современные экономические санкции, они были рассчитаны на изменение отношения населения противника к власти, создания условий её свержения. Впрочем, как показывает исторический анализ – эти меры бессмысленные, приводящие лишь к углублению страданий мирного населения, а в части отношений с собственной властью, часто имеющие обратный задуманному эффект.

Завершая обзор, можно отметить, что в настоящее время новые возможности в сфере «гибридного» противоборства могут открываться с развитием технологий, в том числе – с созданием новых видов оружия. Так, в настоящее время не подтверждено наличие у какой-либо стороны климатического или, например, тектонического оружия, хотя имеется определённая корреляция, находящаяся выше статистической погрешности, между землетрясениями нескольких последних десятилетий и конфликтами, происходящими в разных регионах. Неким аналогом климатического оружия, с определённой долей допущения, можно считать перехват Израилем дождевых облаков над своей территорией и принудительная инициация осадков, что вызывало неоднократные протесты арабских стран и Ирана, до которых дожди не доходили.

Иногда упоминаемая в связи с разработкой климатического оружия американская программа *HAARP* (*High Frequency Active Auroral Research Program*), судя по всему, является лишь экспериментом, без подтверждённых практических результатов воздействия на климат, да и сама разработка такого оружия запрещена «Конвенцией о запрещении военного или любого иного враждебного использования средств воздействия на природную среду» ООН от 1976 года. Но, при наличии подобного оружия, которое принято определять как геофизическое, оно могло бы стать идеальным «гибридным» средством экономического и когнитивного противоборства, разрушающим системы жизнеобеспечения и промышленные объекты, ухудшающим условия жизни населения, без раскрытия явного источника воздействия [26]. И ещё из области «теории заговора»: эффективным средством ведения «гибридных» действий может быть и биологическое оружие, тайное применение модифицированных версий которого, нацеленного на поражение заранее заданных генотипов людей, открывает широкие перспективы таких войн, действуя в современных условиях не только на население, но и на экономику противника. Впрочем, явных доказательств наличия и применения указанных средств в современной истории нет.

Таким образом, исторический анализ «гибридных» действий, в том числе, принадлежащих к новейшей истории, позволяет сформулировать ряд выводов:

- теория и практика ведения «гибридных войн», как средства разрешения конфликтов, не военное «ноу-хау», а давно используемая форма решения геополитических проблем, объединяющая признаки классических proxy-войн, комплексного «гибридного» противоборства и «оффшорного балансирования» (англ. *Offshore balancing*), которая в изменившихся условиях современного мира используется достаточно активно и, вероятно, будет с всё возрастающей интенсивностью использоваться впредь. Современные концепции вооруженного противоборства США и НАТО, такие как «Дистанционные боевые действия» (англ. *Remote Warfare*), «Бой в многодоменном пространстве» (англ. *Multidomain battle*), рекомендации Консультативного совета по международной безопасности (англ. *International Security Advisory Board - ISAB*)

Федерального консультативного комитета США по действиям в «серых зонах» (англ. *Gray zone - GZ*), наглядно подтверждают предыдущий тезис;

- отдельные, в первую очередь несиловые, составляющие «гибридных» действий могут использоваться обособленно, не приводя к явной конфронтации, в «гибридную» войну ситуация переходит только при комплексном их применении;

- в то же время, содержание «гибридных войн» в современных условиях смещается в сторону применения невоенных методов противоборства, при этом как разрушительные последствия, так и опасность последних, переход при их использовании от «гибридного» конфликта в «горячую» фазу, в условиях глобализации современного мира возрастает.

С учётом последнего фактора – опасности перерастания «гибридной» войны в «горячую», а также с учётом постоянного повышения всеобщей информационной осведомленности, любые гибридные действия в настоящее время превращаются в балансировку на грани «фола». История, начиная с эпохи Наполеновских войн и до нашего времени, показывает, что неосмотрительные действия с высокой вероятностью приводят к разжиганию конфликта и переходу его в «горячую» фазу со всеми вытекающими последствиями.

3. О перспективах развития «гибридного» противоборства

Проведённый исторический анализ не просто позволяет сделать вывод о том, что история не чисто теоретическая наука, исследующая прошлое, а эффективный инструмент, обеспечивающий получение и оценку практических рекомендаций: он позволяет выявить некоторые закономерности в части развития теории «гибридных войн» и выработать рекомендации по парированию «гибридных» угроз.

