Е.В.Горгола, доктор экономических наук, профессор
В.А.Кваша, кандидат экономических наук, доцент

Развитие военно-экономической науки в эпоху сетевых войн

Возникновение и развитие постиндустриального общества изменило методологический подход к достижению военно-политических целей и привело к возникновениюв концепции ведения боевых действий на основе «операций базы эффектов», которые связаны не с фронтальный столкновением противоборствующих группировок войск, а с моделированием поведения противостоящих вооруженных сил, населения, политических элит и руководства страны на основе активного использования возможностей тотального сетевого информационного воздействия.

Развитие военного дела на протяжении всей истории человечества всегда выступало противоречивым фактором прогресса общества: с одной стороны, оно инициировало и подталкивало научно-технический прогресс, а с другой – отбрасывало разрушенные страны на десятилетия назад; с одной стороны, заставляло человека быстро самосовершенствоваться, а с другой – тормозило социальный прогресс. Третье тысячелетие переносит это противоречие на новый уровень.

Традиционное представление о военных действиях непосредственно связано с такими понятиями, как фронт и армия. Собственно само боевое соприкосновение происходило лобовым образом – противники непосредственно осуществляли огневое поражение друг друга, а победа доставалась тому, у кого вооружение и техника были более совершенны, лучше обучен личный состав, или тому, у кого имелся численный перевес. Сама победа измерялась количеством потерь с той или иной стороны и установлением военного контроля над захваченной территорией – с другой. Все эти категории относятся к войнам эпохи модерна.

Возникновение и развитие постиндустриального общества в наиболее развитых странах связано с наступлением информационной эпохи, эпохи постмодерна, когда концептуально изменяется сам подход к достижению военно-политических целей. Для наглядности это можно представить схематически: устройство национального государства рассматривается стратегами сетевых войн в виде концентрических кругов. В центре находится национальный лидер, как правило, глава государства, вокруг него располагаются политические элиты. Следующим кругом является экспертное сообщество, формирующее политические смыслы и интерпретации, и медиапространство, переводящее все на язык масс.

Следующий слой – это сами массы: общество, население страны. А снаружи – внешний слой: располагается армия, вооруженные силы как средство защиты всей этой концентрической конструкции. Эта схема впервые была предложена американским стратегом, одним из разработчиков теории сетецентричных войн Джоном Уордоном, полковником вооруженных сил США. Впоследствии она была заимствована технологами гуманитарных социальных трансформаций[1].

1 См. например Arquilla J. Ronfeldt D.F. The emergence of noopolitik: toward an American information strategy. Rand Corporation, 1999; Arquilla J. Ronfeldt D.F. Networks and netwars: the future of terror, crime, and militancy. Santa Monica: Rand Corporation, 2001; Cebrowski A.K. and Garstka J.J.Network-Centric Warfare: Its Origin and Future. Proceedings (January 1998) и др.

При таком подходе основой стратегии, которая получила название Effects-bases operations (операции, основанные на эффектах или «на базе эффектов» – ОБЭ), является осуществление агрессии в отношении такой модели государства не извне, то есть не против вооруженных сил, не напрямую «лобовым образом». Более эффективной становится так называемая концепция ведения войны «изнутри наружу».

Это важнейшая концепция в данной теории. ОБЭ определяются как «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны»[1]. Иными словами, ОБЭ – это такое качественное влияние на среду, при котором участникам ничего не навязывается прямым образом, но при этом они делают то, что хотят сетевики, выстраивающие эту модель управления.

ОБЭ предполагает преднамеренное установление эффективного контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях – и тогда, когда война ведется, и тогда, когда она назревает, и тогда, когда царит мир. В этом вся суть сетевой войны – она не имеет начала и конца, она ведется постоянно, и ее цель обеспечить тем, кто ее ведет, способность всестороннего управления всеми действующими силами человечества. Это означает, что внедрение сети представляет собой лишение стран, народов, армий и правительств мира какой бы то ни было самостоятельности, суверенности и субъектности, превращение их в жестко управляемые, запрограммированные механизмы[2].

В понимании сегодняшних архитекторов мирового порядка за скромной «технической» аббревиатурой ОБЭ стоит план прямого планетарного контроля, глобального господства нового типа, когда управлению подлежат не отдельные субъекты, а их содержание, их мотивации, действия, намерения и т.д. Это проект глобальной манипуляции и тотального контроля в мировом масштабе, что видно из определения ОБЭ. Задачей такой «операции» является формирование структуры поведения не только друзей, но и нейтральных сил и врагов, т.е. и враги, и занимающие нейтральную позицию силы, по сути, заведомо подчиняются навязанному сценарию, действуют не по своей воле, но по воле тех, кто осуществляет ОБЭ, т.е. США. Если враги, друзья и нейтральные силы в любом случае делают именно то, чего хотят от них американцы, они превращаются в управляемых (манипулируемых) марионеток заведомо – еще до того, как следует окончательное поражение. Это выигрыш битвы до ее начала. Цель сетевых войн – абсолютный контроль надо всеми участниками исторического процесса. И здесь необязательна прямая оккупация, массовый ввод войск или захват территорий. Армейские действия и собственно военные затраты излишни. Сеть – более гибкое оружие, она манипулирует насилием и военной силой только в крайних случаях, и основные результаты достигаются в контекстуальном влиянии на широкую совокупность факторов – информационных, социальных, когнитивных и т.д. При этом военная сила, если и применяется, то лишь точечно, дозированно, или как фактор демонстрации и устрашения.

Кроме того, сеть представляет собой новое пространство: информационное пространство, в котором и развертываются основные стратегические операции как разведывательного, так и военного характера, а также их медийное, дипломатическое, экономическое и техническое обеспечение. Сеть в таком широком понимании включает в себя различные составляющие, которые ранее

1 Цит. по: Edward A. Smith, Jr. Effects based Operations. Applying Network centric Warfare in Peace, Crisis and War, Washington, DC: DoD CCRP, 2002.

2 Arquilla J. Ronfeldt D.F. The emergence of noopolitik: toward an American information strategy. Rand Corporation, 1999; Arquilla J. Ronfeldt D.F. Networks and netwars: the future of terror, crime, and militancy. Santa Monica: Rand Corporation, 2001; Cebrowski A.K. and Garstka J.J.Network-Centric Warfare: Its Origin and Future. Proceedings (January 1998).

рассматривались строго раздельно. Боевые единицы, системы связи, информационное обеспечение операций, формирование общественного мнения, дипломатические шаги, экономическая политика, социальные процессы, разведка и контрразведка, этнопсихология, религиозная и коллективная психология, военно-экономическое и военно-техническое обеспечение, академическая наука, технические инновации и т.д. – все это отныне видится как взаимосвязанные элементы единой «сети», между которыми должен осуществляться постоянный информационный обмен.

Следует заметить, что в сетевой войне предпочтительны непрямые и асимметричные методы воздействия. Как отмечается в концепции, в сетевой войне могут применяться такие формы операций, как восстание, сопротивление восстанию, нестандартная война, террор, сопротивление террору, обеспечение безопасности в другой стране, стабилизация, переходные процессы и восстановление, стратегические связи, психологическая борьба и информационная война. Влиять на иностранные правительства и общества в рамках сетевой войны – это тонкая, многоаспектная и многопрофильная деятельность. Ведение подобной войны только военными средствами неизбежно приводит к провалу. Сетевая война связана с народами. Исход такой войны зависит не от военных средств и методов, а от понимания и манипулирования социальной динамикой. Еще одним плюсом использования концепции сетевых войн, которые непосредственно работают с населением, является то, что в момент реализации этих стратегий у стороны, против которой они реализуются, нет причины, нет повода и оснований для использования ядерного оружия.

