МРНТИ 17.03.02
https://doi.org/10.56132/2791-3368.2024.2-49-01

К.Ж. Койчыкулов[1], К.В. Федосеенко[1], И.В. Зарубин[1]

[1]*Военный институт Сухопутных войск имени С. Нурмагамбетова, Алматы, Казахстан*
*(E-mail: koichkulov bk ru.)**

“Гибридные войны” в XXI веке: социальные и политические аспекты

В данной статье исследованы тактика и противодействие, используемые противоборствующими сторонами в ходе подготовки и ведении гибридной войны, а также описана суть и их содержание. Установлено, современные формы конфликтов, в которых применяются различные сочетания военных, информационных, экономических и политических методов. Авторы обращают внимание на влияние таких войн на социальные и политические процессы в современном мире, а также на их последствия для глобальной безопасности и стабильности. Статья также рассматривает возможные стратегии противодействия гибридным войнам и необходимость развития международного сотрудничества для их предотвращения.

В дополнение к этому, предложены рекомендации по противодействию гибридным угрозам и организации противодействия в случае развязывания гибридной войны в современных реалиях.

Ключевые слова: гибридная война, стратегия, контрстратегия, информационная пропаганда, кибератаки, пропаганда, дезинформация.

Введение

В последнее время заметно активизировалась дискуссия о реализации принципов, так называемых гибридных войн, как одного из новых способов межгосударственного противоборства. Существует несколько определений этой формы вооруженного противоборства. «Гибридная война» (или гибридные вооруженные конфликты) (англ. hybrid warfare) представляет собой форму агрессии, при которой нападающая сторона избегает традиционного военного вторжения и вместо этого использует такие методы, как скрытые операции, диверсии, кибервойна, а также оказание поддержки повстанцам, действующим на территории вооружения [1].

В международном варианте иногда можно встретить такое определение: «Гибридная война — это совокупность совмещение открытых и скрытых военных операций или действий, провокаций и диверсий, при этом страна агрессор умышленно отрицает свою причастность, что позволяет эффективно реагировать на эти действия» [2].

В предисловии справочника Military Balance подробно описана «гибридная» война, описывающая использование объединенных военных и невоенных методов в единой стратегии, направленной на преодоление

неожиданностей, инициативных захватов, а также достижение психологических преимуществ с использованием экономических мер; проведение масштабных и быстрых операций в информационной, электронной и кибернетической среде; выяснить прикрытия и скрытность военных и разведывательных действий совместно с учетом экономического давления.

Постановка проблемы. На сегодняшний день существуют различные способы, которые противник может использовать для развязывания военного конфликта против государства в современных условиях. Это и подготовка, поддержка так называемой «цветной революции провоцирования», поддержка внутреннего вооруженного конфликта и проведение агрессии под прикрытием «миротворческой операции» [3]. В то время как большинство государств стремятся разрешить конфликты с помощью политических и дипломатических средств, военная сила все еще остается одним из возможных аргументов для разрешения межгосударственных и внутригосударственных противоречий путем осуществления комплексных мер военной организации государства по защите страны [4] от гибридной агрессии.

Цель статьи. Определить на системной основе особенности гибридных войн в современном мире, которые представляют сложную и многогранную угрозу, которая требует комплексного и инновационного подхода к противодействию, для анализа и разработки инновационных стратегий в области национальной безопасности.

Методы исследовании

В данном исследовании была применена методологическая основа, включающая системный подход, а также принципы историзма и объективности. Системный подход позволил провести анализ предмета исследования, учитывая взаимосвязь и взаимозависимость его элементов. Принцип историзма обеспечил учет исторического контекста и развития предмета исследования во времени. Объективность, в свою очередь, гарантировала беспристрастность и точность результатов исследования. Комбинация этих методологических подходов и принципов позволила провести всесторонний и глубокий анализ, а также получить объективные и надежные результаты.

Данный подход также обеспечил возможность разбить процесс анализа и понимания природы возникновения и ведения гибридных войн на отдельные этапы. Чтобы добиться поставленной цели, авторы статьи использовали методы сравнительного анализа и обобщения. Эти методы позволили сопоставить различные случаи и ситуации, выявить общие закономерности и различия. В качестве источников информации для исследования были использованы исторические документы, которые находятся в открытом доступе. Это обеспечило доступ к широкому спектру

данных и материалов, что позволило провести всесторонний анализ и обеспечить объективность исследования.

Изучив опыт прошлых войн и вооруженных конфликтов, мы пришли к выводу, что угроза гибридных войн является очень актуальной в современных условиях и сохранится в будущем. Кроме того, было определено, что в будущем могут возникнуть и другие виды гибридного противостояния, которые имели место в прошлом, но будут адаптированы к новым реалиям современности. Это включает в себя использование цифровых технологий, искусственного интеллекта, а также высокотехнологичного оборудования и вооружения. Таким образом, для эффективного противодействия гибридным угрозам необходимо постоянно следить за тенденциями развития технологий и адаптировать свои стратегии и тактику.

Результаты и обсуждение

Новые концепции и способы ведения гибридной войны в настоящее время развиваются очень быстро, что требует пересмотра классических военных методов прогнозирования и планирования как наступательных, так и оборонительных стратегий. Как и всякая другая война, гибридная война представляет собой область недостоверного и неопределенного. Основываясь на недостоверных данных и в условиях постоянных случайных вмешательств, стороны конфликта могут обнаружить, что их исходные предположения о соперничающей стороне, о собственных ресурсах и возможностях оказались далеки от реальности. Это может привести к ошибочным оценкам и стратегиям, основанным на неверных предпосылках.

