Артамонов В.А.
д.т.н., профессор, академик Международной академии информационных технологий, Минск
artamonov@itzashita.ru
Артамонова Е.В.
к.т.н. (PhD), член-корреспондент Международной академии информационных технологий, Минск

ГИБРИДНЫЕ ВОЙНЫ: НОВЫЕ ВЫЗОВЫ XXI ВЕКА

Ключевые слова: *война, информационная война, кибервойна, киберпространство, киберустойчивость, гибридная война, когнитивная война, консциентальная война, сетецентрическая война.*

Введение

История войн – это и история человеческой цивилизации. Войны всегда сопровождали эволюцию человечества. Велись войны за обладание новыми территориями, за рынки сбыта и сферы влияний, за мировое господство и во имя достижения других целей (колониальных, рабовладельческих, религиозных, за обладание сырьевыми, энергетическими, продовольственными ресурсами и пр.).

Ученые подсчитали, что за прошедшие пятьдесят веков народы пережили более 14 500 больших и малых войн. За все годы существования человечества только около 300 лет были абсолютно мирными. Статистика свидетельствует: с 1601 по 1700 г. в войнах погибло 3,3 млн. человек, с 1701 по 1800 – 5,3 млн. человек, с 1801 по 1913 – 5,6 млн. В XX веке с развитием новых технологий войны и новых вооружений потери стали несравнимо больше – счет шел уже на десятки миллионов людей.

Во все времена люди пытались осмыслить феномен войны, выявить ее природу, дать ей моральную оценку, разработать методы ее наиболее эффективного использования (теория военного искусства) и найти способы ее ограничения или даже искоренения. Наиболее дискуссионным являлся и продолжает оставаться вопрос о причинах возникновения войн: почему они случаются, если большинство людей их не хотят? На него даются самые разнообразные ответы.

Теологическая интерпретация, имеющая ветхозаветные корни, основывается на понимании войны как арены реализации воли бога (богов). Ее приверженцы видят в войне или способ утверждения истинной религии и вознаграждения благочестивых (завоевание иудеями «земли обетованной», победоносные кампании арабов, принявших ислам), или средство наказания нечестивых (уничтожение ассирийцами Израильского царства, разгром варварами Римской империи).

Конкретно-исторический подход, восходящий к античности (Геродот), связывает происхождение войн единственно с их локальным историческим контекстом и исключает поиск каких-либо универсальных причин. При этом неизбежно акцентируется роль политических лидеров и рационально принятых ими решений. Нередко возникновение войны воспринимается как результат случайного стечения обстоятельств.

Психологическая школа имеет влиятельные позиции в традиции исследования феномена войны. Еще в древности доминировало убеждение (Фукидид), что война есть следствие дурной человеческой природы, врожденной склонности к «деланию» хаоса и зла. В наше время эта идея была использована З. Фрейдом при создании теории психоанализа: он доказывал, что человек не мог бы существовать, если присущая ему потребность в саморазрушении (инстинкт смерти) не направлялась на внешние объекты, в том числе на других индивидов, иные этносы, иные конфессиональные группы. Последователи З. Фрейда (Л.Л. Бернард и др.) рассматривали войну как проявление массового психоза, который является результатом подавления обществом человеческих инстинктов. Ряд современных психологов (Э.Ф.М. Дарбен, Дж. Баулби) переработали фрейдовскую теорию сублимации в гендерном смысле: склонность к агрессии и насилию – свойство мужской природы; подавляемая в мирных условиях, она находит необходимый выход на поле боя. Их надежда на избавление человечества от войны связывается с переходом рычагов управления в руки женщин и с утверждением в обществе феминистских ценностей. Другие психологи трактуют агрессивность не как неотъемлемую черту мужской психики, а как результат ее нарушения, приводя в пример политиков, одержимых манией войны (Наполеон, Гитлер, Муссолини); они считают, что для наступления эпохи всеобщего мира достаточно эффективной системы гражданского контроля, закрывающей безумцам доступ к власти.

Особая ветвь психологической школы, основанная К. Лоренцем, опирается на *эволюционную социологию*. Ее приверженцы считают войну расширенной формой животного поведения, прежде всего выражением соперничества самцов и их борьбы за обладание определенной территорией. Они подчеркивают, что хотя войны и имеют естественное происхождение, технологический прогресс усилил их разрушительный характер и довел ее до уровня, невероятного для животного мира, когда под угрозой оказывается само существование человечества как вида.

Антропологическая школа (Э. Монтегю и др.) решительно отвергает психологический подход. Социальные антропологи доказывают, что склонность к агрессии передается не по наследству (генетически), а формируется в процессе воспитания, то есть отражает культурный опыт конкретной социальной среды, ее религиозные и идеологические установки. С их точки зрения, не существует никакой связи между различными историческими формами насилия, ибо каждая из них порождалась своим специфическим социальным контекстом.

Политический подход отталкивается от формулы немецкого военного теоретика К. Клаузевица (1780–1831), который определил войну как «продолжение политики другими средствами». Его многочисленные приверженцы, начиная с Л. Ранке, выводят происхождение войн из международных споров и дипломатической игры.