Главный вывод из исторического анализа – учитывая неоднократно отмеченную опасность перерастания «гибридной» войны в «горячую», необходимо прогнозировать последствия предпринимаемых действий. Наиболее объективным инструментом для такого прогноза специалистами считается математическое моделирование. Анализ исторического опыта позволяет, как вариант, сформировать обобщённую модель оценки интенсивности «гибридной» войны. Структура модели может определяться перечнем составляющих «гибридного» противоборства и привлекаемых сил.

Структуру такой модели можно считать условно постоянной:

- вооруженная составляющая;

- информационные действия;

- экономическое противоборство;

- организационные меры.

В качестве математического аппарата для моделирования всех составляющих противоборства может быть использована интерполяция функций на основе ранее полученной статистики. Очевидно, что такая модель корректно работает только на непрерывных функциях, неточно реагируя на их разрывы, которые могут случаться, например, в ситуации революционных изменений. Впрочем, ни один существующий матаппарат, за исключением аппарата теории устойчивости, не обеспечивает работу с функциями, имеющими разрывы. Но искать точки бифуркации на системах, описанных с грубой детализацией, характерной для описания глобальных систем и процессов – дело неблагодарное. Поэтому приходится довольствоваться возможным, а именно аппаратом

на основе временных рядов.

Отображение результатов моделирования может быть реализовано в форме «тепловой» матрицы (рисунок 2). Интенсивность каждой составляющей определяется привлекаемыми силами и совершаемыми ими действиями. А общая интенсивность «гибридных» действий определяется совокупной «температурой» матрицы действий, формируемой с учётом весовых коэффициентов каждой составляющей.

Вооруженная составляющая			
Поддержка вооруженной оппозиции внутри страны-противника	Военно-техническая помощь, предоставление разведданных	Привлечение наёмников и коммерческих ЧВК	Задействование своих войск и сил
Информационная составляющая			
Когнитивные действия по формированию положительного своего облика	Когнитивные действия по формированию отрицательного облика потенциального противника	Целенаправленные информационные действия в СМИ и социальных сетях	Проведение информационных и психологических операций
Экономическая составляющая			
Принятие внутренних экономических и технологических ограничений	Блокирование доступа к технологиям, введение внешних санкций	Блокирование доступа к счетам, мировым сервисам и технологиям	Блокада
Организационная составляющая			
Создание политических союзов	Дипломатические меры воздействия: протесты, заявления	Юридические действия по формированию судебных решений в рамках обеспечения противоборства	Создание вооруженных союзов и коалиций, блокирование союзников

Рис. 2. Модель «гибридных» действий, вариант представления выходной информации в виде матрицы составляющих (вариант)

«Температура» каждой из составляющих может формироваться как по внешним признакам, получаемым на основе анализа текущей обстановки (см. рис. 1), так и по состоянию противоборствующей стороны, определяемому исходя из нормативов зарубежных армий. Например, в части информационного противоборства, эти нормативы определяются уровнями информационной войны и составом привлекаемых сил (включая необходимость задействования Госдепартамента или МИД), указанных в документе «Открытые психологические операции, проводимые Вооруженными силами в мирное время и в особой обстановки незадолго до объявления войны» (*Department of Defense Directive S-3321.1, Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War*).

Использование подобной, либо любой другой модели с соответствующим набором исходных данных для неё позволит проводить оценку текущей интенсивности «гибридных» действий и, главное, прогнозировать тенденцию их развития.

Кроме формирования предложений по описанию модели, исторический анализ позволяет сформулировать ряд закономерностей, характерных для данной формы противоборства.

Во-первых, учитывая развитие этой формы противоборства, нелогично признавать «гибридную войну» принципиально новым способом разрешения политических конфликтов. Хотя название это появилось относительно недавно, сам принцип ведения «гибридных» действий используется довольно давно, сначала в форме proxy-войн, ибо практически в любом вооруженном конфликте кроме двух заинтересованных сторон в том или ином виде присутствует как минимум, третья. В дальнейшем, с развитием информационной и экономической составляющих, для решения геополитических проблем стали применяться методы относительно несилового «оффшорного балансирования», в том числе, реализуемые технологиями создания «дуг нестабильности» (англ. *Arc of Instability*), а позже, с объединением, развитием и усилением всех составляющих этих концепций, такие действия стали называть «гибридными».

