

7

На правах рукописи



003062578

—

БЕДРИЦКИЙ Александр Владимирович

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ
ИНФОРМАЦИОННОЙ ВОЙНЫ
ВОЕННО-ПОЛИТИЧЕСКИМ РУКОВОДСТВОМ США
НА СОВРЕМЕННОМ ЭТАПЕ

Специальность – 23.00.04 – политические проблемы
международных отношений и глобального развития

A stylized handwritten signature in black ink, consisting of several fluid, connected strokes.

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата политических наук

Москва – 2007

Работа выполнена в Российском институте стратегических исследований

Научный руководитель Евгений Михайлович Кожокин,
доктор исторических наук

Официальные оппоненты Воробьева Людмила Михайловна,
доктор политических наук

Юрий Алексеевич Дубинин,
кандидат исторических наук,
профессор

Ведущая организация Институт международной экономики и
международных отношений РАН,
отдел стратегических исследований
Центра международной безопасности

Защита состоится 24 апреля 2007 г в 15 часов на заседании
Диссертационного совета Д 002 015.05 по политическим наукам в
Институте философии РАН по адресу 121019, г Москва,
ул Волхонка, 14

С диссертацией можно ознакомиться в библиотеке Института
философии РАН

Автореферат разослан "20" марта 2007 г

Ученый секретарь
Диссертационного совета,
Доктор политических наук

Самарская Е А Самарская

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы

В период после окончания холодной войны и распада Советского Союза Соединенные Штаты стали бесспорным политическим и военным лидером в мире. Одним из приоритетных направлений, от которого зависит сохранение и упрочение достигнутых позиций, является достижение информационного превосходства над любым возможным противником.¹ Поэтому одним из наиболее дискутируемых в американском экспертном сообществе вопросов стала концепция информационной войны (ИВ), как форма межгосударственного противоборства в постиндустриальном обществе (которое, начиная с работ Дэниела Белла ассоциировали с информационным).

Появление термина “информационная война” в его современном звучании непосредственно связано с прогрессом информационных технологий. В результате произошедшей технической революции резко возросли возможности сбора, хранения, обработки и передачи информации, обеспечивая тем самым условия для оперативного обмена информацией в глобальном масштабе. Информационные средства при всей их технической и технологической сложности стали доступными не только для государств или крупных корпораций, но и для рядового пользователя. Уже к концу прошлого века использование информационных устройств в военных целях создало реальные перспективы для качественного изменения средств и методов ведения войны.

Однако разработка новых военных концепций, адекватных происходящим комплексным изменениям в военном деле, военных технологиях и системе международной безопасности, оказалась весьма непростой задачей, требующей решения фундаментальных социологических проблем. И хотя к вопросам реализации поставленных

¹ Joint Vision 2020 — The Joint Chiefs of Staff — Washington, DC US Government Printing Office — June 2000 — p. 10-11

задач специалисты-практики подошли только в последние годы, первые дебаты о необходимости комплексной модернизации ВС США и выработки новых оперативных концепций начались еще в 90-х годах XX века. Онтологически они восходят к работам исследователей постмодерна (Жана Бодрийяра, Жана-Франсуа Лиотара, Марка Постера и Ролана Барта), политологов-экономистов (Мануэля Кастельса, Роберта Райха, Герберта Шиллера) и социальных философов Энтони Гидденса, Юргена Хабермаса и др. При всем различии точек зрения, эти исследователи сходятся в том, что хотя процесс информатизации прослеживается на протяжении всей истории человечества, за последнее время он ускорился до такой степени, что стал определяющим фактором развития социума. В конце XX века стремительная информатизация общества оказала непосредственное воздействие на процесс глобализации и развитие международных организаций, которые стали такими же субъектами мировой политической системы, как и национальные государства. Таким образом информация и формирование информационного общества преобразуют внутри- и межгосударственные отношения, формируя новые риски и угрозы.

Анализ американского опыта реализации концепции информационной войны, осуществленный в диссертационной работе, позволяет более взвешенно оценить реальность возникающих в связи с глобальной информатизацией угроз для России и соответственно определить приоритетные направления российской политики, а также оценить перспективы международного переговорного процесса в сфере информационной безопасности. За видимым нежеланием американцев публично обсуждать тему информационной войны прослеживается намерение ограничить данную проблему только вопросами кибербезопасности и борьбы с киберпреступностью² и тем самым избежать обсуждения межгосударственного информационного противоборства, хотя в самих США всем аспектам ИВ уделяется значительное внимание, и в этом направлении уже достигнуты определенные успехи.

