ГЛАВА 3.
ВОЙНЫ ИНФОРМАЦИОННЫЕ

«Компьютеры – это оружие, а линия фронта проходит повсюду».
Джеймс Адамс. Следующая мировая война, 1998 г.

«Информация – это оружие. Что произойдет, когда каждый солдат получит это оружие?» - под таким заголовком авторитетный научный журнал «Дарвин мэгэзин» опубликовал в ноябре 2001 года статью Дэйнтри Даффи[1]. Вопрос этот уже сейчас не праздный. В США не один год ведутся теоретические исследования и практические разработки в области информационных технологий в военной области.

Информационная революция, внедрение современных информационных технологий коренным образом изменяют не только облик современных социальных систем, но и военную сферу. Меняется сущность и облик современных войн, уже сегодня проявляются черты войн будущего, которые еще вчера были темой для смелых предположений фантастов.

Научные дискуссии, развернутые на страницах американских военных изданий по вопросам информационных технологий в военной сфере, были позитивно встречены в Пентагоне. Военное руководство США, высший генералитет вслед за военными теоретиками сошлись на том, что успех войн будущего будет определяться не столько соотношением военных сил и боевых средств воюющих сторон, сколько информационным превосходством над противником.

Вскоре после операции «Буря в пустыне» опыт достижения информационного превосходства на поле боя был подвергнут серьезному анализу в армейском руководстве, а уже в ноябре 1991 года генерал Гленн Отис, бывший командующий Командованием сухопутных войск США по обучению и доктринам, опубликовал работу, в которой прямо указывалось: «Из операции «Буря в пустыне» можно извлечь много уроков. Некоторые из них – новые, другие – старые. Один урок, однако, является поистинне фундаментальным: природа войны коренным образом изменилась. Та сторона, которая выиграет информационную кампанию, - победит. Мы продемонстрировали этот урок всему миру: информация является ключом к современной войне – в стратегическом, оперативном, тактическом и техническом отношениях»[2].

---

[1] Daintry Duffy. Information Is a Weapon. What Will Happen When Every Soldier Is Armed With It?// Darvin Magazine. November, 2001.
[2] См.: James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 55.

По мнению авторитетных американских экспертов Джона Аркуилла[3] и Дэвида Ронфельдта, работающих в корпорации РЭНД, «информационная революция приводит к появлению такого способа ведения войны, когда … сторона, обладающая большим знанием, способная рассеять «туман войны», создаваемый противником, получит решающие преимущества»[4].

Понятие информации применительно к сущности войн будущего понимается в самом широком смысле. Американские авторы подчеркивают, что под информацией подразумевается широчайший спектр всесторонних и подробных данных о себе и противнике.

Сама по себе идея важности информации на поле боя не нова. Об этом еще в VI веке до нашей эры говорил в своем трактате «О военном искусстве» древнекитайский классик военной мысли Сунь Цзы: «Если знаешь противника и знаешь себя, проводи хоть сто сражений, и ты будешь непобедим; если знаешь его и не знаешь себя, один раз победишь, другой раз потерпишь поражение; если не знаешь ни себя, ни его, каждый раз, когда будешь сражаться, будешь терпеть поражение»[5]. Эту идею великого китайского стратега повторяют в своих теоретических исследованиях все американские эксперты.

Солдат-пехотинец будущего, в представлении военных футурологов, будет обладать объемом информации, аналогичным своему командиру и вышестоящим начальникам. Это, кстати, может создать целый ряд морально-этических и технических трудностей. Ведь в армии традиционно степень владения информацией является отличием начальников и подчиненных. Будут ли солдаты и младшие офицеры так же беспрекословно выполнять приказы командиров и начальников? Не захотят ли они получить реальный доступ к процессу принятия решений на поле боя? Как все это отразится на процессе планирования боевых действий и управления войсками?

Эти и многие другие вопросы остаются пока открытыми…

Информационная эпоха: достижения и угрозы

Конец XX века ознаменовался вступлением человечества в новую эпоху своего развития, которую на Западе окрестили информационной. Информация пронизывает собой все сферы жизни и деятельности людей, превратившись в главный ресурс научно-технического и социально-экономического развития мирового сообщества. Наряду с привычным физическим пространством или средой обитания человечества уже сформировалось и развивается новое – виртуальное – информационное пространство. «Всемирная паутина» - информационная компьютерная сеть

[3] Джон Аркуилл в период операции «Буря в пустыне» был советником командующего группировкой войск США в регионе генерала Н. Шварцкопфа.
[4] John J. Arquilla, David F. Ronfeldt. Cyber War is Coming// Comparative Strategy, Vol. 12, 1993.
[5] Сунь Цзы цзяоши (Комментарии и толкования трактата Сунь Цзы). Перевод с китайского Ши Ехуа. Пекин, 1990. С. 341 - 375.

Интернет – все более явно и осязаемо становится новой электронной средой обитания человеческой цивилизации.

Человечество все более и более становится зависимым от виртуального информационного пространства, и эта тенденция принимает универсальный и необратимый характер. Информационное пространство дает огромные возможности развитию науки и бизнеса, культуры и образования, экономики и социальной сферы государства, равно как и творческим способностям индивидуального человека. Понятия географических границ, физического пространства теряют свое былое значение. Стираются языковые и культурные барьеры, рушится традиционная иерархическая структура обществ. Сегодня житель отдаленной африканской деревушки в центре Черного континента гипотетически имеет такие же информационные возможности, что и профессор Стэнфорда.

Все это коренным образом ломает привычные представления человека о себе, своем месте в этом мире и самом мире.

Современный мир уже невозможно представить без интенсивных обменов информационными потоками. Мировая экономика и торговля, коммуникации и связь, бизнес и финансы не только не могут без них нормально функционировать, но и вообще существовать.

Однако единое информационное пространство несет с собой не только огромные возможности и преимущества, но и создает потенциально огромные угрозы.

Так, по оценкам некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний в течение нескольких часов, 48% потерпят крах в течение нескольких суток. Около 33% банков будут разорены через несколько часов после такой катастрофы, а 50% из них разорятся через несколько суток[6].

Конкретных примеров возможных последствий отключения компьютерных систем множество. Так, 13 мая 1997 года в одном из центров по обработке информации «Бэнк оф Америка» в Сан-Франциско проводились плановые работы по техническому обслуживанию электрических подстанций. Один из рабочих случайно отключил рубильник, выключив электричество. Свою ошибку он сразу же исправил, однако было уже поздно. Эта подстанция обеспечивала электропитанием всю сеть банковских банкоматов. Потребовалось два часа на то, чтобы восстановить нормальное функционирование компьютерной сети, обслуживающей банкоматы Северной Калифорнии, так как 1529 (40%) банкоматов оказались выведенными из строя[7].

Таким образом, даже одна лишь маленькая ошибка или оплошность в обслуживании систем информации может вызвать громадный ущерб.

---

[6] Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия// Журнал теории и практики Евразийства. № 19.

[7] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 173-174.

Возможный ущерб от намеренных акций против информационных и компьютерных сетей может принять катастрофические масштабы.

В США уже с конца 80-х годов проводятся исследования по информационной безопасности, изучению уязвимости информационных систем различного назначения.

В связи с этим интересный эксперимент был проведен еще в 1994 году на Нью-Йоркской бирже. Руководство биржи пригласило одного из известных немецких хакеров показать, насколько серьезна для биржи угроза компьютерного терроризма. К их удивлению, хакер даже не пытался проникнуть в хорошо защищенные внутренние сети биржи, а атаковал компьютеры, обслуживающие систему вентиляции и охлаждения внутри здания биржи. В результате, защищенная от несанкционированного вторжения сеть биржи перегрелась и вышла из строя[8]. Хоть и «нечестным» способом, но немецкий хакер «переиграл» специалистов биржи.

Соединенные Штаты, согласно данным Агентства национальной безопасности, по сравнению с другими странами в наибольшей степени зависят от компьютерных информационных сетей (информационной инфраструктуры): здесь сосредоточено более 40% компьютерных ресурсов мира (для сравнения: в России - менее 1%) и около 60% информационных ресурсов Интернет[9].

По итогам 1999 года в США зафиксировано около 250000 случаев вторжения в информационные сети государственного назначения (не считая сетей военного назначения). Почти 160000 (65%) таких вторжений оказались успешными.

Количество несанкционированных вторжений в информационные ресурсы США в 2001 г. по сравнению с 2000 г. увеличилось более чем в 2 раза - с 21756 до 52658. Всего, начиная с 1988 года, после принятия Конгрессом США специального закона о компьютерных преступлениях, было зафиксировано 100369 таких правонарушений, большинство из которых остаются нераскрытыми[10].

Количество вторжений в информационные сети государственного назначения каждый год увеличивается в среднем в два раза.

Одними из наиболее привлекательных для хакеров объектов для взлома являются военные сети. Это – наиболее совершенные и защищенные сети, что по разным причинам привлекает повышенное внимание не только «профессиональных» хакеров-разведчиков, но и так называемых хакеров-хулиганов. По данным министерства обороны США, в 1999 году было зафиксировано 22 тысячи хакерских атак на военные сети США, а в 2002 году – уже 45 тысяч[11].

---

[8] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 175.

[9] Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия// Журнал теории и практики Евразийства. № 19.

[10] Леваков С. Анатомия информационной безопасности США// Jet Info. Информационный бюллетень. 2002. № 6 (109). С. 29.

[11] Хакеры атакуют американских военных// www.washprofile.org

Данные по несанкционированному проникновению в информационные сети не дают полной и реальной картины. Так, в 1995-1996 гг. министерство обороны США провело серию тестирований, в которых применялись средства проникновения, используемые хакерами. Проверке были подвергнуты 8932 сети Пентагона, но в 7860 (88%) случаях попытки проникновения обнаружены не были[12]. Агентство по информационным системам министерства обороны США в ходе изучения статистики несанкционированных вторжений в компьютерные сети пришло к выводу, что только 5% таких вторжений оказываются замеченными и лишь о 5% таких инцидентов докладывается по команде[13].

Летом 1997 года Комитет начальников штабов вооруженных сил США организовал проведение специальных учений, на которых исследовались возможности военных и государственных структур противостоять организованным кибер-атакам. Учения были названы Eligible Receiver («Правомочный получатель»). Для большей достоверности «Команда Красных» - внешних хакеров – имела право использовать только те приемы и информацию, которую можно было загрузить свободно из Интернета; не имела доступа к внутренней информации и должна была действовать в соответствии с американским законодательством.

В течение трех месяцев «Команда Красных» воздействовала на три ключевых сферы – национальную информационную инфраструктуру, военное руководство и политическое руководство страны. В каждой из этих трех сфер хакеры легко смогли проникнуть в хорошо защищенные системы. В результате система управления воздушными перевозками была выведена из строя; силовые электрические сети оборвались; нефтеперегонные сооружения замерли.

В соответствии со сценарием учений на этом фоне возник международный кризис, который вынудил США начать переброску своих войск в отдаленный регион мира. Однако хакеры проникли в сети тылового обеспечения создаваемой группировки американских войск, полностью запутали снабжение частей и сорвали все грузоперевозки и транспортировку войск в кризисный регион.

Политическое руководство первоначально пыталось игнорировать случайные атаки со стороны хакеров. Однако «Команда Красных» начала перегружать сети политического руководства ложной информацией, которая уже не позволяла ему принимать адекватные решения. Политическое руководство полностью потеряло контроль над ситуацией.

Все это привело к тому, что Пентагон не смог развернуть соответствующую группировку войск в кризисном районе. Но даже если бы это развертывание состоялось, как сочли руководители учения, вряд ли президент взял бы на себя смелость ввести эти войска в бой.

---

[12] Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия// Журнал теории и практики Евразийства. № 19.

[13] David S. Alberts. Defensive Information Warfare. National Defense University Press, 1996.

В связи с этим Джеймс Адамс делает вывод: «Другими словами, группа наемных хакеров, использующая только открытую информацию и действующая в рамках законов и правил игры, успешно показала, что электронный Перл-Харбор сегодня не только возможен, но и может быть абсолютно успешным»[14].

Намеренное проникновение в компьютерные и информационные сети государственного и военного назначения США даже в мирное время имеет целью не только получение закрытой информации, но и намеренное уничтожение всей информации посредством внедрения компьютерных вирусов. В 1995 году таких случаев в США отмечено 583, в 1996 – 896, а в 1999 году – 1200[15].

С каждым годом совершенствуются возможности потенциальных кибер-террористов использовать в качестве «оружия» различные вирусы. Летом 2001 года компьютерные сети США подверглись атакам со стороны вируса NIMDA (термин ADMIN, прочитанный наоборот). Вирус проникал по различным каналам в компьютер и полностью разрушал все файлы с информацией. Ему потребовался один час, чтобы охватить своим воздействием всю страну. Вирус просуществовал всего несколько суток, однако успел поразить 86 тысяч компьютеров.

За два месяца до вируса NIMDA компьютерные сети США были поражены вирусом Code Red («Красный код» или «Красный червь»). Он развивался с молниеносной скоростью: за 14 часов им были поражены 150 тысяч компьютеров.

Только по официальным данным, летом 2001 года от действия двух компьютерных вирусов Code Red и NIMDA американские компании понесли убытки в размере свыше 4 млрд. долларов.

По разным оценкам, борьба с компьютерным вирусом Love Bug («Любовный жук»), созданным на Филиппинах в 2002 году, потребовала расходов во всем мире общим объемом от 3 до 15 млрд. долларов.

Насколько велики эти затраты для американской экономики и налогоплательщиков?

Американский исследователь Дж. Левис в качестве контраста приводит следующие данные: ущерб от самого разрушительного в истории США урагана Эндрю составил 25 млрд. долларов; ежегодно в США тратится 11 млрд. долларов на борьбу со стихийными бедствиями (последствиями ураганов, торнадо, наводнений); в 2002 году в США на покупку сладостей по случаю ежегодного праздника Хэллоуин населением было потрачено 7 млрд. долларов[16].

