https://doi.org/10.30853/manuscript.2020.2.22

Седых Татьяна Николаевна

Теория "непрямых боевых действий" и возможности ее применения в современных условиях

Целью статьи является рассмотрение теории "непрямых боевых действий", анализ механизмов ее практического применения на современном этапе развития общества и выявление возможных угроз в будущем для России. Теоретическую и методологическую основу статьи составили работы американских экспертов корпорации "RAND" и сербских специалистов-аналитиков. Проведенное исследование демонстрирует возрастающий интерес различных акторов мирового политического процесса к разработке новых методик ведения "непрямых боевых действий" в условиях ужесточения конкуренции на мировой политической арене. В заключении работы обозначены основные угрозы, с которыми может столкнуться Россия ввиду ведения против нее сетевых боевых действий; обоснована необходимость выработки эффективной российской стратегии противостояния "негативной социальной манипуляции".

Адрес статьи: www.gramota.net/materials/9/2020/2/22.html

Источник

Манускрипт

Тамбов: Грамота, 2020. Том 13. Выпуск 2. С. 125-130. ISSN 2618-9690.

Адрес журнала: www.gramota.net/editions/9.html

Содержание данного номера журнала: www.gramota.net/materials/9/2020/2/

УДК 1; 327.83 Дата поступления рукописи: 14.01.2020
https://doi.org/10.30853/manuscript.2020.2.22

Целью статьи является рассмотрение теории «непрямых боевых действий», анализ механизмов ее практического применения на современном этапе развития общества и выявление возможных угроз в будущем для России. Теоретическую и методологическую основу статьи составили работы американских экспертов корпорации "RAND" и сербских специалистов-аналитиков. Проведенное исследование демонстрирует возрастающий интерес различных акторов мирового политического процесса к разработке новых методик ведения «непрямых боевых действий» в условиях ужесточения конкуренции на мировой политической арене. В заключении работы обозначены основные угрозы, с которыми может столкнуться Россия ввиду ведения против нее сетевых боевых действий; обоснована необходимость выработки эффективной российской стратегии противостояния «негативной социальной манипуляции».

Ключевые слова и фразы: сетевая война; теория непрямых боевых действий; smart power; социальные манипуляции; система безопасности; цифровые технологии; сетевые структуры; информационное доминирование; мировое лидерство.

Седых Татьяна Николаевна, к. полит. н.
Московский государственный университет имени М. В. Ломоносова
Tatiana_sedykh@mail.ru

Теория «непрямых боевых действий» и возможности ее применения в современных условиях

Статья подготовлена в рамках деятельности Выдающейся научной школы МГУ имени М. В. Ломоносова «Трансформации культуры, общества и истории: философско-теоретическое осмысление».