² Конвенция Совета Европы о киберпреступности № 185 от 23 ноября 2001 г., например, содержат определения четырех основных киберпреступлений: преступления против конфиденциальности, целостности и

Постановка проблемы и задачи исследования

Общей целью настоящей работы является выявление основных направлений развития американской концепции информационной войны как средства разрешения международных и межгосударственных конфликтов на этапе становления информационного общества и анализ ее влияния на предпринимаемые военно-политическим руководством США шаги по реформированию вооруженных сил. С этой целью в диссертации решаются следующие *задачи*:

- выявление политико-философских предпосылок появления концепции информационной войны,
- анализ американских теоретико-политологических подходов к ведению информационной войны с начала 90-х годов прошлого века до настоящего времени и классификация видов информационных операций,
- выявление путей практической реализации обозначенной концепции в политике США

Объект исследования – политика США по использованию вооруженных сил в условиях перехода к постиндустриальному обществу и взгляды американских экспертов на ведение войны в условиях развития и глобального распространения информационных технологий

Предмет исследования – политические направления реализации руководством США концепции информационной войны

доступности компьютерных данных и систем, правонарушения, связанные с использованием компьютерных данных, правонарушения, связанные с нарушением авторского и смежных прав

Степень научной разработанности проблемы и анализ источников

В России проблематике влияния информатизации на общественные и политические отношения, а также исследованию феномена информационной войны, как способа разрешения противоречий в информационном обществе, значительное внимание уделено в работах Урсула А. Д., Бирюкова Б. В., Мелюхина И. С., Расторгуева С. П., Черешкина Д. С., Цыгичко В. Н., Смоляна Г. Л., Гареева М. А., Федорова А. В., Гриняева С. Н., Слипченко В. И., Роговского Е. А. Однако устоявшегося и общепринятого понимания терминов “информационное общество” и “информационная война” так и не сложилось.

Более того, ментальное и теоретическое расхождение во взглядах на развитие социума, на суть противоречий в информационном обществе и возможных формах и методах его разрешения между российскими и американскими исследователями не позволяет при рассмотрении американской политики по реализации концепции информационной войны в полной мере опираться на труды российских ученых. Для объективной и полной проработки изучаемой проблемы требуется анализ в первую очередь американских источников и сопоставление позиций политиков, ученых и специалистов этой страны. Среди современных специалистов, наиболее активно разрабатывающих в США проблематику информационной войны, можно назвать А. Цебровски, Д. Альбертса, Дж. Гарстку, Р. Моландера, П. Вилсона, М. Занини, Д. Ронфельдта, Дж. Арквиллу, Р. Шафрански, М. Либики, О. Иенсена, З. Халилзада.

Источниковедческую базу работы также составили официальные документы администрации США, конгресса, Министерства обороны, публичные высказывания официальных лиц и вторичные источники (отчеты научных подразделений министерства обороны США и исследовательских организаций).

Методы исследования. В рамках проведенного исследования при анализе предпосылок появления концепции информационной войны и изучения эволюции взглядов на ее ведение в американском экспертном сообществе использованы исторический метод и метод системного анализа. Информация о путях реализации данной

концепции военно-политическим руководством США была получена на основе отбора наиболее важного фактографического материала в первую очередь из официальных и программных документов. Отличительным моментом данной работы является верификация используемых теоретических разработок, которая осуществлялась путем их сопоставления с действующими в Соединенных Штатах программами военного строительства.

Положения работы, содержащие научную новизну и выносимые на защиту, заключаются в следующем.

1 На основе проведенного исследования можно сделать вывод, что в результате разнонаправленных теоретических дискуссий по вопросам информационного общества и информационной войны, имевших место в американском экспертном сообществе на протяжении 90-х годов XX века, была выработана единая позиция по способам обеспечения информационного доминирования, и с учетом этого началась разработка и реализация прикладных программ по модернизации вооруженных сил США.

2 Впервые на основе комплексного изучения американских теоретических разработок и практических действий в военном строительстве исследованы программы реализации концепции информационной войны в США, что позволило определить приоритетные направления развития силовой составляющей государства.

3 Доказывается безусловная взаимосвязь между программами модернизации ВС США (в соответствии с принципами сетевой организации) и решением вопросов обеспечения информационной безопасности.

4 На основе анализа информации об американской политике по реализации концепции информационной войны, прикладных оборонных программах, а также участии Соединенных Штатов в вооруженных конфликтах последнего времени обосновывается тезис, согласно которому основные усилия по достижению информационного превосходства США в условиях становления постиндустриального общества сосредоточены на создании единой информационной

архитектуры вооруженных сил и интеграции боевых и разведывательных средств, что качественно повышает их возможности за счет синергетических процессов

5 Выявлен новый спектр угроз безопасности Российской Федерации, связанных с реальной возможностью принятия на вооружение Соединенными Штатами информационных средств воздействия на противника и осуществления ими информационных операций, в том числе и в мирное время

Практическая значимость полученных результатов обусловлена возможностью использовать их в интересах обеспечения национальной безопасности России в такой важной сфере, как информационная безопасность

Апробация работы

Основные положения диссертационной работы были апробированы в ряде коллективных и индивидуальных публикаций соискателя

