DOI 10.35775/PSI.2025.76.11.001

УДК 32

А.В. ЛОМТЕВ
кандидат политических наук, доцент
кафедры политологии Института истории и политики
Московского педагогического государственного
университета, Россия, г Москва

ОСОБЕННОСТИ МЕР ПРОТИВОДЕЙСТВИЯ «ГИБРИДНЫМ ВОЙНАМ» В СОВРЕМЕННОЙ РОССИИ

На сегодняшний день для обозначения современной войны получил распространение термин «гибридная война», который в течение последних трех десятилетий употреблялся в оборонном сообществе. Официальное значение гибридная война приобрела после отражения в основных стратегических документах НАТО, ЕС и национальных правительств, став своеобразной стратегической теорией, в основе которой лежат определенные способы ведения военных действий, которые предполагают выбор и реализацию определенных мер противодействия, которые становятся особенно актуальными для России на фоне противостояния с западным миром. Автором выделяются военные и невоенные меры противодействия, а также обосновывается необходимость построения системы информационного противоборства внешним воздействиям и институционализированной организационно-аналитической системы по управлению программами и мероприятиями противоборствующего характера.

Ключевые слова: *гибридная война, Россия, меры противодействия, стратегическая теория, НАТО, ЕС.*

Гибридные войны подразумевают агрессивное поведение активных акторов их ведения во всех базовых видах политических пространств государств-мишеней (экономического, политического, социального, информационно-кибернетического, информационно-идеологического и географического) с использованием разнообразных специфических технологий и методов. При этом, военные методы, как правило, уступают невоенным по соотношению 1 к 4.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 6; 7; 8; 11; 12; 16; 17; 18].

Однако проблему разработки мер по противодействию гибридным войнам в Российской Федерации нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Гибридные войны могут предполагать отрицаемую или скрытую деятельность, которая поддерживается обычными или при такой возможности ядер-

ными силами, для оказания влияния на внутреннюю политику стран-мишеней. Гибридную агрессию можно подразделить на три категории: ненасильственная подрывная деятельность, поддерживаемая подрывная деятельность, обычные военные действия и скрытые насильственные действия. В любом случае данное явление связано с динамизмом, высокой сложностью и широким спектром применяемых стратегий [4. С. 245-254].

Для ведения любой войны нужны политическая цель и стратегия, которая может быть сопряжена с военными и невоенными способами ее ведения. Гибридная война может одновременно и в любых сочетаниях быть информационной, кибер-войной, когнитивной, финансово-экономической, политическим и военно-политическим противостояниями, «цветной революцией», вооруженным конфликтом жесткой силы («hard power») ассиметричного и/или симметричного плана, сетевой или сетецентрической войной, прокси-войной и т.д.

Особенностью гибридной войны является то, что никаких сдерживающих факторов в поведенческой сфере как морального, так и правового характера акторов-агрессоров в этой войне нет, поскольку на первое место встает результат подобной активности, сопряженной с психологической ожесточенностью, вызванной реальной опасностью утраты геополитического статуса с его ресурсами экспансии, мощью и возможностями. При этом перспективы проведения подобной войны заявляются странами во всеуслышание. Так, согласно официальным положениям Оперативной концепции армии США «Победа в сложном мире 2020-2040 гг.» (AOC) [21] американская армия готова к ведению гибридной войны.

Поэтому на первый план выходит поиск и нахождение приемов, средств, технологий и методов противостояния атакам противника-агрессора в рамках войн гибридного характера, как в военной сфере, так и невоенной.

В качестве **невоенных методов противостояния** специалисты предлагают, в первую очередь, создать систему оперативного «стягивания» в самых угрожаемых участках, а именно фронтах экономической и информационной войны (в частности когнитивной и кибервойны) наиболее значимых ресурсов и усилий.