Начало нового тысячелетия стало для человечества временем стремительного развития информационно-коммуникационных и цифровых технологий. И, безусловно, можно со скепсисом отнестись к мнению многих экспертов: философов, политологов, экономистов, – утверждающих, что подобное взрывное ускорение научно-технического прогресса далеко не всегда оказывается позитивным, а порой и пагубно влияет на многие сферы жизни человека [6]. Но с некоторой определенностью можно сказать, что на политической арене все больший вес обретают те, кто способен «овладеть умами» и тем самым оказать определяющее влияние на формирование общественного мнения. И именно новые технологии предоставляют набор средств, необходимых для завоевания лидирующих позиций на мировой арене. Как описал сложившуюся ситуацию Е. Н. Мощелков, «в качестве доминирующей в системе безопасности становится информационная компонента, при помощи которой "неизвестный и невидимый противник" может оказать разрушительное воздействие не только через физическую и материальную среду, но и (и даже главным образом) через духовно-идеологическую подоснову общества, через сознание людей» [4, с. 19]. Потому актуальным в настоящий момент представляется рассмотрение методов и технологий воздействия, которые активно используют страны, претендующие на мировое политическое господство. Актуальность темы исследования предопределяет и тот факт, что подобные технологические решения уже активно использовались США в военных кампаниях против ряда стран и доказали свою эффективность, а новые подобные программы, где одним из главных противников открыто называется Россия, уже находятся в стадии разработки. Теоретическую основу подобных разработок во многом составляют исследования экспертов «фабрик мысли» США (например, корпорации "RAND"). В связи с чем внимание автора к недавно опубликованным и не до конца изученным аналитическим материалам американских исследователей – сотрудников подобных структур, посвященным механизмам сотрудничества и борьбы с Россией и другими союзниками и оппонентами на мировой политической арене, представляется обоснованным и определяет **научную новизну**, а также **актуальность** статьи. Важно также подчеркнуть, что панорамное рассмотрение темы невозможно без обращения к вопросу практической реализации разработанных в США программ «непрямого воздействия». Одним из ярких примеров такой кампании (проводится в настоящее время) является деятельность американских структур и агентов в Республике Сербия. По этой причине в статье достаточно подробно анализируются данные, представленные сербскими аналитиками, доказывающие факт ведения США «сетевой войны» против Сербии, что, как представляется, будет способствовать некоторому изменению и уточнению в сложившихся подходах и направлениях анализа данной проблематики.

Цель статьи – рассмотреть теоретико-методологические основы создания технологий и механизмов непрямых боевых действий, несущих потенциальную угрозу стабильному развитию современного российского общества. Основными **задачами** исследования являются всесторонний анализ теоретических оснований и подходов к формированию стратегии непрямых боевых действий, рассмотрение механизмов их практического применения (в том числе с использованием исторического опыта стран Балканского полуострова), изучение современных программ и рекомендаций американских аналитиков и политтехнологов, связанных с ведением сетевых войн.

Сетевая война как реализация «стратегии непрямых действий»

Еще в середине прошлого столетия английский военный историк Бэзил Лиддел Гарт в книге «Стратегия непрямых действий» [2] обратил внимание на то, что как в политике, так и в экономике, и даже в межличностных отношениях «метод непрямых действий» всегда эффективнее, чем прямое, «лобовое» столкновение. Удивительным по своей эффективности «комплексом» подобных непрямых действий вполне определенно можно назвать «сетевые войны», которые США ведет уже несколько десятилетий. О том, как и почему этот комплекс работает на конкретных примерах из истории своей Родины, рассказывает на страницах книги «Сетевая война против сербов. Уроки для России» [5] юрист, член «Изборского клуба» Слободан Стойичевич. Представляется, что в настоящий момент, когда широту охвата и степень влияния на российское общество различных по интенсивности и устремленности воздействий сложно представить и оценить, подобные исследования могут быть полезны как представителям научного сообщества, так и всем интересующимся вопросами национальной безопасности. Так как без конкретных примеров и «подсказок» мы сами не всегда способны понять, как меняемся на глубинном уровне, касающемся сознания, ценностных установок, поведения и реакций.