Отдельные положения диссертации неоднократно докладывались на научно-практических конференциях, в том числе на научно-практической конференции “Информационная безопасность и внешняя политика России в XXI веке” (Москва, 4 декабря 2001 года), организованной МИД России, а также на круглом столе “Трансформация понятия национальной безопасности в информационную эпоху” (Москва, февраль 2004 года), проведенном ПИР-Центром и Фондом гражданских инициатив в политике Интернет

Структура диссертационной работы

Диссертация состоит из введения, трех глав, заключения и списка литературы

II. ОСНОВНОЕ СОДЕРЖАНИЕ ИССЛЕДОВАНИЯ

Во введении обосновывается актуальность темы исследования, ставятся цель и задачи диссертации, формулируются объект и предмет исследования, определяются хронологические рамки работы и ее методологическая основа, характеризуются источники, отмечаются практическая значимость и научная новизна диссертации

Первая глава – “Предпосылки возникновения концепции информационной войны” – состоит из трех параграфов. В ней рассматриваются основные предпосылки появления концепции информационной войны, связанные с быстрым прогрессом информационных технологий, начавшимся в середине 70-х годов XX века. Прослеживается влияние этого прогресса на международную систему социально-политических отношений, создание новых систем вооружения и военное дело в целом.

В первом параграфе – “Трансформация системы международных отношений под влиянием информатизации” – прослеживается влияние процесса развития информационных технологий на различные аспекты международных отношений.

Глобализация, одной из причин которой среди прочего является распространение информационных технологий³, начинает постепенно размывать границы компетенции государства как основного субъекта отношений на международной арене, поскольку приводит к появлению на этом поле новых, негосударственных, игроков⁴. Однако формирование основ нового типа общества лишь до определенной степени определяется технологическими факторами. На процесс формирования информационного общества оказывают также фундаментальные преобразования в экономике, социальной структуре

³ См напр Toffler A The Third Wave, New York Bantam Books, 1980

⁴ Smith G S New Challenges For High Level Leadership Training In Public Management And Governance In A Globalizing World – August 19th, 2002 – p 4, Held D, McGrew A, Goldblatt D, Perraton G, Global Transformations Politics, Economics and Culture – Stanford, Calif Stanford University Press – 1999 – p 7

общества, политическом процессе, общественном сознании и т.п.⁵ Комплексный характер изменений создает новые, асимметричные, угрозы национальной безопасности для ведущих государств мира

Уже к началу 90-х годов минувшего столетия сложились основные признаки формирующихся негосударственных структур,⁶ среди которых можно выделить децентрализацию, разветвленность, а также высокую динамику развития, которую обеспечивают хорошо налаженный информационный обмен и способность к быстрой реорганизации. Сетевая организация стала основной для считавшихся ранее маргинальными террористических и экстремистских групп и позволяет им противостоять военной мощи наиболее развитых государств или напрямую угрожать их национальным интересам и национальной безопасности

Сетевые принципы организации находят свое применение также и в экономическом управлении, которое послужило моделью для организационно-технических преобразований в военной сфере США.⁷ Применительно к военной сфере информация становится таким же инструментом, как совершенное оружие или средства защиты

Лидерство США в экономической, технологической и военной сферах обеспечивает им преимущества в складывающейся системе международных отношений и заставляет другие страны и негосударственных игроков искать новые, асимметричные, стратегии и тактики, позволяющие противостоять заведомо более сильному противнику

⁵ Мелюхин И.С. Концепция "информационного общества" и кризис // Информационное общество – 1998 – вып. 6 – с. 20-22

⁶ Zanini M, Edwards S, J. A. The Networking of Terror in the Information Age in Networks and Netwars// The Future of Terror, Crime, and Militancy – RAND Corporation MR-1382-OSD 2001 p. 31

⁷ IT Industries-Of Growing Importance to the Economy and Jobs / The Emerging Digital Economy, app. 1 – Washington: Government Printing Office, 1998

Характерно, что поиск асимметричных действий равно актуален как для самих США, занимающих позицию бесспорного лидера, так и для государств, имеющих менее технологически оснащенные армии

Во втором параграфе – “Революция в военном деле” – рассматриваются масштабные изменения в военном деле, произошедшие в последней четверти XX века

Термин “революция в военном деле” – РВД (введенный историком Майклом Робертсом в 1955 году, чтобы показать важность изменений в методах ведения военных действий, произошедших в XVI–XVII веках) отражает эпохальные перемены в военной организации, стратегии и технике

В годы правления администрации Р Рейгана Соединенные Штаты, добившись повышения качества вооружений с помощью “умных” технологий (лазеры, радары, глобальная навигационная спутниковая система и пр), приступили к реализации концепции борьбы со вторыми эшелонами противника (или так называемой концепции “глубокой атаки”) ⁸ Основной ее целью было уничтожение возможно большего количества войск противника, прежде чем те смогут приступить к военным действиям

Таким образом, революция в военном деле уже тогда позволила США создать вооруженные силы, хотя и ориентированные еще на реалии холодной войны, но которые можно эффективно использовать в новых политических реалиях