Современным развитием «гибридных» действий можно считать так называемую «умную силу» (англ. *Smart Power*) – концепцию, комбинирующую в себе все формы «гибридных» действий и, по сути, являющуюся высшей формой их развития, обеспечивающей максимальную реализацию принципов минимизации усилий, прилагаемых для достижения цели. Данному виду действий пока нет официального определения, хотя большинство специалистов, такие как *Joseph S. Nye, Chester A. Crocker, Fen Osler Hampson, Pamela R. Aall* и другие, в целом описывают «умную силу» как комплексное и длительное применение всех составляющих «гибридных» действий, обеспечивающее достижение поставленной цели, но с уровнем воздействия, не допускающего перехода в фазу прямого вооруженного конфликта.

Во-вторых, так как «гибридная война» является логичным развитием proxy-войн, как реакция на информатизацию общества и глобализацию экономики, логично предположить, что этот исторический процесс не остановится, «гибридное» противоборство будет развиваться и активно использоваться. Это предположение подтверждают попытки создания очередной «дуги нестабильности» вокруг России, осуществляемой США в последние полтора десятилетия: от применяемых ранее процессов создания относительно безопасной «тлеющей» зоны нестабильности, виден переход к раскачке ситуации для создания «государств-брандеров», способных «раскачать» ситуацию у соседей. Вероятно, развитие и трансформация форм «гибридного» противоборства продолжится, например, с учётом возможностей, порождаемых «цифровизацией» экономики. Каким образом и какую роль сыграют изменения, предположить сложно. Но прогнозировать и готовиться к новым угрозам необходимо, для чего нужно вести дальнейшие исследования данного процесса, совершенствовать тактику противодействия «гибридным» действиям [27].

В-третьих, на исторической ретроспективе мало менялся принцип, но существенно изменились применение и структура участвующих в «гибридных» конфликтах «гибридных сил», произошло их своеобразное «расслоение». Слабо подготовленные в военном отношении, но приспособленные к району ведения боевых действий формирования по-прежнему формируются на основе «туземных» армий или набираются из местных ополченцев. А подготовленная к ведению современной войны компонента, роль которой постоянно возрастает: технически оснащённые и обученные силы специальных операций

и всё более активно привлекаемые ЧВК, авиация, в том числе беспилотная, космическая разведка – предоставляются скрытыми участниками конфликта и, чаще всего, базируются вне театра военных, действуя в «серых зонах».

В рамках этой же тенденции, для руководства «гибридными» действиями создаются специализированные органы управления, временные, но на профессиональной основе и с высокотехнологичным оснащением, такие, как многодоменные оперативные группы (англ. *Multi-DomainTask Force - MDTF*), создаваемые в рамках концепции *Civil Military Cooperation (CIMIC)* и в соответствии с наставлением ВС США по взаимодействию*Joint Publication (JP)*, военно-гражданские администрации в местах ведения конфликтов.

Эти факты в очередной раз подтверждают, что в странах НАТО воспринимают повышение активности использования «гибридных» действий и сил не как случайный процесс, а как тенденцию, которая может изменить подходы к геополитическому противоборству в будущем, кадры и технические средства управления для которой нужно готовить заблаговременно.

В-четвёртых, важным фактором является то, современные «гибридные» действия, особенно их несиловые составляющие, расширяются в пространственной области, вовлекая не только участников конфликта, но и сторонние государства, не позволяя практически никому остаться непричастным. Особенно это заметно в информационной и экономической составляющих. Привлечение может осуществляться путём убеждения и принуждения (в терминологии руководящих документах НАТО:*persuasive communications or coercive force*), например, введением так называемых «вторичных санкций». Привлечение к информационному противоборству может также осуществляться введением в заблуждение с использованием источников информации с неявной принадлежностью. Последнее наглядно проявлялось в ходе «гибридных» действий против России, а также при реализации информационной составляющей боевых действий в Секторе Газа в 2023 году. Указанные факторы требуют учёта как в развитии теории «гибридного» противоборства, так и непосредственно в практике управления им.