Геополитическое направление является ответвлением политологической школы, представители которого видят главную причину войн в недостатке «жизненного пространства» (К. Хаусхофер, Дж. Киффер), в стремлении государств к расширению своих границ до естественных рубежей (рек, горных хребтов и т.д.).

Демографическая теория, восходящая к английскому экономисту Т.Р. Мальтусу (1766–1834) рассматривает войну как результат нарушения баланса между численностью населения и количеством средств существования и как функциональное средство его восстановления путем уничтожения демографических излишков. Неомальтузианцы (У. Фогт и др.) полагают, что война имманентна человеческому обществу и является главным двигателем социального прогресса.

Социологический подход является наиболее востребованным при трактовке феномена войны в настоящее время. В противовес последователям К. Клаузевица, его сторонники (Э. Кер, Х. Велер и др.) считают войну продуктом внутренних социальных условий и социальной структуры воюющих стран. Многие социологи пытаются разработать универсальную типологию войн, формализовать их с учетом всех влияющих на них факторов (экономических, демографических и пр.), смоделировать безотказные механизмы их предотвращения. Активно используется социостатистический анализ войн, предложенный еще в 1920-х гг. Л.Ф. Ричардсоном; в настоящее время созданы многочисленные прогностические модели вооруженных конфликтов (П. Бреке, участники «Военного проекта», Уппсальская исследовательская группа).

Информационная теория, популярная среди специалистов по международным отношениям (Д. Блейни и др.) объясняет возникновение войн недостатком информации. По мнению ее приверженцев, война есть результат взаимного решения – решения одной стороны о нападении и решения другой об оказании сопротивления; проигрывающей стороной всегда оказывается та, которая неадекватно оценивает свои возможности и возможности другой стороны – в противном случае она или отказалась бы от агрессии, или капитулировала бы, чтобы избежать напрасных человеческих и материальных потерь. Следовательно, решающее значение приобретает знание намерений врага и его способности вести войну (эффективная разведка).

Космополитическая теория связывает происхождение войны с антагонизмом национальных и наднациональных, общечеловеческих, интересов (Н. Энджел, С. Стречи, Дж. Дьюи). Она используется преимущественно для объяснения вооруженных конфликтов в эпоху глобализации.

Экономическая интерпретация считает войну следствием соперничества государств в сфере международных экономических отношений, анархических по своей природе. Войну начинают для получения новых рынков сбыта, дешевой рабочей силы, источников сырья и энергии. Эту позицию разделяют, как правило, ученые левого направления. Они утверждают, что война служит интересам имущих слоев, а все ее тяготы выпадают на долю обездоленных групп населения. Экономическая интерпретация является элементом марксистского подхода, который трактует любую войну как производную от войны классовой. С точки зрения марксизма, войны ведутся ради укрепления власти господствующих классов и ради раскола мирового пролетариата посредством апелляции к религиозным или националистическим идеалам. Марксисты утверждают, что войны суть неизбежный результат свободного рынка и системы классового неравенства и что они канут в небытие после мировой революции.

XXI век внёс свои коррективы в понятия, методы и формы ведения войны. Промышленная революция Индустрия 4.0 и 6-й технологический уклад внесли в нашу жизнь такие сущности как Интернет, цифровая трансформация (ЦТ) экономики и общественных отношений, искусственный интеллект (ИИ), Интернет вещей (IoT), «Облачные технологии», большие данные (Big Date) и, наконец, гибридные войны.

Гибридные войны

«*Гибридная война*» – термин относительно новый. Его начали применять в начале XXI столетия. Формулировку использовали американские военные публицисты Джеймс Мэттис и Френк Хоффман в статье Future Warfare: The Rise of Hybrid Wars, которую опубликовали в 2005 г. Затем Хоффман уточнил: по его мнению, в гибридной войне асимметричные (нетрадиционные) компоненты, например, партизаны, имеют важнейшее оперативное значение, в то время как в обычном военном конфликте их роль сводится, скорее, к отвлечению сил противника. То есть, согласно современным представлениям, гибридная война сочетает методы классической войны, диверсии/партизанские действия и новые информационные технологии.

Фактически, под определением «гибридная война», могут подразумевать любые недружественные действия одной страны по отношению к другой, без явных действий вооруженных сил. Обычно данным термином пользуется «слабая сторона», чтобы при неявном применении или при отсутствии доказательств наличия вооруженных сил противника все-таки указать, что недружественные действия являются войной. Это фактически выводит данный термин из юридической и политической плоскости, требующих точных и фактических доказательств или протоколирования

международными организациями, мониторинговыми миссиями наличия действий вооруженных сил той или иной стороны и делает данный термин пропагандистским.

Природа гибридных войн позволяет нападающему растягивать враждебные действия на длительное время, испытывая стратегическое терпение противника – обычно время играет в пользу стороны, использующей методы гибридной войны. Особенно сильно этот эффект ощущается в случае регулярной армии, вовлечённой в гибридную войну на чужой территории. Лоуренс Аравийский отмечал в связи с арабским восстанием: «Конечная победа выглядит несомненной, если только война продлится достаточно долго».