Техническая сторона современной РВД основана в первую очередь на достижениях в области информатики и электроники, на улучшении характеристик точности и дальности действия оружия, полноте и оперативности разведки и наблюдения, повышении способности противодействовать и подавлять оборону противника и эффективно управлять и командовать войсками

Согласно “классическому” взгляду на РВД ВС будут становиться все более универсальными. Например, ВМС смогут

⁸ Алман Х Война, мир и будущее // Экспорт вооружений Центр АСТ — № 5 (сентябрь-октябрь)

непосредственно участвовать и в наземных операциях, поражая цели в глубине территории противника на большом удалении от береговой линии. Подтверждением тому служат предпринимаемые в последнее время МО США усилия по повышению интероперабельности отдельных видов ВС и совершенствованию доктрин, структур и систем боевого управления и командования.

Таким образом, современная РВД не является простым следствием непрерывного технологического прогресса, а представляет собой очередной этап адаптации вооруженных сил, к меняющимся геополитическим условиям.

В третьем параграфе – “Военно-технические революции” – рассматриваются особенности процесса развития военной техники во второй половине XX века.

Появление новых технологий, в конце концов, всегда приводило к созданию качественно новых видов вооружений. Один из видных военных теоретиков Джон Боднар считает, что со времени окончания Второй мировой войны военно-техническая революция (ВТР)⁹ последовательно прошла три следующих этапа:

1 *Революция в военной технике*, которая изменила облик оружия, боевых платформ и военной амуниции. Эта стадия ВТР началась еще в ходе Второй мировой войны и фактически закончилась в 80-х годах прошлого века.

2 *Революция в военных системах обнаружения*, связанная с появлением электронных систем обнаружения и внедрением информационных систем управления оружием. В этот период, начавшийся в середине 70-х годов минувшего столетия и завершающийся в настоящее время, существенно повысились возможности отдельных боевых комплексов (например, самолетов, кораблей, танков и т.п.) за счет более быстрой и эффективной обработки боевой информации и создания высокоточных систем управления оружием.

3 *Революция в военной связи*, начавшаяся в конце 70-х годов XX века и продолжающаяся по сей день. Она позволила качествен-

⁹ Bodnar John W The Military Technical Revolution — From Hardware to Information // Naval War College Review — Summer 1993 — Vol 46 — p 7

но улучшить системы боевого управления и связи (комплекс СЗІ), что, в свою очередь, дает возможность объединить разнородные подразделения в единые комплексы и координировать их действия при проведении совместных воздушных, морских и наземных операций. Именно это направление РВД, по мнению Д. Боднара, в полной мере продемонстрировало свою эффективность в ходе войны против Ирака в 1991 году.

Завершение каждого этапа ВТР связано с достижением пределов роста, когда дальнейшее улучшение характеристик вооружений в определенном направлении принципиально возможно, но нецелесообразно по критерию стоимость–эффективность.

Представленный обзор основных этапов развития РВТ во второй половине XX века позволяет сделать следующие выводы:

- с середины 80-х годов основное внимание при разработке боевых комплексов стало уделяться их информационному “насыщению”, а не повышению ударной мощи,

- необходимость управления разнородными подразделениями и координации их действий, а также применение высокоточного оружия большой дальности резко повысили значимость систем комплекса СЗІ,

- увеличение объема поступающей информации, необходимость ее быстрого и адекватного анализа и распределения между задействованными подразделениями ставит задачу введения в систему управления “фильтрующих” и распределяющих элементов, своего рода информационных менеджеров,

- внедрение информационных систем в военную сферу создает предпосылки для интеграции разнородных сил в единый комплекс на новом технологическом уровне.

Вторая глава – “Эволюция концепции информационной войны в США” – состоит из трех параграфов. В ней исследуются основные этапы эволюции американской концепции информационной войны с начала 90-х годов XX века по настоящее время. Выявляются основные направления теоретических исследований в данной области и характер их трансформации, вызванной изменением

военно-политического курса США и анализом военных операций этого периода

Первый параграф – “Теоретико-политические концепции ИВ середины 90-х годов XX века” – посвящен обзору взглядов ряда американских экспертно-аналитических групп, принадлежащих к различным теоретическим школам и исследующих разные аспекты ведения информационной войны

Сотрудники RAND Corporation Джон Арквила и Дэвид Ронфельдт выдвинули концепции кибернетической и сетевой войны¹⁰ предполагающие, что в ходе будущих военных конфликтов ключом к успеху станет достижение информационного превосходства за счет широкого внедрения новых технологий в системы боевого управления и связи и, что особенно важно, за счет совершенствования военной организации

Необходимо отметить, что большинство положений указанных концепций (которые сами по себе не получили дальнейшего развития) вошло в успешно реализуемую в ВС США концепцию построения сетевых вооруженных сил, или сетевой войны. Это представляется особенно важным, поскольку устанавливает четкую связь между прикладными задачами реформирования ВС США и более ранними теоретическими построениями, касающимися ведения информационной войны