Если в стране начнутся социальные волнения, когда несогласные выходят на площади и проводят массовые акции, то возможность применения ядерного оружия здесь необоснованно ни с какой стороны. Даже если найдена сила, которая дала старт этим процессам, даже если есть уверенность, что все это происходит неслучайно, если даже достоверно установлено, что волнения и требования ухода в отставку лидеров государства имеют искусственное происхождение и центр их инициирования находится в конкретной стране, использование ядерного потенциала будет носить неправомерный характер и выглядеть как агрессия. Это будет явно неадекватным ответом. Поэтому здесь нет возможности его использовать, а это единственное, чего реально боятся американцы.

Таким образом, *наличие ядерного зонтика и поддержание его на уровне современных требований в условиях крайне нестабильной многополярности мировых интересов уже не может служить гарантией суверенитета и территориальной целостности*.

Необходимо отметить, что к этим выводам и теоретическим построениям американские политики и военные пришли в результате обобщения опыта холодной войны против СССР. На первом этапе (80-е – начало 90-х) сетевые войны рассматривались как дополнение обычных форм ведения холодной войны и как чисто теоретические разработки. Лишь с началом третьего тысячелетия они стали превращаться в самостоятельное явление. СССР, не догадываясь об этом, с конца 70-х годов становился объектом все более и более интенсивных и эффективных сетевых атак со стороны США и Западной Европы. Падение СССР стало результатом успеха сетевой войны. Само появление РФ и других республик СНГ есть зримый результат эффективности сетевых войн.

США не могли победить СССР ни в военном столкновении, ни в прямой идеологической борьбе, ни путем лобового противоборства спецслужб. Иерархические структуры СССР были достаточно эффективно защищены от этого. Тогда был задействован главный принцип сетевых стратегий: неформальное проникновение, поиск слабых, неопределенных, энтропических составляющих советской иерархии. СССР свернула не контрсила, не ан-

тисоветская организация, но грамотно организованная, манипулируемая и мобилизованная «энтропия». В еще большей степени объектом сетевой войны стала Россия в 90-е годы. Этому, безусловно, способствовало втягивание страны в глобализационные процессы, проникновение в страну и в сознание граждан воздействий глобальной сети. И это воздействие не ослабевает, а наращивается и в настоящее время.

Сегментами этой глобалистской сети выступает как прямое проамериканское лобби экспертов, политологов, аналитиков, технологов, которые окружают власть плотным кольцом, так и многочисленные американские фонды, которые все еще активно действуют на территории России, подключая к своей сети интеллектуальную элиту. Представители крупного российского капитала и высшего чиновничества естественным образом интегрируются в западный мир, где хранят свои сбережения. Средства массовой информации массировано облучают читателей и телезрителей потоками визуальной и смысловой информации, выстроенной по американским лекалам. И большинство этих процессов невозможно квалифицировать как действия «внешней агентуры», как это было в индустриальную эпоху. К сожалению, технологии информационного века не улавливаются классическими системами и методиками индустриальных спецслужб.

Концептуальные мотивы внедрения сетевого подхода в военную политику США

Мотивами перехода ВС США к сетевым моделям являются:

– расширение влияния США, круга союзников и друзей;

– внушение всему миру мысли об отказе и бессмысленности военной и политической конкуренции с США;

- предупреждение угроз и агрессивных действий против США;

- обеспечение быстрой и решительной победы над противником в случае возникновения угроз;

- реализация конкретных преимуществ, которые дает сетевой подход тем, то опережает всех в его внедрении, а именно :

а) лучшая синхронизация событий и их последствий на поле боя;

б) достижение большей скорости передачи команд;

в) максимизация жертв среди противников, сокращение жертв среди собственных войск, повышение самостоятельности и личной ответственности военных за результат во время проведения военной операции и подготовки к ней.

Сферы ведения сетевых войн

Теория сетевых войн утверждает, что современные конфликты развертываются в четырех смежных областях человеческой деятельности: в физической, информационной, когнитивной (рассудочной) и социальной. Каждая из них имеет важное самостоятельное значение, но решающий эффект в сетевых войнах достигается синергией (однонаправленным, умноженным, согласованным действием) всех этих элементов[1].

1. *Физическая область* – это та область, в которой боевые действия развертывались преимущественно в прежние эпохи. Она не отменяется сетевыми войнами, но ей придается иной смысл. Это реализация традиционных методов ведения войны. В сегодняшних реалиях это означает, что в эпоху сетевых войн никто не отменяет политические организации, движения и людей. И если раньше война в основном зависела от боевой (физической) мощи армии, и ее успехов в физическом противостоянии с противником, то сейчас это лишь одна из четырех областей противоборства.

1 Arquilla J. Ronfeldt D.F. Networks and netwars: the future of terror, crime, and militancy. Santa Monica: Rand Corporation, 2001.

2. *Информационная область* – сфера, в которой создается, обрабатывается и передается информация. В результате возникает информсфера, в которой выигрываются или проигрываются современные войны. Если о той или иной операции не сообщили по телевидению, не дали репортаж в СМИ, то этой операции как бы не существует, она отсутствует в информационной картине дня, а значит, может не учитываться. И наоборот: в роли агрессора против Грузии в 2008 году мировые СМИ выставили Россию при ее полной информационной изоляции.

3. *Когнитивной областью* является сознание бойца. Она является тем пространством, где преимущественно осуществляется ОБЭ. Все основные войны и битвы развертываются и выигрываются именно в этой сфере. Именно в когнитивной области располагаются такие явления, как намерение(замысел) командира, доктрина, тактика, техника и процедуры. Сетецентричные войны придают этому фактору огромное значение, хотя процессы, происходящие в этой сфере, измерить значительно сложнее, чем в физической области. Но их ценность и эффективность подчас намного важнее.

4. *Социальная область* представляет собой поле взаимодействия людей. Здесь преобладают исторические, культурные, религиозные ценности, психологические установки, этнические особенности. В социальном пространстве развертываются отношения между людьми, выстраиваются естественные иерархии в группах – лидеры, ведомые, пассивные массы и т.д., складываются системы групповых отношений. Социальная область является контекстом сетевых войн, который следует принимать во внимание самым тщательным образом.

5. *Синергетический эффект пересечения сфер*. Войны информационной эпохи основаны на сознательной интеграции всех четырех областей. Путем их избирательного наложения и создается сеть, которая лежит в основе ведения военных действий. Речь идет о том, что война в сетевом смысле выигрывается на четырех уровнях, из этого и складывается сетевое управление.

Сферы пересечения этих областей имеют принципиальное значение. Настройка всех факторов сети в гармоничном сочетании усиливает военно-политический эффект от действий вооруженных сил, в то время как прямые действия, направленные против противника, хоть и расстраивают его ряды, но при этом разводят эти области между собой, исключая, тем самым, важнейший фактор превосходства. И хотя сам сетевой подход был позаимствован из концепции сетецентрической организации собственно боевых действий, сами боевые действия становятся либо второстепенным дополнением к уже реализованным мероприятиям в других сферах, либо ограничиваются демонстрацией силы, фактором устрашения.

Основные принципы сетевых операций

1. Достижение информационного превосходства:

а) искусственное увеличение потребности противника в информации и одновременное сокращение для него доступа к ней;

б) обеспечение широкого доступа к информации резидентов через сетевые механизмы и инструменты обратной связи, надежная защита их от внедрения противника;

в) сокращение собственной потребности в статичной информации через обеспечение доступа к широкому спектру оперативного и динамичного информирования[1].

2. Обеспечение всеобщей осведомленности:

а) построение интегральной информационной сети, выстраиваемой и постоянно обновляемой через сырые и обработанные данные, поставляемые разведкой и иными инстанциями;

1 Burke M. Information Superiority, Network Centric Warfare and the Knowledge Edge. DSTO Electronics and Surveillance Research Laboratory, Salisbury, Australia, 2000.

б) превращение пользователей информации одновременно в поставщиков информации, способных незамедлительно активировать обратную связь;

в) максимальная защита доступа к этой сети от противника с одновременной максимальной доступностью ее для подавляющего числа резидентов[1].