Под гибридной войной в политологии понимается одновременное использование в качестве театра военных действий геополитических пространств всех типов. В каждом из основанных типов геополитических пространств «гибридная война» ведется с применением институтов, ресурсов и технологий, соответствующих конкретному типу геополитических пространств. В настоящее время доминирующим геополитическим пространством является информационно-идеологическое. Следовательно, для получения или сохранения мирового господства наибольшее значение имеют институты и технологии управления массовым сознанием. Гибридная война охватывает всё население, заполняет ниши информационного пространства, включая печатные и электронные СМИ, кибератаки, организацию семинаров, обучающих курсов и т.п. Распространяется на самые различные сферы общественной жизни – политическую, экономическую, социальную, культурную. Ее мишень – ментальная составляющая и сама система общественной организации противника. В конечном итоге, гибридные войны – это не только вооруженные конфликты, не имеющие пределов во времени, пространстве или в используемых средствах. Их главное отличие – в том, что они размывают границы, отделяющие войну от других форм политического, экономического или идеологического противостояния. Одной из существенных черт гибридной войны является пренебрежение всеми нормами морали и нравственности, использование самых грязных социальных технологий, включающих распространение слухов, ложь, клевету, искажение фактов, фальсификацию истории. Эта война втягивает в антагонизм все население и охватывает все сферы общественной жизни: политику, экономику, социальное развитие, культуру. Кроме того, гибридные войны используются в целях а государства. В большинстве случаев результатом становится экономическое и политическое ослабление государств. Гибридные войны наносят существенный удар по социальной стабильности и приводят к внутриполитической напряженности. Таким образом, гибридные войны, направлены на то, чтобы ослабить или разрушить суверенитет отдельного государства.

Процессы гибридной войны просты, но чрезвычайно эффективны: они подрывают демографию, экономику, научно-технический, промышленный и политический потенциал, одновременно предоставляя сверхдержавам возможность их усиливать (конечно же, за счет тех, кто попал под этот каток невоенного противостояния). Следует сделать важное замечание – гибридная война не стала основным видом войны. Она не подменила собой научно-техническое противоборство, не заместила тотальную, крупномасштабную или же локальную войну. Гибридная война является не более чем средством контроля покоренных государств и народов или же инструментом для вялотекущей борьбы с «колоссами на глиняных ногах». Она не заменила собой привычное человечеству кровопролитие и не отменила все ранее установленные правила. Гибридные боевые действия это лишь эффективный механизм для укрощения амбициозных экономических и политических аутсайдеров мирового обустройства.

Оперативные составляющие гибридной войны

Военный блок НАТО опробовал новые методы гибридной войны против своих противников, включая экономическую войну, кибервойну, информационную войну и психологическую войну. Некоторые исследователи включают в состав гибридной войны так называемую *сетецентричесую войну*, основные характеристики которой будут нами несколько позже представлены.

Рассмотрим основные понятия и определения гибридных войн.

Экономическая война — это экономическая стратегия, используемая воюющими или противоборствующими странами с целью ослабления экономики других государств. Сюда входят санкции, захват рынков сбыта продукции, недобросовестная конкуренция, подкуп и шантаж, блокирование или разрушение транспортных коммуникаций (магистральных газопроводов, ЛЭП, железных и автомобильных дорог, водных путей), коррупционные предложения и другие противоправные действия.

Информационная война – это воздействие на противника посредством информации с деструктивными целями. Понятие это очень широкое и в наш век информатизации и информационных технологий включает в себя очень многое. Но все эти методы, технологии и техники объединяет общая цель – деструктивное воздействие на противника и то, посредством чего это воздействие осуществляется (информация). На Западе информационные войны иногда (не совсем правильно) принято называть кибервойнами (Cyber ware).

Информационная война – частный случай информационного противоборства, ведущегося между государствами или против любого государства как в целом, так и против его составных частей: территории, власти или народа.

Информационное противоборство – любая деятельность в информационном пространстве, имеющая в большей или меньшей степени антагонизм целей. Выражение «информационная война», по сути, заимствовано из военной среды США, в которой означает воздействие на население какой-либо страны путем использования определенной информации (или дезинформации). Синонимом этого выражения может являться термин «психологическая война».

Кибервойна – представляет собой вид военных действий с использованием компьютеров и Интернета, посредством электронных, а не физических способов. Во многих документах, в том числе и международных, понятие информационной войны включает в себя признаки кибервойны. Главной целью информационной войны является изме-

нение психологического состояния людских ресурсов с целью дестабилизации политической или общественной ситуации. Главным оружием является информация как таковая – увиденная, услышанная или прочитанная. Кибервойна же нацелена в первую очередь на важнейшие системы функционирования и жизнеобеспечения государства – электростанции, энергетические сети, пути сообщения, водооборотные, трубопроводные транспортные системы и тому подобные. Несмотря на то, что оба понятия подразумевают воздействие на информационные активы, сферы их приложения все же различны как и виды информации, на которые распространяется их влияние.