Представители теоретической группы Университета ВВС США (Air University, Maxwell Airforce Base, Alabama) Джордж Стейн¹¹, Ричард Шафрански¹² и Оуэн Дженсен¹³ полагали, что

¹⁰ Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Information-Age Terrorism // The Changing Role of Information in Warfare – Rand Corporation – 1999 – p 88–89. Arquilla J., Ronfeldt D. The Advent of Netwar // In Athena's Camp – Rand Corporation – 1997 – p 275–279

¹¹ Stein George J. Information Attack Information Warfare In 2025, research paper presented to 'Air Force 2025', August 1996

¹² Szafranski R. Harnessing Battlefield Technology Neocortical Warfare The Acme of Skill, Military Review, November 1994, Szafranski, R. Parallel War and Hyperwar Is Every Want a Weakness?, Chapter 5 in Air Chronicles compilation on Battlefield of the Future, March 1996

в будущем конфликте решающую роль будет играть сама информация (точнее – знания), а не традиционные средства ведения войны. Сами информационные технологии рассматриваются в данной концепции только как средство, обеспечивающее достижение стратегического информационного доминирования, под которым в данном случае понимается создание таких информационных условий, в которых действия противника в конечном итоге неизбежно окажутся выгодными противоположной стороне или будут направлены на обслуживание ее интересов.

Один из наиболее влиятельных теоретиков в области ИВ Мартин Либики (приложивший много усилий для того, чтобы его теоретические разработки нашли свое практическое воплощение) полагал, что в будущем информация станет основным средством сдерживания вооруженных конфликтов.¹⁴ По его мнению, взаимосвязанная информационная система, состоящая из сети космических спутников слежения, наземных, воздушных и морских датчиков, даст возможность контролировать любую военную активность на планете, а значит, и применять превентивные меры против агрессора, поскольку глобализация мировых информационных систем позволит парализовать и отрезать его экономические и информационные системы от остального мира.

Эта концепция в значительной мере пересекается с концепцией, предложенной аналитиками Университета ВВС США, но в отличие от нее, акцентируется не на психологическом, а на экономическом и военном (в традиционном смысле) аспектах ИВ.

Для автора диссертационного исследования в данном случае важно то, что анализ подобных теоретических построений позволяет выявить общий вектор развития концепции ИВ. В соответствии с теми объектами, на которые предполагается оказывать целенаправленное информационное воздействие в ходе ведения ИВ, можно выделить четыре основные группы таких целей.

¹³ Jensen, Owen E. Information warfare: Principles of third-wave war // *Airpower Journal* – Winter 1994 – p. 35-43.

¹⁴ Libicki M. What is Information Warfare – National Defense University ACIS paper 3 – August 1995.

- системы управления и принятия решений (гражданские, военные, социальные, культурные),
- гражданская информационная инфраструктура (системы телекоммуникации, информационные системы транспорта, энергетики, финансов, промышленности),
- военная информационная инфраструктура (системы контроля, управления и связи, разведка),
- системы вооружении

Указанные цели могут подвергаться различному воздействию в ходе конкретных информационных операций (ИО)

Во втором параграфе – “Направления ведения информационной войны” – в соответствии с классификацией, предложенной М Либики, проводится анализ основных направлений информационной войны ¹⁵

Борьба с системами управления - это вид информационных операций, предусматривающих физическое уничтожение систем управления или отсечение командных структур вооруженных сил противника от воинских частей с целью нарушения стабильности боевого управления и руководства ¹⁶ Решение данной задачи достигается за счет уничтожения непосредственно управляющих структур (так называемое *обезглавливание*) или разрушения коммуникаций, связывающих системы управления с подчиненными подразделениями (*удушение*) Выбор метода борьбы во многом определяется характером поставленных тактических и стратегических целей¹⁷

¹⁵ Stein George J Information Attack Information Warfare In 2025, research paper presented to ‘Air Force 2025’, August 1996

¹⁶ Information Warfare – DoD Directive TS- 3600 1 – 21 December 1992

¹⁷ Libicki M What is Information Warfare – National Defense University ACIS paper 3 – August 1995 (Поскольку страницы не указаны следует в тексте ссылаться на номер первого упоминания, т е 24)

Концепция ведения *разведывательно-ударных*¹⁸ операций в определенном смысле является развитием концепции оперативной разведки. По сути дела, речь идет об интеграции оперативной разведки и ударных элементов ВС, что требует внесения значительных коррективов в архитектуру и идеологию сбора, обработки и распределения разведывательной информации.

Радиоэлектронная борьба ставит целью снижение информационных возможностей противника. Соответственно она подразделяется на собственно радиоэлектронную борьбу (создание условий, при которых передача или прием информации противником становятся невозможными, в частности, из-за постановки активных и пассивных помех), криптографическую борьбу (искажение и ликвидация собственно информации) и борьбу с коммуникационными системами противника.