В целом, по различным оценкам, США ежегодно несут финансовые потери в сумме 5 млрд. долларов из-за сбоев оборудования, потери и

---

[14] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 187-188.

[15] Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия// Журнал теории и практики Евразийства. № 19.

[16] James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, December 2002. P. 9.

искажения данных, компьютерного мошенничества и хулиганства, связанных с нарушением регламента использования информационных систем и сетей[17].

По оценкам Отдела науки и техники администрации президента США, ежегодный урон, наносимый американскому бизнесу компьютерными хакерами, достигает 100 млрд. долл. Средний ущерб от одного компьютерного преступления в США составляет 450 тыс. долларов[18].

Потери от несанкционированного доступа к информации, связанной с деятельностью банковских и финансовых структур США, по понятным причинам скрываются прежде всего самими же банками. Однако, по словам представителя одной из ведущих американских компаний в сфере компьютерной безопасности, «один из престижных американских банков только от действий хакеров ежегодно теряет 500 миллионов долларов»[19].

Наиболее часто используемый канал, по которому осуществляется несанкционированный доступ - это сеть Интернет (65% случаев). И это не случайно, так как 2/3 коммерческих и государственных узлов сети Интернет не защищены от вторжения хакеров.

Бюджетное управление при президенте США, Счетная палата Конгресса США и созданный после событий 11 сентября 2001 г. при президенте специальный Комитет по вопросам защиты критической инфраструктуры во главе с Ричардом Кларком выявили, что из 24 основных федеральных министерств и ведомств в 22 не в полной мере выполняются, а в отдельных случаях нарушаются основные требования, связанные с обязательным выполнением принятых нормативных положений в области информационной безопасности.

По мнению американских специалистов в области компьютерной и информационной безопасности, атаки против информационных систем государственного и тем более военного назначения способны привести к самым серьезным последствиям, парализовать жизнедеятельность целых стран и регионов, политических, экономических, финансовых и военных структур на национальном и глобальном уровнях.

Наглядным примером в данном отношении выступает террористический акт 11 сентября 2001 года против США, когда за считанные минуты был уничтожен комплекс зданий Международного торгового центра в Нью-Йорке. Обрушение комплекса зданий в результате двух воздушных ударов повлекло за собой не только огромные человеческие жертвы. Уже в первые часы катастрофы были выведены из строя несколько подземных станций метро, разрушены путепроводы, отключена энергетическая система, уничтожена информация в компьютерах сотен фирм и офисов, потеряны десятки тысяч волоконно-оптических каналов передачи данных. Все это

---

[17] Леваков С. Анатомия информационной безопасности США// Jet Info. Информационный бюллетень. 2002. № 6 (109). С. 29.

[18] Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия// Журнал теории и практики Евразийства. № 19.

[19] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 175.

сказалось на нормальном функционировании биржи, привело к падению курса акций и закрытию на несколько дней самой биржи.

Согласно оценкам независимой исследовательской корпорации «Компьютер Экономикс» (Computer Economics), сумма ущерба, нанесенного информационной инфраструктуре США в результате террористических актов в Нью-Йорке и Вашингтоне с учетом финансовых потерь и затрат на восстановление, составила величину порядка 15,8 млрд. долларов. Более 25 тысяч специалистов из телекоммуникационных компаний всего мира в течение нескольких недель были заняты восстановлением утраченных и перераспределением сохранившихся информационных и телекоммуникационных ресурсов, и около 100 тысяч человек, занятых в сфере банковских и финансовых онлайн-операций, были вынуждены сменить место работы по техническим причинам[20].

Угроза «кибер-терроризма»

В конце 2002 года ФБР проинформировало президента и правительство США о намерении террористической организации Аль Кайеда провести серию терактов против символов американской экономической мощи. Основываясь на опыте событий 11 сентября, ФБР предупредило:

«Мы считаем, что такие цели являются приоритетными для Аль Кайеда из-за того экономического краха, который такие атаки могут вызвать. Атаки против высокотехнологического бизнеса могут нанести урон информационным технологиям и лишить работы тысячи людей.

Финансовый сектор в своей деятельности во многом зависит от телекоммуникационных технологий. Нарушение критических телекоммуникационных узлов – будь то физическое или посредством кибер-средств – создаст огромные сложности, пока их деятельность не будет восстановлена. Нарушения, причиненные намеренно, могут длиться дольше, ликвидировать их и восстанавливать нормальную работу узлов будет намного труднее. Все это приведет к возрастанию состояния неустойчивости и неизвестности, увеличению экономических потерь»[21].

Вместе с тем, даже несмотря на печальный опыт 11 сентября 2001 года, некоторые американские авторы склонны считать угрозу национальной информационной инфраструктуре явно преувеличенной. Этой позиции, например, придерживается Джеймс Левис, сотрудник вашингтонского Центра стратегических и международных исследований[22]. По его мнению, никакой серьезной угрозы «критической национальной инфраструктуре» - то есть ключевым объектам инфраструктуры США – в настоящее время нет, и в ближайшем будущем она маловероятна.

---

[20] Леваков С. Анатомия информационной безопасности США// Jet Info. Информационный бюллетень. 2002. № 6 (109). С. 20.

[21] Robert S. Mueller. War On Terrorism. Statement before the Select Committee on Intelligence of the United States Senate. 11 February 2003.

[22] James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, December 2002.

Свою оптимистическую точку зрения американский исследователь мотивирует тем, что какие-либо вмешательства со стороны в компьютеризованные системы управления объектами энергетики и транспорта, водяными дамбами и другими объектами критической инфраструктуры могут привести лишь к частным сбоям, локальным трудностям, но не к национальной катастрофе.

Так, например, утверждает Левис, энергетическая сеть США действительно является вожделенным объектом воздействия для хакеров, которые постоянно совершают компьютерные атаки против электростанций. В одном из исследований приводятся данные, что «за первые шесть месяцев 2002 года 70% энергетических компаний США подверглись серьезным компьютерным атакам»[23]. Однако национальная электрическая сеть представляет собой взаимосвязанную структуру из 3 тысяч государственных и частных объектов, организаций и структур. Созданная ими сеть имеет огромное количество обходных и запасных каналов связи и управления на случай чрезвычайных ситуаций. Более того, входящие в это «сообщество» объекты и организации используют различные информационные технологии.

В результате хакеру или даже большим группам хакеров, утверждает Дж. Левис, потребуется слишком много времени для нахождения слабых мест в энергетической сети США, однако даже если это случится, такая компьютерная атака может привести лишь к перебою на несколько часов с поставкой электроэнергии[24].

И все же угрозу национальным компьютерным информационным сетям, как единодушно считают все американские авторы, нельзя полностью сбрасывать со счетов. «Кибер-терроризм», как его определяет Дж. Левис, представляет собой «использование средств компьютерных сетей для выведения из строя критической национальной инфраструктуры (в частности энергосистемы, транспорта, правительственных учреждений) или подавление или запугивание правительства или гражданского населения».

Появление «кибер-терроризма» стало возможным по мере того, как системы государственного и экономического управления в государстве становятся все более и более зависимыми от компьютеров, что стало их «серьезной электронной ахиллесовой пятой». Левис приходит к заключению: «Враждебная нация или группа могут воспользоваться этими слабыми местами для проникновения в плохо защищенные компьютерные сети и нарушить или даже вывести из строя их критические функции»[25].

Сталкиваясь с необходимостью защиты своих информационных сетей и ресурсов, США ежегодно тратят огромные суммы на исследования и разработки в сфере информационной безопасности. На ближайшие пять лет только на проведение НИОКР в области информационной безопасности в

[23] Riptech Internet Security Threat Report, July 2002.
[24] James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, December 2002. P. 5.
[25] James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, December 2002. P. 9.

Соединенных Штатах выделено 880 млн. долларов. Начиная с 2003 г. Национальная академия наук США получит на исследования в области безопасности компьютерных сетей 233 млн. долларов и 144 млн. долларов будет выделено на создание и развитие специальных исследовательских центров при ведущих американских университетах, а также коммерческих и правительственных лабораториях. Национальному институту стандартов выделено 275 млн. долларов на поддержку совместных с частными компаниями исследований, направленных на совершенствование систем защиты информационных систем и компьютерных сетей[26].

Свидетельством того, насколько серьезно в современных США относятся к проблеме информационной безопасности, служат несколько документов, принятых в США после трагических событий сентября 2001 года.

В июле 2002 года президент США подписал директиву, которая ввела в действие «Национальную стратегию территориальной безопасности»[27]. В документе определялись задачи и цели деятельности государственных и негосударственных структур, организаций и населения в целом по защите территории Соединенных Штатов от возможных террористических атак.

В феврале 2003 года президент Дж. Буш подписал две новых директивы, которые ввели в действие два серьезных государственных документа: «Национальную стратегию по физической защите критической инфраструктуры и ключевых объектов»[28] и «Национальную стратегию в области защиты кибер-пространства»[29].

Оба документа нацеливают государственные и частные структуры США, равно как и все население на необходимость первостепенной защиты так называемых объектов критической инфраструктуры, от функционирования которых зависит физическое существование государства и нации. В документах определяется: «Национальная критическая инфраструктура состоит из общественных и частных институций (объектов, учреждений, структур и т.п.) в сфере сельского хозяйства, пищевой промышленности, водных ресурсов, общественного здравоохранения, спасательных служб, правительственных учреждений и организаций, оборонно-промышленной базы, информации и телекоммуникаций, энергетики, транспорта, банковского дела и финансов, химической промышленности, почтовой службы и службы доставки. Киберпространство является их нервной системой – системой управления нашей страны»[30].

Как утверждается в официальных документах, «обе стратегии - по физической и информационной защите - основаны на единых принципах и целях. Вместе они указывают путь достижения одной из важнейших целей территориальной безопасности США».

---

[26] Леваков С. Анатомия информационной безопасности США// Jet Info. Информационный бюллетень. 2002. № 6 (109). С. 8.
[27] The National Strategy For Homeland Security. July 2002.
[28] The National Strategy For the Physical Protection of Critical Infrastructures and Key Assets. February 2003.
[29] The National Strategy to Secure Cyberspace. February 2003.
[30] The National Strategy to Secure Cyberspace. February 2003. P. VII.

В качестве объектов критической инфраструктуры и ключевых для объектов в современных США выступают[31]:

Объекты	Объемы и численность
Сельское хозяйство	• 1912000 ферм • 87000 предприятий пищевой промышленности
Водные ресурсы	• 1800 федеральных водохранилищ • 1600 муниципальных очистных сооружений
Здравоохранение	• 5800 зарегистрированных клиник
Спасательные службы	• 87000 объектов
Военно-промышленная база	• 250000 фирм 215 разных отраслей промышленности
Телекоммуникации	• 2 млрд. миль кабелей
Энергетика • Электроэнергия • Нефте- и газо-добывающие объекты	 • 2800 электростанций • 300000 предприятий
Транспорт • Авиационный • Железнодорожный • Автомобильный • Трубопроводный • Водный • Транзитные перевозки	 • 5000 общественных аэропортов • 120000 миль основных железнодорожных путей • 590000 шоссейных мостов • 2 млн. миль трубопроводов • 300 крупных речных и морских портов • 500 крупных городских транзитных операторов
Банки и финансовые структуры	• 26600 учреждений федерального уровня
Химическая промышленность	• 66000 химических заводов
Почтовая служба	137 млн. пунктов по доставке почты
Ключевые объекты: • Национальные монументы • Атомные электростанции • Дамбы • Правительственные объекты • Коммерческие	 • 5800 исторических памятников • 104 коммерческие атомные электростанции • 80000 объектов • 3000 объектов • 460 небоскребов

[31] The National Strategy For the Physical Protection of Critical Infrastructures and Key Assets. February 2003. P. 9.

объекты	

Об угрозе «кибер-терроризма» говорил в феврале 2003 года в своем выступлении перед сенатским комитетом по разведке директор ФБР США Роберт Мюллер. Несмотря на осторожный стиль своего выступления, массу оговорок («возможно, вероятно, судя по всему»), он отметил тенденцию явного роста этой угрозы для США:

«Угроза кибар-терроризма становится все более серьезной. Компьютерная грамотность террористических групп возрастает, некоторые из них достигли уровня, позволяющего им проводить кибер-атаки, способные на отдельных направлениях временно вывести из строя инфраструктуру США. Благодаря свободному доступу к хакерским средствам многие из этих групп, возможно, уже способны провести атаки против включенных в Интернет информационных сетей, что может привести к сбоям и другим незначительным перебоям в их функционировании. По мере того, как террористы будут совершенствовать мастерство владения компьютерами, возможные варианты их атак будут расширяться»[32].

Угрозу терроризма с применением кибер-средств рассматривают как вполне реальную и в Пентагоне. Полковник Брэдли Эшли, руководящий одним из подразделений министерства обороны, специализирующемся на противостоянии кибер-атакам, считает, что террористы пока не очень активно используют возможности информационных технологий. Однако в ближайшем будущем они могут пересмотреть отношение к этому. Террористическая организация Аль-Каеда в 2000 – 2002 гг. уделяла этому направлению своей деятельности повышенное внимание.

По мнению Б. Эшли, террористы, которые пытаются взломать информационные сети, могут не только собирать информацию, но и готовить реальный теракт с помощью кибер-оружия. Прецеденты этому уже существуют. В частности, в 1998 году 12-летний хакер взломал систему доступа к пульту управления дамбой одного из крупнейших вощохранилищ США. Фактически ребенок получил дистанционный контроль над системами водосброса. Он мог дать команду полностью открыть затворы, тогда по длавиной воды погибли бы жители как минимум двух близлежащих городков[33].