В частности, в качестве мер противодействия выступают: 1) налаживание кибербезопасности наиболее значимых инфраструктурных объектов; 2) мониторинг и проведение непрерывных разведывательных действий в тесном взаимодействии с управленческими политическими и военными структурами для оперативного формирования и применения на угрожаемом направлении создавшегося преимущества; 3) пополнение резервов качественных кадровых ресурсов, которые могут наладить приготовление и выполнение стратегии предупреждения и противостояния технологиям и методам гибридных войн [3]; 4) подготовка национальной стратегии контргибридной войны, что особенно актуально для стран постсоветского пространства, в том числе и России; 5) разработка системы противодействия на общегосударственном уровне в отношении гибридных операций, направленных против населения и руководства страны; 6) формирование в армейской структуре спецслужб подразделений и национальных сил специальных операций для собственного ведения психологических и информационных мероприятий; 7) разработка национального законодательства

по предупреждению и пресечению реализации гибридных технологий и методов, прежде всего «цветного» характера; 8) обнаружение, блокирование и диагностика работы отрицательных блогеров и коммуникаторов, пытающихся ущемить национальный информационный суверенитет; 8) ведение постоянного мониторинга социальных сетей и блогосферы для своевременной блокировки отрицательных информационных ресурсов, связанных с подстрекательству к терроризму и экстремизму, розни межконфессионального и межнационального характера; 9) превентивная блокировка организационных, финансовых, информационных и иных каналов и структур элитарной (олигархической) и внешней (иностранной) помощи экстремистски и радикально настроенной оппозиции в стране; 10) активизация международного сотрудничества и информационного обмена с союзниками в финансово-экономической, информационно-психологической и военно-силовой областях для обеспечения возможности принятия своевременных мер по обнаружению и устранению угроз национальной безопасности [13. С. 60-65].

Показателен в этом отношении опыт самих США. Так, при Министерстве обороны США работают контркиберразведка, Объединенное командование структурных компонентов сетевых боевых действий (Join Functional Component Command — Network Warfare) по подавлению вражеской активности в электронных и интернет-сетях и Объединенная группа по операциям в глобальной Сети (Join Task Force — Global Network Operation), охраняющая сети компьютеров Пентагона.

В Европе к схожим структурам по охране от кибер-атак и промышленного шпионажа наиболее значимых IT-систем европейских государств, в частности Германии, относятся специально созданный в Бонне Федеральный центр кибер-защиты (Cyberabwehrzentrum) и Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency).

Для предупреждения киберактивности извне в США реализуется программа специального характера Digital Outreach Team, бойцы которой занимаются устранением информации отрицательного характера об Америке.

В качестве способов информационного противоборства используются информационно-технические и информационно-психологические средства, которые предполагают ведение стратегического анализа и собственного информационного воздействия и противодействия.

Информационно-технические средства противостояния включают защиту информационно-технических систем, прежде всего: систем защиты информации и передачи данных.

Информационно-психологические средства противостояния включают защиту психики населения и политэлиты уязвимой страны, создание системы формирования сильного национального общественного сознания, мнения и независимого справедливого принятия решений на всех уровнях власти и управления.

В России, например, целям информационной защиты служат мессенджер MAX, а также блокировка популярных в мире сайтов и сервисов.

Интересен опыт Китая, где под предводительством ШеньВей Гуана в 1998 году был разработан и в 2003 году введен в работу проект «Золотой щит» или «Великий китайский файрвол» (The Great Firewall of China), представляющий собой систему интернет-фильтрации, блокирующей доступ из внешнего интернета к ресурсам, которые запрещены коммунистической партией, как на территории страны, так и с иностранных сайтов. Исключением пользуются специальные административные районы Макао и Гонконг. Кроме того, китайские веб-сайты без специального одобрения не могут размещать и давать ссылки на новостные материалы с иностранных новостных контентов или массмедиа.

Проект является одним из 12 значимых проектов в области электронного правительства (e-governement). К данному проекту относятся подсистемы: информирования о правонарушениях (刑事 案件 信息 系统), информационного мониторинга (监管 员 信息 系统), управления трафиком (通 管理 信息 系统) контроля ввода и выхода (出入境 管理 信息 系统) и управления безопасностью (治安 管理 信息 系统) [20. С. 91].