Кибервойна — компьютерное противостояние в пространстве Интернета, которое направлено прежде всего на дестабилизацию компьютерных систем и доступа к Интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на Интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в Интернете в виде кибервойны: вандализме, пропаганде, шпионаже и непосредственных атаках на компьютерные системы и серверы. Одно из определений термина звучит так: «кибервойна – использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информационной безопасности и суверенитету другого государства». Как писал эксперт по безопасности правительства США Ричард А. Кларк в своей книге «Кибервойна» (вышла в мае 2010 года), «кибервойна – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Американский журнал ***The Economist*** описывает кибервойну как «пятую область войны, после земли, моря, воздуха и космоса»[1].

Более наглядно соотношение понятий «кибервойна» и «информационная война» представлено на рис. 1.

Оружие кибервойны *(кибероружие)*, с точки зрения кибернетики как науки об управлении – это перехват управления в автоматизированных и информационных системах, что во многом является целью информационного противоборства.

Рисунок 1.
Соотношение понятий «кибервойна» и «информационная война»

Кибероружием чаще всего называют различные утилиты и системы ИКТ, средства РЭБ, призванные нейтрализовать безопасность компьютеров, сетей, АСУТП, систем военного назначения и критической информационной инфраструктуры (КИИ), с целью деградации или полной потери их функциональности. Для того, чтобы иметь представление, что же такое кибероружие (которое бывает нескольких типов), нужно детально рассмотреть принцип действия кибероружия хотя бы одного типа. Для того, чтобы понять, как действует кибероружие первого типа, нужно рассмотреть, как оно воздействует на систему с обратной связью. Для примера возьмём самонаводящуюся ракету с инфракрасным наведением на цель. Данная ракета является автоматом, который настроен на наведение к источнику инфракрасного излучения, после чего происходит его (источника) поражение. Кибероружие, которое должно вывести из строя ракету, создаёт ложные сигналы, вмешиваясь в систему обратной связи автомата. Нарушение системы обратной связи приводит к сбою наведения ракеты, в результате чего она промахивается мимо цели. Уже на этом примере можно выделить характерные особенности применения кибероружия первого типа:

[1] https://dic.academic.ru/dic.nsf/ruwiki/1519964

- При воздействии на систему исключается физический контакт;
- Воздействие происходит именно на определённую систему или ряд систем, которые связаны между собой;
- Результатом воздействия будет постоянный и одинаковый эффект;
- Целью воздействия чаще всего является не уничтожение, а нарушение функционирования системы;
- Кибероружие определённого типа может воздействовать только на определённые виды систем.

Автоматизированная система – организационно-техническая система, обеспечивающая выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и т.д. в любых их сочетаниях).

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий (в том числе с использованием средств вычислительной техники и связи), реализующих информационные процессы в ней.

О важности готовности к ведению военных действий в киберпространстве свидетельствует факт создания в США целого воинского подразделения – киберкомандования США.

Основными задачами обеспечения информационной безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. А с другой стороны информационная безопасность – это процесс поэтапного максимального приближения к идеальному состоянию защищенности интересов в информационном пространстве в пределах имеющихся ресурсов и технологий.

Информационное пространство – совокупность результатов семантически- интеллектуальной деятельности человека, вне зависимости от формы их представления.

Кибербезопасность являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберпространства, ресурсов организаций и пользователей.

Киберпространство – совокупность информационных систем (в том числе банков и баз данных, телекоммуникационных систем), технологий их сопровождения и использования.

Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Фундаментальным понятием в теории технических систем является их *устойчивость*. Применительно к техническим системам определение устойчивости было дано выдающимся русским математиком, академиком Петербургской Академии наук А.М. Ляпуновым (1857–1918): «Устойчивость – это способность системы функционировать в состояниях близких к равновесному, в условиях постоянных внешних и внутренних возмущающих воздействий». Применительно к системам информационно-коммуникационных технологий (ИКТ) и Интернет, в контексте киберугроз, **киберустойчивость** – это способность *киберсистемы*, функционирующей по определенному алгоритму, достигать цели функционирования в условиях информационно-технических воздействий внешних угроз, при наличии внутренних уязвимостей, иногда с заранее допустимой деградацией своей функциональности[1].

В настоящее время НАТО и прежде всего США разрабатывает совершенно новый вид боевых действий, который назван *когнитивной войной*[2]. Описанный как «вооружение науки о мозге», новый метод включает в себя «взлом личности» путем использования «уязвимостей человеческого мозга» для реализации более сложной «социальной инженерии».

До недавнего времени США и блок НАТО разделяло войну на пять различных *оперативных областей*: воздушную, наземную, морскую, космическую и кибернетическую. Но с развитием стратегий когнитивной войны военный альянс обсуждает новый*, шестой уровень – «человеческую область»*[3].