В результате такой ситуации может возникнуть необходимость постоянно адаптировать свои планы и стратегии к изменяющейся реальности. Каждая сторона может оказаться на неизвестной территории, где нельзя полагаться на привычные шаблоны и планы, и приходится принимать быстрые решения на основе ограниченной и не всегда достоверной информации.

Таким образом, недостоверность информации и вмешательство случайностей играют значительную роль в конфликтах, заставляя стороны адаптироваться к изменяющейся реальности и пересматривать свои планы и ожидания. Эта динамика делает конфликты ещё более непредсказуемыми и сложными для участников [5].

Гибридная война представляет собой форму конфликта, в которой противоборствующие стороны используют различные методы и инструменты не только в военном, но и в политическом, экономическом, информационном и кибернетическом пространстве. В ходе гибридной войны регулярные вооруженные силы противоборствующих сторон часто сочетаются с нестандартными (неклассическими) действиями, такие как кибератаки, информационная пропаганда и другие тактики действий, для достижения своих целей.

Гибридная война часто характеризуется отсутствием явного объявления войны и использованием непрозрачных тактик. Цели и методы гибридной войны могут быть неясными, что делает противодействие еще более сложным на современном этапе.

Сочетание вооруженных и невооруженных действий в гибридной войне включает в себя использование классических военных действий, таких как боевые действия с применением оружия, а также невоенные методы, такие как пропаганда, кибератаки, информационные вмешательства и экономические санкции.

Гибридная война часто включает в себя использование негосударственных организаций, таких как террористические организации, незаконные вооруженные формирования или частные военные компании. Это позволяет государствам избегать прямой ответственности и создает дополнительные вызовы для сопротивления. Использование иррегулярных вооруженных организаций приводит к неясности и неопределенности, где деморализует повседневную жизнедеятельность государства.

Одним из основоположников концепции гибридной войны является крупнейший американский теоретик в области военно-политической стратегии, сотрудник министерства обороны США Ф.Г. Хоффманн. В своих работах он доказывает, что межгосударственные конфликты XXI в. имеют и будут носить мульти модальный и многовариантный характер, и представляют собой гибридное сочетание традиционных (конвенциональных) и иррегулярных (не конвенциональных) тактик, основанное на разнообразных простых и сложных технологиях [6].

Проводя анализ ведения гибридной войны на современном этапе, результаты показывают, что она становится все более распространенной и эффективной стратегией для достижения политических или военных целей. Она может быть использована для дестабилизации вражеских государств, разрушения их экономики, дезинформации общественности и вмешательства в их внутренние дела.

Традиционные методы военных действий могут оказаться неэффективными против невоенных действий, таких как кибератаки и информационная война. Необходимо разработать новые стратегии и тактику действий, чтобы эффективно противостоять гибридной войне.

Борьба с гибридной войной требует сотрудничества и координации между различными организациями и государствами. Это может быть сложно, учитывая различие в интересах и приоритетах участников конфликта.

Стратегический план политической борьбы в гибридной войне включает в себя комплекс разнообразных действий, с целью достижения политических целей в контексте конфликта, с использованием различных политических, информационных, экономических и культурных инструментов, для манипулирования общественным мнением, нарушение политической стабильности или оказание воздействия на противоборствующую сторону.

Политическая стратегия включает в себя следующие элементы:

- использование пропаганды и информационных операций для формирования определенного образа противника и управления общественным мнением;

- применение экономических санкций и финансового давления для ослабления экономической стабильности противника;

- проведение специальных военных операций, направленных на подрыв противника изнутри, включая поддержку оппозиционных группировок или провокации политического кризиса;

- использование кибератак для нанесения ущерба противнику в виртуальном пространстве.

Таким образом, целью политической стратегии в гибридной войне является достижение преимущества в конфликте или изменение политической ситуации в свою пользу. Часто применяется вместе с военными и информационными аспектами, чтобы достичь комплексного воздействия на противника.

Экономическая стратегия в гибридной войне подразумевает использование экономических инструментов и тактики действий для достижения политических целей и ослабления противника.

Рассмотрим следующие аспекты экономической стратегии при ведении гибридной войны:

- экономические санкции - применение ограничений и запретов на экономическое взаимодействие с противником с целью нанесения ущерба его экономике, например, запрет на торговлю, ограничения на инвестиции, замораживание активов и т.д.;

- финансовое давление - использование экономического влияния для ослабления финансовой системы противника. То есть, ограничение доступа к международным финансовым рынкам, блокировка банковских счетов или манипуляции с валютным курсом;

- экономический шпионаж - осуществление кибератак и хакерских действий для получения доступа к конфиденциальной экономической информации противника или воровства технологических разработок;

- финансирование оппозиции - поддержка оппозиционных группировок или экстремистских организаций в целях ослабления противника и создания внутренних проблем;

- экономическая пропаганда - использование информационных каналов и ресурсов для влияния на экономическое мнение и создания негативного образа противника.

Учитывая вышеперечисленные факторы, целями экономической стратегии в гибридной войне можно считать достижение экономического преимущества и ослабление противника, что в итоге должно способствовать достижению политических целей. Это служит дополнением к политическим, информационным и военным факторами гибридных операций.

Информационная стратегия в гибридной войне представляет собой использование информационных средств и тактики действий для достижения

политических целей и манипуляции общественным мнением. Она включает в себя следующие факторы:

- пропаганда и дезинформация – распространение ложной или искаженной информации для влияния на общественное мнение, создание стереотипов и формирование определенной позиции по отношению к конфликту или противнику;

- кибератаки и хакерские действия - злоупотребление информационными технологиями, в целях атаки на информационные системы противника, включая взлом, кибершпионаж, распространение вредоносных программ и т.п.;

- манипуляция социальными сетями - использование платформ социальных сетей для распространения информации, провокации конфликтов и манипуляции публичным мнением;

- манипуляция в СМИ - влияние на средства массовой информации с целью контроля или манипуляции сообщениями и освещения конфликта в пользу своих интересов;

- информационная поддержка операций - предоставление оперативной информации и координация информационных действий во время гибридных операций для достижения тактических и стратегических целей.