Китайская информационная фильтрация (цензура) в социальных сетях подразумевает не тотальное устранение общественной или политической критики, а препятствование ее разрастанию в массовое движение или выступление, включая подобную активность виртуального характера. Методы «Золотого щита» сводятся к следующим: фильтрация DNS-запросов с последующей переадресацией и фильтрация на этапе пересылки пакетов, блокировка подозрительных IP-адресов, интернет-адресов (URL), а также соединений, проводящихся через VPN.

В России основы системы информационного противоборства внешним воздействиям, которая смогла бы адекватно и эффективно работать на глобальном, национальном, групповой и индивидуальном уровнях, а также организационно-аналитической системы (ОАС) по управлению проводимыми программами и мероприятиями противоборствующего характера на различных уровнях стали закладываться с 2012 года.

Разработчиком данных систем выступил профессор Игорь Панарин, являющийся основоположником теории информационных войн в России. По его мнению, основы российской информационно-идеологической доктрины лежат в утверждении государственной идеологии (ДДД — духовность, державность и достоинство) и создании специального аналитического инструмента организационно-управленческого и информационного характера для успешного развития российской государственности,

Система информационного противоборства по И. Панарину включает в состав не только государственные, но и частные структуры, и объединяет пять структурных элементов (политических институтов): 1) Государственный Совет при Президенте РФ по информационно-идеологической политике, в состав которого входят представители всех фракций Государственной Думы РФ, органов исполнительной власти, бизнеса и гражданского общества; 2) Советник Президента РФ по вопросам информационного противоборства; 3) Государственный интернет-холдинг; 4) Внешнеполитический государственный медиа-холдинг, подотчетный Президенту РФ и занимающийся созданием положительного образа страны на мировой арене; 5) Комитет информационной безопасности РФ, учрежденный

совместно Администрацией Президента РФ с Правительством РФ, информационно-разведывательными структурами, а также ведущими государственными массмедиа и частными, включающий подразделения информационного реагирования (Информационный спецназ): Службу информационной контрразведки, Службу информационной безопасности, Бюро информационного спецназа и Ситуационный Центр анализа и прогноза.

При этом основной стратегической задачей Комитета информационной безопасности РФ выступает установление ведущих центров ведения против России информационной войны и разработка ответных мер, исходя из опыта Сирии, Ливии и Южной Осетии [15].

Идею учреждения Информационного спецназа, как стратегической разведки информационного характера, работающей в глобальном информационном масштабе по прогнозированию реальных и потенциальных угроз стране, была предложена И. Панариным еще в 2003 году [14]. Однако практическое воплощение она получила в США еще при президентстве Дж. Буша.

На практике 07 сентября 2018 года в Москве была создана Ассоциация «Информационный Спецназ» [22], а в 2021 г. военными экспертами для информационного противоборства в медиапространстве было предложено сформировать киберспецназ [23].

Реализация поставленных целей и задач предполагает проведение научно-просветительской работы, в частности для обмена информацией и ситуационных анализов с проведением экспертных опросов в рамках организации круглых столов и международных конференций, обучающих семинаров в интересах осуществления целей ООН, к которым относятся согласно Уставу ООН: поддержание безопасности и международного мира, подавление агрессивных актов, устранение и предотвращение угрозы миру, урегулирование международных споров мирными средствами, укрепление между нациями отношений дружественного характера на основе уважения принципа самоопределения и равноправия народов; осуществление международного сотрудничества в гуманитарных, экономических, культурных и социальных сферах, развитие и поощрение уважения к основным свободам и правам человека без различия пола, расы, религии и языка [19].