Эшли убежден, что кибер-терроризм потенциально представляет значительно большую угрозу для мира, чем представлялось ранее. Его подразделение уже несколько раз препятствовало попыткам хакеров не только похитить секретную информацию с военных серверов, но и получить контроль над системами управления стратегическими силами США.

[32] Robert S. Mueller. War On Terrorism. Statement before the Select Committee on Intelligence of the United States Senate. 11 February 2003.
[33] Хакеры атакуют американских военных// www.washprofile.org

Информационная война: кто же такой слон?

Именно под таким названием в 1995 году в Университете национальной обороны США вышло исследование Мартина Либицки, посвященное сути и формам информационной войны в новую информационную эпоху. Эта работа заслуживает самого пристального внимания по нескольким причинам. Во-первых, М. Либицки считается одним из главных идеологов информационной войны в современных США. Будучи старшим научным сотрудником Института национальных стратегических исследований при Университете национальной обороны США, он длительное время специализировался на проблемах применения информационных технологий в системе национальной безопасности. Во-вторых, подходы автора к понятию информационной войны, в отличие от многих других исследователей, очень широкие. Он не ограничивается только «своим ведомством» – Пентагоном. В его представлении, легче определить, что не является информационной войной, чем дать четкую дефиницию этого понятия и явления.

Хотя сам термин «информационная война» появился в США еще в 1976 году, единства взглядов различных научно-практических школ на это понятие до сих пор нет. В связи с этим профессор Мартин Либицки отмечает: «Дать определение информационной войне так же трудно, как двум слепым понять, кто такой слон. Один, трогая ногу, сравнивает слона с деревом; другой, трогая хвост, сравнивает слона с веревкой»[34].

Один из первых авторов концепции информационной войны Томас Рона, столкнувшись с невозможностью загнать определение этого понятия в «прокрустово ложе» конкретной дефиниции, дал ему широкое определение: «соревнование между соперниками, конкурентами или противниками на стратегическом, оперативном и тактическом уровнях всего спектра состояний мира, кризиса, эскалации кризиса, конфликта, войны, прекращения войны, восстановления мира с применением информационных средств для достижения своих целей»[35].

Признавая правоту подхода Т. Рона к определению понятия информационная война, Мартин Либицки заключает: «Информационная война представляет собой мозаику различных форм, а не какую-то одну определенную форму».

Основных компонентов в этой «мозаике форм», по мнению профессора Либицки, семь. Отсюда проистекают и семь форм информационной войны.

Война в сфере руководства и управления войсками. Она ведется на реальном поле боя и не является чем-то новым для вооруженных сил США. По своей сути, как то определяется в американским наставлениях, она нацелена на «обезглавливание» системы управления войсками противника, то есть на физическое уничтожение центров и пунктов управления,

---

[34] См.: James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 58; Martin C. Libicki. What Is Information Warfare? National Defense University. August 1995. P. 3.

[35] См.: Martin C. Libicki. What Is Information Warfare? National Defense University. August 1995. P. 4.

нарушение систем управления войсками, линий коммуникаций и в целом системы управления противника на стратегическом, оперативном или тактическом уровнях.

Разведывательно-информационная война. В отличие от остальных форм ведения информационных войн, разведывательно-информационная война предполагает нанесение противнику физического ущерба (огневого поражения, уничтожения) на основе широкого внедрения сенсоров и датчиков. На поле боя на всю глубину боевого расположения противника в огромном количестве внедряются сенсоры различных типов и назначения, которые смогут в режиме реального времени передавать всю информацию о противнике в информационно-аналитические системы своих войск. На поле боя будущего будут господствовать не «платформы, соединяющие в себе оператора, сенсоры и вооружение», а «раздельные системы, электронно соединенные друг с другом». Идея разведывательно-информационной войны заклдчается в том, что благодаря развитию информационных технологий можно получить абсолютное знание о противнике, то есть устранить фактор «тумана войны», о котором говорили все классики военного дела, отзываясь о противнике.

Электронная война как форма информационной войны ведется в сфере коммуникаций и включает в себя радиоэлектронную борьбу и криптографическую войну. Сама по себе эта форма ведения военных действий – не нова. Она предполагает борьбу с РЛС противника, нарушение сетей радиосвязи противника, организацию засекреченных линий связи и «взлом» шифров противника.

Психологическая война предполагает использование информационных возможностей и ресурсов против человеческого сознания. Мартин Либицки выделяет четыре формы ведения психологической войны: 1) операции против национальной воли противника; 2) операции против военного руководства противника; 3) операции против войск противника; 4) культурный конфликт. Если первые три формы более или менее традиционны и понятны, то «культурная война», по словам американского эксперта, «есть нечто, что Соединенные Штаты хотели бы навязать другим»[36]. «Когда французы или канадцы жалуются на экспорт американской культуры в их страны, - заключает М. Либицки, - США рассматривают эти жалобы как угрозу мировой торговле и отказываются считать обеспокоенности в области культуры законными. В то же время, политика США хотела бы видеть американскую политическую культуру (например, власть большинства, права меньшинства) продвигаемой и воспринимаемой во всем мире; … политика абсолютно безмолвна по отношению к культурным влияниям».

«Хаккер-война». Это – новая форма ведения информационных войн, родившаяся вместе с появлением и внедрением компьютерных технологий. Употребление понятия «войны» применительно к действиям и акциям

[36] Martin C. Libicki. What Is Information Warfare? National Defense University. August 1995. P. 46.

хаккеров, как признают американские эксперты, достаточно спорно. Нарушение компьютерных сетей может осуществляться и в мирное, и в военное время, как в отношении военных, так и в отношении государственных и частных (бизнес) компьютерных сетей и информационных ресурсов. Средствами поражения в «хаккер-войне» являются компьютерные вирусы, логические бомбы, чиппинг-технологии. С военной точки зрения, операции «хаккер-войны» в зависимости от целей и объектов могут быть оборонительными и наступательными. Другими словами, вооруженные силы США должны быть готовы как к отражению «хаккер-атак» извне и изнутри, а также быть в состоянии самым серьезным образом нарушить компьютерные сети противника. Наступательная «хаккер-война», по мнению М. Либицки, может создать достаточно серьезную моральную проблему для «добропорядочных» специалистов в области компьютерных технологий, так как любое вмешательство в инфосферу, даже из благородных побуждений, официально считается иллегальным.

Экономическая информационная война, как ее определяет профессор Мартин Либицки, является производным от сочетания информационной войны и экономической войны. Она может принимать одну из двух основных форм – информационную блокаду и информационный империализм. Информационная блокада строится на предположении, что в будущем государства будут зависеть от информационных потоков так же, как сегодня они зависят от материального обеспечения и обмена. Государства-нации будут стремиться ограничить доступ своих противников к внешней информации, что приведет их экономику к краху и «поставит их на колени». Информационная блокада имеет много общих черт с экономической блокадой, вся разница заключается только в том, что она ведется в виртуальном мире, посредством блокирования информационных потоков банков, фирм, предприятий, учреждений и организаций страны-противника. В ближайшие десятилетия, по мнению М. Либицки, США вряд ли могут оказаться жертвой информационной блокады, скорее всего они сами будут прибегать к этой форме ведения войны для достижения своих целей. Информационный империализм, в представлении американского эксперта, основывается на сути экономического империализма: торговля – это война. Государства ведут борьбу за установление доминирования своих экономических систем на мировой арене. В этих же целях государства будут «продвигать» свои информационные системы, стремиться получить преимущества, представляемые доступом к информации.

«Кибер-война» - информационная война будущего. Из всех семи форм информационной войны она наиболее трудна для определения и понимания. Профессор Мартин Либицки считает, что «рассуждать о ней сегодня - аналогично ведению разговоров о системе противовоздушной обороны в Викторианскую эпоху». В понятие «кибер-войны» он включает информационный терроризм, «семантические атаки», симуляционные войны, «Гибсон-войну».

Информационный терроризм в данном контексте является действиями хаккеров, направленными не на нарушение функционирования всей информационной системы, а на использование ее базы данных для нанесения удара (ущерба) конкретному индивидууму. Базы данных создаются и хранятся в разных ведомствах (налоговые службы, здравоохранение, социальные службы, кадровые службы, персональные компьютеры), несанкционированный доступ к ним чреват серьезными последствиями – политическими, экономическими, социальными.

«Семантические атаки» по форме имеют много общего с «хаккер-войной», однако по сути в корне отличаются от последней. В рамках «хаккер-войны» целью является в конечном счете выведение из строя информационных систем противника. В ходе «семантических атак» информационная система противника продолжает функционировать, причем чисто внешне ее функционирование не вызывает никаких нареканий со стороны пользователей. Однако выходящая информация оказывается не адекватной реальности. В этом и состоит суть «семантических атак». Классическими примерами таких атак могут служить «хаккер-операции» по проникновению в сети банков и переводу денег с чужого счета на свой. Такие акции очень трудно вскрыть, причем для этого часто требуется вмешательство человека.

Симуляционные войны, в представлении М. Либицки, будут представлять собой виртуальное столкновение двух сторон, когда реальные боевые действия на реальном поле боя будут перенесены в компьютерную реальность. Военные действия превратятся в военные компьютерные игры, в ходе которых противники будут мериться силой в виртуальной реальности.

«Гибсон-война» получила свое название от имени Уильяма Гибсона, автора фантастического романа «Неоромансер»[37]. В этом произведении герои и злодеи трансформируются в виртуальные образы, которые населяют внутренности огромных систем и ведут виртуальные виртуозные поединки друг с другом. Как признает М. Либицки, всерьез говорить об этой форме ведения информационных войн в настоящее время вряд ли возможно, однако в будущем это может стать реальностью. Возможности так называемой «агент-технологии» позволят создать в компьютерных сетях виртуального «агента», наделенного даже обликом, способного представлять интересы и желания «хозяина» в широком спектре деятельности. Такой «агент» будет способен искать работу по заданным параметрам, вести переговоры от имени «хозяина» и по его заданию, обсуждать и заключать сделки. М. Либицки, в связи с этим, задается вопросом – а не будут ли эти виртуальные «агенты» вступать в споры друг с другом, отстаивая интересы «хозяев», и не приведут ли эти споры к столкновениям в стиле «Гибсон-войны».

[37] William Gibson. Neuromancer. N.Y.: Ace Science Fiction, 1984.

Информационное оружие в арсенале Пентагона

Информация и способность передачи информации на поле боя играли важную роль в достижении победы в войнах всех прошлых эпох. Научно-технический прогресс применительно к вооруженным силам сказывался не только в развитии средств нападения и защиты, но и в развитии систем коммуникации.

Анализируя зарубежные публикации на эту тему, российский военный эксперт С.В. Анчуков приводит следующие данные о войнах XIX – XX вв.:

Война	Скорость передачи информации	Плотность обороны
Гражданская война в США 1861-1865 гг.	Телеграф: 30 слов/мин	38830 чел/10 кв.км
Первая мировая война 1914-1918 гг.	Телеграф: 30 слов/мин	4040 чел/10 кв.км
Вторая мировая война 1939-1945 гг.	Телетайп: 66 слов/мин	360 чел/10 кв.км
Война в Персидском заливе 1991 г.	Компьютер: 192 тысяч слов/мин	23,4 чел/10 кв.км
Гипотетическая «Война 2010 года»	Компьютер: 1,5 млрд. слов/мин	2,4 чел/10 кв.км

Подытоживая эти показатели, С. Анчуков делает вывод: «Западные стратеги уже не мыслят в привычных категориях гигантских малоповоротливых армий, стоящих на страже с их многочисленными бронетанковыми соединениями и пропыленными батальонами мотопехоты»[38].

Роль и значение информации в конфликтах и войнах будущего неизмеримо возрастут. Информация станет и оружием, и ключом к достижению успеха в вооруженной борьбе. «Информационная эпоха начала проявлять себя в вооруженных силах США, – писал еще в 1992 году тогдашний председатель Комитета начальников штабов США генерал К. Пауэлл. - Всего несколько лет назад облик солдата с винтовкой в одной руке и лэптоп компьютером в другой приводил всех в шок. Но именно это можно было видеть в песках Саудовской Аравии в 1990 и 1991 гг. Информационные системы стали сегодня неотъемлемыми слагаемыми успеха боевых операций на поле боя»[39].

Война в Персидском заливе 1991 года, по мнению многих американских авторов, явилась последней «классической» и первой крупномасштабной

[38] С.В. Анчуков. Война и военная стратегия: реквием современности (Постмодернистский взгляд и посильные размышления о будущем).
[39] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 58.

информационной войной. В ходе конфликта со стороны США и коалиционных войск было задействовано 300 систем телефонной, в том числе спутниковой связи, и 30 компьютерных сетей. Ежедневно осуществлялось около 700 тысяч телефонных разговоров и передавалось более 150 тысяч информационных сообщений.

В вооруженных силах США термины «информационные операции» и «информационная война» уже утвердились и широко употребляются, в том числе и в официальных военных документах.

«Информационные операции, - как это определено в «Словаре военных терминов» (Наставление комитета начальников штабов ВС США JP 1-02), введенном в силу в 2001 и уточненном в июне 2003 года, - акции, предпринимаемые против информации и информационных систем противника, с одновременной защитой своей информации и своих информационных систем»[40].

Аналогичное определение информационным операциям содержится и в других документах вооруженных сил США. Так, в Наставлении армии США FM 3-0 от 2001 года информационные операции определяются как «акции, предпринимаемые с целью воздействия на противника и оказания влияния на процессы принятия решения, информацию и информационные системы других при параллельной защите своей информации и информационных систем».