3. Управление через замысел командира. В сетевых войнах понятие намерение командира (англ. commander's intent) призвано заменить собой традиционную форму приказа.

В сетевой структуре важной составляющей является уход от иерархического управления, отказ от прямых приказов. Намерения командира – это управление через систему намеков, считывания конечного замысла командира подчиненными. Подчиненные же решают поставленные перед ними задачи, оценивая возможности, с долей автономности в принятии решений. Результатом чего является освобождение командира от ответственности за отдаваемые приказы, подчиненных – за их исполнение, а в целом – повышение эффективности проведения операций. По сути дела, это отдание приказаний с помощью намеков. Намек становится главной формой управления войной. Эффективность армии, управляемой намеками, еще и в том, что намек нельзя перехватить[2].

4. Повышение скорости командования. Скорость командования должна быть увеличена в критической пропорции, чтобы:

– через адаптацию к условиям боя сокращать скорость принятия решений и их передачи, переводя это качество в конкретное оперативное преимущество;

– в ускоренном темпе блокировать реализацию стратегических решений противника и обеспечить заведомое превосходство в соревновании на уровне решений.

Скорость командования в сетевых войнах должна повышаться до невероятных размеров. Смысл ускоренного командования заключается в том, что если одна из противоборствующих сил выполняет приказ быстрее, она лучше и результативнее выполняет поставленную задачу. Для того, чтобы повысить скорость командования, американцы идут на различные ухищрения. В том числе на «разгерметизацию» разведданных (обмен закрытой информацией среди спецслужб).

5. Самосинхронизация (англ. selfsinchronisation) призвана обеспечить возможность базовых боевых подразделений действовать практически в автономном режиме, самим формулировать и решать оперативные задачи на основе всеобщей осведомленности и понимания намерения командира. Для этого следует:

а) усилить значение инициативы для повышения общей скорости ведения операции;

б) соучаствовать в реализации намерения командира, где намерение командира отличается от формального приказа и представляет собой осознание скорее финального замысла операции, нежели строгое следование буквальной стороне приказа;

в) быстро адаптироваться к важным изменениям на «поле битвы» и устранить логику пошаговых операций традиционной военной стратегии[3].

Самосинхронизация означает, что базовое подразделение само формулирует и решает тактические боевые задачи на основе всеобщей осведомленности. Каждая ячейка, действующая в рамках сети, сама способна поставить себе цель.

1 McCormick J.M. Achieving battlespace awareness in network-centric warfare by integrating web and agent technologies // Battlespace Digitization and Network-Centric Systems IV. Edited by Suresh, Raja. Proceedings of the SPIE, Volume 5441, 2004, P. 61-68.

2 Forgues P. Command in a network-centric warfare // Canadian Military Journal. Summer 2001. P. 23-30.

3 Hutchins, S. G., Kleinman, D. L., Hocevar, S. P., Kemple, W. G., and Porter, G. R. Enablers of Self-synchronization for Network-Centric Operations: Design of a Complex Command and Control Experiment //Proceedings of the 6 the international command and control research and technology symposium, CCRP, Annapolis, MD,USA, 2001.

6. Распределенные силы. Задача сетецентричных войн перераспределить силы от линейной конфигурации на поле боевых действий к ведению точечных операций. Для этого следует:

а) преимущественный переход от формы физического занятия обширного пространства к функциональному контролю над наиболее важными стратегически элементами;

б) переход к нелинейным действиям во времени и пространстве, но чтобы в нужный момент иметь возможность сосредоточить критически важный объем сил в конкретном месте;

в) усиление тесного взаимодействия разведки, операционного командования и логистики для реализации точечных эффектов и обеспечения временного преимущества с помощью рассеянных сил[1].

Основной упор в данном случае делается на распределенность – это переход от линейной конфигурации (развертывание фронта) к ведению точечных операций, что похоже на практику партизанской войны. Наступать не фронтом, а мелкими бригадами, синхронизированными между собой. Все это создает предпосылки к наступлению эпохи постмассовых войн, в которых количество людей, физической силы – перестает иметь значение, как, например, перестает иметь значение количество политических активистов в партии.

7. Демассификация.

Принцип демассификации отличает войны постмодерна от войн модерна, где почти все решало количество и качество боевых единиц. Демассификация основана на:

а) использовании информации для достижения желаемых эффектов, ограничивая необходимость сосредоточения крупных сил в конкретном месте;

б) увеличении скорости и темпа перемещения на поле действий, чтобы затруднить возможность противника к поражению цели[2].

8. *Глубокое сенсорное проникновение*. Этот принцип сетецентричной войны представляет собой требование увеличения количества и развития качества датчиков информации как в районе боевых действий, так и вне его. Это проникновение обеспечивается за счет:

а) объединения в единую систему данных, получаемых разведкой, наблюдением и системами распознавания;

б) использования сенсоров как главных маневренных элементов;

в) использования датчиков и точек наблюдения как инструмента морального воздействия;

г) снабжения каждого орудия и каждой боевой единицы (платформы) от отдельного бойца до спутника – разнообразными датчиками и информационными сенсорами.

Глубокое сенсорное проникновение означает, что информация собирается из различных источников. Боевая единица должна иметь различные устройства считывания информации – от микрофона до различных счетчиков и датчиков. При этом человек не задумывается над их работой, однако информация обо всем, происходящем вокруг него, поступает на командный пункт. Глубокое сенсорное проникновение ведет к оснащению различных боевых единиц максимальным количеством средств наблюдения[3].

9. *Изменение стартовых условий ведения военных действий*. Еще классическая военная стратегия обнаружила, что результативность войны напрямую зависит от стартовых условий. От того, в каком контексте и при каком балансе сил начнется война, во многом зависит, как будут развертываться дальнейшие

1 The implementation of network-centric warfare. Washington. D.C. Office of the Secretary of Defense, 2005.

2 Vego M. Joint operational Warfare. Washington. D.C. 2009.

3 The implementation of network-centric warfare. Washington. D.C. Office of the Secretary of Defense, 20.

события. В этой связи задача сетевых войн заключается в том, чтобы:

а) заранее повлиять на стартовые условия войны, заложить в них такую структуру, которая заведомо приведет (американскую) сторону к победе;

б) спровоцировать сочетание во времени и в пространстве ряда событий, которые призваны повлиять на потенциального противника и блокировать его ответную инициативу.

Оптимизация стартовых условий ведения боевых действий наиболее близка к принципу ОБЭ. То, в какой конкретно конфигурации, каком состоянии страна начинает войну, на 90% определяет ту реальность, в которой она окажется по результатам ведения военных действий.

10. *Сжатые или компрессионные операции* – это такие операции, в которых преодолеваются структурные и процедурные разграничения между различными службами, а полный доступ к разнородной информации обеспечивается даже на низшем уровне боевых единиц. Для этого:

1) повышается скорость развертывания и применения боевой силы, а также обеспечения боеприпасами;

2) отменяется фрагментация процессов (организация, развертывание, использование, обеспечение и т.д.) и функциональных областей (операций, разведки, логистики и т.д.);

3) отменяются структурные разграничения на низовых базовых группах.

Таким образом, сжатые или компрессионные операции состоят в преодолении структурных процедурных ограничений между службами и обеспечении полного доступа к разнородной информации.

Применение принципов сетевых войн

Сетевые войны на основе перечисленных принципов предназначены для реализации в тех условиях, когда необходимо избежать ядерного столкновения и невозможно (или накладно) полноценно использовать технические средства индустриальных войн. Пространством сетевой войны становится вся территория планеты, так как в эпоху глобализации между внутренней и внешней политикой граница все более стирается, и все факторы начинают прямо влиять друг на друга. Осваивание стратегий ведения сетевых войн только начинается – как при ведении военных действий (армия США в Ираке, Афганистане), так и при создании «стартовых условий» конфликта до его начала (позиционные действия проамериканских сетей на постсоветском пространстве) – через экспорт «цветных революций» в Грузии (2004), Украине (2004), Киргизии (2005), события «арабской весны» и т.д. В основу построения и деятельности молодежных оппозиционных движений, таких как «Отпор» (Сербия), «Кмара» (Грузия), «Пора» (Украина), «Зубр» (Белоруссия) были положены принципы гражданской обороны(civil defense) и ненасильственных действий (non-violent actions), разработанные по той же самой логике и теми же самыми мозговыми центрами, которым принадлежит авторство доктрины сетевых войн. В доступной форме эти принципы изложены в работе Джина Шарпа «От диктатуры к демократии».