В современном мире, в условиях тотальной информатизации и «гиперподключения», когда у каждого человека имеется постоянный доступ к мобильным устройствам приема, формирования и передачи информации, возможности по ведению информационных действий возросли кратно. Сложившаяся ситуация требует не только совершенствования методов информационного противоборства, но и развития мер противодействия: как ограничения подачи информации противником и соблюдения мер «цифровой гигиены», так и выработку своеобразного «информационного иммунитета» у населения, защищающего и позволяющего критически воспринимать фейковую информацию. Эта задача нетривиальная, но без её решения победа в современных «гибридных» действиях невозможна.

В-пятых, «гибридные» войны, как и «классические», редко начинаются внезапно. Из-за структуры и особенностей отдельных составляющих, они чувствительны к ранней подготовке и очень инерционны в части ведения – большинство составляющих «гибридных» действий являются долговременными, часто срабатывают в отдалённой перспективе. Этот фактор влияет двояко: с одной стороны, необходимо предпринимать ряд мер противодействия «гибридному» противоборству заранее, с другой – на длительном периоде планирования тяжело обеспечивать приемлемую величину доверительной вероятности эффективности реализации применяемых мер.

Примером необходимости заблаговременной подготовки, может служить экономическая

составляющая войны против Ливии, Сирии, России, когда блокирование государственных и частных финансовых активов готовилось заранее, а сделано было, когда противостоять этим действиям было уже поздно. При таком раскладе, если подвергающаяся «гибридному» воздействию сторона будет выжидать с ответной реакцией до наступления последствий, действия реактивно, она однозначно опоздает с ответом. Соответственно, и противодействовать таким воздействиям нужно начинать заранее, обеспечив переход от использующихся сейчас реактивных методов управления противоборством к проактивным, основанным на прогнозировании и долгосрочном планировании. Не менее наглядным подтверждением данного тезиса являются и так называемая «ментальная война» [11] и технологическое противоборство, осуществляемые в рамках организационной и экономической составляющей «гибридных» действий соответственно. Анализ показывает, что даже в эпоху глобализации и взаимовыгодного международного распределения труда, может возникнуть ситуация быстрого прекращения использования технологий и поставок высокотехнологичной продукции, порождающая комплексные проблемы, обладающие кумулятивным эффектом.

С учётом перечисленных факторов, для обеспечения высокой вероятности реализации принимаемых мер, необходимо как повышать точность планирования действий, так и расширять спектр принимаемых мер, обеспечивающих гарантированную реализацию хотя бы части из них.

Относительно последнего примера – для любой крупной экономики, желательно прогнозировать и быть готовым к критической ситуации: развивать собственные технологии, пусть и менее эффективные, чем покупные, диверсифицировать поставки, обеспечивая их из заведомо некоррелируемых источников, предпринимать другие меры. Разумеется, эти меры требуют затрат и снижают текущую прибыль, но безопасность никогда не была дешёвой.

В-шестых, кроме длительности реализации действующих факторов «гибридной» войны, она отмечается существенной асимметричностью применяемых мер, что определяется сложной структурой данной формы противоборства. Соответственно, фактор асимметричности, наряду с инерционностью действий, необходимо детально учитывать при планировании действий. В этой асимметрии наиболее опасными представляются несиловые методы противоборства, в том числе потому, что меры борьбы с ними ещё недостаточно отработаны. Впрочем, это можно сделать, например, ориентируясь на методики их организации. Для информационных, например, на положения методик по организации «цветных революций» [20].

Принятие правильных решений способствует победе, цена ошибки очень высока и может быть исправлена только за счёт больших затрат. Наглядный пример, подтверждающий данный тезис, привёл в одном из своих интервью академик РАН С.Ю.Глазьев: Россия с 1991 по 2014 год вложила в экономику Украины около 30 миллиардов долларов, пытаясь наладить взаимодействие, а США в сопоставимый период потратили порядка 5,4 миллиардов для информационного воздействия на население страны и подготовку её будущих управленцев антироссийской направленности. Результат известен. Чтобы подобная ситуация не повторялась, необходим набор определённых инструментов: планирующих методик, средств прогнозирования и математического моделирования и других, создание которых должно являться предметом научного исследования [28].