Разработкой новых «непрямых» методов и соответствующего им инструментария, необходимого для отстаивания собственных позиций на мировой политической арене, наиболее активно занимались многочисленные научно-исследовательские центры США, и именно в этой стране появилось и было концептуально обосновано понятие «сетевая война». Лидерство американцев в исследовании «новых техник» ведения международной борьбы представляется вполне закономерным, потому как США – пожалуй, единственное на сегодняшний день государство, способное «вести борьбу» одновременно на нескольких уровнях: укреплять свою позицию как единственной мировой сверхдержавы, используя при этом такие формы применения власти, как “hard power”, “soft power”, а также “smart power”, которая подразумевает «развитие комплексной стратегии, ресурсной базы, набора инструментов для достижения целей США, с опорой на hard, и soft power» [7, p. 7]. По словам заместителя министра иностранных дел России С. В. Вершинина, в настоящий момент США и их союзники «все отчетливее берут курс на коренное переформатирование не устраивающих их международных институтов. <…> Решения все чаще стали приниматься в формате узких ситуативных союзов. Остальным государствам предлагается присоединиться к уже согласованным решениям, выдаваемым за позицию всего мирового сообщества» [1, с. 60]. «Неприсоединившихся» же ожидает массированная атака по нескольким направлениям, среди которых можно назвать и применение санкций (с середины прошлого века США чаще других государств вводили односторонние санкции или инициировали санкции против других стран), и воздействие с помощью новых «непрямых» методов ведения политической борьбы. Теоретическая основа таких методов разрабатывалась в одной из так называемых «фабрик мысли» (think tank) – «РЭНД Корпорации» (“RAND Corporation”), основанной в Санта-Монике в 1948 году под эгидой военно-воздушных сил США. Авторы концепции «сетевой войны» (netwar) Джон Аркилла и Дэвид Ронфельдт утверждают: «сетевая война» представляет собой тип конфликта «на наивысшем уровне между обществами и странами. Когда предпринимаются попытки разрушить и изменить то, что люди, на которых направлено воздействие, “знают” или думают, что знают, о себе и окружающем их мире. Сетевая война концентрирует на мнении масс или элит, или тех и других вместе» [9, p. 25]. Сетевой принцип построения социальных взаимосвязей, по мнению американских исследователей, предполагает восприятие информационного пространства как совокупности свободно соединенных децентрализованных организационных форм (научных, технических, религиозных, военных, дипломатических и т.д.), являющихся каналами продвижения интересов, утверждения позиций. Сети могут иметь разнообразную форму (например, цепи или звезды) в зависимости от поставленных целей (криминальные группировки, как замечают Дж. Аркилла и Д. Ронфельдт, чаще используют форму звезды), но существуют и гибридные варианты, использующие разные формы [10, p. 47]. Построение подобных сетей, по мнению авторов концепции, мы можем наблюдать, если обратимся к «полезному способу» прогнозировать будущее – изучать прошлое, а именно к истории Византийской империи, где по сетевому принципу были выстроены оборонительная и разведывательная и некоторые части наступательной системы, которые активно использовали и тактику роя, и сеть узлов и ячеек – форпостов и гарнизонов, мобильные ударные силы. Как подчеркивают эксперты, именно византийские сетевые структуры наглядно демонстрируют основное условие для их строительства: «…стремление создать значительное количество компактных активных образований, независимо функционирующих и имеющих главной задачей достижение общих целей при возможном отсутствии общей системы их управления и контроля» [8, p. 27-28].

Сетевые боевые действия против Сербии

Описывая методы и технологии ведения сетевых войн, многие эксперты совершенно оправданно обращаются к понятиям «сетецентрическая война» (*подробное освещение эта военная концепция получила в работах У. Оуренса, Д. Гартски, Ф. Штейна, Дж. Альбертса и др.*), «сетецентрические боевые действия» (Net-Centric Warfare). Оба понятия близки по звучанию и содержанию, но имеют существенные различия, потому как концепция сетецентрических боевых действий (разрабатываемая с 1993 года и через пять лет представленная общественности авторами: вице-адмиралом ВМС США А. Себровски и профессором Дж. Гарстка, повлиявшая на американскую военную стратегию и ставшая основой модернизации вооруженных сил США) сугубо военная, тогда как основные средства, задействованные в сетевых войнах, – социальные сети между социальными субъектами – остаются гражданскими. С. Стойичевич, анализируя общее и различное этих двух понятий, указывает, что, используя невоенным путем невоенными средствами и к невоенным объектам основные принципы и приемы сетецентрических боевых действий, сетевая война имеет вполне военную цель –