Сегодня надо отдавать себе отчет, что в пространстве постмодерна защититься можно только используя адекватные методы – методы сетевых войн. Ни наличие многомиллионной армии, ни ядерное оружие, ни спецслужбы «старого образца» не гарантируют надежной защиты. Вернуть эффективность и действенность оружия прошлой исторической эпохи – индустриальной – можно только одним-единственным способом. Для этого необходимо в масштабах планеты уничтожить всю технологическую инфраструктуру глобальных коммуникаций. Едва ли это реальная перспектива, за исключением, конечно, эсхатологического сценария глобальной «ядерной зимы». США понимают это как ни одно другое государство, поэтому в последние годы выступают главными инициаторами ядерного разоружения, одновременно наращивая и институциализируя свое превосходство в об-

ласти оружия шестого поколения, создавая наряду с этим глубоко эшелонированную систему национальной противоракетной обороны (готовность ПРО – к 2020г.) и другие новейшие схемы защиты своих коммуникаций.

Чтобы эффективно противостоять такой стратегии, необходимо четко понимать содержание такой войны и те силы, которым надо противостоять.

Сущность сетевой войны: информационный контроль

Конечная цель сетевой войны – как и любой войны – установление контроля над зоной, которая не принадлежит воюющей стороне, или сохранение контроля над зоной, которая ей принадлежит, от посягательств противника. Здесь ничего нового. Меняется только понимание того, что есть: 1) зона, 2) контроль и 3) противник.

В сетевой войне реальность является вторичной по отношению к виртуальному образу. Имидж, информация гораздо важнее реальности. Сама реальность становится «реальной» только после того, как сообщения о ней попадают в информационное поле. Отсюда вывод: главное – контроль над информационным полем.

Тот, кто контролирует информационное поле – тот контролирует все. Информационное сопровождение войны становится не второстепенным обслуживающим моментом (как классическая пропаганда), но смыслом и сутью войны. По сути, война носит информационный характер. Классические боевые операции эпохи модерна носят подсобный второстепенный характер.

Пространство в сетевых войнах

1. Меняется качество представления о зоне. Зона, над которой устанавливается контроль – не просто физическая территория со строго определенными границами, но виртуальное пространство, помещенное на плоскости переплетенных информационных потоков. Подчас необходимо контролировать лишь несколько важнейших точек этой зоны, чтобы это пространство оказалось управляемым в информационном поле. А в некоторых случаях не обязателен даже точечный контроль – достаточно имиджа, симуляции или постановочных кадров.

Если в информационном пространстве создается образ контроля над данной зоной, то тем самым достигается эффект и по отношению к союзникам, и противникам, и по отношению к тем, кто находится внутри этой зоны. Даже если их взгляды свидетельствуют о том, что никакого контроля нет, за счет информационной блокады они не могут поделиться этим «знанием», которое тем самым обесценивается, оставаясь на «подинформационном» уровне.

2. Зона, над которой устанавливается контроль, не обязательно включается в общее пространство на общих основаниях. Колонии Великобритании были частью Британской Империи только в одностороннем порядке: метрополия брала у них все, а им ничего не давала, контролируя побережье, лавным образом, орты.

В сетевых войнах необязательно напрямую оккупировать или аннексировать территории: достаточно установить над ними сетевой контроль. Это означает контролировать СМИ, финансовые потоки, потоки сырья, доступ к технологиям (их ограничение), политическую и культурную элиту, болевые центры активности молодежи.

Основой любой сети является «активное меньшинство» – «acting minority», «minorite agissante», которому уделяется особое внимание.

Контроль в сетевых войнах: манипуляции с алгоритмом

Контроль также меняет свое качество. В сети главное контролировать протокол, алгоритм, а не сами потоки информации. Информация может циркулировать достаточно свободно, важнее всего то, как ее декодировать. В центре внимания не столько контроль над самой информацией, сколько над кодом.

Специалисты сетевых стратегий могут придать даже негативной или опасной информации на выходе или в процессе ее передачи прямо противоположный характер, сделать ее безвредной или погасить ее основной импульс.

По мере увеличения объема свободно циркулирующей информации на первое место становится сокрытие и управление кодом. Главное в сетевой войне – держать в секрете алгоритмы дешифровки информации, ее структуризации, обобщения и конечного использования. Эффективное обращение с информацией позволяет изменить в свою пользу даже те информационные потоки (включая денежные средства, перемещения войск или политических групп противника и т.д.), которые на первый взгляд невыгодны. Поскольку главный контроль – это контроль не просто над пространством, но над информационным (виртуальным) пространством, то первостепенное значение приобретают манипуляции с алгоритмом.

Противник в сетевых войнах: «все – противники» («панхостия»), виртуальность противника

Виртуальный характер сетевых войн меняет идентичность противника. Во-первых, теоретики сетевых войн поясняют, что сетевые операции ведутся не только против врагов, но и против нейтральных сил или друзей. Контролировать надо всех, а значит, алгоритм ведения операций скрывается от всех (включая союзников).

Во-вторых, сеть – явление динамическое, и сегодняшний союзник может превратиться в завтрашнего противника (и наоборот), поэтому распределение ролей в сетевой войне носит отчасти условный характер. Так как они все равно ведутся против всех, поэтому «образ врага» становится все более и более подвижным.

Этим, кстати, во многом объясняется стремление США к тотальной прослушке, тотальному контролю за десятками миллионов людей по всему миру, включая лидеров полутора десятков государств, в т.ч. союзных.

В-третьих, враг становится все более и более виртуальным. В каком-то смысле, его может и не быть, и сетевая война может вестись с фиктивным противником, ежду тем боевые действия и последствия войны могут быть вполне реальными.

Аль-Каеда и международный терроризм являются практически нелокализуемой и не фиксируемой силой. Под ней всякий раз можно понимать различные реальности – то Афганистан и талибов (имеет некоторое отношение к радикальным салафитским структурам «чистого ислама» наподобие структур Бен-Ладена), то Ирак Саддама Хусейна (ни малейшего идеологического или организационного отношения к Аль-Каеде не имевшего), то шиитский Иран (являющийся политически, религиозно, идеологически и организационно прямой противоположностью Аль-Каеды).

Таким образом, специфический противник в условиях сетевой войны может (и скорее всего так и будет) представлять собой достаточно разнообразные и «разномастные» силы, в той или иной степени управляемые сетевыми операторами.

Терроризм как сетевое явление

После теракта 11.09.2001 г. американские специалисты по сетевым войнам столкнулись с тем, что сетевые методы, до этого используемые только ими, взяли на вооружение маргинальные экстремистские группы. Согласно официальной версии Вашингтона представители Аль-Каеды осуществили сетевую атаку, которая была проведена по всем правилам сетевых войн. В ней использовались самолеты гражданской авиации, зубные щетки с заточенным концом в руках смертников, захвативших лайнеры, ножи для резки бумаги, взлом компьютерных сетей, ответственных за контроль над воздушным пространством США, перевод денег по линии гуманитарных фондов, мелкие религиозные секты и т.д.