Фактор новизны современных тенденций становится все более очевидным в свете быстрого развития средств коммуникации, глобальной сети интернета и ее средств для мобилизации средств, а также расширения возможностей для ведения информационно-психологической войны. Например, во время Первой мировой войны использовалось всего 2 средства массовой коммуникации в этих целях, во Второй мировой войне их число возросло до 13, а во время конфликта в Персидском заливе (1991 г.) -25 и в ходе боевых действий на востоке Украины в нынешний момент – до 4011 СМИ [7].

Информационная стратегия в гибридной войне направлена на формирование образа противника, повышение собственной легитимности и ослабление противника с помощью информационных средств. Она важна для создания информационного преимущества и контроля над конфликтом.

Следующим элементом является военная стратегия, она включает в себя использование различных военных средств и тактики действий (боевых действий), которые дополняют политические, экономические и информационные факторы конфликта. Она включает в себя следующие аспекты:

- специальные операции - проведение секретных операций для получения разведывательной информации, дестабилизации противника и нанесения точечных ударов по важным целям;

- асимметричные методы борьбы - использование нестандартных военных действий (тактики) и методов для создания преимущества в неравных противостояниях, с использованием неправительственных сил и террористических групп партизанской войны, низкоинтенсивных конфликтов, террористических акций и поддержку прокси-войн;

- гибридные операции - комбинирование различных военных средств, тактики действий и новых технологий для создания комплексного и эффективного воздействия на противника, включая совместные операции с политическими, экономическими и информационными компонентами;

- психологическая война - использование психологических механизмов и тактики действий, для дезориентации противника и влияния на поведение его силовых структур и остального населения.

Военная стратегия в гибридной войне направлена на достижение военного превосходства и поддержку политических и других стратегических целей. Она требует интеграции различных военных и невоенных средств для достижения комплексного и гибкого воздействия на противника.

Защита национальной безопасности противоборствующей стороны направлена на максимальное снижение эффективности и результативности использования гибридной войны. Противодействие гибридной войне требует разработку мер по сокращению уязвимостей в политической, экономической, информационной и военной сферах, улучшение силовых структур и развитие специализированных умений и технологий для противодействия гибридным угрозам [8]. Однако, следует отметить, что гибридная война по своей природе является динамическим процессом, стратегии и противодействие могут эволюционировать и меняться в зависимости от развития ситуации.

Продолжая анализировать стратегии и противодействия в гибридной войне, можно углубиться в некоторые конкретные аспекты, которые оказывают существенное влияние в условиях гибридной войны:

1. Киберстратегия – это использование кибератак и хакерских атак для вторжения в системы противника, нарушения его сетевой безопасности и внедрения вредоносного программного обеспечения. Противодействием против киберстратегии является укрепление киберзащиты для предотвращения вторжений и сокращения уязвимостей в информационных системах.

2. Психологическая стратегия - использование противоборствующих сторон психологической войны для манипулирования психологическим состоянием соперника и населения, путем создания страха, паники и неуверенности среди населения противника через информационные операции. А также дестабилизация населения пограничных зон для создания противостоящих фракций и разделения общества.

Психологическая стратегия играет решающую роль в гибридных войнах, поскольку она направлена на воздействие на общественное мнение, убеждение и психологическое состояние населения. Основным направлением психологической стратегии в гибридной войне является дезинформация и манипуляция.

Враждебные субъекты могут распространять дезинформацию, фейки и манипулировать информацией, чтобы воздействовать на общественное мнение. В социальных сетях активно используются методы управления аудиторией с помощью алгоритмов, а также платные рекламные кампании.

3. Управление границами при гибридной войне и способы противодействия по ним играют ключевую роль в обеспечении безопасности и защите интересов государства. Управление границами представляет собой комплекс мер и действий, направленных на контроль, защиту и обеспечение безопасности государственных границ. Оно включает следующие факторы:

- государственный контроль - включает в себя усиление контроля над пограничными переходами, проверку документов и заявлений, а также обмен информацией с другими странами для обнаружения и предотвращения угроз;

- физическая безопасность - установка физических преград, таких как заборы, ограждения, барьеры, а также систем видеонаблюдения, радаров и датчиков для обнаружения незаконных пересечений границы;

- технологическое противодействие - использование передовых технологий в области радиолокации, дистанционного обнаружения, анализа данных и прогнозирования для обнаружения и предотвращения угроз;

- информационная борьба - использование информационных технологий, в том числе социальных сетей и средств массовой информации, для противодействия вражеской пропаганде и дезинформации;

- разведывательная деятельность - это сбор информации о потенциальных угрозах и противниках, анализ и оценка полученных данных для принятия решений;

- международное сотрудничество - включает в себя сотрудничество с другими странами для обмена информацией, координации действий и совместных операций по границам.

Для эффективного противодействия гибридной войне и обеспечения безопасности границ необходимо применять комплексный подход, включающий все описанные аспекты управления границами. Кроме того, важно развивать и совершенствовать эти меры в соответствии с изменяющимися угрозами и технологическими достижениями.

Наконец, для эффективного управления границами и противодействия гибридной войне также необходимо развивать специализированные кадры, проводить обучение и тренировки сотрудников на все более сложных и современных методах атаки и защиты.

4. Развитие эффективности систем силовых структур. Развитие силовых структур при гибридной войне требует особого внимания к адаптации и совершенствованию существующих методов и тактики действия [9]. Военные организации должны быть готовы к непредсказуемой природе гибридных войн, которые объединяют в себе как классические, так и нестандартные формы борьбы.