завоевание и порабощение определенного общества [5, с. 37]. Такими приемами и принципами, разработанными авторами концепции сетецентрических боевых действий, применяемыми впоследствии в войнах сетевых, С. Стойичевич называет тактику роя, информационное доминирование, демассификацию, самосинхронизацию и др. и наглядно демонстрирует, каким образом и кто использовал и продолжает использовать эти практики против Сербии. Уже не вызывает сомнений, что военные действия против Сербии в 1999 году являются одним из первых примеров ведения гибридной войны (с привлечением как вооруженных сил, так и большого количества информационных ресурсов) странами НАТО в Европе [3, с. 19]. Но С. Стойичевич в своем исследовании анализирует ситуацию в Сербии с 2000 года и показывает эффективность именно сетевых техник, используемых против его страны.

Обращаясь к экономике Сербии, С. Стойичевич акцентирует внимание на том, что, несмотря на смену соотношения политических сил в парламенте и правительстве страны, курс преобразований оказывался на протяжении всего изучаемого периода неизменным. В результате банковский и финансовый секторы, рынок страхования перешли под контроль иностранных акторов, крупные предприятия подвергаются долговременной реструктуризации, что практически делает их неконкурентоспособными, возможное экономическое сотрудничество с Россией и Китаем «притормаживается». Все это, по мнению автора, является яркой демонстрацией одного из важнейших элементов сетевой структуры – нового принципа управления, не использующего прямые приказы, но дающего исполнителям общее представление о замыслах «командира». Такое намерение командира (commander's intent), с одной стороны, освобождает как исполнителей, так и командование от ответственности в случае невыполнения задачи, а с другой стороны, дает возможность подчиненным творчески подойти к решению проблемы, самостоятельно оценить обстановку и выбрать оптимальную и наиболее эффективную стратегию. «Стержнем» всей сетевой системы, оказывающей колоссальное влияние, а порой и определяющей внутреннюю и внешнюю политику в Сербии, по мнению автора, являются так называемые парагосударственные фонды. Такие организации, как Национальный демократический институт (NDI), Совет по международным исследованиям и обмену (IREX), "Freedom House", представляют интересы США, и вся их деятельность направлена на соответствующую работу (в том числе идеологическую), которая особенно активно ведется в странах, «нуждающихся в Евроатлантической интеграции». «Помочь» в осознании необходимости подобных интеграционных процессов гражданам Сербии призваны также разнообразные НПО и НКО, активно финансируемые из государственных бюджетов Австралии, Норвегии, всех стран – членов ЕС [5, с. 92] и самой Сербии, несмотря на заявления политиков о нехватке средств на здравоохранение, коммунальное хозяйство, науку и образование. Подобные организации призваны не только эффективно и своевременно сформулировать для общества определенные идеологические лейтмотивы, но способствуют их дальнейшей популяризации, чему содействуют и средства массовой информации, являющиеся одними из самых активных участников проводимых США сетевых боевых действий. О том, какова степень влияния США на сербские СМИ, свидетельствует тот факт, что еще шесть лет назад американский инвестиционный фонд "Kohlberg, Kravis, Roberts & Co. L. P." (KKR) приобрел медийную компанию "United Group", объединявшую самых крупных интернет-провайдеров и операторов кабельного и спутникового телевидения на территории бывшей Югославии и насчитывавшую около двух миллионов пользователей. Одним из руководителей "KKR" является экс-глава ЦРУ Дэвид Петреус (входивший в группу планирования и координации действий НАТО в Югославии в 1999 году), по словам которого «новым полем битвы сегодня становится Интернет» [13]. Деятельность Д. Петреуса как со-руководителя "KKR" стала предметом не одного журналистского расследования (напр., расследование "L'Observatoire des Journalistes" [14]), и их результаты дают основания с уверенностью утверждать, что за неполное десятилетие была создана настоящая медиа-империя, формирующая и контролирующая информационные потоки в большинстве стран Балканского полуострова. Так, "KKR" имеет региональную телесеть – "N1 TV", эксклюзивного партнера "CNN", со студиями в крупнейших городах Хорватии, Боснии и Герцеговины и Сербии; владеет "Central European Media Enterprises" (CME) в Словении и Хорватии, включающим самые популярные информационные каналы данных стран; является собственником гиганта развлекательной индустрии "Grand Production" и контрольного пакета оператора кабельного телевидения Черногории "ВВМ", совладельцем информационного сайта Сербии "Blic.rs" и продолжает расширять сферу своего влияния, в том числе на рынке мобильной связи.