Ничтожная по сравнению с мощью США структура с помощью творческого воображения, понимания устройства американской системы и сути сетевой войны нанесла США такой удар, который сопоставим с потерями в реальной войне. Так крохотная сетевая Аль-Каеда стала на один уровень с мировой державой. Тогда американские стратеги впервые осознали, что те же методы могут быть направлены против них самих. Причем не сопоставимыми с ними силами, обладающими ядерным потенциалом (такими как, например, Россия), а горсткой разыскиваемых по всему миру фанатиков.

Террористы первыми усвоили уроки информационного общества: *реальность есть то, о чем сообщают СМИ*. Поэтому, чтобы сообщить о своих взглядах (политических, религиозных и т.д.), которые оставались за кадром основных информационных потоков, они прибегали к актам насилия и жестокости (заложники, теракты и т.д.), о которых нельзя было промолчать. С другой стороны, террористические сети также использовали весь арсенал сетевой стратегии: небольшие самостоятельно функционирующие группы, понимание *намерения командира* (commanders intent), *всеобщую* (распределенную) *осведомленность* (shared awareness), *обратную связь*, *самосинхронизацию* (self sinchronisation), ставку на *деятельное меньшинство*. На первом этапе инициатива сетевых войн была в руках американцев. Сегодня они столкнулись с тем, что им самим брошен асимметричный, но болезненный вызов.

Разрабатывая меры противодействия – *сетевые команды* (network team) американцы пока не придумали ничего нового, как усиление тоталитарных мер для противодействия сетевым вызовам на своей территории или на территории, находящейся под контролем США (как, например, Грузия, Украина и т.д.), хотя сами же американцы широко используют и поддерживают террористические организации и группы боевиков в своих сетевых атаках в других странах.

Естественные сети: этнические и религиозные меньшинства

В сетевой войне могут использоваться как готовые сети, так и создаваться новые. Наиболее подходящими готовыми сетями являются этнические и религиозные общины (чаще всего меньшинства и секты). В государственных машинах эти факторы в современном мире чаще всего не имеют строго регламентированного административного положения, поэтому этнические и религиозные меньшинства существуют де-факто, но не де-юре. Это позволяет им действовать вне зоны прямого внимания закона и юридических процедур.

Сами эти сети почти никогда не могут ставить перед собой масштабных стратегических задач, но сетевые операторы способны легко превратить их в эффективный и действенный инструмент сетевых атак. В любой стране этнические меньшинства и миноритарные религиозные общины представляют собой объект повышенного внимания стратегов сетевой войны, и прежде чем создавать искусственные структуры, используются именно эти готовые механизмы. Инвестируя внимание, средства и технические навыки в ключевые точки таких сетей, можно добиться колоссального успеха.

Искусственные сети: НПО, фонды, правозащитные организации, научные сети, молодежные движения

Естественные сети, поставленные под структурный контроль, дополняются искусственными сетевыми структурами, имеющими чаще всего безобидный вид: правозащитная деятельность, некоммерческие партнерства, образовательные инициативы, центры распределения грантов, научные и социологические сети, общественные организации разных видов. Так как деятельность таких структур ни в уставах, ни в рутинной практике не имеет ничего предосудительного, противозаконного, чрезвычайно трудно фиксировать те состояния, в которых эта сеть (или ее отдельные, на

вид безобидные сегменты) переводится в режим подрывной деятельности.

Продвижение таких искусственных сетей Запад сделал своей официальной политикой и всячески критикует те страны, которые препятствуют этому процессу.

Поскольку нити управления деятельностью сети находятся не в самой сети и, тем более, не у ее членов, а в удаленном центре сетевого управления, сами ее участники могут не иметь ни малейшего представления, на кого они работают и какую роль выполняют. Поэтому чаще всего они действуют искренне, что делает этот вид сетевого оружия особенно эффективным и трудно преодолимым [1].

Агентура влияния в сетевом мире

В сетевых войнах меняется сама структура агентов влияния. Все чаще стратеги сетевых войн избегают прямой вербовки, предпочитая действовать в полутонах. Активное меньшинство в социально-политической сфере, намеченное в качестве потенциального агента влияния, обрабатывается более изящно: через повышенное внимание западной прессы, приглашение на научные конференции, через гранты и симуляцию интереса к идеям и проектам какого-либо деятеля или группы. В случае невнимания (недостаточного внимания) в отечественной среде при таком подходе (искусственном внимании со стороны) человек психологически подталкивается в нужном направлении.

Глобализация как форма ведения сетевой войны

Важнейшим элементом сетевых стратегий является включение локальных сетей в более широкие и глобальные. Сам факт подключения экономических, энергетических, информационных, научных ресурсов страны к глобальным сетям автоматически дает преимущество тем, кто контролирует код, протокол и алгоритм функционирования этих сетей.

Глобализация в таких случаях подается как «объективный», «демократический», «позитивный», «прогрессивный», «неизбежный» процесс, ведущий к «развитию» и «модернизации». На самом деле, в большинстве случаев это действительно так лишь отчасти. Подключение к глобальной сети может дать определенные преимущества. Но вместе с ними резко возрастает риск установления внешнего управления, так как архитекторы, создавшие и контролирующие глобальные сети, а также управляющие их развитием, заведомо находятся в более выигрышном положении, чем те, кто только к этим сетям подключается. Скорость сетевых процессов такова, что даже краткого замешательства или тайм-аута, необходимого для освоения правил сетевых игр, достаточно, чтобы потерять контроль над собственной сетью.

Подготовка внешнеполитических условий для сетевой агрессии

Практика последних десятилетий наглядно свидетельствует о том, как США совершенствуют глобальные сетевые технологии, стремясь упрочить и расширить свое влияние, в первую очередь, в странах бывшего социалистического лагеря, странах СНГ, а также в странах арабского Востока и Африки.

Все «бархатные революции», происходящие в мире и, в частности, на постсоветском пространстве, – есть явление, спровоцированное США для установления геополитического контроля над теми государствами и территориями, которые прежде находились в зоне влияния России.

США используют новейшую технологию ведения войны – «войну шестого поколения», т.е. сетевую войну – технологическую разработку, полностью находящуюся в компетенции госдепа США и Пентагона и сегодня успешно реализуемую на пространстве СНГ.

Обычно когда речь идет о сетевых войнах, результат достигается с помощью социальных сетей, т.е. с помощью самого общества, в котором выделяется сегмент, где формируется определенным образом общественное мнение, направленное против действующего режима. Характерная особенность сетевых тех-

нологий и «бархатных революций» то, что на них основаны главные алгоритмы : под предлогом якобы очевидных претензий к власти – спровоцировать волну самоиндуцирующегося протеста, развивающегося по нарастающей под воздействием «психоза соучастия». Само же общество выводится из состояния равновесия, нарушаются социальные устои, падает авторитет власти, растет недовольство. А о нормальном функционировании экономики, которая подорвана инициированным кризисом, говорить не приходится.

Все это – идеальные условия для навязывания и установления западных моделей социального устройства. В страну заходят США. Никаких преимуществ ни политические силы этих государств, ни их общества от реализации сценариев «бархатных революций» не получают.

Единственная сила, в любом случае получающая с этого политические дивиденды, – это США, устанавливающие таким образом безболезненный, невоенный, «мягкий» контроль над своими новыми территориями.

Однако, все еще оставаясь ядерной державой, большая Россия вызывает обоснованные опасения у наших «друзей по перезагрузке». Прямое вероломное вмешательство в дела стран постсоветского пространства не может не вызывать у России недовольства. А вот это как раз для США нежелательно. Потому что основной целью для США, чего они практически не скрывают, является контроль над самой Россией.

Реализуя главную задачу своей геополитики – не пропустить Россию через Южный Кавказ к Ирану, – США стремятся максимально дестабилизировать это небольшое пространство (где помимо Грузии находятся еще Азербайджан и Армения) или установить там свой прямой военно-стратегический контроль, физически перегородив выход России к Индийскому океану.

Эта задача осуществлялась по сценарию «бархатной революции» в Грузии. И была практически решена, сли бы не вышедшие из под американского контроля патриотические силы, нейтрализовавшие влияние Саакашвили.