Один из способов совершенствования силовых структур при гибридной войне - это фокусирование на развитии и использовании новых технологий. К примеру, вооруженные силы могут инвестировать в разработку кибербезопасности и средств обнаружения и защиты от кибератак. Также важно развивать искусственный интеллект и автоматизацию, чтобы эффективно обрабатывать огромные объемы информации и быстро принимать решения.

Другой способ совершенствования - улучшение кадрового состава и обучение военнослужащих с учетом особенностей в условиях гибридной войны. Военнослужащие должны быть готовы к применению новых методов и тактик в борьбе с гибридными угрозами. Регулярное обучение и тренировки помогут сохранить высокую боеспособность военных структур.

Также необходимо улучшить международное сотрудничество и информационный обмен между союзниками и партнерами. В гибридных конфликтах часто применяется информационная война и дезинформация, поэтому важно иметь возможность оперативно обмениваться информацией и координировать действия для эффективной борьбы с этими угрозами.

В целом, совершенствование систем силовых структур при гибридной войне требует комплексного подхода, включающего развитие технологий, обучение и тренировки военных, а также улучшение международного сотрудничества. Это поможет сохранить боеспособность и эффективность в условиях быстро меняющейся боевой среды.

5. Международное сотрудничество играет важную роль при борьбе с гибридной войной. Международное сотрудничество при гибридной войне имеет несколько тенденций, рассмотрим некоторые из них:

- обмен информацией и разведывательное сотрудничество. Поддержка международного сообщества в сборе и анализе информации о действиях и методах противника может помочь разоблачить его действия и защитить свою страну. Разведывательное сотрудничество, обмен аналитической информацией и общие исследования могут помочь раскрыть методы применения гибридных войн и разработать стратегии по их предотвращению;

- обмен опытом и передача знаний. Международное сотрудничество позволяет странам обмениваться опытом и передавать знания о своих лучших практиках в борьбе с гибридной войной. В целях обучения военных и гражданских кадров, обмен экспертами, проведение совместных учений и тренировок;

- разработка международных норм и правил. Международное сотрудничество может способствовать разработке и установлению международных норм и правил, регулирующих поведение государств в гибридной войне, соглашения об ограничении кибератак, правила информационной безопасности, международные нормы по защите от пропаганды и манипуляций информацией;

- развитие и укрепление международного сотрудничества и партнерства в области противодействия гибридной войне;

- проведение совместных тренировок и учений с другими государствами для обмена опытом и улучшения практики в противодействии гибридным угрозам;

- создание международных механизмов и организаций для совместного анализа и реагирования на гибридные атаки;

- коллективные меры и санкции. Международное сотрудничество может включать совместные усилия стран по введению санкций и других коллективных мер против противника в гибридной войне, таких как

экономическое давление, ограничение доступа к финансовым ресурсам, торговле или других видов сотрудничества.

Таким образом, место международного сотрудничества в борьбе с гибридной войной находится на пересечении политической, военной, информационной и экономической сфер. Обмен информацией, координирование действий, совместные исследования и разработка международных норм могут способствовать эффективной борьбе с гибридной войной и защите интересов государств.

6. Социальная стратегия при гибридной войне включает в себя ряд мер и действий, основной целью которых является защита и поддержка населения, укрепление национального единства и подавление влияния противника на общественное мнение [10]. Вот некоторые основные факторы социальной стратегии при гибридной войне:

- противодействие дезинформации. Противник может использовать массовые коммуникации, включая социальные сети и СМИ, для распространения дезинформации и создания негативного общественного настроения. В ответ на это, государство должно активно контролировать и контр аргументировать дезинформацию, предоставлять достоверные и проверенные данные и информацию, а также вовлекать общественность в процесс борьбы с фейками;

- поддержка психологического здоровья. Гибридная война может оказывать серьезное влияние на психологическое состояние людей, вызывая стресс, тревогу и тревожные расстройства. Правительство должно обеспечивать психологическую поддержку и консультирование для пострадавших, а также проводить информационные кампании, направленные на поддержку и мотивацию населения;

- обеспечение безопасности населения. Защита и безопасность граждан является приоритетной задачей. Государство должно усилить меры безопасности и обороны, а также предоставить поддержку и ресурсы для защиты и эвакуации населения в случае необходимости;

- мобилизация ресурсов. Во время гибридной войны важно мобилизовать ресурсы общества для решения срочных потребностей, к примеру, мобилизацию добровольцев, вовлечение бизнес-структур в поддержку усилий государства, а также принятие специальных мер в экономической и социальной сферах, чтобы обеспечить устойчивость и укрепление страны в условиях гибридной войны.

Таким образом на основе вышеперечисленного, государство должно создать условия, способствующие укреплению национального единства и солидарности населения. Важно подчеркнуть общие ценности, идеалы и идентичность нации, а также проводить информационные кампании, направленные на укрепление патриотического духа государства.

7.Технологическая стратегия при гибридной войне связана с использованием современных технологий и информационных средств [11] для достижения военных целей, и воздействия на противника.

Развитие технологической стратегии в гибридной войне включает следующие факторы:

- кибератаки - использование компьютерных сетей и информационных систем для проникновения во вражескую инфраструктуру, получения доступа к чувствительной информации, управления важными объектами и нарушения нормального функционирования систем;

- информационная война - активное использование СМИ и социальных сетей для распространения информации, создания и распространения фейковых новостей, навязывания определенной интерпретации событий, манипуляции общественным мнением и дезинформации;

- хакерские атаки - использование атак на информационные системы, включая взломы, уничтожение данных, блокирование доступа к важным ресурсам и сервисам;

- разведка и сбор информации - активное использование шпионажа, съемки и слежки, а также сбора информации из различных открытых источников (интернет, социальные сети, средства массовой информации);

- разработка и использование новых технологий - разработка новых военных технологий, таких как беспилотные аппараты, искусственный интеллект, кибероружие, применение новых материалов и методов производства;

- противодействие и защита - разработка и внедрение технологических решений для обнаружения и предотвращения атак, защита информационных систем от несанкционированного доступа, анализ и мониторинг информационной обстановки;

- поддержка союзников - использование технологической помощи и сотрудничества со стороны союзников, включая обмен информацией, разработку совместных проектов и обеспечение взаимной помощи в технологической сфере.