Психологическая борьба – это метод информационного противоборства направленного не против информационных систем противника, а непосредственно против человеческого сознания. В самом общем виде психологическую борьбу можно определить как манипулирование общественным мнением на различных социальных уровнях. Выделяют четыре основные категории информационно-психологических операций, проводимых в рамках психологической борьбы¹⁹.

- операции против структур государственного управления,
- операции против структур военного командования,
- операции по деморализации личного состава вооруженных сил,
- война культур (“культуркампф”)

Кибернетическая борьба (осуществляемая хакерскими методами) сводится главным образом к осуществлению “атак” на различные компоненты компьютерных сетей и хранящиеся в них

¹⁸ Libicki M. What is Information Warfare – National Defense University ACIS paper 3 – August 1995 (Ссылка на номер первого упоминания – 24)

¹⁹ Libicki M. What is Information Warfare – National Defense University ACIS paper 3 – August 1995

информационные ресурсы. Некоторые западные аналитики, например Винн Швартау и Рето Хаени²⁰, склонны были даже считать, что информационное противодействие в целом может быть сведено исключительно к хакерской борьбе.

Однако сегодня невозможно согласиться с этим популярным в середине 90-х годов мнением. Во-первых, хотя имевшие место случаи воздействия на информационные системы и вызывали определенные финансовые потери и влияли на психологический климат в обществе, они, тем не менее, не разрушали жизненно важные системы и не влекли за собой человеческие жертвы. Во-вторых, сами по себе хакерские действия лишь с очень большой натяжкой можно отнести к действиям “военным”, а значит, и к информационной войне. Таким образом, кибернетическую борьбу можно рассматривать в лучшем случае лишь как фактор повышения эффективности традиционных боевых действий. Говорить же о хакерском воздействии на информационные системы как о самостоятельном виде военных действий пока преждевременно.

Тем не менее нельзя полностью исключать возможность атаки на информационные системы, связанные с жизнеобеспечением, транспортом, энергетикой и военной сферой – те с комплексом, получившим название *критически важных инфраструктур* (critical infrastructures).

Именно возможность такой атаки, способной нанести значительный экономический ущерб, как акт *кибернетической борьбы* стала предметом пристального изучения военных и гражданских экспертов с середины 90-х годов прошлого века.

В третьем параграфе – “Современная концепция информационной войны” – прослеживаются современные взгляды американских экспертов на ведение информационной войны.

Особенность современной геополитической ситуации в мире заключается в неопределенности характера и источников военных

²⁰ Haeni R E Information Warfare An Introduction – The George Washington University – Washington DC – Jan 1997

угроз. В таких условиях наиболее важным и сложным в осуществлении военной политики становится повышение “приспособляемости” к возникающим угрозам. Классификация возможных военно-политических конфликтов позволяет несколько упростить эту задачу.

Переоценка приоритетов оборонной политики на основе опыта военных конфликтов и представлений о конфликтах будущего заставила американское экспертное сообщество скорректировать точку зрения на ведение информационной войны.

В настоящее время доминирует подход, согласно которому адаптация вооруженных сил к новым политическим реалиям требует в первую очередь изменения доктринальных и оперативных концепций, организационной структуры ВС и системы военной подготовки. При этом на первый план выдвигается задача создания оптимальной структуры вооруженных сил, в которую будут органично вписываться будущие технические инновации.

Таким образом, сегодня основная роль информационных систем в военной сфере заключается не столько в повышении точности поражения цели, сколько в том, что с их помощью можно реорганизовать структуру вооруженных сил, сделать их более гибкими и эффективными, повысить скорость реагирования на поле боя, а также выработать новые тактические приемы. Результатом осознания данного факта в США стала теория сетевой организации ВС (*network-centric defense*), или сетевой войны (*network-centric warfare*), которая уже усиленно внедряется в практику, тем более что информационное насыщение вооруженных сил и “интеллектуализация” боевых платформ создали для этого необходимые предпосылки.

В самом общем виде сетевая организация ВС предполагает смещение акцента с создания и совершенствования тех или иных боевых платформ (танков, самолетов, кораблей) на их интеграцию в единую структуру для совместного использования.

Однако опора на информационные и космические технологии, их интеграция в единые разведывательно-ударные комплексы является и наиболее сильной, и потенциально уязвимой стороной высокотехнологичных армий, что отмечают практически все эксперты.

Например, по словам сенатора Стелтона, ключевую роль в асимметричной тактике возможных противников будет играть снижение эффективности ударных операций ВС США с массированным применением высокоточного оружия, а также разведывательных и иных обеспечивающих мероприятий, в которых наиболее отчетливо проявляются преимущества использования информационных технологий

По мере насыщения информационными системами вооруженных сил различных государств и приближения последних к “стандартам” США количество и сложность возникающих асимметричных угроз будут расти, при одновременном увеличении затрат на реализацию мер по их отражению. В связи с этим повышается вероятность активизации гонки вооружений в сфере высоких (космических, информационных) технологий между странами, обладающими современной технологической базой, что существенно затрудит международные процедуры контроля военных технологий

Логическим развитием прослеживаемой тенденции “милитаризации информационной сферы” стало появление концепции стратегической информационной войны (СИБ),²¹ ориентированной не столько на использование информационных технологий для повышения эффективности традиционных военных действий, сколько на асимметричное воздействие на те сегменты критически важных инфраструктур противника, нарушение работоспособности которых может вызвать последствия, сопоставимые с результатами традиционных военных действий (политический и экономический коллапс страны, выход из строя объектов энергоснабжения, паралич работы транспорта и т.д.)