Более широкое определение информационных операций содержится в Наставлении сухопутных войск США FM 3-13 с последними уточнениями от 2003 года: «Информационные операции – это использование ключевых возможностей электронной войны, операций в компьютерных сетях, психологических операций, операций по введению в заблуждение и операций по обеспечению безопасности в координации со специфическими поддерживающими и второстепенными возможностями в целях нарушения или защиты информации и информационных систем и оказания влияния на процесс принятия решений».

В Наставлении FM 3-13 отмечается: «Информация является элементом боевой мощи. Она укрепляет руководство и умножает эффективность маневра, огневой мощи и защиты, поэтому достижение информационного превосходства создает возможности, позволяющие командиру формировать оперативную обстановку и укреплять другие элементы боевой мощи.

Информационные операции являются средствами, которые позволяют командирам использовать этот элемент мощи. Сфокусированные информационные операции, синхронизированные с эффективным информационным менеджментом, разведкой, наблюдением и войсковой разведкой, позволяют командиру в достижении и поддержании информационного превосходства. Информационные операции являются главным средством достижения информационного превосходства».

---

[40] Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. 12 April 2001. (As amended through 5 June 2003). P. 254.

С информационными операциями тесно связано понятие информационной войны. В «Словаре военных терминов» Комитета начальников штабов определяется: «Информационная война – информационные операции, проводимые в периоды кризисов или конфликтов для достижения или обеспечения определенных целей в борьбе с определенным противником или противниками»[41].

Вооруженные силы США уже имеют определенный опыт организации и проведения информационных операций в разных условиях.

По свидетельству многих авторитетных американских авторов, американская разведка в 1990 году накануне войны в Персидском заливе провела успешную операцию по внедрению в компьютерные сети системы ПВО Ирака. Дело в том, что для управления иракскими радарами использовались компьютеры, закупленные во Франции и через Иорданию поставленные в Багдад. В декабре американским спецслужбам в Иордании удалось получить доступ к этим компьютерам и «начинить» их вирусами и логическими бомбами. Предполагалось, что вся эта «начинка» будет приведена в действие с началом боевых действий, что парализует систему ПВО и, как следствие, неизбежно поразит всю систему управления вооруженными силами Ирака. Однако военная операция развивалась по сценарию военных, который не был согласован с разведкой. Авиация США в ходе первых же вылетов физически вывела из строя объекты системы ПВО Ирака, на которых находились зараженные вирусами компьютеры противника. Как пишет Дж. Адамс, «разведка была очень обижена на ВВС, ведь вся ее работа оказалась напрасной!»[42].

Эпизод с попыткой внедрения вирусов в компьютеры системы ПВО Ирака накануне операции «Буря в пустыне» повторяют многие американские авторы, придавая ему свою интерпретацию. Однако еще в мае 2000 года реальность американской информационной операции была поставлена под сомнение. Автором этого сюжета был назван журналист Джон Гантц, который в качестве шутки опубликовал материал об операции Агентства национальной безопасности США против Ирака в первоапрельском номере издания “Infoworld”. Этот сюжет впоследствии был подхвачен и развит достаточно авторитетными западными авторами[43]. И все же, даже если антииракская операция АНБ США была всего лишь домыслом, принципиальная возможность такой акции является абсолютной реальностью.

Приемы и способы ведения информационной войны, примененные американцами в Ираке в 1990-1991 гг., не получили какого-либо ответа со стороны Саддама Хусейна. Однако, по словам авторитетного отечественного эксперта С.В. Анчукова, накануне войны группа голландских хакеров

---

[41] Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. 12 April 2001. (As amended through 5 June 2003). P. 255.

[42] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 39.

[43] См. подробнее: www.soci.niu.edu?~crypt/other/nr.htm

предлагала иракскому лидеру свои услуги, обещая за один миллион долларов прервать информационную связь группировки вооруженных сил в зоне Персидского залива с континентальной частью США. Сделка по ряду причин не состоялась, хотя гипотетически была возможна.

Информационная война: к теории вопроса

С середины 90-х годов XX века, когда тема «информационной войны» оказалась в фокусе внимания военных теоретиков и практических специалистов, в США появилось множество публикаций, авторы которых пытались подойти по-новому к оценке сущности войны будущего, в которой решающую роль будут играть информационные ресурсы. Среди тех, кто попытался подойти к этой проблеме с новых концептуальных позиций был полковник ВВС США Ричард Сафрански из Колледжа ВВС (база ВВС США Максвелл, штат Алабама). Весной 1995 года в журнале «Airpower Journal» он опубликовал статью «Теория информационной войны. Готовясь к 2020 году»[44].

В своей работе полковник Сафрански прежде всего проводит различие между классическим пониманием термина «война», когда требуется выступить с объявлением войны и ввести состояние войны, и новым пониманием этого слова[45]. Автор дает свое определение новому пониманию термина «война»:

«Война – это комплекс смертоносных и несмертоносных действий, предпринимаемых с целью подавления враждебной воли неприятеля или противника… Война может предприниматься группами или против групп, которые контролируются и спонсируются государством или не ассоциируют себя с государством. Война является враждебной деятельностью, направленной против неприятеля или врага. Цель войны не обязательно заключается в убийстве противника. Цель войны заключается всего лишь в покорении (подчинении) противника».

Достижение этой цели предполагает, по мнению Р. Сафрански, подавление воли противника к сопротивлению и склонение его к прекращению военных действий на условиях, которые ему необходимо навязать. Непосредственное физическое уничтожение противника в современных условиях вовсе не является целью войны. Ссылаясь на авторитетных американских исследователей, Р. Сафрански подчеркивает: «Противник покорен, когда его поведение совпадает с тем представлением, которое мы – агрессоры или защитники – имеем в отношении его поведения»[46].

---

[44] Richard Szafranski. A Theory of Information Warfare. Preparing For 2020// Airpower Journal. Spring 1995.

[45] В английском языке данные два понятия передаются различными терминами: War и Warfare. При этом термин Warfare в отличие от War по своему значению более конкретен – «вооруженная борьба, столкновение; способы, приемы ведения войны». Именно этим термином пользуется в своей статье Р. Сафрански.

[46] Richard Szafranski. A Theory of Information Warfare. Preparing For 2020// Airpower Journal. Spring 1995.

В своей работе полковник Р. Сафрански приходит к выводу: «Целью информационной атаки на всех уровнях является передача противнику достаточно убедительного сигнала остановить военные действия. Что может заставить противника остановить военные действия? Причин может быть множество: невозможность контроля над войсками на поле боя; деморализация; осознание или убеждение в том, что его военная мощь уничтожена; осознание того, что прекращение боевых действий предпочтительней их продолжения».

Таким образом, войну, или скорее военные действия, могут вести как вооруженные силы и другие государственные структуры (силовые ведомства), так и любые иные социальные группы, организации, структуры (партизаны-повстанцы, банды, этнические кланы и племена и т.д.). В любом случае главной целью воздействия в этой войне будет сознание лидеров, руководителей, непосредственно принимающих решения. Именно лидеры, как подчеркивает полковник Р. Сафрански, принимают принципиальные решения – продолжать военные действия или прекратить их. Члены группы, организации структуры (равно как и граждане государства) могут оказать лишь определенное влияние на процесс принятия решения лидером. Именно поэтому целью войны (военных действий) является покорение (подчинение) воли лидеров противника, а достижение этой цели осуществляется в ходе информационной войны.

Эту идею другими словами применительно к тактическому уровню ведения боевых действий выразил генерал-майор Джон Стюарт в статье «Стратегия разведки для XXI века», опубликованной в бюллетене «Военное обозрение» в 1995 году: «Теперь мы вступаем в информационную эпоху. Для того, чтобы добиться успеха, боевые командиры должны наносить удар по способности вражеских командиров принимать решения и распространять информацию. Мы должны внедриться во вражеский цикл принятия решения и исполнения решений, чтобы в нужное время нарушить его»[47].

«Информационная война, - как определяют ее американские теоретики Аркуилла и Ронфельдт, - это форма конфликта, в ходе которого непосредственные атаки на информационные системы противника являются средством подрыва его систем знания и убеждений. Информационная война может представлять собой составную часть более широкого и всеобъемлющего понятия враждебных действий – сетевой войны или кибер-войны – а может представлять собой и форму ведения враждебных действий в «чистом виде»[48].

Идею американских авторов полковник Р. Сафрански развивает следующим образом: «Информационная война является враждебной деятельностью, направленной против любых компонентов систем знаний и убеждений противника. Противником являются все, не разделяющие целей лидера»[49].

---

[47] Цит.: Энциклопедия военной мысли. Под ред. П. Тоураса. М.: «ЭКСМО», 2002. С. 128.
[48] John Arquilla and David Ronfeldt. Cyberwar is Coming! Comparative Strategy 2 (April-June 1993).
[49] Richard Szafranski. A Theory of Information Warfare. Preparing For 2020// Airpower Journal. Spring 1995.

Системы знаний и убеждений разных государств разительно отличаются друг от друга, неся в себе «налет» национальной специфики. Они лежат в основе национальных систем принятия решений. Именно эта сфера является главным объектом воздействия в ходе информационной войны. Р. Сафрански в связи с этим уточняет:

«Так как целью войны является воздействие на поведение противника посредством воздействия на принимаемые противником решения, акции информационной войны должны быть направлены против систем знаний и убеждений противника»[50]. Другими словами, информационная война предполагает соответствующее информационно-психологическое воздействие на противника таким образом, что он перестает верить в то, во что всегда верил, и забывает то, что всегда знал.

Главным оружием информационной войны являются слова, иллюстрации, символы, которые, благодаря сегодняшним техническим средствам, внедряются в сознание объектов воздействия самыми разнообразными и необычными способами.

Информационная война, будучи абсолютно непохожей на классическую войну, требует новых кадров профессионалов. Р. Сафрански пишет: «Информационная война требует включения в «оперативный штаб» философов, культурологов-антропологов, страноведов, лингвистов, специалистов в области семантики. Прошли те дни, когда военные колледжи или штабные колледжи могли игнорировать эти курсы»[51].

Кибер-война и сетевая война

Одними из самых авторитетных специалистов-теоретиков в сфере информационных технологий считаются Джон Аркуилл и Дэвид Ронфельдт, работающие в ведущем исследовательском центре США - корпорации РЭНД. В 1993 году в журнале «Comparative Strategy» она опубликовали программную статью под заголовком «Наступает кибер-война»[52].

Характеризуя нынешнюю эпоху как информационную, авторы утверждают: «Информация становится стратегическим ресурсом, который в постиндустриальную эру может оказаться настолько же ценным и влиятельным фактором, как капитал и рабочая сила в эру индустриальную». Информационная революция полностью рушит и размывает иерархические структуры общества, ведет к перераспределению власти, причем как правило в пользу более слабого и небольшого «игрока». Информационная революция в корне меняет саму структуру организаций, низовых социальных ячеек общества, принуждая к открытию любые закрытые структуры.

Дж. Аркуилла и Д. Ронфельдт, анализируя изменения в социальных стратах общества, приходят к выводу о неизбежном влиянии этих изменений на военную организацию общества. В связи с этим они предлагают разделять

[50] Richard Szafranski. A Theory of Information Warfare. Preparing For 2020// Airpower Journal. Spring 1995.
[51] Richard Szafranski. A Theory of Information Warfare. Preparing For 2020// Airpower Journal. Spring 1995.
[52] John J. Arquilla and David F. Ronfeldt. Cyber War Is Coming// Comparative Strategy. 1993. Vol. 12. P. 141-165.

понятия сетевой войны (социальный конфликт) и кибер-войны (военная сфера).

«Сетевая война, - пишут американские исследователи, - представляет собой информационный конфликт на стратегическом уровне между нациями-государствами или обществами. Она означает попытки исказить или подорвать знания и представления населения противника о себе и своем месте в мире»[53].

Сетевая война может в качестве объекта воздействия иметь широкие слои населения, элиту общества или тех и других одновременно. Она может включать в себя дипломатию, пропаганду и психологические кампании, политические и культурные диверсии, введение в заблуждение или вмешательство в деятельность местных средств массовой информации, внедрение в компьютерные сети или базы данных, поддержку диссидентских и оппозиционных движений.

Сетевая война представляет собой конфликт, развивающийся во всем диапазоне экономических, политических, социальных и чисто военных аспектов. В экономических войнах все усилия концентрируются на подрыве сферы производства и распределения товаров, в политических – на руководстве и институтах власти в стране. В информационной войне, как подчеркивают Дж. Аркуилла и Д. Ронфельдт, все усилия сосредоточиваются на сфере информации и коммуникаций.

Формы ведения сетевых войн могут быть различными: от конфликта между государствами до конфликта между государством и негосударственными структурами. Так, сетевая война может иметь место между правительством и нелегальными криминальными структурами, вовлеченными в терроризм, наркобизнес, торговые аферы с оружием массового поражения.

По признанию авторов концепции Дж. Аркуилла и Д. Ронфельдта, «сетевые войны не являются реальными войнами в их традиционном определении». Они могут лишь затрагивать некоторые военные аспекты, особенно когда речь идет о борьбе с терроризмом или распространением оружия массового поражения. В то же время, сетевая война может оказаться своеобразным сдерживающим механизмом для предотвращения возникновения реальной войны.

«Кибер-война, - как ее определяют Дж. Аркуилла и Д. Ронфельдт, - представляет собой военные операции, проводимые в соответствии с информационными принципами. Это означает нарушение и уничтожение информационных и коммуникационных сетей. Это означает стремление узнать все о противнике и не допустить того, чтобы противник знал много о нас. Это означает поворот «баланса информации и знаний» в свою пользу, особенно если баланс сил не в свою пользу»[54].

---

[53] John J. Arquilla and David F. Ronfeldt. Cyber War Is Coming// Comparative Strategy. 1993. Vol. 12. P. 141-165.
[54] John J. Arquilla and David F. Ronfeldt. Cyber War Is Coming// Comparative Strategy. 1993. Vol. 12. P. 141-165.