Седьмое, несмотря на все новации, в «гибридной» войне, как и в «классических»

боевых действиях, победа решается на поле боя. Но, учитывая, что силовая составляющая, это тактика, а не стратегия конфликта, нельзя не вспомнить высказывание Клаузевица: «Стратегические просчеты невозможно компенсировать тактическими успехами»: победа, по-прежнему, достигается на поле боя, но обеспечивается она действиями в тылу, как своём, так и противника. То есть, данный тезис в современных условиях приобретает новое звучание. Учитывая это, для достижения победы, крайне важным является целенаправленное и скоординированное использование несиловых составляющих «гибридного» противоборства [29, 30]. Именно эффективное управление является залогом успешных действий в любой сфере деятельности [31], и управление военными действиями не является исключением. Этот фактор необходимо учитывать при подготовке и ведении «гибридных» действий. И, в этой связи, возрастание уровня «гибридности» в современных конфликтах, высокая вероятность сохранения этой тенденции в будущем, требует изменений в военной науке и образовании. Как с точки зрения разработок методов и моделей комплексного исследования компонентов «гибридных» действий, так и обучения особенностям их ведения будущих командиров и начальников. Ведущие военные державы в полной мере озаботились этим вопросом, примером чему может служить создание при Министерстве обороны США Центра изучения иррегулярных военных действий (*Irregular Warfare Center, IWC DOD*), организация Европейского центра противодействия «гибридным» угрозам (*European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE*) и других им подобных.

В нашей стране, в рамках этого процесса Минобрнауки включило в учебный процесс некоторых ВУЗов (Севастопольский университет, РГСУ, МИРЭА) дополнительные курсы по подготовке специалистов по «гибридным» войнам. В 2022 году в программу факультета политологии МГУ вошел магистерский курс «Информационные и гибридные войны». Впрочем, при всей своевременности указанных мер, перечисленные курсы направлены, преимущественно, на изучение информационной составляющей «гибридных» действий для подготовки политологов, журналистов или специалистов по кибер-безопасности, а не на системное изучение этого явления в целом и придание процессу подготовки системного характера. Кроме того, это достаточно небольшие по объёму обучающие курсы, что не идёт ни в какое сравнение с объёмом преподавания особенностей «гибридного» противоборства в ведущих зарубежных странах. Для сравнения, по данным агентства «Р-Техно», по состоянию на 2023 год в США реализуются 36 программ по подготовке специалистов по «гибридным» конфликтам, в Китае 28, в Индии 14, в странах Евросоюза суммарно 9, а в Великобритании – 3.

И последнее, применение «гибридных» методов приводит к существенной трансформации структуры противоборства за счёт расширения использования условно несиловых методов, что приводит к расширению перечня явных и скрытых участников конфликта, вовлечению в конфликт негосударственных структур и межгосударственных корпораций, изменению объектов воздействия, размыванию границ и этапов развития конфликта. Особенно опасно то, что одновременно с усилением в структуре «гибридных» войн информационной и экономической составляющих, происходит рост участия в них негосударственных организаций, своеобразный «аутсорсинг насилия».

Эти факторы приводят к тому, что к невозможно оценивать «гибридные» конфликты на основе существующего международного законодательства. И если для proxy-участия в конфликтах существуют международные нормативные акты, пусть и не всегда применяемые, например, «Парижский договор об исключении войны в качестве оружия национальной политики» (пакт Бриана-Келлога 1928 года, *Kellogg-Briand Pact*) и

Будапештская резолюция к этому пакту от 1934 года, для остальных составляющих «гибридных» действий подобных документов пока не существует. В то же время, как показывает исторический опыт, большинство «гибридных» конфликтов, если их не предотвратить, рано или поздно переходят в активную фазу и становятся классическими войнами. Более того, несиловые методы «гибридных» действий, как показывает исторический опыт, периодически применяются целенаправленно для активации вялотекущего конфликта и привлечения новых участников, намеренного перевода его в силовую фазу.

Для предотвращения подобных ситуаций, имеется необходимость уточнения законодательства о военных конфликтах в части предотвращения «гибридных» действий на ранних стадиях. В первую очередь, это должно быть обеспечено даже не столько в военной сфере, сколько в части трансграничных и экстерриториальных форм несиловых «гибридных» действий: информационного и экономического противоборства, организационных методов действий. Для таких форм необходимо или законодательно отказываться от принципа экстерриториальности некоторых институтов, либо узаконить экстерриториальность ответа на них. В рамках регулирования таких действий, требуется чётко определить границы перехода от экономической конкуренции, через «недружественные действия» экономического и юридического характера, к экономической войне, как составной части «гибридной войны». Аналогичные границы должны быть установлены в информационном пространстве. И хотя большинство государств понимает важность этого процесса и принимает определённые меры информационной защиты, такие как российский Федеральный закон от 14 июля 2022 г. №255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием» или белорусский Закон «Об изменении Закона Республики Беларусь "О средствах массовой информации"» 2023 года, эти меры представляются неполными. Если считать «гибридные» действия войной, то и реагировать необходимо на них как на вооруженное нападение: жестко, не оглядываясь на принципы мирного времени.