²¹ Molander R C, Wilson P A, Anderson R H US Strategic Vulnerabilities Threats Against Society // The Changing Role of Information in Warfare – RAND Corporation – 1999 – p 253

Третья глава – “Реализация концепции информационной войны в политике США” – состоит из двух параграфов. В ней основное внимание уделено действиям военно-политического руководства США по реализации концепции информационной войны, в частности, по трансформации вооруженных сил в соответствии с сетевыми принципами и принципами проведения информационных операций.

В первом параграфе – “Сетевая структура вооруженных сил” – рассматриваются усилия американского военно-политического руководства, по внедрению принципов сетевой организации в практику строительства вооруженных сил.

Концепция проведения сетевых операций является ключевым элементом осуществляемой МО США трансформации вооруженных сил, цель которой – обеспечение американских национальных интересов за счет подавляющего военного превосходства над любым потенциальным противником.²² В МО США утверждают, что для решения этой задачи требуется создание единой информационной сетевой структуры ВС, позволяющей более оперативно реагировать на возникающие угрозы.

В соответствии с данной концепцией предусматривается координировать действия рассредоточенных на обширном боевом пространстве разнородные силы и средства за счет внедрения сетевой архитектуры – глобальных и локальных информационных сетей. По оценкам экспертов Пентагона, это предоставит безусловные преимущества в конфликтах будущего.

В настоящее время в вооруженных силах США проводятся мероприятия в рамках первого этапа реализации концепции ведения военных действий с использованием объединенных информационно-управляющих сетей.²³

²² Transformation Planning Guidance // U S Department of Defense – 2003 – April

²³ Азов В. О реализации в США концепции ведения военных действий в едином информационном пространстве // Зарубежное военное обозрение – 2004 – № 6 – с. 10

Второй параграф – “Политика США, связанная с ведением информационных операций”

В начале XXI века информационная война и информационные операции окончательно перестали считаться сугубо теоретической проблемой, и перешли в практическую плоскость

В настоящее время разработанная Пентагоном концепция ведения ИВ реализуется на общегосударственном и военном уровнях.

Для государства цель информационного противоборства в широком смысле слова заключается в ослаблении позиций стран-конкурентов, подрыве их национально-государственных устоев, нарушении системы государственного управления путем информационного воздействия на политическую, дипломатическую, экономическую и социальную сферы жизни общества, проведения психологических операций, подрывных и иных деморализующих пропагандистских акций

Информационные операции (ИО) на государственном уровне решают задачи защиты национальных интересов США, предупреждения международных конфликтов, пресечения провокационных и террористических акций, а также обеспечения безопасности национальных информационных ресурсов

На военном уровне ИО представляют собой комплекс мероприятий, проводимых в масштабах вооруженных сил страны, их видов, объединенных командований, и являющихся составной частью военных кампаний. Они направлены на достижение информационного превосходства над противником (в первую очередь в управлении войсками) и защиту собственных систем управления. Для этого могут использоваться любые военные и технические силы и средства, имеющиеся в распоряжении, при формальном соблюдении правовых, моральных, дипломатических, политических и военных норм. Перед ВС США впервые поставлена задача воздействовать на противника еще до начала активных боевых действий с тем, чтобы обеспечить выгодную для Соединенных

Штатов направленность процессов управления и принятия решений противоборствующей стороны ²⁴

Идея завоевания информационного превосходства над противником путем проведения информационных операций последовательно воплощалась в документах КНШ МО США “Единые перспективы 2010” и “Единые перспективы 2020”, а также в документах МО США “Четырехлетний обзор состояния вооруженных сил” от 2001 и 2006 годов. В них определены цели, задачи и основные принципы информационной борьбы, обязанности руководящих органов и должностных лиц по ее организации и планированию в мирное время и в кризисной обстановке. Практическая реализация этих доктринальных положений должна осуществляться в рамках ведения информационных операций.

В военном ведомстве США под информационными операциями (ИО), понимается использование основных возможностей радиоэлектронной борьбы, операций в компьютерных сетях, психологических операций, военного обмана и мер по обеспечению информационной безопасности с целью воздействия или защиты информации и информационных систем и влияния на процессы принятия решения. Основные ИО сопровождаются специфическими вспомогательными и обеспечивающими мероприятиями. Данное определение полностью соответствует ранним теоретическим построениям, касающимся информационной войны, и положениям военно-политических документов, подобных “Единым перспективам”, а также “Четырехлетнему обзору состояния вооруженных сил” от 2001 и 2006 годов.