Технологии, применяемые в кибер-войне могут включать в себя системы управления и командования, разведывательного обеспечения, обработки и распространения разведданных, тактической связи, навигации и целеуказания, систем определения «свой-чужой» и т.д. При проведении военных операций в рамках кибер-войны могут использоваться приемы электронного ослепления, постановки помех, введения в заблуждение, перегрузки или внедрения в информационные и компьютерные сети противника.

Аркуилла и Ронфельдт считают, что кибер-война потребует разработки «новой военной доктрины, в которой были бы определены виды и характеристики необходимых сил, места и способы их развертывания, способы действий по отношению к противнику». Американские специалисты подчеркивают: «Вопросы о том, как и где развернуть какие виды компьютеров, сенсоров, сетей и баз данных может стать столь же важным, как когда-то был вопрос о развертывании бомбардировщиков и поддерживающих из компонентов».

В заключение своей статьи сотрудники корпорации РЭНД приходят к выводу, что вооруженные силы, как огромная иерархически построенная и функционирующая организация, в информационную эпоху не только не обладают какими-либо преимуществами, а, наоборот, обречены на поражение. Общая тенденция общественного развития по пути разукрупнения, организационного распада больших структур и социальных образований, требует соответствующих изменений в военной сфере.

В настоящее время, по мнению Аркуилла и Ронфельдта, главными противниками, с которыми США и их союзники сталкиваются в диапазоне конфликтов низкой интенсивности, представляют собой организации международных террористов, партизан-повстанцев, наркоторговцев, банды и племенные образования в регионах этно-конфессиональных конфликтов.

Главный вывод авторов: «Институционные организации могут быть разбиты сетевыми структурами, для противодействия последним целесообразно использовать именно сетевые структуры. Будущее будет принадлежать тому, кто достигнет совершенства в развитии сетевых форм»[55].

Сете-центрическая война

Авторами концепции сете-центрической войны считаются вице-адмирал ВМС США Артур Себровски и Джон Гарстка. Опубликованная ими в журнале «Proceedings» в январе 1998 года статья «Сете-центрическая война: ее происхождение и будущее» стала своеобразным манифестом новой концепции[56].

[55] John J. Arquilla and David F. Ronfeldt. Cyber War Is Coming// Comparative Strategy. 1993. Vol. 12. P. 141-165.
[56] Cebrovski, A. and Garstka, J. Network-Centric Warfare: Its Origin and Future// Proceedings. 1998, January.

Нынешняя эпоха глобализации, информационных технологий и революции в менеджменте ознаменовалась серьезнейшими изменениями в мире и обществе, в бизнесе и военном деле. Тот, кто отдает себе отчет в этом, кто не закрывает глаза на происходящие в мире изменения, а стремится активно взять их на вооружение – побеждает. Побеждает в бизнесе, побеждает и в войне. А. Себровски и Дж Гарстка повторяют ставший уже на Западе аксиомой тезис американских футурологов Алвина и Хэйди Тоффлер о том, что «нации ведут войну таким же образом, как они создают богатства»[57].

Происходящие в современном мире изменения многие авторы называют революционными. Именно в этом состоит главная исходная мысль А. Себровски и Дж. Гарстка, которые пишут: «Мы переживаем эпоху революции в военном деле, подобной которой ничего не было с эпохи наполеоновских войн, когда Франция впервые претворила в жизнь концепцию массовой армии».

Суть современной революции в военном деле А. Себровски и Дж. Гарстка выразили словами начальника штаба ВМС США адмирала Джея Джонсона, который заявил о «фундаментальном сдвиге от того, что мы называем платформо-центрической войной, к тому, что мы называем сете-центрической войной»[58].

Авторы концепции сете-центрической войны не сразу переходят к рассмотрению ее сути. Они начинают издалека – с рассмотрения сути изменений, происходящих в социально-экономической сфере: в экономике, технологиях, бизнесе. В основе всех этих изменений лежат информационные технологии, которые полностью изменили окружающий мир.

Применительно к военной сфере, сете-центрическая война позволяет перейти от войны на истощение к более скоротечной и более эффективной форме, для которой характерны две основных характеристики: быстрота управления и принцип самосинхронизации.

Быстрота управления, в представлении американских экспертов, подразумевает три аспекта:

1. Войска достигают информационного превосходства, под которым понимается не поступление информации в большем количестве, а более высокая степень осознания и более глубокое понимание ситуации на поле боя. В технологическом плане все это предполагает внедрение новых систем управления, слежения, разведки, контроля, компьютерного моделирования.
2. Войска благодаря своим информационным преимуществам претворяют в жизнь принцип массирования результатов, а не массирования сил.
3. В результате таких действий противник лишается возможности проводить какой-либо курс действий и впадает в состояние шока.

---

[57] Toffler, A. and Toffler, H. War And Anti-War. Survival At the Dawn Of the 21st Century. Little, Brown and Co., 1993.

[58] Заявление адмирала Дж. Джонсона было сделано им в ходе ежегодного выступления на семинаре Института ВМС в Аннаполисе 23 апреля 1997 года.

В качестве примера того, как может и должна работать вся военная машина в условиях сете-центрической войны, А. Себровски и Дж. Гарстка рассматривают ситуацию гипотетического начала войны. На самой начальной стадии необходимо вывести из строя всю систему ПВО противника: командные пункты и пункты управления, центры связи, позиции РЛС, боевые позиции зенитных ракет и авиации ПВО. Авторы утверждают: «Когда в самом начале конфликта противник теряет 50% чего-то очень важного для себя, это неизбежно сказывается на его стратегии. Это может остановить войну – а в этом как раз и состоит суть сете-центрической войны».

Принцип самосинхронизации пришел из теории сложных систем. В соответствии с этой теорией, сложные явления и структуры в наилучшей степени организуются по принципу снизу вверх. Другими словами, под самосинхронизацией американскими специалистами подразумевается способность военной структуры самоорганизовываться снизу, а не изменяться в соответствии с указаниями сверху. Организационная структура частей и подразделений, формы и методы выполнения ими боевых задач, как ожидается, будут видоизменяться по своему усмотрению, но в соответствии с потребностями вышестоящего командования.

Этот принцип противоречит традиционным основам военной организации как таковой: она представляет собой централизованную иерархическую систему, построенную на подчинении директивным указаниям сверху. Сломать такую систему сложно, ибо это требует изменения не только в организационных формах и методах управления, но и в менталитете начальников и подчиненных.

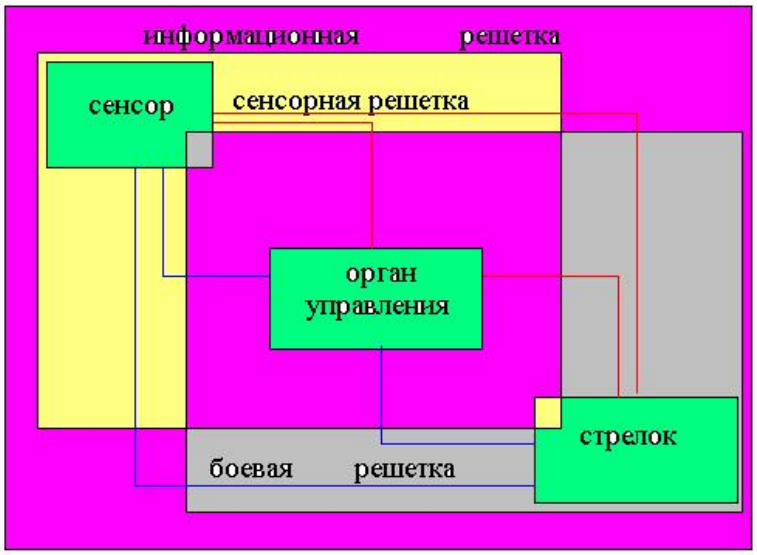
Применение системы самосинхронизации позволяет достичь превосходства над противником в скорости и внезапности действий. Исчезают тактические и оперативные паузы, которыми противник мог бы воспользоваться, все процессы управления и сами боевые действия становятся более динамичными, активными и результативными. Военные действия приобретают не форму последовательных боев и операций с соответствующими промежутками (паузами) между ними, а форму непрерывных высокоскоростных действий (операций, акций) с решительными целями.

В концептуально-теоретическом плане А. Себровски и Дж. Гарстка представили модель сете-центрической войны как систему, состоящую из трех решеток-подсистем: информационной, сенсорной и боевой. Основу этой системы составляет информационная решетка, на которую накладываются взаимно пересекающиеся сенсорная и боевая решетки. Информационная решетка-подсистема пронизывает собой всю систему в полном объеме. Элементами сенсорной системы являются «сенсоры» (средства разведки), а элементами боевой решетки – «стрелки» (средства поражения). Эти две группы элементов объединяются воедино органами управления и командования.

Взаимоотношения между всеми элементами подсистем и самими подсистемами достаточно сложные и многоплановые, что позволяет, например, «стрелкам» поражать цели сразу по получении информации от «сенсоров» или по получении приказа от органов управления, или в некоторых случаях самостоятельно.

Графически логическая модель сете-центрической войны А. Себровски и Дж. Гарстка была представлена следующим образом.

Схема: логическая модель сете-центрической войны



Пояснения: *красные линии обозначают линии контроля (управления); синие линии – линии информационного обмена.*

Таким образом, сете-центрическая война, в представлении авторов концепции адмирала А. Себровски и Дж Гарстка, представляет собой разветвленную сеть хорошо информированных, но географически рассеянных сил. Главными характеристиками-компонентами этих сил являются: высокоэффективная «информационная решетка», доступ ко всей необходимой информации, высокоточное оружие с большой дальностью поражения цели и маневренностью, высокоэффективная система управления и командования, интегрированная «сенсорная решетка», соединенная в единую сеть с системой «стрелков» и системой управления и командования.

Сете-центрическая война может вестись на всех уровнях ведения военных действий – тактическом, оперативном и стратегическом. Принципы ее ведения никоим образом не зависят от географического региона, боевых задач, состава и структуры применяемых войск (сил).

В заключение своей статьи А. Себровски и Дж. Гарстка отмечают, что эффективность действия модели сете-центрической войны немыслима без соответствующих преобразований в системе подготовки войск, без изменений в их организационно-штатной структуре и без перераспределения ресурсов. В каждой новой революции в военном деле, как отмечают

американские эксперты, возникает своя «элита», которая сейчас представлена так называемыми «новыми (компьютерными) операторами».

В военной среде, в том числе и в США, процесс освоения и внедрения новых информационных технологий идет медленнее, чем, например, в бизнесе. Традиционная военная культура отрицает роль и значение «нового оператора», ибо это требует изменения многих стереотипов и внутренних установок офицеров и генералов. Такую ситуацию необходимо изменить. В подтверждение своих слов А. Себровски и Дж. Гарстка приводят крылатое высказывание Б. Лидделл-Харта: «Единственной вещью, которую сделать труднее, чем внедрить новую идею в голову военных, является выбить оттуда старую».

Насколько реальна и осуществима концепция сете-центрической войны и действительно ли эта модель обеспечит вооруженным силам США победу в будущих войнах? Не все американские авторы дают на эти вопросы положительные ответы. Профессор Т. Барнетт из Военного колледжа ВМС США вскоре после выхода в свет статьи А. Себровски и Дж. Гарстка выступил с критической позицией по этому вопросу[59].

По мнению Т. Барнетта концепция сете-центрической войны «забегает вперед»: в мире нет противников, которые смогли бы сравниться с США и вооруженными силами этой страны в сфере информационных технологий. А если это – так, то тогда с кем и как вести войну в этой сфере. В частности, где гарантии, что полученные американской стороной данные о противнике соответствуют действительности. Как считают авторы концепции сете-центрической войны, применение этой модели позволяет вторгнуться в процесс принятия противником решения.

Американские «супервозможности» по обработке информации могут сыграть злую шутку: противнику будут приписаны намерения, которых он даже не имел. Базовый принцип быстроты управления опасен тем, что «командир становится рабом собственного компьютера, а по сути глупой машины, достоинством которой является способность быстро считать». В этих условиях велика вероятность принять неправильное решение. Т. Барнетт делает вывод: «Мы можем оказаться в ситуации, подобной той, в которой находится собака Павлова, которая звонит в колокольчик и удивляется, почему у нее течет слюна в предвкушении пищи». Другими словами, подчеркивает автор, применение концепции сете-центрической войны может утвердить в сознании военных знаменитый принцип американских ковбоев «Сперва стреляй, а затем задавай вопросы».

В результате, делает вывод американский профессор, задача состоит не в том, чтобы сократить время принятия решения, а, наоборот, удлинить его, повысив тем самым эффективность процесса принятия решений. В противном случае – можно получить лишь «два неэффективных решения на одной решение противника». Скорость не должна являться самоцелью, скорость – это лишь средство к достижению цели. Поэтому главной задачей

[59] Barnett, T. The Seven Deadly Sins of Network-Centric Warfare// Proceedings. 1999, January. P. 36-39.

должно быть не достижение быстроты управления, как то требует концепция сете-центрической войны, а наиболее оптимальное использование преимуществ во времени, которые дает применение этой модели над противником.

Профессор Т. Барнетт приводит и целый ряд других недостатков концепции сете-центрической войны. Так, в глазах населения противника она будет актом терроризма и военным преступлением, сходным с массовыми бомбардировками мирных немецких городов союзниками в конце второй мировой войны. Определенные сомнения у него вызывает и сама концепция информационного доминирования, которая может привести к информационным перегрузкам в системе принятия решений. А это, в свою очередь, никак не гарантирует качества принимаемых решений. Ну и самое главное – модель сете-центрической войны, по мнению Т. Барнетта, рассчитана на прошлые войны, на «нормального» противника в форме вооруженных сил страны-противника. С учетом нынешних тенденций мирового развития наиболее вероятным противником вооруженных сил США будут негосударственные структуры на субнациональном уровне, то есть полувоенные, криминальные и иные структуры внутри и вне своего национального государства.