В исследовании 2020 года, спонсируемом НАТО, об этой новой форме ведения войны говорится предельно четко: «В то время как действия, предпринимаемые в пяти областях, выполняются для того, чтобы оказать влияние на сферу человека, цель когнитивной войны состоит в том, чтобы сделать каждого человека оружием». «Мозг станет полем битвы 21 века», – подчеркивается в исследовании. «Люди – это спорная область», и «будущие конфликты, скорее всего, произойдут среди людей сначала в цифровом виде, а затем физически в непосредственной близости от центров политической и экономической власти»[4].

Соотношение вышеупомянутых понятий представлено на рис. 2.

---

[1] Более подробную информацию о выше обозначенных сущностях см.: Артамонов В.А., Артамонова Е.В., Сафонов А.Г. Кибернетические и информационные войны: основные вызовы и игроки: методическое пособие. – СПб.: Издательский дом «Афина», 2022. – 120 с.

[2] Когнитивная война – это воздействие на высший уровень мышления человека, его смыслы и ценности, которые предопределяют его поведение. Меняя их, меняя интерпретации физических событий, нападающая сторона в результате ведет его к иному типу поведения.

[3] Le Guyader H. Weaponization of Neuroscience. Technical Report. 2000. –https://www.innovationhub-act.org/sites/default/files/docs/WoNS.pdf

[4] https://www.innovationhub-act.org/sites/default/files/2020-06/WF2040Report.pdf; https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf; https://zvezdaweekly.ru/news/20211021176-cPkGh.html

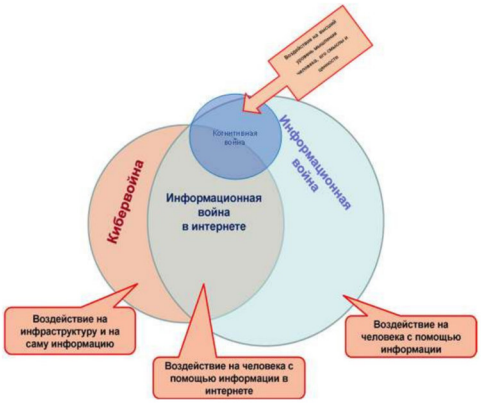

Рисунок 2.
Основные составляющие гибридной войны

Как написано в стратегическом документе НАТО *Warfighting 2040*[1], характер войны изменился. Текущие конфликты остаются ниже порога традиционно принятого определения ведения войны, но появились новые формы, такие как когнитивная война (англ. – Cognitive Warfare, CW), в которой человеческий разум теперь рассматривается как новая сфера ведения войны. На рис. 3 представлен коллаж, показывающий, на что и на кого производится воздействие CW.

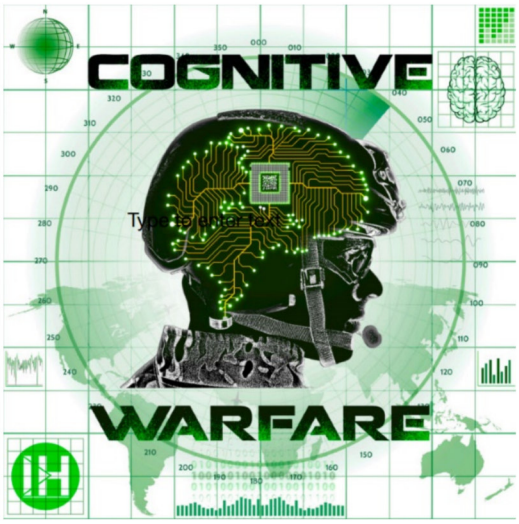

Рисунок 3.
Предмет когнитивной атаки

Когнитивная война – это война идеологий, стремящаяся подорвать доверие, лежащее в основе каждого общества. Дестабилизация и влияние – основные цели когнитивной войны. Эти цели реализуются с задачей посеять недовольство в обществе и поощрять определенные убеждения и деструктивные действия. Хотя когнитивная война является производной от информационной войны, между ними существуют кардинальные отличия. Коротко говоря, информационная война ведется с целью контролировать поток информации. Основное различие между информационной войной и когнитивной войной заключается в том, что первая не проводит различия между тактической информацией поля боя и информацией, направленной на общественный порядок. Например, информационная война имеет дело с DDoS-атаками и армиями-призраками, в то время как ни один из них не попадает в сферу когнитивной войны. Возможно, более четкое разграничение заключается в том, что информационная война стремится контролировать информацию во всех её формах, а когнитивная война стремится контролировать то, как люди и популяции реагируют на представленную информацию. Когнитивная война – это стратегия, которая фокусируется на том, чтобы изменить образ мышления целевой группы населения и на том, как это достигается.

Cognitive Warfare бросает коварный вызов. Это нарушает обычное понимание и реакции на события, что приводит к существенным негативным последствиям. Когнитивная война имеет универсальный охват – от отдельных лиц до государств и многонациональных организаций. Она питается методами дезинформации и пропаганды, направленными на психологическое истощение реципиентов информации. Каждый в той или иной степени вносит в это свой вклад сознательно или подсознательно, и это дает бесценные знания об обществе, особенно в открытых обществах. Затем эти знания можно легко использовать в качестве оружия. Это, по определению НАТО, – средство обхода традиционного поля боя со значительными стратегическими результатами, которые могут быть использованы для радикального преобразования обществ вероятных противников.