Подобное информационное доминирование вкупе с деятельностью других не менее эффективных и активных, но менее заметных участников сетевых боевых действий против Сербии представляются весьма впечатляющими: сербская экономика полностью зависима от евроатлантического интегрирования, страну покидают (или намерены покинуть в ближайшей перспективе) высококвалифицированные специалисты, представители творческой элиты. А печатные СМИ, радио и телевидение, Интернет шаг за шагом формируют у населения страны желаемое видение ситуации – евроинтеграция альтернативы не имеет, противостоять этому процессу невозможно, и можно либо «влиться» в этот процесс, либо пассивно наблюдать за происходящим без какой-либо надежды на сопротивление [5, с. 175]. Единственным институтом, который, несмотря на предпринимаемые массированные сетевые атаки, пока остается вне «сети», является Сербская православная церковь. Как утверждает автор, сама история страны, насыщенная трагическими событиями, ставшими настоящими испытаниями для сербского народа – войнами, восстаниями, революциями, периодами объединения и раздробленности, – сформировала особую сербскую религиозность – «Православие сербского стиля и опыта – Святосавие», что привело к тому, что СПЦ – это не просто обычный общественный институт, одна из конфессий в Сербии, но основа сербской национальной идеи [Там же], без которой жизнь сербского народа как самостоятельной

единицы, полноправного участника мирового политического процесса, невозможна. И это объясняет возникающие в последние два десятилетия и ярко освещающиеся в СМИ скандалы, сенсации, конфликты, касающиеся СПЦ и являющиеся составными частями продуманной и планомерной сетевой войны, ведущейся против оплота национального духа Сербии. Помочь выстоять Сербии в этой борьбе, по мнению автора, могла бы Россия. Но, как утверждает С. Стойичевич, в сетевой войне Россия не имеет ресурсов и кадров не только для помощи кому-либо (ярким примером чему могут служить события в Молдавии, Грузии, Украине, Армении), но и для активных действий по защите собственных интересов, однако может занимать сугубо оборонительную позицию. Потому «разсетевление» Сербии является задачей настоящих ее граждан, опорой этого процесса может быть СПЦ, а начать его необходимо с создания «атласа сетей Сербии» [Там же, с. 282].