Несмотря на определенные критические публикации, концепция сете-центрической войны прижилась в ВМС США и начала завоевывать своих сторонников в других видах вооруженных сил и среди военно-политического истэблишмента. Концепция наполнялась новым содержанием, приобретала более универсальный характер. Выступая в 2000 году в Лондоне адмирал Себровски, директор управления трансформации вооруженных сил МО США и один из «отцов-основателей» теории сете-центрической войны, охарактеризовал ее как «зарождающуюся теорию войны, основанную на концепциях нелинейности, сложности и хаоса». В качестве ее характеристик он назвал «меньший акцент на физических аспектах и больший – на поведенческих аспектах; меньший акцент на объектах, материальных факторах и больший – на отношениях»[60]. Другой «отец-основатель» концепции сете-центрической войны - эксперт комитета начальников штабов Джон Гарстка – сосредоточился более на информационных аспектах своей теории[61].

«Сете-центрические операции, - отмечает Дж. Гарстка, - обеспечивают войскам доступ к новому, ранее недостижимому пласту информационной сферы». Доступ к новым пластам информации позволяет своим силам неизмеримо увеличить свои боевые способности.

Под информационной сферой автор подразумевает «сферу, в которой происходит создание информации, манипулирование и обмен ею; сферу, в которой осуществляются все операции по руководству и командованию войсками, в которой оформляется решение командира». В борьбе за

[60] Cebrovski, A. Network Centric Warfare and information Superiority. RUSI. Whitehall, London, 2000.
[61] Garstka, J. Network Centric Warfare: An Overview of Emerging Theory// PHALANX. Vol. 33. No. 4. December 2000.

информационное превосходство «информационная сфера является основополагающим плацдармом».

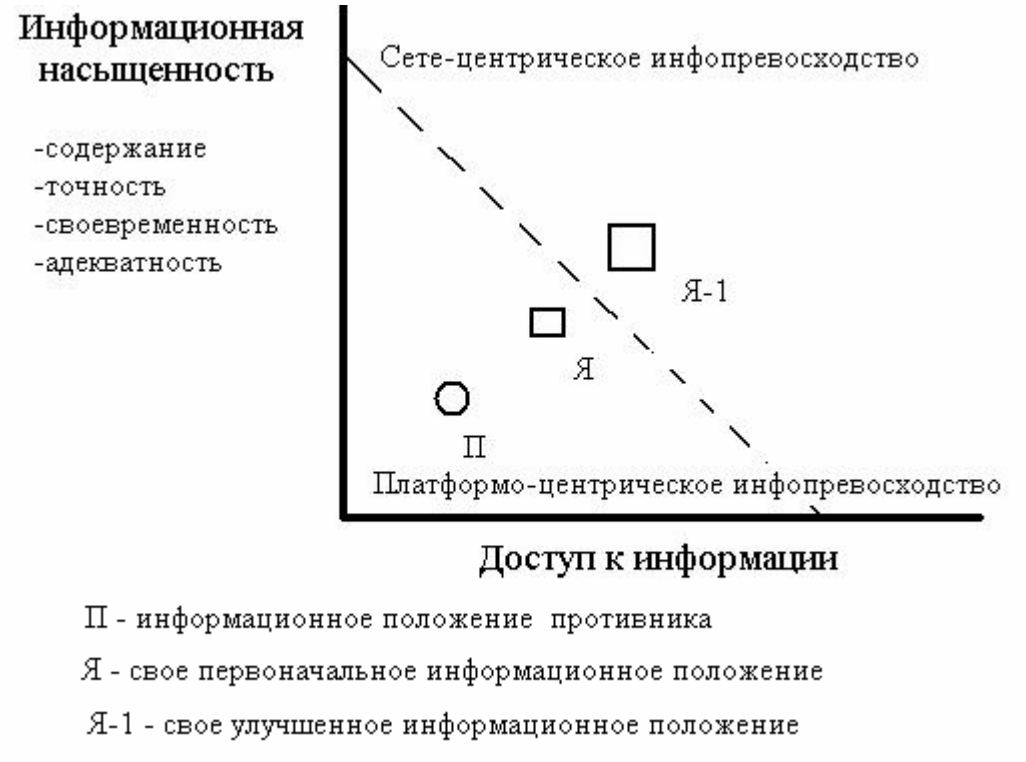
Информационное превосходство характеризует состояние информационной сферы, когда одна из сторон получает «превосходящие информационные позиции» по отношению к противнику.

Сете-центрическими силами Джон Гарстка называет вооруженные силы, связанные (или включенные в сеть) единой информационной инфраструктурой (или инфоструктурой). Сете-центрические силы имеют возможности доводить и обмениваться информацией с географическими разбросанными элементами этих сил: сенсорами (всеобъемлющей системой разведки противника), стрелками (различными типами огневых средств) и структурами, ответственными за принятие решений и поддержку (штабами и тылами). Сете-центрические силы – «эффективные силы, имеющие глобальный доступ к достоверной информации тогда и там, где это необходимо».

Принцип включения в единую информационную сеть позволяет своим силам расширить существующие рамки информационной сферы, обеспечивает им доступ к новым информационным пластам.

Графически модель информационного превосходства в условиях платформо-центрической войны (прошлых эпох) и сете-центрической войны будущего, в представлении профессора Гарстка, выглядит следующим образом:

Схема: Информационная сфера и информационное превосходство



Под понятием «доступ к информации» автор концепции сете-центрической войны подразумевает пространственные и временные

характеристики доступа к информации (о противнике, своих силах и обстановке). «Информационная насыщенность» характеризует «качество» информации, что подразумевает ее объем, достоверность, актуальность, своевременность, адекватность обстановке и многое другое. Эти два аспекта определяют фактическую информационную среду военных действий. Пунктирной линией обозначены условные пределы информационного превосходства в обычной (платформо-центрической) войне и будущей (сете-центрической) войне.

В условиях платформо-центрической войны информация о противнике, например, поступает от «платформ» (боевых машин, разведывательных машин, вертолетов, армейской авиации, разведывательных групп, наблюдательных постов и т.д.). Командиры разных степеней имеют свои пространственные пределы доступа к информации: у командира взвода нет данных космической разведки.

В условиях сете-центрической войны пределы информационной среды безгранично расширяются (положение «Я» смещается в направлении «Я-1» и далее, к новым и новым информационным пластам).

Вместе с тем, как подчеркивает Дж. Гарстка, информационную сферу нельзя рассматривать в отрыве от двух других сфер, которые в своем триедином взаимодействии и создают «среду войны». Речь идет помимо информационной еще и о физической и когнитивной сферах.

Физическая сфера, в определении американского ученого, это – «место развития ситуации, на которую оказывается военное влияние». В этой сфере – на суше, воде, воздухе и космосе – разворачиваются военные действия в форме ударов, защитных акций и маневра. В этой сфере действуют «физические платформы», соединенные коммуникационными сетями. Именно в этой сфере традиционно измеряется боевая мощь и боевые возможности сторон. Это – та сфера войны, которую можно реально ощутить, сравнить и оценить.

Когнитивная (рационально-ментальная) сфера, по словам Дж. Гарстка, складывается в умах участников конфликта. С одной стороны, она характеризуется такими понятиями, как представление, осознание, понимание, убеждения, ценности, а с другой – процессом принятия решений. Американский ученый в длинном списке элементов и аспектов конгнитивной сферы упоминает лидерство, моральное состояние, сплоченность, уровень подготовки и боевого опыта, общественное мнение, мыслительные процессы командиров и начальников, способы принятия решений, интеллект и эрудицию. Эта сфера в отличие от физической практически не поддается количественным оценкам. Успех деятельности в этой сфере во многом зависит от индивидуальных качеств и характеристик личности – генерала, офицера, солдата. Однако именно в этой сфере «выигрываются битвы и проигрываются сражения».

Информационная сфера – это та сфера, в которой происходит обмен информацией, в которой формируется и передается решение командира, осуществляется контроль и управление войсками. Не всегда эта сфера

адекватно отражает реальную ситуацию, складывающуюся в физической сфере военных действий. Но в любом случае именно в этой сфере формируются знания и представления о физической сфере, она отражает физическую сферу в виртуальной реальности.

Непосредственно затрагивая все три сферы военных действий концепция сете-центрической войны, по мнению ее авторов, способна за счет абсолютного информационного превосходства над противником обеспечить полную синхронизацию боевых действий и акций на поле боя, гарантировать быстроту управления и поднять уровень боевых возможностей и боевых способностей своих сил.

«Технологии» информационной войны

Информационная война, в какой бы форме она ни велась, предполагает прежде всего борьбу за информацию и вокруг информации. Американские специалисты выделяют в связи с этим два основных уровня информационной войны: стратегический, когда воздействию подвергаются общие информационные ресурсы и сети противника, и тактический, предполагающий достижение информационного превосходства над противником на поле боя.

По форме ведения и решаемым задачам информационная война на тактическом уровне может быть «наступательной» или «оборонительной».

Под «оборонительной» информационной войной понимается достижение полного информационного превосходства над противником – другими словами знать о нем все, знать о себе все и защитить свои информационные сети и ресурсы от проникновения противника. Доктор Дэвид Альбертс отмечает: «Термин «оборонительная информационная война» применяется для обозначения любых действий, направленных на защиту от информационных атак, т.е. атак в отношении лиц, принимающих решения, информации и информационных процессов, на которые они полагаются в своей деятельности и коммуникационные средства передачи ими своих решений в войска»[62]. «Оборонительная информационная война» нацелена на защиту информации в своих телекоммуникационных системах и обрабатывающих центрах с одновременным учетом своих технологически уязвимых мест, возможностей противника, а также ресурсов, необходимых для своей защиты» - так определяет сущность и задачи «оборонительной информационной войны Джон Коал в журнале «Military Review». И далее он продолжает: «Соединенные Штаты должны преуспеть в деле оборонительной информационной войны еще до того, как наступательная информационная война из-за рубежа, начатая еще в «мирное время», не окажет негативного воздействия на информацию и информационные системы США»[63].

[62] David S. Alberts. Defensive Information Warfare. National Defense University Press, 1996.
[63] John C Coale. Fighting Cybercrime// Military Review. March-April 1998. P. 77-82.

«Наступательная» информационная война предполагает проникновение и активное воздействие на информационные сети и ресурсы противника. Джон Коал отмечает: «Наступательная информационная война наносит удар противнику в голову, вместо того, чтобы вести войну на истощение силой против силы. Информационная война оказывает влияние на политиков, принимающих решения, на военных стратегов и военачальников, на бизнес структуры с целью заставить их принять курс действий, выработанный на основе неполной, видоизмененной, ложной информации или прямой дезинформации»[64].

Будучи виртуальной по своей сути, информационная война имеет в своем арсенале специфические «средства поражения», применяет особые способы и «технологии» поражения и уничтожения информационных сетей и систем противника.

Главным средством ведения информационной войны является компьютер, включенный в информационную сеть противника - единую глобальную сеть Интернет или в самостоятельные (изолированные) военные или иные сети противника.

Важным компонентом средств ведения информационной войны на тактическом уровне является система датчиков и сенсоров для сбора информации о противнике в реальном режиме времени. В представлении американских специалистов, реальное поле боя будущего для ведения наземных боевых действий будет представлять собой многослойный «пирог» датчиков и сенсоров, размещенных на земле, в воздухе и космосе, которые будут способны «видеть противника насквозь».

В вооруженных силах США уже сейчас применяются разнообразные системы беспилотных летательных аппаратов разведывательного назначения. Одна из них – беспилотный летательный аппарат морской пехоты США «Dragon Eye» - представляет собой аппарат, похожий на модель самолета, весом 2 кг и с размахом крыльев всего 1,3 м. В ходе последней военной кампании в Ираке вооруженные силы США применяли десять различных типов разведывательных беспилотных летательных аппаратов.

По мнению американских военных аналитиков, в будущем бригада сухопутных войск США численностью 3 – 5 тысяч человек будет применять в своих целях до 200 беспилотных летательных аппаратов.

Развитие разведывательных средств в направлении минимизации размеров ведет к созданию беспилотных летательных аппаратов еще более крошечных по размерам с размахом крыльев до 20 сантиметров.

Эти аппараты оснащаются телевизионными камерами, инфракрасными приборами наблюдения и другими электронными средствами разведки, а также средствами связи. В идеале, такой «самолетик» способен летать длительное время над позициями противника, будучи практически незаметным для него. На экран компьютера передается реальная «картинка», вплоть до окопов отдельных солдат противника и выражений лиц вражеских

[64] John C Coale. Fighting Cybercrime// Military Review. March-April 1998. P. 77-82.

солдат. Укрыться от электронного ока такого «самолетика» будет в принципе невозможно.

Другим примером тактических систем сенсоров и датчиков поля боя являются разработки специалистов ВВС США. Именно ВВС являются тем видом вооруженным сил, где активно обсуждаются и внедряются самые современные и перспективные технологии, которые могут быть с успехом реализованы в военной области. В середине 90-х годов XX века американскими военными специалистами был разработан серьезный долговременный проект под названием «ВВС-2025», в котором нашли отражение многие технологические инновации.

Среди некоторых разработок в области информационных технологий, датчиков и сенсоров, отличающихся своей необычностью, выделяются следующие концепции[65].

«Муха на стене» (Fly on the Wall, AF 2025 Concept #900280). Возможности нанотехнологии позволят снабдить специальными чипами мух, которые, благодаря этому, станут управляемы с удаленного пункта управления. Фактически, мухи превратятся в своеобразные мобильные сенсоры. Оператор получит возможность полного визуального контроля над обстановкой в зоне нахождения мухи. Муха может быть направлена на конкретную цель, а затем сама сможет обеспечить абсолютную точность наведения систем поражения на эту цель.