В рамках решения указанных проблем, необходима юридическая регламентация деятельности в техногенном сегменте кибер-сферы, в процессах экономического взаимодействия, организация ряда других мер: как в части разработки регламентирующих документов, позволяющих вывести участников противоборства из «серых зон», так и создания международных органов контроля и регулирования кибер-сферы и процессов экономической конкуренции, подобных созданным сейчас в сфере применения ядерной энергии (МАГАТЭ,*International Atomic Energy Agency - IAEA*) или запрещения химического оружия (ОЗХО,*Organisation for the Prohibition of Chemical Weapons - OPCW*). Важность законодательного регулирования несиловых составляющих «гибридных» действий показывает отношение основных бенефициаров этой формы противоборства к мерам противодействия внешним информационным воздействиям и действиям внутренней оппозиции, чаще всего тоже координируемой извне. Одним из первых примеров законодательного противодействия в современной истории можно считать немецкий «Закон против вероломных нападок на государство и партию и защите партийной униформы» 1934 года (нем. *Gesetz gegen heimtückische Angriffe auf Staat und Partei und zum Schutz der Parteiuniformen*) . Современные апологеты таких действий продолжают разрабатывать подобные акты, например, законы об иноагентах, активно применяемые у них (закон США *Foreign Agents Registration Act, FARA*) и недопускаемых к принятию в других странах.

Более того, в рамках совершенствования международного законодательства, может потребоваться уточнение самого понятия «агрессия», определяемого Резолюцией

Генеральной ассамблеи ООН от 14 декабря 1974 года № 3314 как «применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций». Это, впрочем, относится и к другим международным законодательным актам, регулирующим поведение в кибер-пространстве, международное экономическое взаимодействие и конкуренцию, поставки вооружений и множество других нерешенных проблем, которые могут служить потенциальными источниками активизации конфликтов.

Заключение

Как показал исторический анализ, «гибридные» действия прошли долгую историю развития: от простых «операций под чужим флагом» (*false flag operation*) и proxy-войн на тактическом уровне, до методов «оффшорного балансирования» на глобальном, их компоненты развивались от разобщённо используемых методов пропаганды и блокадных действий в рамках экономической войны, от использования «мягкой силы» (*soft power*) до перехода к «умной силе», в рамках которой объединяются все формы «гибридного» противоборства. Несмотря на длительный период использования, современное международное сообщество оказалось не вполне готово к их ведению: особенности «гибридных войн», возросшая частота использования данной технологии противоборства, исторически высокая вероятность перехода «гибридного» конфликта в «классическую» войну, требуют адекватной реакции на геополитические процессы, например, уточнения международных и внутренних концептуальных и планирующих документов, регулирующих области, в которых могут быть реализованы «гибридные» действия.

Но, главное, исторический анализ показывает, что «гибридная» война - системный процесс и выиграть, или хотя бы не проиграть в ней, можно только действуя системно.

Библиография

1. Liddel Hart B.H. Strategy The Indirect Approach. New-York: Pentagon Press, 1954. 560 p.
2. *Samuel P. Huntington.* The Clash of Civilizations and the Remaking of World Order. 1996. 353 p.
3. James N. Mattis, Frank Hoffman, Future Warfare: The Rise of Hybrid Wars. Proceedings Magazine. 2005, Vol. 132/11/1,233 URL: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (13.09.2022).
4. Kandrik M. Rethinking Russian Hybrid Warfare // IWC Perspectives. 2023. May. pp. 1-4. URL: https://irregularwarfarecenter.org/wp-content/uploads/2023-05-17-Perspectives_No_7_Rethinking-Russian-Hybrid-Warfare.pdf (12.08.2023).
5. Williamson Murray, Peter R. Mansoor. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. – Cambridge University Press, 2012.
6. Манойло А.В. Цветные революции в контексте гибридных войн // Право и политика. 2015. № 10. С. 1400-1405.
7. Fox A. C., Rossow A. J. Making. Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo–Ukrainian War (англ.) // The Land Warfare Papers. 2017. Март (№ 112).
8. Roger N. McDermott. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Centre for Defence and Security. Tallin. 2017 – 48 с.
9. Boda M. Hybrid War: Theory and Ethics. Academic and Applied Research in Military and Public Management Science. 2024, 1(23): 5-17. DOI: 510.32565/aarms.2024.1.
10. Caliskan Murat. Hybrid warfare through the lens of strategic theory. Defense & Security