Таким образом, это лишь некоторые факторы развития технологической стратегии при гибридной войне. Она постоянно меняется и развивается, требуя постоянного обновления и улучшения технологической базы и организации военной подготовки.

8. Образовательная стратегия при гибридной войне должна быть направлена на грамотное обучение и подготовку населения к различным методам [12] такого типа конфликта. Вот несколько ключевых пунктов, которые могут включаться в данную стратегию:

- информационная грамотность - люди должны быть обучены анализу информации, различению фактов от манипуляций, а также умению оценивать источники информации. Это поможет им разоблачать ложные и дезинформационные материалы, которые могут быть использованы в гибридной войне;

- кибербезопасность - обучение основам кибербезопасности позволит людям защитить себя от кибератак, которые являются одним из инструментов гибридной войны. Важно научить людей создавать сложные

пароли, не открывать подозрительные ссылки и быть осторожными в использовании интернета;

- способы предотвращения и реагирования на гибридные атаки - государству следует обучить население противодействию различным техникам и тактикам, используемым в гибридной войне, таким как психологическое воздействие, хакерские атаки, информационные кампании и др. Обучение этим основам позволит предотвращать и своевременно реагировать на такие атаки, организует более эффективную защиту;

- развитие критического мышления. Гибридная война часто основывается на манипуляции и обмане. Развитие критического мышления среди мирного населения позволит своевременно анализировать и оценивать информацию, аргументировать свою точку зрения и принимать информированные решения;

- осведомленность о гибридной войне. Люди должны быть осведомлены о существовании гибридной войны и о ее последствиях. Хорошо информированное население будет более готово и бдительно реагировать на потенциальные угрозы и атаки;

- сотрудничество и обмен опытом. Образовательные учреждения, правительство и специализированные организации должны содействовать сотрудничеству и обмену опытом в области гибридной войны. Это позволит объединить усилия в борьбе с таким типом конфликта и разработать эффективные стратегии предотвращения и реагирования.

Эффективная стратегия государства по противодействию гибридной войне требует комплексного подхода, включающего в себя политические, экономические, информационные, военные, киберстратегии и другие аспекты. Противодействие в данном факторе должно быть непрерывно обновляемым и адаптивным, сфокусированным на противодействии современным угрозам и учитывающим развитие технологий и тактик противников.

9. Защита критической инфраструктуры:

- обеспечение безопасности ключевых объектов и систем, таких как энергетические сети, телекоммуникационные системы, транспортная инфраструктура и финансовые системы;

- разработка и внедрение мер по защите информационной инфраструктуры от кибератак и других форм гибридной атаки;

- регулярный мониторинг и улучшений систем защиты, а также обучение персонала, работающего с критической инфраструктурой.

Защита критической инфраструктуры во время гибридной войны является одной из основных задач, так как критическая инфраструктура является жизненно важной для функционирования общества и государства. В гибридной войне противник может использовать не только военные, но и нестандартные методы воздействия на инфраструктуру, такие как кибератаки, информационная война, террористические акты и другие формы гибридной угрозы.

Для защиты критической инфраструктуры необходимо применять комплексный подход, охватывающий следующие меры и принципы:

- разработка планов защиты. Необходимо разработать планы защиты критической инфраструктуры, которые должны включать в себя оценку уязвимостей, анализ рисков и разработку мер по предотвращению и реагированию на гибридные угрозы;

- кибербезопасность. Защита от кибератак является одной из наиболее важных задач. Необходимо осуществлять регулярный аудит кибербезопасности, внедрять защитные меры и организовывать обучение сотрудников по обеспечению безопасности информационных систем;

- физическая защита. Необходимо организовать физическую защиту критической инфраструктуры, включающую в себя ограждения, контроль доступа, системы видеонаблюдения и другие меры;

- информационная война. Следует применять превентивные меры, чтобы обнаружить и нейтрализовать дезинформацию и информационные атаки на критическую инфраструктуру, для организации систем мониторинга и анализа социальных сетей и средств массовой информации, а также проведение информационно-просветительских мероприятии;

- контингентное планирование. Необходимо разработать стратегии и планы для оперативного реагирования при кризисной ситуации, обучение сотрудников и персонала по проведению мероприятий во время кризиса, а также создание резерва необходимых ресурсов;

- общественное сознание. Проведение информационно-просветительской работы среди населения, чтобы повысить его осведомленность об угрозах и содействовать защите критической инфраструктуры. Это может включать в себя проведение мероприятий по информированию о мерах защиты, проведение учений и тренировок совместно со службами безопасности.

Защита критической инфраструктуры во время гибридной войны требует комплексного подхода, включающего меры кибербезопасности, физическую защиту, информационную войну, международное сотрудничество, контингентное планирование и общественное сознание. Только так можно обеспечить надежную защиту и обеспечить устойчивость функционирования критической инфраструктуры в условиях гибридной войны.

10. Развитие средств коммуникаций и информационной поддержки при гибридной войне является важным фактором современных военных операций.