«Робот-жук» (ROBOBUGS, AF 2025 Concept #900341). Эта концепция аналогична проекту «Муха на стене», только вместо мух могут быть использованы насекомые.

«Я чувствую твой запах» (I Can Smell You, AF 2025 Concept #900567). Специальные электронные чипы обеспечат обнаружение цели, ее сопровождение и наведение систем поражения по запаху, источаемому этой целью.

Американские эксперты ожидают в ближайшие годы качественных скачков в развитии биотехнологий, в результате чего будут созданы киборги различного назначения. В начале 2000 года ученые соединили человеческую клетку с электронным чипом, добившись возможности компьютерного контроля над жизнедеятельностью органической клетки. Перспективы этого технологического прорыва в медицинском отношении огромны, однако специалисты в области информационной войны увидели свою «выгоду».

Реальным становится создание своеобразных киборг-платформ, которые оказываются значительно эффективнее и дешевле обычных роботов. Так например, эксперты утверждают, что роботы размером с таракана только через несколько десятилетий смогут достичь мобильности живого таракана. Однако уже сейчас есть успешные попытки имплантации электронных чипов в живых тараканов, что делает их «дистанционно управляемыми»[66].

---

[65] 2025. Air University Press, 1996.

[66] Steven Metz. Armed Conflict In the 21st Century: The Information Revolution and Post-Modern Warfare. Strategic Studies Institute, US Army War College, 2000. P.47.

В будущей войне в городских условиях, например, такие оснащенные сенсорами тараканы могут направляться солдатом-оператором в нужном направлении, обеспечивая поступление необходимой информации из разных малодоступных мест.

Главными «средствами поражения» в «наступательной» информационной войне как на стратегическом, так и на тактическом уровнях, являются компьютерные вирусы, логические бомбы, информационные бомбы, чиппинг-технологии, электромагнитные бомбы.

Разновидностей и типов компьютерных вирусов огромное количество. Часть из них относится к «доброкачественным», другие – к «злокачественным». Если первые возможно «вылечить», а вызываемые им сбои не вызывают катастрофического ущерба, то вторые разрушают данные или целостность всей информационной системы. В военных целях при проведении операций информационной войны именно «злокачественным» вирусам будет отдаваться предпочтение.

Логическая бомба является в определенной степени разновидностью «злокачественного» вируса «замедленного действия». Они внедряются заранее в компьютерные сети, однако активизируются только через какое-то время – или самостоятельно, или по команде оператора.

Информационная бомба предполагает перегрузку информационных сетей противника ненужной, пустой информацией, практически парализующей все его действия.

Чиппинг-технология предполагает внедрение «заминированных» чипов в военную технику противника. Чип – интегральная микросхема, покрытая защитной оболочкой, препятствующей копированию или прочтению заложенной информации.

Электромагнитная бомба – это устройство, предназначенное для радиоэлектронных средств посредством мощного электромагнитного импульса. Разрушительное воздействие электромагнитной бомбы сопоставимо с электромагнитным импульсом, возникающим при ядерном взрыве. Это – подобие СВЧ печи, которая выводит из строя все электронные и электрические сети, инициирует пожары в радиусе действия импульса.

«Оцифрованная» армия

Военные действия в эпоху информационных войн будущего, как считают американские специалисты, будет не только вестись в виртуальном пространстве, но и на реальном поле боя. Однако военные действия на будущем поле боя будут вести так называемые «оцифрованные» войска.

«Оцифрование»[67] - термин, введенный в сухопутных войсках США, означающий качественный скачок в системах управления, связи, разведки и компьютерных сетях. «Оцифрование» предполагает перевод всей информации, необходимой для планирования и ведения боевых действий, в

[67] В американских публикациях используется термин Digitization.

цифровую форму и размещение ее в единой боевой информационной сети. В специальном пособии, подготовленном Ассоциацией армии США в 2001 году, трактуется: «Информационные технологии, взятые на вооружение, а также доктрины и тактика их использования приведут к новой революции в военных делах. Оцифрование армии США представляет собой самое серьезное изменение в военном деле с эпохи Наполеона и закладывает фундамент для ведения войны в XXI веке»[68].

Что понимают американские военные специалисты под термином «оцифрование»? В вышеупомянутом пособии Ассоциации армии США указывается:

«Оцифрование – это общий термин, означающий интеграцию всех информационных систем обмена информацией с разнообразными платформами и системами оружия – вплоть до индивидуального солдата – через систему «Воин сухопутных войск» (Land Warrior)». Оцифрование обеспечивает эффект умножения возможностей информационной сети в режиме реального времени с представлением единой оперативной картины каждой системе или пользователю в форме изменяемой и многоуровневой «картинки» на экране монитора компьютера… Оцифрование соединяет воедино сенсоры и стрелков. Оно соединяет систему тылового обеспечения с теми, кто в нем нуждается. Оно обеспечивает передачу приказов и донесений. Оно предоставит вам все – от огневой поддержки до прогноза погоды»[69].

Бригадный генерал Джозеф Одер, возглавлявший работы по «оцифрованию» в сухопутных войсках США, в своей статье в журнале «Army» в мае 1994 года определял «оцифрование» как «применение информационных технологий на всем пространстве поля боя для получения, обмена и использования своевременной цифровой информации, специально приспособленной к нуждам каждого лица принимающего решения (командира), стрелка и обеспечивающего лица, позволяя каждому из них составить четкое и точное представление о поле боя, что необходимо при планировании и выполнении боевых задач»[70].

Процесс «оцифрования» армии США начался в марте 1992 года, когда генерал Р. Салливан, бывший тогда начальником штаба сухопутных войск США, санкционировал создание так называемую «Боевую группу маневров в Луизиане»[71]. Такое название было не случайным: в 1941 году в Луизиане состоялись крупномасштабные маневры, которыми было положено практическое начало подготовки США ко второй мировой войне. Накануне большой войны в маневрах участвовало 400 тысяч солдат, однако в начале 90-х годов «мобилизации» подверглись интеллектуальные ресурсы армии США.

---

[68] Dennis Steele. The Army Magazine Hooah Guide to Army Digitization. The Association of the U.S. Army, 2001.
[69] Dennis Steele. The Army Magazine Hooah Guide to Army Digitization. The Association of the U.S. Army, 2001. P. 13.
[70] Joseph. E. Oder. Digitizing the Battlefield: The Army's First Step to Force XXI// Army. 1 May 1994. P. 38.
[71] The Louisiana Maneuvers Task Force.

«Боевая группа маневров в Луизиане» действовала вплоть до 1996 года, когда ее функции были переданы Отделу по оцифрованию армии[72], а впоследствии работы в этой области перешли в ведение заместителя начальника штаба армии по программам. Все исследовательские работы велись под наблюдением Командования сухопутных войск США по обучению и доктринам – специального органа американской армии, ответственного за развитие и внедрение новых идей в сфере подготовки войск к войнам будущего.

Командование сухопутных войск по обучению и доктринам с 1992 года активно разрабатывало концепцию «Сила XXI» (Force XXI), которая затем была трансформирована в концепцию «Армия пост-следующего этапа» (Army After Next), а затем и концепцию «Трансформация армии» (Army Transformation).

В августе 1994 года Командование по обучению и доктринам опубликовало Устав 525-5 «Операции Силы XXI», в котором особое внимание было уделено роли и значению информации в современной войне. Так, там определялось: «Цель создания армии XXI виделась в формировании вооруженных сил, способных вести войну в соответствии с принципами стратегии гибких действий и применять информационные технологии таким образам, чтобы достигать наибольшей смертоности в бою, наивысшей защищенности своих войск и высочайшим темпом оперативного маневра»[73].

Для практической проверки теоретических выкладок американских специалистов армейским командованием было принято решение создать так называемое «Экспериментальное соединение дивизионного звена» (EXFOR). В декабре 1994 года в качестве базового соединения для этой цели была выбрана 2-я бронетанковая дивизия, дислоцировавшаяся в Форт-Худе (Техас). В январе 1996 года эта дивизия была преобразована в 4-ю пехотную дивизию (механизированную), которая и стала своеобразным «полигоном» для отработки всех аспектов концепции «оцифрования» армии США.

В последующие годы на базе 4-й пехотной дивизии (механизированной) были проведены десятки так называемых «экспериментов» - виртуальных и реальных учений и тренировок – целью которых была практическая отработка концептуальных наработок специалистов. По мнению экспертов, все они завершились успешно.

Сердцевиной американской концепции «оцифрования» армии стало создание Тактического интернета, т.е. боевой информационной системы. В отличие от обычной сети Интернета, тактический интернет представляет собой хорошо защищенную информационную систему. Другой отличительной чертой тактического интернета является способность в беспроводном режиме соединять все звенья от вышестоящих штабов до отдельных боевых машин и (в идеале) отдельного солдата.

---

[72] The Army Digitization Office.

[73] См.: Dennis Steele. The Army Magazine Hooah Guide to Army Digitization. The Association of the U.S. Army, 2001. P. 10.

В сеть тактического интернета включена целая сеть информационных подсистем, которые в совокупности представляют собой Систему боевого командования армии ABCS (Army Battle Command System).

Система ABCS состоит из трех важнейших компонентов:

- Глобальной сети командования и управления сухопутных войск, которая является в свою очередь компонентом объединенной сети командования и управления вооруженных сил США.
- Тактической сети командования и управления сухопутных войск, которая поддерживает связь преимущественно в звене корпус-бригада. Она включает пять субсистем на поле боя: систему управления маневром; систему тактических данных полевой артиллерии; всеобъемлющую аналитическую систему; систему управления боевого обеспечения; рабочую станцию ПВО и противоракетной обороны.
- Системы боевого командования Сил XXI в звене бригада и ниже $FBCB^2$ (Force XXI battle command brigade and below system), которая представляет собой современнейшую систему графического отображения информации на тактическом уровне вплоть до отдельного военнослужащего. Эта система дает ответы на три главных вопроса, которые составляют сердцевину всей деятельности по «оцифрованию» армии: «Где нахожусь я? Где мои соседи? Где противник?».

В единой информационной системе тактического интернета командиры всех степеней получили доступ к необходимой им информации в реальном масштабе времени. На экране компьютера командира дивизии отражается полная тактическая обстановка вплоть до батальонного звена. Сверху на эту «картинку» можно наложить, например, метеопрогноз на ближайшее время. Благодаря этому командир дивизии имеет четкое представление, где и когда можно использовать беспилотные летающие разведывательные комплексы, а где необходимо прибегать к другим средствам разведки противника. На ту же «картинку» комдив может наложить схему тылового обеспечения своего соединения.

Информационные потребности командира роты или взвода на поле боя значительно проще и конкретнее. Единая информационная сеть тактического интернета представляет им детальную информацию обо всех штатных и приданных системах оружия – их количестве, боевых возможностях, дислокации и передвижениях. Командиры подразделений имеют необходимо представление о боевых возможностях соседей и резервов старших начальников. Вся информация о противнике в режиме реального времени передается на экраны тактических компьютеров командиров всех звеньев. Они фактически получили возможность всеобъемлюще видеть как бы всю картину боя, а не только свою конкретную боевую задачу.

Солдат информационной эпохи

Военнослужащий современных вооруженных сил США по своей экипировке и вооружению в корне отличается от бойца эпохи второй

мировой войны. Не менее разительным будет и отличие солдата будущего. Роль отдельного военнослужащего на поле боя становится все более значительной и значимой. Из обычного «винтика» в единой военной машине подразделения, части, соединения солдат превращается в своеобразный «интеллектуальный разведывательно-ударный комплекс», включенный в единую информационную сеть.

Солдат будущего будет обладать абсолютным информационным превосходством над противником. Всеобъемлющая сеть датчиков и сенсоров позволит ему видеть противника и все поле боя насквозь. Грань между родами войск будет достаточно расплывчата: солдат на поле боя не будет пехотинцем или танкистом. Это будет «универсальный солдат», задача которого будет заключаться не в стрельбе по живой силе противника, а в координации маневра и огня самых разнообразных сил и средств, вплоть до авиационных и ракетно-артиллерийских.

С начала 90-х годов в США на разных уровнях ведутся научно-исследовательские разработки в области создания своеобразной «системы солдата», объединяющей военнослужащего с другими компонентами: оружием, системами управления, связи, навигации, системами энергоснабжения и микроклимата, системами защиты тела и организма от враждебных факторов боевой среды.

В итоге многочисленных экспериментов, проводившихся в разных географических и боевых условиях, был представлен экспериментальный вариант «системы солдата», получивший название «Land Warrior».

Главным достоинством новой «системы солдата» считаются повышенные боевые возможности по поражению противника и по обеспечению собственной живучести в бою за счет включения каждого солдата в общую цифровую сеть боевого управления части. Опытный образец «Land Warrior» прошел полевые испытания в период 1998 - 2000 гг. и признан перспективным. Он включает в себя пять подсистем: головного шлема-каски, индивидуальной связи и портативного компьютера, интерфейса оружия, защиты и микроклимата[74].

Подсистема головного шлема-каски из высокопрочного кевлара является ключевым элементом всей «системы солдата». В нее входят: индивидуальный дисплей для отображения информации о боевой обстановке с высокой четкостью изображения, переговорное устройство, видеокамера, система ночного видения, тепловизионная система и оптическая система прицеливания, конструктивно выполненные в одном корпусе. Шлем выдерживает прямое попадание 9-мм пули и обеспечивает защиту глаз от лазерного излучения.