В рамках нейтрализации целенаправленного и системного масштаба мероприятий гибридного характера И. Панарин предлагает учреждение Бюро контргибридной войны [13. С. 60-65] наподобие сформированному в декабре 2015 г. американскому Бюро противодействия гибридной войне (Hybrid warfare resistance Bureau), которая официально позиционируется как общественная организация, хотя и не имеет своего сайта, распространяя информацию посредством социальных сетей [5].

По мнению ряда специалистов, военными мерами противодействия для государств-объектов гибридной агрессии могут служить: освоение современных средств связи и высокоточного оружия, сбалансированное развития разведки, всех родов и видов сил (войск), РЭБ и автоматизированного управления, увеличение мобильности средств и сил для своевременных войсковых перегруппи-

ровок для переброса в удаленные районы, решительная и быстрая реакция на конфликтные ситуации, нелинейность которого ведет к получению результативных итогов наряду с малыми возмущающими воздействиями [3; 10].

Так, например, для предупреждения сетецентрических приемов ведения гибридной войны специалистами предлагается формирование сверхнадежной среды коммуникации в рамках глобальной информационной сети вооруженных сил страны, способной защитить военные компьютерные сети, использование в рамках объединенной сети малозаметных для противника, управляемых, надежных, информативных и долговечных средств разведки, работа с программной средой распределенного характера, которая способна в режиме реального времени многоуровневую комплексную интеллектуальную обработку потоков довольно противоречивых и малоинформативных первичных сведений о тех или иных проявлениях объектов. В качестве более приземленных мер предлагается: переход вплоть до батальона в тактическом звене на «ручное» управление вместо копирования сетецентрических систем противника и разработка образцов кратковременного воздействия по выводу на определенный срок из строя средств противника [9. С. 3-8].

Последние асимметричные приемы на практике имели воплощение в 1999 г. в Югославии, когда применялось новое оружие в виде электромагнитных бомб со сверхмощным электромагнитным импульсом. Те же бомбы использовались в 2003 году в Ираке при нанесении США и Великобританией ударов по объектам Багдада.

Специалисты также не обходят стороной и правовой аспект гибридных технологий и методов, поскольку к ним не применяются современные международно-правовые нормы, в частности, дающие содержательные характеристики термина «агрессия» или применяющие к конфликтной ситуации термины «тыл» и «фронт» [3]. В данных условиях государство-объект агрессивных гибридных действий испытывает значительные трудности для их адекватного и своевременного отражения.

В целом к невоенным средствам противостояния гибридным методам и технологиям можно отнести: оперативное системное «стягивание» наиболее значимых ресурсов и усилий в самых опасных зонах, прежде всего экономическом и информационном фронтах, подготовка стратегии контрмер, информационный мониторинг и проведение непрерывных разведывательных действий, пополнение резервов качественных кадровых ресурсов, формирование в армейской структуре спецслужб подразделений и национальных сил специальных операций, разработка национального законодательства предупредительного и пресекательного характера, просветительская работа с населением (повышение информационной грамотности), превентивная блокировка и информационная цензура (фильтрация DNS-запросов с последующей переадресацией и фильтрация на этапе пересылки пакетов, блокировка подозрительных IP-адресов, интернет-адресов (URL), а также соединений, проводящихся через VPN) опасных или сомнительных организационных, финансовых, информационных и иных каналов и структур, международное сотрудничество и информационный обмен с союзниками в фи-

нансово-экономической, информационно-психологической и военно-силовой областях.