Один из основных факторов развития средств коммуникации и информационной поддержки при гибридной войне – это разработка эффективных систем связи и передачи информации для оперативной передачи данных между различными военными и гражданскими структурами. Этого можно достичь путем использования высокоскоростных сетей передачи данных, космической связи, спутниковой передачи данных и

других технологии для обеспечения надёжности и конфиденциальности обмена информацией между военными и гражданскими структурами.

Важной частью развития средств коммуникации и информационной поддержки при гибридной войне является разработка и использование систем электронного боевого сопровождения и противодействия электронным средствам нападения. Требует разработку систем обнаружения, анализа и подавления сигналов радиоэлектронной разведки, обеспечение безопасности коммуникационных и информационных систем от кибератак и других форм электронной агрессии.

Кроме того, развитие средств коммуникации и информационной поддержки при гибридной войне также включает в себя обучение и подготовку военнослужащих к работе с новыми технологиями и системами связи. Это включает в себя обучение военных специалистов в области кибербезопасности, специалистов по связи и информационным технологиям, а также их практическое применение в условиях гибридной войны.

Развитие средств коммуникации и информационной поддержки при гибридной войне является важным фактором обеспечения эффективной военной операции и защиты национальных интересов. Усиление современной инфраструктуры связи и информационных систем, разработка новых технологий и систем, а также обучение и подготовка военных специалистов – все эти меры направлены на повышение эффективности военных действий в условиях гибридной войны.

11. Консолидация национальных ресурсов и сил является важным направлением успешной борьбы в условиях гибридной войны [13]. Одной из первоочередных задач при консолидации национальных ресурсов и сил является координация и согласование действий различных государственных органов и силовых структур, таких как военные, полицейские, разведывательные, информационные и другие службы. Важно учесть, что гибридная война требует не только милитаризации, но и участия различных ведомств и организаций, таких как правительство, международные организации, бизнес-сектор и гражданское общество.

Второе направление консолидации национальных ресурсов и сил в гибридной войне - это мобилизация национального потенциала. Это требует своевременную мобилизацию военных резервов, повышение готовности военных и гражданских структур, укрепление критической инфраструктуры и обеспечение ее защиты, создание резервов материальных ресурсов и т.д.

Третье направление консолидации национальных ресурсов и сил в гибридной войне - это создание и развитие международных партнерств. Гибридная война может иметь глобальный характер, и поэтому необходимо сотрудничество с другими государствами и международными организациями. Это может быть организовано в форме обмена информацией и опытом, координации действий, общего анализа угроз, проведения совместных операций и так далее.

В целом, консолидация национальных ресурсов и сил в гибридной войне требует комплексного и системного подхода. Она должна быть основана на

анализе угроз, планировании и координации действий, и быть направлена на достижение конкретных целей. Задача руководства государства и военного командования в таких условиях - обеспечить максимальную эффективность и координацию всех ресурсов и сил для успешной борьбы в гибридной войне.

12. Медиа и публичная дипломатия:

- использование медийных кампаний для информирования и формирования международного общественного мнения о реальных угрозах, связанных с гибридной войной;

- проведение публичных дебатов и мероприятий для повышения осведомленности и активного участия граждан в усилиях по противодействию гибридным угрозам;

- разработка системы контроля и противодействия дезинформации с помощью публикации достоверной информации и трезвого анализа событий.

Эти стратегии и противодействия могут помочь государствам и союзникам при разработке и реализации эффективных мер по противодействию гибридной войне. Однако, каждая стратегия должна быть адаптирована под конкретные условия и потребности каждой страны или региона.

Ключевыми факторами успешной защиты являются сотрудничество, обучение и адаптивность. Государства должны постоянно развивать и совершенствовать свои методы и подходы, чтобы быть готовыми к возрастающей сложности и совершенству атак гибридной войны.

Борьба с гибридной войной также требует сотрудничества и координации между различными организациями и государствами [13, с.33].

Возможно, это будет затруднительно, учитывая различие в интересах и приоритетах участников конфликта.

В целом, гибридная война на современном этапе представляет собой серьезную угрозу для безопасности и стабильности мира. Это требует постоянного мониторинга, анализа и развития новых стратегий и тактики действий для эффективного противодействия этой форме конфликта.

Исходя из анализа и изучения основных направлений гибридной войны с учётом особенностей и географического местоположения государство должно разработать собственную стратегию в зависимости от специфики и условий конфликта. Важно обеспечить объединение усилий государства, общества и всех его компонентов для эффективной борьбы с гибридной войной. Начальный этап гибридной войны начинается в приграничной зоне государства, поэтому важно развивать международное сотрудничество, обмениваться информацией и опытом с соседними и другими странами для повышения эффективности защиты инфраструктуры государства.

Заключение

Изучение сущности гибридных войн и развития их компонентов позволяет сделать несколько выводов. Во-первых, стратегия применения гибридных войн странами агрессии будет продолжать активно

использоваться в контексте на пассивном этапе. Поэтому каждое государство должно быть готово к этому, разрабатывать и внедрять принципы противодействия таким действиям и их предотвращения на ранних этапах, до появления угрозы перехода к активной фазе.

Во-вторых, анализ структуры и последовательности гибридных действий требует уточнения применения в настоящее время методов оценки и прогнозирования развития военно-политической стратегии, а также учета современного межгосударственного противостояния для раннего предупреждения угрозы и разработки мер по их предотвращению.

Основной результат исследования заключается в следующем, усиленное применение гибридных методов противостояния поднимает вопрос о необходимости уточнения системы международных нормативных актов, соблюдения в них положений, запрета применения экономических санкций и информационных операций без международных организаций. В противном случае подобные действия следует рассматривать как акты враждебности и агрессии. Для осуществления данной концепции крайне важно четко разграничить сферы конкуренции, будь то в экономической или идеологической областях, определяя точные границы, за пределами которых конкуренция прекращается. Это позволит обеспечить безопасность современного мира, предотвращая эскалацию конфликтов и стабилизируя международные отношения.