Угрозы для России

Представляется важным и необходимым озаботиться проблемами выявления разнообразных «сетевых» структур и организаций в современной России. Как отечественные, так и зарубежные эксперты все чаще высказывают мнение, что избежать нового этапа холодной войны между США и Россией не удастся [17], в связи с чем теория «непрямых воздействий» на противника может получить новый импульс для развития, а практическое ее применение на международной политической арене – приобрести более широкий охват. И России, для которой на нынешнем этапе ее развития создание своих «сетей» является проблематичным (что связано и с необходимым для этого высоким уровнем финансирования и с наличием у оппонентов уже отлаженных механизмов для противостояния чужеродным сетевым агентам), жизненно необходима своя стратегия сетевых боевых действий, основой которой должно стать понимание важности выработки инструментов для борьбы с уже имеющимися сетевыми игроками и недопущение появления новых агентов влияния, сетевых узлов. Актуализировать разработку такой стратегии, по нашему мнению, могут два доклада упоминаемой выше корпорации “RAND”. Первый из них – «Слишком большая и несбалансированная Россия. Оценка влияния затратных вариантов» – был опубликован в начале лета 2019 года [11]. Целью авторов доклада (среди которых Дж. Доббинс – дипломат, занимавший должность посла США в ЕС, помощника госсекретаря по европейским делам, профессор Бруклинского исследовательского института Р. С. Коэн, специалисты в области международных отношений, военной промышленности) было показать уязвимые стороны России, нацеленные и разноплановые воздействия на которые могли бы привести к «перенапряжению» внутри государства и, в конечном счете, как экономической, так и политической его разбалансировке. Интересно, что в качестве подзаголовка доклада американские эксперты использовали цитату У. Черчилля, перефразированную В. В. Путиным в 2002 г., к которой довольно часто обращаются представители американских СМИ: «Россия никогда не была такой сильной, какой она хотела быть, и никогда не была такой слабой, как о ней думали» [12]. Авторы доклада обратились к мысли, что эффективно конкурировать и бороться за лидерство с Россией можно и нужно в тех сферах, где у США есть заметное преимущество (данная идея была высказана их коллегами из корпорации “RAND”, разработавшими в 1972 году концепцию долгосрочной стратегической конкуренции США и СССР) [16]. Поэтому, исследуя четыре основных направления возможного воздействия на Россию (экономическое, геополитическое, идеологическое и информационное, военное), эксперты “RAND” проанализировали возможные риски и издержки для США и нашли, по их мнению, самые эффективные на настоящий момент механизмы влияния, способные заставить Россию взять на себя новые (в том числе и финансовые) обязательства, выполнение которых в разы снизит конкурентоспособность страны на международной арене. Таким образом, оценивая возможные экономические меры, авторы приходят к выводу, что наиболее эффективным может быть расширение добычи и экспорта энергоносителей в США (приведет к стрессу в российской экономике, ограничивая ее госбюджет и, соответственно, расходы на оборону). Более высокозатратными называются такие меры, как введение новых санкций против России и поиск новых поставщиков СПГ для стран Европы. Низкозатратными, с минимальными рисками, но одновременно имеющими самую маленькую «отдачу» эксперты назвали меры поддержки оттока из России квалифицированной и образованной молодежи. В геополитическом блоке оцениваются такие сценарии, как поставки оружия Украине, поддержка сирийский боевиков, содействие либерализации Белоруссии и перевороту в Приднестровье и др. Наибольшее число мер представлено в «военном блоке»: от наращивания сухопутных сил США и НАТО в Европе до расширения аэрокосмических исследований и разработок (НИОКР) (в общей сложности более тридцати вариантов). Наконец, среди идеологических и информационных мер эксперты выделяют снижение доверия к российской избирательной системе, поощрение протестных настроений внутри страны, создание антиобщественного имиджа политической элиты, снижение авторитета и влияния России за рубежом. В конце исследования авторы отмечают, что все перечисленные методы воздействия могут спровоцировать ответные действия, что особенно опасно, учитывая обладание Россией ядерным оружием, поэтому реализация каждой обозначенной меры должна быть тщательно спланирована и «откалибрована». Подобные исследования, как представляется, являются не чем иным, как достаточно подробным планом сетевых боевых военных действий, которые не просто делаются по определенному заказу в США, но и находятся в открытом доступе, что демонстрирует нам не только намерения США на международной арене, но и отсутствие каких-либо «ширм и вуалей», которыми можно было бы прикрыть такую позицию как от союзников, так и от противников.

Второй доклад «Враждебная социальная манипуляция. Настоящие реалии и новые тенденции» [15] был опубликован осенью 2019 года. По мнению его авторов, методы, описываемые нами выше и применяемые

агентами сетевых боевых действий на информационном поле, несут значительную угрозу США и «союзным странам», а основными «пользователями» таких методик социальной манипуляции в настоящий момент являются Россия и Китай. Американские исследователи подчеркнули, что пока в их распоряжении нет достаточной фактологической основы для доказательства оказываемого влияния на конкретную аудиторию, целевую группу (с этой точки зрения у экспертов "RAND" вызывает интерес, например, направление российского спонсорства за рубежом). Но в намерениях изучаемых держав у авторов доклада сомнений не возникает, потому они считают целесообразным предложить правительству США незамедлительно принять меры, призванные обезопасить страну от возможных воздействий со стороны России и Китая, среди которых называются разработка более формальной и конкретной основы для понимания проблемы и финансирование дополнительных исследований в данной области, которые дадут возможность оценить масштабы возможного влияния на американских граждан.