Грузия, выведенная из-под остаточного геополитического контроля России, который еще сохранялся там с момента распада СССР, новь стремится к восстановлению отношений с РФ.

Попытки «цветных» переворотов были осуществлены и в Армении, и в Азербайджане. Что касается Украины, здесь задача была примерно схожей. Украина для России является своего рода мостом в Европу. Как пишет З.Бжезинский, без Украины Россия перестает быть евразийской державой и становится державой азиатской.

К тому же Украина является важнейшим элементом «санитарного кордона», который отсекает Россию от стран ЕС и не дает ей возможности наладить полноценное стратегическое партнерство с Европой.

На пути к этому партнерству, в первую очередь, с Германией, и выстраивается «санитарный кордон», простирающийся от холодных северных морей по странам Балтии, через Украину, Молдавию, далее вниз, к Грузии.

Пока минуя Беларусь, которая все еще является последней брешью в этом «санитарном кордоне», а его функции все еще активно выполняет Польша.

Пояс, отсекающий Россию от Европы, создан американцами для решения важнейших стратегических, геополитических задач путем последовательного инициирования «бархатных революций» в этих государствах в рамках сетевой войны, ведущейся против России.

Несмотря на нынешнюю риторику о выводе американских войск из Афганистана страны США никогда не отступятся от задачи установления полного контроля и над среднеазиатским регионом. И для этого они будут продолжать дестабилизировать там ситуацию, пытаясь взять Узбекистан и Киргизию под полный контроль.

Обычно за такими не до конца состоявшимися попытками совершения «бархатного

переворота», какие мы наблюдали в узбекском Андижане, или несколько смазанной ситуацией с «каскадом революций» в Киргизии следуют более жесткие сценарии. То есть воздействие ужесточается по нарастающей. «Бархатный» сценарий сменяется более жестким – стычки с полицией, первые жертвы, погромы, – ну а дальше обычно начинается раскачка ситуации по этническому принципу, так как это наиболее тяжелая для разрешения стадия, это выход ситуации из-под контроля. Цель – заставить руководство этих государств согласиться с тем, что контроль над ситуацией со стороны власти потерян, что власть выпала у них из рук. Результат в любом случае – взятие территории государства под американский контроль.

Таким образом, несмотря на заверения американцев, что пространство СНГ останется в зоне геополитических интересов России, фактически мы наблюдаем стремительную потерю своего влияния там, где еще совсем недавно стояли наши военные базы, жили наши люди, говорящие на нашем языке, а русская культура формировала поколения народов и этносов единого стратегического пространства большой России.

Проведенный, даже беглый, анализ содержания, особенностей и последствий сетевых войн позволяет сформулировать несколько существенных, на наш взгляд, **выводов**, касающихся решения проблем обеспечения национальной безопасности РФ в сложившейся обстановке.

1. Адекватным ответом на сетевые угрозы, безусловно, может стать только сетевая же оборонительная стратегия, кардинально меняющая саму концепцию обеспечения национальной безопасности, а, значит, и военную доктрину.

2. Имеющаяся военная мощь государства, военно-экономический потенциал не являются теперь ни интегральными показателями, ни измерителями, ни гарантами национальной безопасности. Да, конечно, их роль как фактора влияния, устрашения, эффективного щита при ведении традиционных боевых действий, пока еще сохраняется, но при определенных обстоятельствах, о чем мы говорили выше, может оказаться, что они бесполезны.

3. В силу разного рода причин все труднее становится отделить военную безопасность одного государства региона от других государств, что неизбежно ведет к региональной военно-политической интеграции. Примером тому являются блоки и военно-политические союзы, прежде всего Североатлантический блок, который стал ярким примером не только военно-политической интеграции, но и фактически стимулировал интеграцию в рамках Евросоюза. В этом смысле Организация Варшавского Договора также являлась закономерным примером региональной военно-политической интеграции.

Простой пример. Создание региональных систем ПРО США (с перспективой глобальной ПРО) неизбежно ставят по-новому проблему ВКО не только стран ОДКБ, но и других евразийских государств. Не случайно поэтому на Ашхабадском саммите глав государств еще в декабре 2012 года речь шла уже не столько об экономических проектах, сколько о создании Объединенной системы противовоздушной обороны (ОС ПВО) государств СНГ, для чего был не только создан специальный координационный комитет, но и назначен его руководитель – бывший командующий ВКО России (а затем заместитель министра) О.Остапенко[1]. Это означает, что уникальные свойства суверенитета – возможности ПВО – некоторые государства готовы делегировать наднациональному органу. В целом же, как уже говорилось, эти решения соответствуют объективным тенденциям развития региональной безопасности, которые отчетливо просматриваются на примере эволюции НАТО.

1 McCormick J.M. Achieving battlespace awareness in network-centric warfare by integrating web and agent technologies // Battlespace Digitization and Network-Centric Systems IV. Edited by Suresh, Raja. Proceedings of the SPIE, Volume 5441, 2004. P. 61-68.

Очевидно, что на этом государства не остановятся: неизбежно не только расширение ОС ПВО до ОС ПВО–ПРО, но и создание единой системы управления (а значит и делегирование полномочий), разработки общей концепции ВКО, планов военного строительства и т.д. И это тоже будет продолжением объективных тенденций.

Безусловно, без создания конкурентоспособных национальных и коллективных информационных ресурсов (в т.ч. элементной базы, ПО, ВВТ, СМИ и т.д.) обеспечить эффективную оборону и суверенитет страны невозможно. В том числе и эффективную ВКО страны, региона или континента. Кроме того, необходимы специальные – сетецентричные, многократно дублированные и защищенные от кибератак – органы коллективного государственного, военного и общественного управления. Следует обязательно заметить, что львиная доля расходов на эти цели, естественно, ридется на долю России.

4. Некоторые действия США наводят на размышления об их серьезных намерениях и возможностях массового полномасштабного воздействия на информационную инфраструктуру страны-противника. Так, США оперативно среагировали на новые возможности, создав в 2009 г. на базе АНБ и подразделений ВВС специализированного киберкомандования (US Cyber Command). Практически сразу аналогичные структуры стали появляться и в других государствах [2].

Формальной миссией киберкомандования США является планирование и координация действий по защите информационных сетей министерства обороны, а также, в особых случаях, проведение полномасштабных военных операций в киберпространстве[1]. То есть киберкомандование США не выполняет задачи по обороне сравнительно уязвимой информационной инфраструктуры страны (ее компоненты – системы управления сетями энергоснабжения, транспортом, информационные сети финансовых организаций и т.п.), концентрируясь на обороне только и исключительно элементов военной инфраструктуры[2]. Частично раскрытая в июле 2011 г. стратегия операций в киберпространстве, кроме подтверждения заявлений о намерении охранять информационные сети министерства обороны, содержит также программное заявление о признании киберпространства доступным для ведения боевых действий наравне с землей, морем, воздухом и космосом[3]. Но наряду с этим в описываемом программном документе содержится тревожащее заявление о допустимости ответа на кибератаки всеми необходимыми средствами, включая прямые силовые воздействия вплоть до проведения военных операций[4].

Таким образом, создается по сути дела новый тип наступательного оружия, которое может быть использовано на самых ранних стадиях военного конфликта. Не представляет сомнений, что США обладают физической возможностью по нарушению функционирования глобальных информационных сетей, даже если эта возможность и не обозначена законодательно. Можно предположить, что крайней мерой в кибервойне, сравнимой с использованием тактики выжженной земли в реальном мире, может стать физическое уничтожение информационно-коммуникационной инфраструктуры, если это будет отвечать принципам обеспечения безопасности государства [2]. Прежде всего с помощью высокоточного оружия, которое в массовых масштабах появляется уже сегодня. Естественно, приходится констатировать, что мероприятия по

1 Cyber Command Fact Sheet / U.S. Department of Defense. 21.05.2010.

2 Cyberwar Commander Survives Senate Hearing, Threat Level // Wired. 15.04.2010.

3 Department of Defense Strategy for Operating in Cyberspace. July 2011 / US Department of Defense / http://www.defense.gov/news/d20110714cyber.pdf

4 David E. Sanger and Elisabeth Bumiller. Pentagon to Consider Cyberattacks Acts of War // The New York Times. 31 мая 2011 г. /http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=1; White House Cyber Czar: 'There Is No Cyberwar' // Wired magazine. 4.03.2010 г.