[1] https://www.innovationhub-act.org/sites/default/files/2020-06/WF2040Report.pdf

Когнитивная область станет одним из полей сражений завтрашнего дня. Эта перспектива еще более усиливается благодаря быстрому развитию NBIC (*нанотехнологии, биотехнологии, информационной технологии и когнитивных наук*) и пониманию работы мозга. НАТО и ряд других высокотехнологичных стран уже вкладывают значительные средства в эти новые технологии.

Каков бы ни был характер и предмет ведения войны, она всегда сводится к столкновению человеческой воли, и поэтому победа будет определяться способностью навязывать желаемое поведение выбранной аудитории. Действия в пяти областях – воздух, земля, море, космос и киберпространство – производятся с целью повлиять на человеческую область. Поэтому, пора добавить к перечисленным особо значимый в настоящее время шестой оперативный домен, а именно – *домен человека*.

Индивидуальные и организационные когнитивные способности будут иметь первостепенное значение, поскольку скорости и объемы информации, доступной в современном боевом пространстве, огромны. Если современные технологии обещают улучшить когнитивные способности человека, они также содержат семена серьезных угроз для военных организаций.

Поскольку организации состоят из людей, человеческие ограничения и предпочтения, в конечном счете, влияют на поведение этих организаций и процессы принятия решений. Военные организации характеризуются ограниченной рациональностью, но это ограничение часто упускается из виду. В среде, пронизанной технологиями и перегруженной информацией, управление когнитивными способностями в военных организациях будут иметь ключевое значение при развитии возможностей нанести ущерб когнитивным способностям противника. Другими словами, нужно получить возможность защищать свой процесс принятия решений и помешать это делать противнику.

В современный исторический период разворачивается ещё одна из форм когнитивной войны – консциентальная война[1].

Консциентальная война имеет несколько форм осуществления. Среди ключевых – так называемая «археологическая война» и «переписывание истории», а также десакрализация пророков и основных постулатов мировых религий. Нельзя не видеть, что за последние 10–15 лет активно разворачивается глобальный процесс так называемой «археологической войны», т.е. сознательное уничтожение памятников истории и культуры определенной цивилизации – зданий, произведений искусства и письменных источников на нескольких континентах одновременно. Уничтожение памятников истории и культуры подрывает основу функционирование данной цивилизации, а вместе с тем и всех соответствующих ей государств в той мере, в какой они впитали в себя ценности «материнской цивилизации». В ходе вооруженных конфликтов современности всегда происходит уничтожение храмов и святынь. Тем самым ведется целенаправленная ликвидация материальной памяти человечества. В современной истории мы являемся свидетелями вандализма и сноса памятников и надгробных мемориалов воинам-освободителям от фашизма и переписывание результатов и вкладов в победу народов победителей во Второй мировой войне.

Далее рассмотрим новую военную концепцию (доктрину) XXI века, базирующуюся на достижениях информационно-коммуникационных технологий, доктрину кибернетических войн и сетевой интеграции всех сил и средств подавления потенциального противника в современной войне. Называется эта доктрина сетецентрической войной[2].

Сетецентрическая война или «Сетецентрические боевые действия», «Сетецентрические операции» (англ. Network-centric warfare) – новая **военная доктрина** (или концепция ведения войны), которая была впервые озвучена Министерством обороны США.

Сетецентрическая война – концепция, ориентированная на повышение боевых возможностей перспективных формирований в современных войнах и вооруженных конфликтах, за счет достижения информационного превосходства, объединения участников боевых действий в единую сеть.

В отличие от сетевых войн, это сугубо военная концепция, прошедшая длительный путь от интеллектуальных разработок и мозговых штурмов через эксперименты и симуляции к практическим действиям, повлиявшим на изменение инфраструктуры Пентагона, а также военную стратегию США. Она во многом стала возможной благодаря информационной эпохе и информационным технологиям.

Подходы к созданию полномасштабной сетевой войны базируются в том числе и на идеях советского генерала Николая Огаркова, изложенных им в начале 1980-х. Первой к развитию и внедрению этой концепции приступила армия США. Подробно концепция представлена в военных доктринах «Joint Vision 2010», «Joint Vision 2020».

Родоначальниками сетецентрической войны принято считать вице-адмирала ВМС США Артура Себровски, научного сотрудника Пентагона Джона Гарстка и адмирала Джея Джонсона. Программной работой по сетецентричной войне называют совместную статью А. Себровски и Дж. Гарстка «Сетецентрическая война, ее происхождение и будущее»[3]. Джей Джонсон говорил, что «информационное превосходство в сочетании с сетевой, распыленной атакующей боевой мощью создаст хорошо продуманные и точные действия на раннем этапе, что приведет к чрезвычайно высоким темпам изменения. Это то, что мы называем скоростью командования. Это то, что мы называем сетецентричной войной».