Принимая во внимание степень влияния, которую исторически оказывают отчеты и доклады экспертов "RAND" на принятие решений в Белом доме, можно с уверенностью утверждать, что появление программы изучения и противодействия «враждебным социальным манипуляциям» – дело времени. Потому представляется, что как российскому научному сообществу, так и лицам, принимающим политические решения, которые определяют контуры развития России, необходимо обратить более пристальное внимание на современные методы сетевых боевых действий и начать активную подготовку собственных эффективных «игроков» на новом поле международной конкурентной борьбы.

Основные выводы

Проведенный анализ теоретических оснований стратегии непрямых боевых действий показал, что методы и технологии обороны и нападения, используемые в далеком прошлом (например, в Византийской империи), на современном этапе развития информационно-коммуникационных технологий вновь становятся актуальными и применимыми на практике. Исследования преимуществ непрямых боевых действий в вооруженных конфликтах в сравнении с тактикой «лобового» столкновения получили наибольшее распространение в США и стали концептуальным основанием теории сетевой войны. В рамках данной теории детально проработаны и описаны новые техники ведения политической борьбы в том числе за мировое лидерство. Подобные техники непрямых боевых действий успешно использовались США не только в военных кампаниях: разработанный американскими экспертами набор сетевых технологий позволяет эффективно воздействовать на страну-оппонента, избегая военного конфликта (деятельность сетевых структур в Республике Сербия является ярким тому примером).

Новейшие исследования американских экспертов, посвященные теоретическим и практическим составляющим сетевых войн и детально изученные автором статьи, с уверенностью можно назвать концептуальной основой для будущих программ ведения непрямых боевых действий, а также системы предупреждения возможных сетевых атак со стороны России и Китая. Это позволяет сделать вывод о том, что уже в ближайшей перспективе российское общество может подвергнуться массированным сетевым атакам, и руководству государства необходимо оперативно принять меры, направленные на защиту страны от подобного рода воздействий.

Кроме того, рассмотренные технологии непрямых боевых действий, успешно применяемые США в Сербии, позволяют сделать выводы о том, что целями непрямых боевых действий, воздействие на которые ведется особенно интенсивно, являются системообразующие структуры, позволяющие сохранять народам единство нации и государственную идею (такие, как СПЦ в Сербской Республике). Это, в свою очередь, актуализирует такой значимый для России вопрос, как отстаивание независимости ключевых социальных институтов, отвечающих за сохранение национальной идентичности и культурных ценностей. Можно с уверенностью утверждать, что комплексный подход, предлагаемый автором, включающий в себя, с одной стороны, продуманную государственную программу противостояния непрямым боевым действиям возможными техническими и информационными средствами, а с другой стороны, масштабную государственную деятельность в образовательной и культурной сферах, поможет минимизировать последствия сетевых атак и избежать разрушительного манипулятивного воздействия на российское общество. Такой подход представляется наиболее эффективным в сложившейся ситуации нарастающей напряженности на мировой политической арене.