защите от подобной агрессии будут достаточно затратны.

5. Эффективное противостояние тотальным сетевым угрозам в дополнение к ядерному арсеналу сдерживания предполагает использование новейших кибернетических методов глобализации и интеграции процессов управления, универсальных сетецентрических средств их реализации.

Стратегия противостояния при этом должна опираться на *достаточную оборону, для которой необходимы асимметричные сетецентрические ответы, которые при минимальных затратах средств и времени могли бы стать фактором сдерживания и нейтрализации сетевых угроз, дополняющим ядерный оборонный потенциал*.

Главная новизна требований к альтернативным сетецентрическим системам и средствам – способность к функциональной адаптации и адекватно-пропорциональному реагированию в реальном времени в непрерывном спектре изменений оперативно-тактических и стратегических угроз при существенно меньших (на порядки) издержках создания и эксплуатации. Для этого необходима единая и универсально программируемая компьютерно-сетевая среда сетецентрического управления (СЦУ), которая в динамически перестраиваемых (на программном уровне) иерархиях сквозных циклов управления способна единообразно охватывать не только все армейские структуры, но и оборонно-промышленный комплекс, а также, в долгосрочной перспективе, и все институты жизнеобеспечения страны (промышленность, экономика, госуправление, безопасность техносферы, здравоохранение, образование, наука, социосфера и т.д.) [4].

В основе сетецентрического противостояния лежит требование полноты и сверхоперативности информации о текущем состоянии всего многофакторного пространства угроз и собственных средств противодействия. Успех определяется не только возможностями точечных воздействий отдельными видами оружия, но и, что крайне важно, превосходящими возможностями сетецентрического интеллекта по управлению сложнейшими процессами многоходового противостояния.

Создание универсального системного интеллекта предполагает новую электронную компонентную базу (ЭКБ). В дополнение к стандартным микропроцессорам, которые являются носителями операционных систем и существующего ПО, *в состав ЭКБ нового поколения, предназначаемой для полномасштабного решения задач СЦУ, о мнению специалистов, должны войти*:

- однокристальные компьютерные устройства с немикропроцессорной архитектурой, обладающие встроенным системным интеллектом, необходимым для формирования единого, универсально-программируемого пространства распределенных/параллельных вычислений и сетецентрического управления;

- высокопроизводительный многопроцессорный ускоритель для задач с массовым параллелизмом, масштабируемая архитектура которого обеспечит наращивание производительности в диапазоне от 1 до 30Т флопс и более, снимаемой с одного кристалла СБИС;

- реконфигурируемый набор устройств сопряжения с объектом, реализуемый посредством ПЛИС-технологии, который включает типовые блоки (библиотечный набор) и специфические блоки, которые программно конфигурируются в рамках ПЛИС-технологий с учетом особенностей конкретных объектов сопряжения.

По их мнению, новая ЭКБ позволит при минимальных затратах средств и времени обеспечить достижение национально-технологической независимости и определяющего превосходства в следующих областях:

- разработка новых и глубокая модернизация существующих видов вооружений на основе отечественной компьютерной ЭКБ, открывающей новые возможности для опережающего решения задач СЦУ с высокими уровнями структурно-динамической сложно-

сти и управляющего компьютерного интеллекта;

- разработка и применение комплексных методов, а также компьютерно-сетевых средств и технологий СЦУ, которые открывают возможности для охвата в едином информационно-алгоритмическом пространстве всех взаимодействий в реальном времени на объединенном пространстве ТВД (суша, воздух, море, космос, глобальное информационное пространство) с обеспечением функциональной полноты и системной целостности оперативного, тактического и стратегического уровней управления;

- разработка систем СЦУ двойного назначения, направленных на массовую интеллектуализацию и кардинальное улучшение качества управления, которые обеспечат возрождение, конкурентоспособное развитие и безопасность национальной экономики в условиях остроконфликтной глобализации мирового экономического пространства [3].

Кстати, все эти мероприятия носят, безусловно, затратный характер, хотя асимметричны соответствующим угрозам и, естественно, должны войти в новую ГПВ.

Кроме того, асимметричная концепция «оборонительного» сетецентризма предполагает формирование универсального алгоритмического пространства распределенных вычислений и сетецентрического управления с метрикой «все влияет на все и сразу», которое способно охватить совокупные сетевые ресурсы всех видов ВС. В этом пространстве открываются возможности оперативного конфигурирования (реконфигурирования), а также программирования (перепрограммирования) и онлайн исполнения любых моделей интеллектуальных сетецентрических систем, обеспечивающих высокодинамичное управление всей совокупностью боевых действий в сильносвязном информационно-алгоритмическом пространстве.

В среднесрочной и долгосрочной перспективе такое пространство может быть распространено (при ограниченных затратах средств и времени) на все виды вооружений и процессы непрерывного ресурсообеспечения этих действий (как в случае тотальных, так и множественных локальных угроз и воздействий). Однако, если это киберпространство не сможет охватить контролем политическое, экономическое, социальное противоборство, управление боевыми действиями просто не потребуется.

6. Безусловно, необходимо переосмысление методологических аспектов организации и функционирования экономики национальной безопасности государства в условиях угрозы сетецентрической войны и борьбы агрессора за мировое господство. В частности, требуются новые, адекватные стоящим задачам, разработки в области теории военной экономики, которая не перестает быть актуальной, но становится еще более многоплановой, многоаспектной, еще более всеобъемлющей по затратам и привлекаемым ресурсам. Например, елевые затраты госдепа США, спецслужб и частных фондов на «поддержку» демократии в России, подрывной деятельности несистемной оппозиции ежегодно составляет более 70 миллионов долларов, всего в эту подрывную деятельность с 1992 года вложено не менее 12 млрд. долл. (на поддержку украинской оппозиции на Евромайдане США тратили 1млн. долл. в день, а всего израсходовали свыше 5 млрд. долл.). Безусловно, противостояние такому напору, во-первых, будет иметь, в конечном счете, военно-политическое значение, во-вторых, отребует также серьезных затрат, оторые будут носить, несомненно, военно-экономический характер. Поэтому следует по-новому трактовать некоторые военно-экономические категории, их экономическое содержание и сущность.

Так, к критериям эффективности военной экономики в новых условиях, на наш взгляд, следует относить:

а) обеспечение адекватного ответа на угрозы или их предотвращение с минималь-

ными или меньшими, ем у противника затратами;

б) в условиях программно-целевого планирования выполнение программ с минимальными затратами и в заданные сроки;

в) обеспечение комплексного ответа на угрозы, резко сокращающие затраты по другим направлениям и противодействию другим угрозам;

г) обеспечение принятия таких контрмер, которые потребовали бы больших затрат от агрессора для парирования контругроз;

д) обеспечение принятия контрмер, препятствующих наращиванию угроз по другим направлениям;

е) обеспечение достижения военно-политических целей без урона и истощения военно-экономического и военного потенциала государства.

Должны измениться и требования к ресурсообеспеченности новой оборонной стратегии. Среди них, по нашему мнению, основными являются:

а) достаточность ресуров для обеспечения достижения военных, политических, экономических целей без применения или с минимальным участием военной силы;

б) способность ресурсного обеспечения эффективно противостоять сетевым угрозам по любым направлениям и в любых сферах;

в) способность ресурсного обеспечения к осуществлению превентивных мер сетевого характера;

г) способность ресурсного обеспечения обусловливать синергетический эффект и комплексный характер противодействия угрозам.