Список использованной литературы:

1. Гибридная война. Сайт свободной энциклопедии «Википедия». – [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/ Гибридная война (дата обращения 21.07.2023).

2. Маркус Дж. Гибридная война // Сайт BBC. – [Электронный ресурс]. Режим доступа: http://www.bbc.com/russian/internationa l/2014/12/141106 nato russian strategy (дата обращения 13.08.2023).

3. Флерко Г.И. Военная безопасность Республики Беларусь. – Алматы « ВИСВ», 2022. – 55 с.

4. Военная доктрина Республики Казахстан. Указ Президента Республики Казахстан от 29 сентября 2017 года № 554. – [Электронный ресурс]. Режим доступа: https://www.akorda.kz/ru/security_council/national_security/voennuyu-doktrinu(дата обращения 13.08.2023).

5. Бартош А.А. Туман гибридной войны. Неопределенности и риски конфликтов XXI века. - М.: Горячая линия, Телеком, 2019. -28 с.

6. Hoffman F.G. Conflict in the 21st century: the rise of hybrid wars. – Arlington: Potomac Institute for Policy Studies, 2007. -72 p.

7. Оганнисян А. Гибридные войны: традиции и новации. Пути к миру и безопасности. – [Электронный ресурс]. Режим доступа:https://www.imemo. ru/ publications /periodical /pmb/archive/2016 / 150/articles/military-policy-and-strategy/hybrid-wars-traditions-and-innovations. (дата обращения 14.08.2023).

8. Арсалан Билаль. Гибридная война: новые угрозы, сложности и «доверие» как антидот. – [Электронный ресурс]. Режим доступа URL: https:// www.nato. int/docu/ review/ru/articles/2021/11/30/gibridnaya-vojna-novye-ugrozy-sloyonosti-i-doverie-kak-antidot/index.html. (дата обращения 24.02.2024).

9. Манойло А.В. Гибридные войны и цветные революции в мировой политике // Право и политика. – [Электронный ресурс]. Режим доступа: https:// nbpublish. com/ library_ read_ article.php?id=52454. (дата обращения 24.02.2024).

10. Виноградова Е.А. Информационные войны в Латинской Америке // Тренды и управление. - 2014. - 4. - С. 372 - 384. DOI: 10.7256/2307-9118.2014.4.13080. – [Электронный ресурс]. Режим доступа URL: https:/ /nbpublish. com/library_ read_article. php?id=13080. (дата обращения 24.02.2024).

11. Тиханычев О.В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. 2020. № 1. С. 30-43. DOI:10.25136/2409-7543.2020.1.30256. – [Электронный ресурс]. Режим доступа URL: https:/ /nbpublish. com/ library _read_article.php?id=30256. (дата обращения 24.02.2024).

12. Першин Ю.Ю. Гибридная война: много шума из ничего // Вопросы безопасности. – 2019. – № 4. – С. 78-109. DOI: 10.25136/2409-7543.2019.4.30374. – [Электронный ресурс]. Режим доступа : https:/ /nbpublish. com/library _read_ article. php?id =30256. (дата обращения 24.02.2024).

13. Садуев Р. С. Психологическое воздействие в современных вооруженных конфликтах и способы противодействия ему / Садуев Р. С Учебное пособие. – Алматы, ВИ СВ. 2017. - С.10-33.

References:

1. Gibrignai voina sait sdobodnoi enseklopii «Wikipedia». – Retrieved from: https://ru.wikipedia.org/wiki / Gibrignai voina // [hybrid war]. (in Russian).

2. Markus, J. Gibrignai voina Putina golovnai bol - NATO // [hybrid war] Air Force website. – Retrieved from: http://www.bbc.com/russian/international /2014/12/141106 nato russian strategy]. (in Russian).

3. Flerko, G.I. (2022). Voyennaya bezopasnost' Respubliki Belarus. [Military security of the Republic of Belarus]. – Almaty «VISV». – 55 p.

4. Voyennaya doktrina Respubliki Kazakhstan. Ukaz Prezidenta Respubliki Kazakhstan ot 29 sentyabrya 2017 goda № 554. – Retrieved from: https://www.akorda. kz/ ru/ security_council/national_security/voennuyu-doktrinu (in Russian).

5. Bartosh, A.A. (2019). Tuman gibridnoy voyny. Neopredelennosti i riski konfliktov XXI veka. [Fog of hybrid war. Uncertainties and risks of conflicts of the 21st century]. – M.: Goryachaya liniya, Telekom. - 28 p.

6. Hoffman, F.G. (2007). Conflict in the 21st century: the rise of hybrid wars. Arlington: Potomac Institute for Policy Studies. -72 p.

7.Ogannisyan, A. Gibridnyye voyny: traditsii i novatsii. Puti k miru i bezopasnosti. – Retrieved from: https:// www. imemo. ru/publications/ periodical /pmb/ archive /2016/150/ articles/military -policy-and-strategy/hybrid-wars-traditions-and-innovations. (in Russian).

8. Arsalan Bilal'. Gibridnaya voyna: novyye ugrozy, slozhnosti i «doveriye» kak antidot. [Arsalan Bilal. Hybrid war: new threats, difficulties and “trust” as an antidote]. – Retrieved from: https://www.nato.int/docu/review/ru/articles/2021/11/30/gibridnaya-vojna-novye-ugrozy-sloyonosti-i-doverie-kak-antidot/index.html. (data obrashcheniya 24.02.2024). (in Russian).

9. Manoylo, A.V. Gibridnyye voyny i tsvetnyye revolyutsii v mirovoy politike // Pravo i politika. - Retrieved from: https:// nbpublish. com/ library_ read_ article.php?id=52454. [Hybrid wars and color revolutions in world politics]. (in Russian).