Analysis 2019. Vol.35, pp. 40-58.
11. Ильницкий А.М. Ментальная война России // Военная мысль. 2021. № 8. С. 19-33.
12. Богатырёв В.В. Проблемы международно-правового регулирования современных гибридных войн // Вестник владимирского юридического института. 2021. № 2 (59). С. 34-38.
13. Першин Ю.Ю. Гибридная война: неуловимые армии и невидимые руки // Вопросы безопасности. 2020. № 2. С. 48-71. DOI: 10.25136/2409-7543.2020.2.32680 URL: https://e-notabene.ru/nb/article_32680.html
14. Международная конвенция о борьбе с вербовкой, использованием, финансированием и обучением наемников. Принята резолюцией 44/34 Генеральной Ассамблеи от 4 декабря 1989 года. Официальный сайт ООН. URL: http://www.un.org/ru/documents/decl_conv/conventions/mercen.shtml (21.01.2021).
15. Литвиненко В., Долматов В. Высокоточные артиллерийские средства огневого поражения // Армейский сборник. 2023. № 7. С. 26-33.
16. Тиханычев О.В. «Гибридные» войны: история, современное состояние, основы противодействия // Национальная безопасность / nota bene. 2019. № 1. С. 39-48. DOI: 10.7256/2454-0668.2019.1.28100 URL: https://e-notabene.ru/nbmag/article_28100.html
17. Симонов А. Информационная война Запада против Ивана Грозного // Военное обозрение. URL: https://topwar.ru/102277-informacionnaya-voyna-zapada-protiv-ivana-groznogo.html (19.10.2016).
18. Мальцев Д. «Черные мифы» о русских царях // Русская народная линия URL: http://ruskline.ru/monitoring_smi/2012/05/31/chernye_mify_o_russkih_caryah (31.05.2012).
19. Выпасняк В.И., Тиханычев О.В., Гахов В.Р. Кибер-угрозы автоматизированным системам управления // Вестник Академии военных наук. 2013. № 1 (42). С. 103-109.
20. Joint Pub 3-13 «Information Operations», DOD US, December 1998. URL: http://www.c4i.org/jp3_13.pdf (11.11.2009).
21. Sharp Gene. The Politics of Nonviolent Action. Boston, MA: Porter Sargent. 1973. 72 p.
22. Harsin Jayson. "Regimes of Posttruth, Postpolitics, and Attention Economies". Communication, Culture & Critique. 2015. 8(2), 327-333.
23. Parmar Inderjeet. "US Presidential Election 2012: Post-Truth Politics." Political Insight 3#2 (2012): 4-7.
24. Денежное обращение России: Исторические очерки. Каталог. Материалы архивных фондов: в 3-х томах / Банк России; [ред. совет: Г.И. Лунтовский, А.Н.Сахаров, А.В.Юров]. М.: ИНТЕРКРИМ-ПРЕСС, 2010.
25. Бокарев Ю.П. СССР и становление постиндустриального общества на Западе, 1970–1980-е годы / Ю.П. Бокарев; ИРИ РАН. М.: Наука, 2007. – 381 с.
26. Ginestet Andres. Climate-security nexus: System Theory of Violence and Complexity Architecture. COBAWU Institute, Wuppertal, Germany, February15th-November 2019. 8 p.
27. Бартош А.А. Модель гибридной войны // Военная мысль. 2019. № 5. С. 6-23.
28. Глазьев назвал стратегическую ошибку России: США увели из-под носа. Сайт «Царьград» URL: https://tsargrad.tv/news/glazev-nazval-strategicheskuju-oshibku-rossii-ssha-uveli-iz-pod-nosa_690034 (22.12.2022).
29. Манойло А.В. Информационные диверсии в конфликте на Украине // Вестник Московского государственного областного университета. 2022. № 4. URL: https://doi.org/10.18384/2224-0209-2022-4-1130 (31.08.2023).
30. Бартош А.А. Модели эскалации современных военных конфликтов // Военная мысль. 2024. № 1. С. 21-36.
31. Тиханычев О.В., Тиханычева Е.О. Информатизация как путь от искусства управлять к науке управления // The Scientific Heritage, 2020. № 1 (46). С. 58-63.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