Концепция сетецентрической войны по стратегии военной доктрины США представлена на рис. 4.

---

[1] Консциентальная война – процесс замещения основных ценностей массового сознания определенного общества для обеспечения его латентной управляемости извне.

[2] Сетецентрическая война – представляет собой военную доктрину или теорию войны, которая стремится превратить информационное преимущество, частично обеспеченное информационными технологиями, в конкурентное преимущество посредством надежной компьютерной сети для хорошо информированных и географически рассредоточенных сил.

[3] http://all.net/books/iw/iwarstuff/www.usni.org/Proceedings/Articles98/PROcebrowski.htm

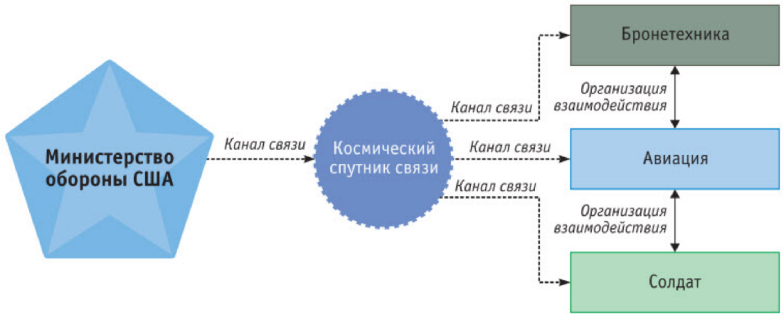

Рисунок 4.
Концепция сетецентрической войны

Эта концепция ведения боевых действий, предусматривающая увеличение боевой мощи группировки объединенных сил за счет образования информационно-коммутационной сети, объединяющей источники информации (разведки), органы управления и средства поражения (подавления), обеспечивающая доведение до участников операций достоверной и полной информации об обстановке практически в реальном масштабе времени. За счет этого достигается ускорение процесса управления силами и средствами, повышение темпа операций, эффективности поражения сил противника, живучести своих войск и уровня самосинхронизации боевых действий. Сами же «сетецентрические» силы (в военном смысле) – это войска и оружие, способные реализовать концепцию сетецентричной войны. Она направлена на перевод информационных преимуществ, присущих отдельным информационным технологиям в конкурентное преимущество за счет объединения в надежную сеть хорошо обеспеченных информационно и географически рассредоточенных сил. Эта сеть, соединенная с отличными технологиями, организацией процессов и людей, возможно, позволит создать новые формы организационного поведения.

Теория сетецентрической войны содержит в своей гипотезе четыре посылки:

1. Силы, объединенные надежными сетями, имеют возможность улучшенного обмена информацией.

2. Обмен информацией повышает качество информации и общей ситуационной информированности.

3. Общая ситуационная осведомленность позволяет обеспечивать сотрудничество и самосинхронизацию, повышает устойчивость и скорость команды.

4. В результате резко повышается эффективность миссии.

Три наиболее отличительные свойства «сетевой войны» по сравнению с традиционной войной в нынешнем её понимании выглядят так:

1. Широкая возможность использования географически распределенной силы. Ранее из-за разного рода ограничений было необходимо, чтобы подразделения и элементы тылового обеспечения располагались в одном районе в непосредственной близости к противнику или к объекту, который обороняется. Новая концепция снимает эти ограничения, и это было практически подтверждено. Так, для организации адресного тылового снабжения – основы боевого применения войск в маневренной войне, армия США в Ираке использовала распределительную информационную систему МТС (Army's Movement Tracing System). В этой системе на основе радиоизлучающих датчиков, стационарных и портативных сканеров, навигационной спутниковой системы GPS, беспроводного доступа и тактического Интернета непрерывно отслеживалось положение всех наземных подвижных объектов (танков, бронетранспортеров, БМП и т.п.) на всем иракском театре военных действий, от экипажей которых органы тыла получали запросы на поставку топлива, боеприпасов, запасных частей и других видов обеспечения. Всего в этой системе было задействовано около 4000 бортовых компьютеров и 100 серверов, работающих под Windows NT. Система МТС обошлась армии США в 418 млн долларов, полученных компаниями *NSI Global inc.* и Comtech Mobile Datacom Corp. за поставки необходимого оборудования в течение трех лет.

2. Второе отличие сетевой войны заключается в том, что силы, которые принимают в ней участие, являются высокоинтеллектуальными. Пользуясь знаниями, полученными от всеохватывающего наблюдения за боевым пространством и расширенного понимания намерений командования, эти силы будут способны к самосинхронизации деятельности, станут более эффективными при автономных действиях.

Так, средства 5 армейского корпуса, принимающего участие в операции «Шок и трепет» – основной ударной силы группировки в Ираке, уже тогда были способны самостоятельно отслеживать до 1000 наземных целей противника в течение часа. Командиры эскадрилий палубной авиации могли принимать участие в планировании вылетов своих экипажей вместе с коллегами из армейской авиации, пользуясь общей информационной системой, чего, например, не было в 1991 г. Более того, 80% боевых вылетов авиации, начиная с операции в Афганистане, уже проводится «вслепую», т.е. в памяти боевых компьютеров нет целей, и информация о них поступает от наземных частей непосредственно с передовой. Для этого американцы развернули специальную систему боевого планирования и управления авиацией на ТВД *«TBMCS»* (Theater Battle Management Core Systems).