10. Vinogradova, Ye.A. (2014). Informatsionnyye voyny v Latinskoy Amerike [Information wars in Latin America]. // Trendy i upravleniye. - 4. - C. 372 - 384. DOI: 10.7256/2307-9118.2014.4.13080. – Retrieved from: https:// nbpublish. com/ library_ read_ article. php?id =13080 (in Russian).

11. Tikhanychev, O.V. (2019). Gibridnyye voyny: novoye slovo v voyennom iskusstve ili khorosho zabytoye staroye? // Natsional'naya bezopasnost' / nota bene. - № 1. - P.39-48. [Hybrid

wars: a new word in the art of war or a well-forgotten old one?]. DOI: 10.7256/2454-0668.2019.1.28100. – Retrieved from URL: https:/ /nbpublish. com/library_ read_article .php? id=3 0256 (in Russian).

12. Pershin, Yu.Yu. (2019). Gibridnaya voina: mnogo shuma iz nichego // Voprosy bezopasnosti [Hybrid war: much ado about nothing]. DOI: 10.25136/2409-7543.2019.4.30374. – Retrieved from: https://nbpublish.com/library_read_article.php?id=30256. – № 4. – P. 78-109. (in Russian).

13. Saduev, R.S. (2017). Uchyebnoe posobie. Psixologicheskoe vozdtqstvie v sovrtmennix voorujennix konfliktax I sposobi protivodeistvia emu. [Psychological impact in modern armed conflicts and ways to counter it]. Uchyebnoe posobie. – Almaty, «VISV». – P 10-33.

К.Ж. Койчыкулов, К.В. Федосеенко, И.В. Зарубин

XXI ғасырдағы «Гибридтік соғыс» оның әлуметтік және саяси аспектілері

Бұл мақалада соғысушы тараптардың гибридті соғысты дайындау және жүргізу кезінде қолданатын тактикалық іс-қымылдары мен оған қарсы шаралары қарастырылады, сонымен қатар олардың мәні мен мазмұны сипатталады. Әскери, ақпараттық, экономикалық және саяси әдістердің әртүрлі комбинациялары қолданылатын қақтығыстардың қазіргі заманғы нысандары белгіленді. Авторлар мұндай соғыстардың қазіргі әлемдегі әлеуметтік және саяси процестерге әсеріне, сондай-ақ олардың жаһандық қауіпсіздік пен тұрақтылық үшін салдарына назар аударады. Мақалада гибридті соғыстарға қарсы тұрудың ықтимал стратегиялары және олардың алдын алу үшін халықаралық ынтымақтастықты дамыту қажеттілігі қарастырылған.

Бұған қоса, гибридті қауіптерге қарсы тұру және заманауи шындықта гибридті соғыс басталған жағдайда қарсы іс-қимылды ұйымдастыру бойынша ұсыныстар ұсынылады.

Кілт сөздер: гибридті соғыс, стратегия, қарсы тұру стратегиясы, ақпараттық насихат, кибершабуылдар, насихаттау, жалған ақпарат.

K.Zh. Koichikulov, K.V. Fedoseenko, I.V. Zarubin

«Hybrid War» in the XXI century: social and political aspects

This article examines the tactics and countermeasures used by the warring parties during the preparation and conduct of a hybrid war, and also describes the essence and their content. Modern forms of conflicts have been established, in which various combinations of military, information, economic and political methods are used. The authors draw attention to the impact of such wars on social and political processes in the modern world, as well as their consequences for global security and stability. The article also examines possible strategies to counter hybrid wars and the need to develop international cooperation to prevent them.

In addition to this, recommendations are proposed for countering hybrid threats and organizing counteraction in the event of a hybrid war breaking out in modern realities.

Keywords. hybrid warfare, strategy, counterstrategy, information propaganda, cyber-attacks, propaganda, disinformation.

Койчыкулов Көмекбай Жумабаевич	полковник, Сағадат Нұрмағамбетов атындағы Құрлық әскерлерінің Әскери институты тактика кафедрасының доценті, Алматы, Қазақстан
Койчыкулов Көмекбай Жумабаевич	полковник, доцент кафедры тактики, Военного института Сухопутных войск имени С. Нурмагамбетова, Алматы, Казахстан
Koichikulov Komekbai	colonel, docent of Department of Tactics of the Military Institute of the Land Forces S. Nurmagambetov, Almaty, Kazakhstan

Федосеенко Константин Владимирович	полковник, С. Нұрмағамбетов атындағы Құрлық әскерлері Әскери институты, тактика кафедрасының аға оқытушысы, Алматы, Қазақстан
Федосеенко Константин Владимирович	полковник, старший преподователь кафедры тактики, Военный институт Сухопутных войск имени С. Нурмагамбетова, Алматы, Казахстан
Fedoseenko Konstantin	Colonel, lecturer of Department of Tactics of the Military Institute of the Land Forces S. Nurmagambetov, Almaty, Kazakhstan

Зарубин Иван Владимирович	майор, ғылыми-зерттеу бөлімі аға ғылыми қызметкер – ғылыми жобалар мен инновациялар зертханасының бастығы, С. Нұрмағамбетов атындағы Құрлық әскерлері Әскери институты, Алматы, Қазақстан
Зарубин Иван Владимирович	майор, старший научный сотрудник – начальник лаборатории научных проектов и инноваций научно – иследовательского отдела, Военный институт Сухопутных войск имени С. Нурмагамбетова, Алматы, Казахстан
Zarubin Ivan	major, Senior Researcher - Head of the Laboratory of Scientific Projects and Innovations of the Research Department, Military Institute of the Ground Forces named after S. Nurmagambetov, Almaty, Kazakhstan