Список источников

1. **Вершинин С. В.** О некоторых аспектах мирового развития на современном этапе // Мировое развитие: проблемы предсказуемости и управляемости: XIX Международные Лихачевские научные чтения (г. Санкт-Петербург, 22-24 мая 2019 г.). СПб.: СПбГУП, 2019. С. 59-62.
2. **Лиддел Гарт Б. Х.** Стратегия непрямых действий. М.: АСТ, 2018. 512 с.
3. **Марков Е. А., Неволина А. А.** Россия как главный объект современных информационных войн // Historia Provinciae – Журнал региональной истории. 2018. Т. 2. № 3. С. 12-48.
4. **Мощелков Е. Н.** На наших глазах рушится старый мировой порядок: что дальше? // Философия политики и права: ежегодник научных работ. М.: Воробьёв А. В., 2019. Вып. 10. С. 5-20.
5. **Стойичевич С.** Сетевая война против сербов. Уроки для России. М.: Книжный мир, 2019. 288 с.
6. **Четверикова О. Н.** Цифровой тоталитаризм. Как это делается в России. М.: Книжный мир, 2019. 320 с.
7. **Armitage R., Joseph S. Nye Jr.** CSIS Commission on Smart Power: A Smarter, More Secure America. Washington: The CSIS Press, 2007. 89 p.

8. **Arquilla J.** To build a network // Prism. Washington, 2014. Vol. 5. № 1. P. 22-34.
9. **Arquilla J., Ronfeldt D.** Cyberwar is coming! // In Athena's Camp: Preparing for Conflict in the Information Age / ed. by J. Arquilla and D. Ronfeldt. Santa Monica, Calif.: RAND Corporation, 1997. P. 23-60.
10. **Arquilla J., Ronfeldt D.** The Advent of Netwar. Santa Monica, Calif.: RAND Corporation, 1996. 127 p.
11. **Dobbins J., Raphael S. Cohen, Frederick B., Geist E.** Overextending and Unbalancing Russia: Assessing the Impact of Cost-Imposing Options [Электронный ресурс]. URL: https://www.rand.org/pubs/research_briefs/RB10014.html (дата обращения: 03.01.2020).
12. **Higgins A.** Putin's Russia, Punching above Its Weight, Keeps Adversaries off Balance [Электронный ресурс] // The New York Times. 2019. December 23. URL: https://www.nytimes.com/2019/12/23/world/europe/russia-putin.html (дата обращения: 10.01.2020).
13. **https://www.bbc.com/news/av/world-41317935/petraeus-cyberwar-is-a-whole-new-domain-of-warfare** (дата обращения: 03.01.2020).
14. **https://www.ojim.fr/david-petraeus-ex-cia-chief-new-media-mogul-in-eastern-europe-the-complete-investigation/** (дата обращения: 10.01.2020).
15. **https://www.rand.org/pubs/research_reports/RR2713.html** (дата обращения: 03.01.2020).
16. **Marshall A. W.** Long-Term Competition with the Soviets: A Framework for Strategic Analysis. Santa Monica, CA: RAND Corporation, 1972. 72 p.
17. **Saradzhyan S.** What Stops US and Russia from Stumbling into War? [Электронный ресурс]. URL: https://www.russiamatters.org/blog/what-stops-us-and-russia-stumbling-war (дата обращения: 10.01.2020).

"Indirect Military Operations" Theory and Possibilities for Its Use under Modern Conditions

Sedykh Tat'yana Nikolaevna, Ph. D. in Political Sciences
Lomonosov Moscow State University
Tatiana_sedykh@mail.ru

The article aims to examine the "indirect military operations" theory, to analyse the mechanisms of its practical usage at the modern stage of the society development and to identify potential dangers for Russia. Theoretical and methodological basis of the research includes the studies of the American "RAND Corporation" experts and the Serbian experts-analysts. The conducted analysis indicates the growing interest of political actors in the development of new "indirect military operations" strategies under conditions of tightening competition in the global political arena. In conclusion, the author identifies potential dangers Russia can face due to military net operations against it, justifies the necessity to develop an efficient strategy to resist "negative social manipulation".

Key words and phrases: netwar; "indirect military operations" theory; smart power; social manipulations; security system; digital technologies; net structures; informational dominance; global leadership.