В ходе операции в Ираке в 2003 году они использовали новую распределенную информационную систему боевого управления *FBCB2* (Force XXI Battle Command Brigade or Below), охватывая уровень «бригада-батальон-рота». Все командиры боевых подразделений и передовые артиллерийские наводчики для ориентирования на местности и передачи боевых донесений получили в свое распоряжение штатные карманные компьютеры с прочным корпусом от фирмы Elbit System.

3. Третье отличие – наличие эффективных коммуникаций между объектами в боевом пространстве. Это дает возможность географически распределенным объектам проводить совместные действия, а также динамически распределять ответственность и весь объём работы, чтобы приспособиться к ситуации. Именно поэтому более чем в семь раз по сравнению с 1991 годом увеличилась суммарная полоса пропускания (до 3 ГГц) арендованных Пентагоном каналов спутниковой связи для передачи информации. Учитывая особенность «сетевой» войны в отношении любого театра военных действий, концепцией предусматривается четыре основные фазы ведения боевых действий:

1. Достижение информационного превосходства посредством опережающего уничтожения (вывода из строя, подавления) системы разведывательно-информационного обеспечения противника (средств и систем разведки, сетеобразующих узлов, центров обработки информации и управления).

2. Завоевание превосходства (господства) в воздухе за счет подавления (уничтожения) системы ПВО противника.

3. Постепенное уничтожение оставленных без управления и информации средств поражения противника, в первую очередь ракетных комплексов, авиации, артиллерии, бронетехники.

4. Окончательное подавление или уничтожение очагов сопротивления противника. Успешное осуществление каждой из фаз основывается на значительно меньшей продолжительности боевого цикла «обнаружение – опознание – целеуказание – поражение» по сравнению с противником, на точных и полных сведениях о группировке противостоящего противника.

Таким образом, последовательность огневого поражения в ходе «сетевых» операций выглядит следующим образом: датчики (sensors) – органы управления – подразделения (units) – отдельные объекты (objects). Даже неспециалисту очевидно, что все предварительные оперативные концепции, такие как «глубокая операция» (СССР, 30-е гг.) и «воздушно-наземная операция» (США, середина 80-х) предусматривали другие последовательности.

Сетецентрическая война (СЦВ) и гибридная война (ГВ) – концепции, ставшие реальностью в XXI веке, хотя в отношении этих именованных сущностей до сих пор нет общего понимания и согласия среди зарубежных и российских экспертов. По мнению некоторых из них, США уже адаптировали свои вооруженные силы к ведению сетецентрических войн, что требует безусловного доминирования в киберпространстве. По оценкам некоторых российских экспертов, МО США используют более 7 миллионов компьютеров, соединенных через 15 тысяч сетей, а также через 20 тыс. коммерческих сетей. Таким образом военные возможности, прежде всего в области управления, определяются в решающей степени общим состоянием технологической базы и информатики в обществе и государстве.

Заключение

В оперативном искусстве и тактике за последние десятилетия произошли принципиальные перемены, которые требуют от государств радикального пересмотра прежних военных доктрин и критической переоценки всего спектра областей военного искусства. По сути дела, сегодня речь идет уже о появлении нового военного искусства, когда прежние оценки, опыт и знания требуют радикального пересмотра, либо даже отказа от прежних взглядов. В первую очередь в области военно-политического управления вооружениями и управления стратегическими наступательными и оборонительными войсками. Достаточно сказать, что в последние годы фактически отпала необходимость в массированном использовании сухопутных войск, когда армии воевавших сторон насчитывали миллионы человек, а численность танков и самолетов измерялась десятками тысяч.

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 распавшаяся Организация Варшавского Договора (ОВД) также являлась закономерным примером региональной военно-политической интеграции.

До информационно-коммуникационного этапа военно-технической революции речь шла об объединении усилий государств одного региона (например, Северной Атлантики или Центральной и Восточной Европы). В 90-е годы XX века обозначилась тенденция перехода от объединения управления к единству управления. Кроме того, отчетливо стала просматриваться тенденция выхода за пределы региона зоны ответственности и функций единого управления в блоке, т.е. расширения его пространственного охвата. Так, блок ***НАТО*** в короткие сроки превратился из региональной в глобальную организацию, управляемую из единого центра с фактической передачей полномочий.

Изменения затронули прежде всего те виды вооруженных сил, которые зависели от двух факторов – стремительного развития информатики и связи и расширения пространственного охвата до космоса и киберпространства. Речь идет о системах противовоздушной обороны (ПВО) и противоракетной обороны (ПРО), которые по сути носят глобальный характер. Даже если районы дислокации противоракетной обороны ограничены, пространство взаимодействия сторон (воздушно-космическое и информационное) выходит далеко за пределы национальных территорий.