Кроме того, следует рассматривать и новые показатели ресурсообеспеченности. Например:

а) ресурсообеспеченность соответствующих программ противостояния угрозам по различным направлениям;

б) ресурсообеспеченность осуществления системных мер на реализацию сетевой оборонной стратегии.

Вследствие значительного расширения сфер и направлений угроз национальной безопасности традиционное толкование военной экономики как объективной реальности в пределах оборонного комплекса и войскового хозяйства Вооруженных Сил уходит в прошлое, потому что все более разнообразными становятся как сами военно-экономические ресурсы, так и их источники. Конечно, необходимы специальные, более глубокие исследования по совершенствованию военно-экономического инструментария, всей теории военной экономики, без которых практическое управление ресурсным обеспечением национальной безопасности невозможно или малоэффективно, особенно, в условиях сетевого агрессивного воздействия в политической, экономической, социальной и морально-политической сферах, тем более в условиях сетевой войны.

7. Главное действующее лицо в современной войне интеллектов, конечно же, тот, кто всем этим управляет, кто все это программирует, контролирует, инициирует саму идею сетевого ведения боевых действий или организацию противодействия им.

Ключевой элемент – не оружие и высокие технологии, а человек. Необходимы терпеливые, настойчивые специалисты со знанием культурных, национальных особенностей и традиций, чтобы развивать региональные связи и партнерства в рамках такого рода войн. Ведение США длительной сетевой войны связано с необходимостью мобилизации глобальных возможностей наших ресурсов, первую очередь, человеческих и развитием их потенциала.

Возникает потребность в новых специалистах, возникает класс сетевого труда. Смысл работы этих специалистов заключается в том, что они имеют очень широкую специализацию, обширную компетенцию. С точки зрения сети, по-новому оценивается понятие дилетанта. Талантливый сетевик – networker – это нечто иное, чем талантливый физик. Как правило, хорошим сетевиком может стать не-

далекий физик, не способный погрузиться в глубинное познание, но при этом способный к компилированию и импровизации. У него есть определенная сетевая парадигма, знание, код, с помощью которого он с легкостью способен отделять в потоке информации сущностное от второстепенного. При отбрасывании деталей он может и теряет профессиональную адекватность, но зато приобретает сетевую адекватность; он схватывает на лету ядро, при необходимости наращивая на него детали. Применительно к теории войн это означает, что сейчас победить противника может тот, кто в состоянии создать наиболее эффективную сеть, в которой возникает наиболее легкий и свободный обмен информацией.

В связи с этим совершенно иное содержание приобретает военно-социальная политика государства во всех ее проявлениях, что обусловлено, в первую очередь, повышающимися требованиями к военнослужащим новой формации, их уровню подготовки, выучке, условиям воспроизводства их рабочей силы и реализации творческого потенциала.

По нашему мнению, речь должна идти о решении следующих проблем, фактически конкретизирующих важнейшие концептуальные направления военно-социальной политики:

а) в области военного образования:

речь должна идти не просто о соответствии стандартов военного образования стандартам ГОС ВПО по всем соответствующим компетенциям, а о придании высшей военной школе опережающего характера развития, причем не только в области военно-технических дисциплин, но и в области военно-гуманитарных, собственно военных обучение должно строиться с учетом передовых рубежей научных исследований в данных областях еще не реализованных в гражданских сферах и отраслях;

высшее военное образование, безусловно, должно обеспечить гораздо более широкий кругозор военному специалисту, особенно в освоении современных достижений административного менеджмента, «кайзен»-философии, бенчмаркинга, военно-экономического анализа, стратегического планирования;

гораздо более акцентированная ориентация военного управленца на овладение методами военно-экономического моделирования, решения оптимизационных задач, позволяющих добиваться максимизации военного эффекта при минимизации военно-экономических затрат;

состояние учебно-материальной базы ВВУЗов должно в полном смысле слова готовить специалистов даже не завтрашнего, а послезавтрашнего дня, т.е. все самое передовое и еще только подводимое к войсковым испытаниям должно использоваться в учебном процессе;

одна из важнейших задач – формирование творческой личности будущего управленца, научно-исследовательской «жилки», аналитического склада мышления;

в связи с вышесказанным, особые требования следует предъявлять и к преподавательскому составу ВВУЗов, подготовка которого, на наш взгляд, становится острейшей проблемой, особенно в связи с несколько поспешной ликвидацией ряда военно-педагогических и военно-научных школ;

б) в области социально-экономического обеспечения военнослужащих-контрактников:

практика построения денежного довольствия последнего десятилетия убедительно доказывает, что экономически эффективная оплата труда военнослужащих должна обеспечивать конкурентоспособность данной профессии на рынке труда в сравнении с наиболее конкурентноуспешными отраслями народного хозяйства – в противном случае ее стимулирующая и развивающая функции просто утрачиваются, остается только воспроизводственная, причем не обеспечивающая фактически расширенного воспроизводства их рабочей силы;

организация социально-экономического обеспечения военнослужащих новой армии должна принципиально отличаться от пуританско-минималистического подхода прошлых лет, поскольку необходимо исходить из концептуально новых требований создания таких условий жизнедеятельности, которые позволяют расти военнослужащему интеллектуально, как можно более полно реализовать свой творческий потенциал;

следует хорошо понимать, что положение, состояние нынешних военных пенсионеров, а также отношение к ним – это тот наглядный пример, который видят перед собой сегодняшние военнослужащие, это их будущее, их социальный статус, их место в обществе, поэтому без реформирования военных пенсий в соответствии с новым денежным довольствием все остальные мероприятия военно-социальной политики могут оказаться не реализованными;

в) новым и весьма непростым направлением военно-социальной политики является подготовка, накопление и поддержание в высокой степени готовности организованного мобилизационного резерва Вооруженных Сил на основе контрактной службы находящихся в запасе военнослужащих. При этом зарубежный опыт, как показывают исследования, не вполне приемлем для российских условий.

Конкретизация военно-социальной проблематики модернизации Вооруженных Сил РФ свидетельствует о явной необходимости применения системного, комплексного подхода к реформированию социально-экономических отношений и самой социальной сферы войск, особенно если мы рассчитываем не на их реновацию, а на достижение синергетического эффекта, реально позволяющего эффективно противостоять самым изощренным военно-стратегическим концепциям.

В начале третьего тысячелетия мировая экономика вступила в полосу перманентных экономических и политических кризисов. Возрастающая амплитуда кризисов стремительно ведет к потере стабильности, росту международной напряженности, увеличению рисков силового противостояния в борьбе за ресурсы и доминирование в регионе. При этом нарастание глобальной нестабильности может способствовать быстрому перерастанию локальных очагов в бесконтрольно расширяющиеся конфликты. Поэтому противостояние тотальным сетевым угрозам предполагает в дополнение к ядерному арсеналу сдерживания широко использовать новейшие кибернетические методы глобализации и интеграции процессов управления и универсальные сетецентрические средства их реализации, которые, в свою очередь, не могут не отразиться как на экономическом и военно-политическом, так на социальном и морально-политическом потенциалах страны, целом.

Таково значение и социальная роль принципиально новой оборонной стратегии, затрагивающей и мобилизующей практически все сферы и аспекты деятельности государства по обеспечению национальной безопасности, становящейся, по сути, важнейшим элементом ядра и условием реализации отечественной модели подлинно социального общества в наше непростое время.

Список использованных источников

1. Бовдунов А.Л. НПО: Сетевая война против России. – М., 2009.

2. Каберник В. Революция в военном деле: возможные контуры конфликтов будущего / http://eurasian-defence.ru.

3. Подберезкин А. Сетецентрическая война и кибервойна. Центр военно-политических исследований // http://euroasian-defence/ru.

4. Затуливетер Ю., Семенов С. Сетецентрическая оборона: новый гарант национальной безопасности // Армейский вестник. – 2012. – 24 декабря.