В конце XIX в. многие философы, писатели предполагали, что двадцатый век обойдется без войн и катаклизмов. Действительность оказалась иной: в прошедшем столетии произошли две мировые войны, массовые гонки вооружений, создание сверхсовременного оружия и т.д. К сожалению, опыт говорит о том, что без армии не возможно обеспечить безопасность государства. В этой связи вызывает важность изучение различных угроз национальной безопасности, среди которых важное место занимают гибридные войны.
Указанные обстоятельства определяют актуальность представленной на рецензирование статьи, предметом которой являются гибридные войны. Автор ставит своими задачами рассмотреть исторический опыт "гибридных действий",
оценить современное состояние и перспективы развития «гибридного противоборства», структурировать существующие проблемы и обозначить возможные пути их решения.
Работа основана на принципах анализа и синтеза, достоверности, объективности, методологической базой исследования выступает системный подход, в основе которого находится рассмотрение объекта как целостного комплекса взаимосвязанных элементов.
Научная новизна статьи заключается в самой постановке темы: автор на основе различных источников стремится охарактеризовать историю развития «гибридных» действий от войн «под чужим флагом» до «умной силы».
Рассматривая библиографический список статьи как позитивный момент следует отметить его масштабность и разносторонность: всего список литературы включает в себя свыше 30 различных источников и исследований. Несомненным достоинством рецензируемой статьи является привлечение зарубежной англоязычной литературы, что определяется самой постановкой темы. Из привлекаемых автором источников укажем на интернет-ресурсы и нормативно-правовые акты. Из используемых исследований отметим труды такого военного теоретика как Б. Лиддел-Гарт, а также исследования А.В. Манойло, Ю.Ю. Перкинс, А.М. Ильницкого, в центре внимания которых находятся различные аспекты изучения феномена гибридных войн. Заметим, что библиография обладает важностью как с научной, так и с просветительской точки зрения: после прочтения текста статьи читатели могут обратиться к другим материалам по её теме. В целом, на наш взгляд, комплексное использование различных источников и исследований способствовало решению стоящих перед автором задач.
Стиль написания статьи можно отнести к научному, вместе с тем доступному для понимания не только специалистам, но и широкой читательской аудитории, всем, кто интересуется как феномен гибридных войн, в целом, так и отдельные составляющие, в частности. Апелляция к оппонентам представлена на уровне собранной информации, полученной автором в ходе работы над темой статьи.
Структура работы отличается определенной логичностью и последовательностью, в ней можно выделить введение, основную часть, заключение. В начале автор определяет актуальность темы, показывает, что гибридная война "до сих пор не признана в официальных оборонных концепциях большинства современных государств, хотя её, как показывает исторический анализ, неоднократно применяли и применяют для решения задач как вооруженного противоборства, так и глобального цивилизационного противостояния". Автор обращает внимание на то, что "гибридные» действия прошли долгую историю развития: от простых «операций под чужим флагом» (false flag operation) и proxy-войн на тактическом уровне, до методов «оффшорного

балансирования» на глобальном". Примечательно, что как отмечает автор рецензируемой статьи, "несмотря на длительный период использования, современное международное сообщество оказалось не вполне готово к их ведению: особенности «гибридных войн"... требуют адекватной реакции на геополитические процессы, например, уточнения международных и внутренних концептуальных и планирующих документов, регулирующих области, в которых могут быть реализованы «гибридные» действия".

Главным выводом статьи является то, что

«гибридная» война - системный процесс и выиграть, или хотя бы не проиграть в ней, можно только действуя системно".

Представленная на рецензирование статья посвящена актуальной теме, снабжена 2 рисунками, вызовет читательский интерес, а ее материалы могут быть использованы как в учебных курсах, так и в рамках разработки военно-политических стратегий.

В целом, на наш взгляд, статья может быть рекомендована для публикации в журнале "Национальная безопасность / nota bene".