²⁴ Жуков В. Взгляды США на ведение информационной войны // Зарубежное военное обозрение, № 1 — 2001

²⁵ Information Operations Doctrine, Tactics, Techniques, and procedures — Headquarters, Department of Army — November 2003

III. ОСНОВНЫЕ ВЫВОДЫ ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ

1 В результате разнонаправленных теоретических дискуссий по вопросам информационной войны, имевших место в американском экспертном сообществе на протяжении 90-х годов XX века, была выработана единая позиция по способам обеспечения информационного доминирования, и с учетом этого были внесены коррективы в военную политику США, началась разработка и реализация прикладных военных программ

2 Взяв курс на достижение информационного превосходства над любым противником, командование ВС США поставило целью обеспечить повышение эффективности оперативного управления войсками, особенно по таким критериям, как осведомленность, корректность принимаемых оперативных решений, скорость реагирования и боевая устойчивость. Основным путем достижения этой цели в МО считают внедрение интегрированных систем управления и модификацию общей военной структуры

3 При определении дальнейших перспектив реализации концепции информационной войны, акцент явно смещается с технических вопросов на организационные. Это обусловлено тем обстоятельством, что насыщение военной техники различными информационными системами уже достигло своего предела, и качественное совершенствование военной техники и вооруженных сил в целом возможно только за счет “интеллектуализации” ВТ и встраивания ее в новую информационную архитектуру ВС

4. В настоящее время военно-политическое руководство США сконцентрировало внимание на системно-интегрированном подходе к формам и методам вооруженной борьбы, в соответствии с которым первостепенное значение придается обеспечению оперативно-технических возможностей для совместных боевых действий разнородных сил и средств на ТВД. Многовекторный процесс интеграции предполагает концентрацию в рамках единой структуры управления ВС все большего числа функций и возможностей систем управления, связи и разведки различного уровня и предназначения,

техническую унификацию использующихся в ВС информационных систем

5 Суть современных представлений американского военно-политического руководства об информационной войне состоит в качественном повышении возможностей вооруженных сил США за счет развития информационно насыщенных видов вооружений, их интеграции с космическими средствами связи и навигации при одновременном осуществлении организационных преобразований в ВС (переход к концепции сетевой войны)

6 Американские доктринальные установки и выводы экспертов доказывают возможность проведения информационных операций по всему спектру международных конфликтов, включая открытые вооруженные столкновения, конфликты низкой интенсивности, тайные операции и т.п. При этом все больше внимания уделяется такой форме международного конфликта, как стратегическая информационная война

7 Дальнейшее развитие и реализация концепции ИВ способны привести к началу “новой гонки вооружений” на новом, информационном уровне. В нее будет вовлечено значительно большее число государств, чем в гонку вооружений периода холодной войны, поскольку практически все страны в том или ином объеме владеют арсеналом средств ведения ИВ. Это может свести к нулю какие бы то ни было перспективы контроля над вооружениями. Милитаризация информационной сферы может нанести непоправимый ущерб глобальным и национальным информационным коммуникационным системам и, как следствие, дестабилизировать систему международной безопасности

8 Практические шаги по реализации в США концепции информационной войны свидетельствуют о возникновении новых угроз для безопасности Российской Федерации

IV. ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

- 1 *Алексеева И Ю, Авчаров И В, Бедрицкий А В, Вотрин Д С, Дьяченко В А, Ильин В Ф, Кононов А А, Крутских А В, Мачабели К И, Смолян Г. Л, Стрельцов А А, Федоров А В, Черешкин Д С, Цыгичко В Н* Информационные вызовы национальной и международной безопасности – М. Библиотека ПИР-Центра, 2001 – 20,5 авт л (авторская часть 4 авт л)
- 2 *Бедрицкий А В, Змеевский А В, Лепский В Е, Лыженков А Л, Петрищев В Е, Федоров А В, Успенский Н Н* Супертерроризм новый вызов нового века – М. Права человека – 2002 – 24,3 авт.л (авторская часть – 3,3 авт л).
- 3 *Бедрицкий А В* Роль информационных технологий в современном терроризме и основные направления противодействия новым формам терроризма / Проблемы внешней и оборонной политики России. – М. РИСИ, 2002 – 0,8 авт л
- 4 *Бедрицкий А В* Эволюция американской концепции информационной войны // Аналитические обзоры РИСИ – 2003 – № 3 – 2,9 авт л
- 5 *Бедрицкий А В* Реализация концепции сетевой войны в ведущих странах Запада / Проблемы внешней и оборонной политики России – М. РИСИ, 2005 – 1 авт л.
- 6 *Бедрицкий А В* “Информационное доминирование” США и асимметричное информационное противоборство / США и Канада Экономика – политика – культура – М. ИСК РАН, № 2 2007 – 1 авт. л

Подписано в печать 01 03 2007 г Тираж 100 экз
Заказ 07/03/АР

Российский институт стратегических исследований
125413, г Москва, ул Флотская, 15Б