Подсистема личной связи сопряжена с портативным компьютером и индивидуальным датчиком глобальной навигационной системы GPS. Эта подсистема должна помочь солдату ориентироваться на местности, оценивать обстановку, вести переговоры в звене отделение-взвод, передавать

[74] Леваков А. Электронный солдат Пентагона// См. подробнее: http://freelance4.narod.ru/index.htm

и получать видео изображения, опознавать цели, вести разведку, в том числе и химическую, обнаруживать мины, осуществлять опознавание цели (по принципу «свой-чужой») и выполнять другие функции.

Связь солдата с его отделением в бою поддерживается с помощью двух компактных радиостанций, смонтированных в едином блоке размером с записную книжку общим весом 656 г. Одновременно поддерживается разговор трех абонентов и передача данных в режиме засекречивания на расстояние до 5 км. Для связи вне зоны видимости используется ретрансляция с автоматическим поиском ближайших радиостанций других пехотинцев или воздушных ретрансляторов (самолетов или вертолетов).

В качестве вычислительной платформы для «системы солдата» в настоящее время используется IBM совместимый портативный мультимедийный компьютер с упрощенной операционной системой Windows-2000, процессором Пентиум-75 Мгц, оперативной памятью 32 Мбайт, жестким диском объемом 340 Мбайт и сменной флэш-памятью 85 Мбайт, сетевой картой Ethernet. Для подключения периферийного оборудования в компьютере имеются шины PCI и ISA, с двумя разъемами RS-232. Общий вес портативного компьютера составляет около 1200 г, а габариты без внешних соединителей 27 см x18 см x4 см. Диапазон рабочих температур от –15 до +49 градусов Цельсия. Предусмотрено несколько типовых вариантов установки вычислительной системы в зависимости от выполняемых боевых задач: для командира, солдата, инженера, разведчика, корректировщика огня. В командирский вариант предусмотрено подключение клавиатуры с трекболом и дисплеем VGA. Для удобства пользования портативный компьютер оснащен индивидуально настраиваемой системой распознавания голоса.

Подсистема интерфейса оружия позволяет солдату в боевых условиях использовать все доступные ему источники тактической разведывательной информации для поражения объектов противника всеми имеющимися огневыми средствами от автоматической винтовки M16 до самоходной гаубицы M203 и боевого вертолета "Аппач". Встроенная в автоматическую винтовку и интегрированная с защитным шлемом-каской система прицеливания с инфракрасной оптикой, лазерным дальномером и цифровым компасом позволяет наводить оружие из-за угла или бруствера в любых условиях видимости. Оптическая система винтовки может быть использована и в качестве «перископа», выставляя который из-за укрытия пехотинец может вести разведку, стрельбу и корректировку огня.

В подсистему защиты входят комплект бронезащиты, выдерживающий попадание пули калибра 7,62 мм, снаряжение и обмундирование. Общий вес снаряжения планируется довести до 40 кг. В боевых условиях в случае необходимости солдат может быстро сбросить весь комплект или его часть. Солдат будущего будет снабжен противоминными сапогами; противоосколочным и антирадиационным бронежилетом; очками защищающими глаза от механических травм и ослепляющих лучей.

Подсистема микроклимата «системы солдата» предполагает оснащение его персональным портативным кондиционером. Вес агрегата составляет 4,5 кг, а его мощность обеспечивает поддержание заданного температурного режима в «оболочке» солдата в течение 4 часов. Перспективность и целесообразность оснащения каждого пехотинца подсистемой микроклимата пока ставятся под большое сомнение: увеличивается физическая нагрузка на солдата, а это в бою недопустимо. Вместе с тем, в особых условиях (в засаде, на блок-посту, на марше и т.д.) индивидуальная подсистема микроклимата себя может оправдать.

Униформа солдата будущего будет оснащена специальными датчиками, которые будут способны поддерживать внутренний комфортный микроклимат. Наружные сенсоры будут вести непрерывный мониторинг параметров окружающей среды, определяя влажность, атмосферное давление, температуру и т.д.

В новую форму будут встроены специальные биосенсоры, которые смогут автоматически передавать данные о состоянии здоровья солдата в централизованную базу данных. Военные медики получат возможность в любое мгновение узнать температуру, пульс, давление каждого из солдат. В случае ранения форма сможет определить его место и «перетянуть» рану, чтобы уменьшить потерю крови. Все данные об окружающей среде, равно как и показатели личного самочувствия, будут отражаться на дисплее персонального компьютера.

Каждый военнослужащий будет оснащен универсальным личным транспортным средством, которое при необходимости будет способно действовать самостоятельно, управляясь дистанционно. В таком случае универсальное транспортное средство будет выполнять разведывательные функции или действовать в качестве огневой платформы.

В комплект разведывательного оснащения солдата на поле боя будет входить дистанционно управляемый микросамолетик, оснащенный видеокамерой и всевозможными микродатчиками для обнаружения противника в непосредственной тактической глубине его расположения. Одновременно солдат будущего будет получать полную разведывательную информацию из общей информационной сети своей части и/или напрямую с датчиков и сенсоров, огромное число которых будет разбросано по всему полю боя.

Общая стоимость программы «Land Warrior» оценивается в 2 млрд. долларов, полномасштабная реализация которой предполагает поставку в войска в течение 2001-2010 гг. 34 тысяч комплектов.

В январе – феврале 2001 года в штате Калифорния были проведены первые полевые учения в ротном звене с использованием нового комплекта снаряжения пехотинца. В ходе учений за счет использования нового снаряжения условные потери противника возросли с 55% до 100%, а собственные потери снизились с 28% до 17%. Все электронные компоненты безотказно работали даже в воде.

Новые разработки американских специалистов в области индивидуального оснащения и вооружения солдата прошли дальнейшую апробацию в ходе боевых действий в Ираке. Даже внешний вид американских солдат, тиражировавшийся телевизионными компаниями на весь мир, создавал психологическое ощущение американского превосходства.

Образы голливудских фантастических боевиков о кибер-солдатах будущего в какой-то степени отражают реальные тенденции.

Когда информационные технологии бессильны…

Широкое внедрение информационных технологий в военную сферу сопровождается не только успехами, но и многочисленными проблемами. Даже союзники США по блоку НАТО – развитые государства Запада – зачастую не успевают за развитием американских военных технологий, что создает огромные трудности при проведении операций коалиционного характера. По мнению канадского эксперта Элиноры Слоан, разрыв в технологиях между США и Западной Европой был очевиден уже в ходе операции «Буря в пустыне» в 1991 году, однако стал значительным в операции НАТО в Косово в 1999 году. Она пишет: «Превосходство Америки в информационных системах означало, что у нее были трудности в осуществлении связи со своими союзниками. Союзники также столкнулись с проблемами совместного развертывания, опознавания целей и совместимости оружия… Существующий разрыв в технологии и потенциале между США и их европейскими союзниками влечет за собой ряд последствий. Наиболее заметным из них является то, что уже скоро вооруженные силы европейских стран не смогут взаимодействовать с американцами из-за их «технологической отсталости»[75].

Информационная война будущего, как представляется военным специалистам США, будет своеобразной компьютерной игрой, ставки в которой окажутся чрезвычайно высокими. Одним щелчком компьютерной мыши можно будет нанести невосполнимый ущерб противнику, от которого последний просто не сможет оправиться. Информационные технологии позволят вести бескровные войны, ставя на колени целые страны и регионы, подчиняя их жестокой воле победителя.

В целом эта картина будет, скорее всего, очень близка к истине, но только при одном главном условии – противник будет оснащен соответствующими информационными технологиями, которые могут стать объектами и целями американского воздействия. Другие государства, включенные в единую глобальную информационную сеть, действительно могут оказаться легкой «добычей» стратегов информационной войны.

[75] Э. Слоан. ИОП: ответ на революцию в военном деле, возглавляемую США// Вестник НАТО, весна-лето 2000. С. 5.

Однако, если противником будет выступать не государство, а какие-то структуры, формирования, организации, политические и криминальные силы и банды, успех проведения акций информационной войны становится проблематичным.

Как утверждают американские эксперты, в принципе возможно вывести из строя такую мощную страну, как США. Всемирно известный американский футуролог Алвин Тоффлер в своем интервью в 1994 году говорил: «Нам известен один в прошлом достаточно высокопоставленный представитель разведки, который утверждает: «Дайте мне миллиард долларов и 20 человек сотрудников, и я покончу с Америкой. Я выключу сеть Федерального резервного банка, отключу все банкоматы; я выведу из строя все компьютеры в этой стране»[76].

Однако что делать, если страна очень бедная и не имеет возможности приобрести самые современные компьютеры и информационные технологии? Ведь тогда она становится неуязвимой для информационного оружия. Кстати, именно здесь кроется одна из причин активности США и стран Запада в форме разнообразных негосударственных организаций и фондов по распространению компьютерных технологий в бедных странах третьего мира, иногда даже в ущерб сиюминутным выгодам и прибыли. Включение все большего количества стран (и других структур, организаций и т.д.) в общую глобальную информационную сеть несет неоспоримые преимущества для их экономического, культурного, цивилизационного развития, однако, с другой стороны, делает их потенциально уязвимыми в будущих конфликтах новой – информационной – войны. Американский эксперт профессор М. Либицки, рассуждая на эти темы, приходит к следующим выводам:

1. Чтобы досконально знать информационные системы противника в военное время, необходимо иметь о них исчерпывающую информацию уже в мирное время.
2. Для того, чтобы постичь информационную инфраструктуру другой страны в мирное время, США необходимо помочь ее создать.
3. Самой проницательной стратегией национальной обороны США могла бы стать поддержка политики развития глобальной информационной инфраструктуры (ценовая политика, программное обеспечение и т.д.)[77].

В современных Соединенных Штатах есть целый ряд специалистов, которые смотрят на возможности информационных технологий не столь оптимистично. Развитие и внедрение в армии новых информационных технологий, дальнейшее «оцифрование» вооруженных сил меняют так называемую «культурную среду» военной организации государства. Меняется взаимоотношения командиров и подчиненных, теряют свой смысл вековые истины и принципы, на которых строились вооруженные силы,

[76] Technology and Weaponry. Alvin Toffler warns of the information battleground// Information Week. 1994. January, 10. P. 50.
[77] Martin C. Libicki. What Iss Information Warfare? National Defense University. August 1995. P. 103.

изменяется роль и место человеческого фактора в бою. К обычному солдату предъявляются все более и более серьезные требования, а солдат будущего должен быть уже «профессором» в сфере информационных и компьютерных технологий. Требуется больше времени на его обучение и подготовку, специфичнее становятся требования к командирам и начальникам. Рядовой солдат будущего будет уже не послушным исполнителем приказа командира, а настоящим «военным стратегом». Все это не может не отразиться коренным образом на всей военной организации общества.

В связи с этим один из авторитетных «техно-скептиков» современных США генерал-лейтенант морской пехоты в отставке Поль К. Ван Райпер с иронией отмечал: Я предпочел бы иметь в качестве помощника специалиста с карандашом и бумагой, чем идиота с компьютером»[78].

По мнению некоторых экспертов, слишком полагаться на технологию грозит многими опасностями, одной из которых является ложное чувство превосходства над противником. Это ощущение очень опасно, ибо не учитывает того факта, что войну все-таки ведут люди, а не техника. Независимо от степени «технологизации» и «оцифрования» вооруженных сил за экранами компьютеров будут сидеть люди, принимать принципиальные ответственные решения будут люди, погибать будут люди. А человек – не бездушная машина-убийца, а существо, подверженное эмоциям, стрессам, чувствам и переживаниям.

Классическим примером переоценки роли и значения техники в недавней военной истории США стала операция в Сомали. 3 октября 1993 года боевая группа «Рэйнджер» американской армии в ходе выполнения миротворческих функций в этой африканской стране подверглась нападению со стороны сомалийских боевиков генерала Айдида. Американское командование недооценило всю сложность и специфику военно-политической ситуации в Сомали, поставив тем самым под удар своих солдат. Итоги операции по спасению боевой группы «Рэйнджер» оказались трагическими: 19 американских военнослужащих погибли или пропали без вести, 84 было ранено; погиб один малазийский военнослужащий, а еще 7 малазийцев и два пакистанца были ранены[79]. В конечном счете американцы были вынуждены вывести свои войска из Сомали.

Главный урок операции «Восстановление надежды» в Сомали состоял в том, что одна только военная сила, какая бы она не была мощная и совершенная, не гарантирует успех и победу. Как подчеркивает Д. Даффи, в ходе той операции на стороне американских войск были преимущества техники и вооружения, однако они «не были готовы действовать в условиях кровавой войны между разными племенами, ибо они не понимали их культуры». «В той ситуации, - продолжает Д. Даффи, - необходима была не

[78] Daintry Duffy. Information Is a Weapon. What Will Happen When Every Soldier Is Armed With It?// Darvin Magazine. November, 2001.
[79] Clifford E. Day. Critical Analysis On the Defeat of Task Force Ranger. U.S. Air Command and Staff College, 1997. P. 11.

совершенная технология, а боевые силы, которые могли бы думать как культурологи-антропологи»[80].

Человеческий фактор – вот тот аспект, который проигнорировали в Сомали и который нередко недооценивается некоторыми ярыми сторонниками информационных технологий. В последнее время стало модным крылатое изречение: «Если ты видишь поле боя – ты выиграл войну». Генерал Ван Райпер со свойственным ему скептицизмом прокомментировал это популярное выражение: «Я тоже могу сказать, что если я вижу шахматную доску – я выиграл партию. Однако это так, пока мастер вновь меня не разобьет в пух и прах»[81].

[80] Daintry Duffy. Information Is a Weapon. What Will Happen When Every Soldier Is Armed With It?// Darvin Magazine. November, 2001.
[81] Daintry Duffy. Information Is a Weapon. What Will Happen When Every Soldier Is Armed With It?// Darvin Magazine. November, 2001.