К невоенным методам можно отнести: формирование сверхнадежной среды коммуникации в рамках глобальной информационной сети вооруженных сил страны, объединенной сети малозаметных для противника, управляемых, надежных, информативных и долговечных средств разведки, работа с программной средой распределенного характера, учитывающей противоречивую и малоинформативную информацию, «ручное» управление в тактическом звене использование новейшего оружия для эффекта устрашения и т.д.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
2. **Алаудинов А.А.** Современные подходы ведения гибридных войн США, Великобритании, Франции, Германии // Вопросы национальных и федеративных отношений. 2024. № 3.
3. **Бартош А.** Гибридная война становится новой формой межгосударственного противоборства // Военное обозрение. 9 апреля 2017 г. // https://topwar.ru/112955-gibridnaya-voyna-stanovitsya-novoy-formoy-mezhgosudarstvennogo-protivoborstva.html.
4. **Бистрина М.Г., Иванников А.А.** Гибридные войны: современные вызовы и перспективы // Вестник Российского университета дружбы народов. Серия: государственное и муниципальное управление. 2025. Т. 12. № 2.
5. Бюро противодействия гибридной войне // Hybrid warfare resistance Bureau: [ФБ-аккаунт] // https://www.facebook.com/hwrbureau/.
6. **Власов М.С.** Особенности информационного противостояния России и США в гибридной войне // Вопросы национальных и федеративных отношений. 2024. № 3.
7. **Гавров С.Н.**, Еремкин М.П. Использование искусственного интеллекта в контексте информационной войны // Вопросы политологии. 2025. № 2.
8. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
9. **Дульнев П.А., Ковалев В.Г., Ильин Л.Н.** Асимметричное противодействие в сетецентрической войне // Военная мысль. 2011. № 10.
10. **Комлева Н.А.** Гибридная война: сущность и специфика // Известия Уральского федерального университета. Сер. 3: Общественные науки. 2017. Т. 12. № 3 (167).
11. **Медведев Н.П.** Неклассические войны: современные подходы к ведению гибридных войн. Часть II // Вопросы политологии. 2025. № 2.

12. **Муравых А.И., Никитенко Е.Г., Стародуб И.В.** Интегральная мировая война (Часть 1) // Вопросы политологии. 2025. № 3.
13. **Панарин И.Н.** Гладиаторы гибридной войны // Экономические стратегии. 2016. № 2.
14. **Панарин И.** Информационная война и Третий Рим. М.: Поколение, 2006.
15. **Панарин И**. О создании Информационного спецназа России // Военное обозрение. 1 марта 2012 // https://topwar.ru/11908-igor-panarin-o-sozdanii-informacionnogo-specnaza-rossii.html.
16. **Скворцов Я.Л., Казарян Г.И., Курилкина Е.А.** Гибридная война: информационные стратегии НАТО и вызовы для России // Вопросы политологии. 2024. № 8.
17. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
18. **Сурма И.В.** Взаимодействие государств-членов Шанхайской организации сотрудничества в области международной информационной безопасности // Евразийский Союз: вопросы международных отношений. 2025. № 5.
19. Устав ООН: официальный сайт Организации Объединенных Наций // https://www.un.org/ru/sections/un-charter/chapter-i/index.html.
20. Goldsmith Jack L., Wu Tim. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press, 2006.
21. The US Army Operating Concept (AOC): Win in a Complex World 2020-2040. 7 October 2014 // http://www.tradoc.army.mil/tpubs/pams/TP525-3-1.pdf.
22. www.infospecnaz.org.
23. https://tass.ru/armiya-i-opk/10791933.

A.V. LOMTEV

Ph.D. (Candidate of Political Sciences),
Associate Professor at the Department of
Political Science of Institute of History and Policy
of Moscow State Pedagogical University,
Moscow, Russia

FEATURES OF MEASURES TO COUNTERACT «HYBRID WARS» IN MODERN RUSSIA

Today, the term «hybrid warfare» has become widespread to refer to modern warfare, which has been used in the defense community for the past three decades. Hybrid warfare acquired official significance after being reflected in the main strategic documents of NATO, the EU and national governments, becoming a kind of strategic theory based on certain methods of warfare, which involve the selection and implementation of certain countermeasures that become especially relevant for Russia against the background of confrontation with the

Western world. The author highlights military and non-military countermeasures, as well as substantiates the need to build a system of information warfare against external influences and an institutionalized organizational and analytical system for managing programs and activities of an adversarial nature.

Key words: *hybrid warfare, Russia, counteraction measures, strategic theory, NATO, EU.*