информационный империализм в контексте ведения информационной войны едва ли целесообразно. Скорее он служит общим фоном для формирования тенденций развития информационных технологий, военного дела и новых концепций информационной войны. Поэтому не удивительно, что одной из идей, лежащих в основе американских теоретических построений в области информационной войны, стала идея достижения информационного доминирования.

Согласно определению Пентагона оно необходимо для достижения общего превосходства над противником через завоевание стратегического технологического преимущества в деле управления информационными потоками в масштабе времени, близком к реальному, а также для воздействия на соперников с тем, чтобы принятые ими решения соответствовали общим задачам и национальным интересам Соединённых Штатов [21].

СОВРЕМЕННЫЕ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ ВОЙНЫ

Научный прогресс и внедрение его результатов быстро меняют условия существования человечества. Именно по этой причине американские концепции информационной войны 90-х гг. прошлого века в настоящее время подвергаются серьёзной ревизии. Безусловно, теоретические построения того времени нельзя назвать бессистемными. Так, рассмотренная выше классификация направлений ведения информационной войны, предложенная М. Либики, в целом выглядит вполне логичной. Однако её основным недостатком является смешение функциональных направлений (борьба с системами управления, экономическая борьба) и методов (электронная, психологическая, хакерская борьба). Дальнейшие теоретические построения в значительной степени были попыткой создать более стройную систему, чтобы начать реализацию прикладных программ достижения информационного доминирования.

Некоторые американские эксперты[1] для лучшего понимания проблемы предложили концептуальную модель информационной

[1] Характерно, что их имена прочно ассоциируются с обозначенными ранее теоретическими школами информационной войны, и именно эти специалисты оказали

войны [22]. В соответствии с ней информационные операции ведутся в информационной среде (рис. 1), границы которой обусловлены высокой зависимостью современных институтов от информационных технологий и информации как таковой и распространяются на наземное, морское, воздушное и космическое, а также на кибернетическое пространства. Информационная среда имеет три измерения: физическое, собственно информационное и когнитивное.

Физическое измерение – это материальный мир, где ведутся классические боевые действия, а также киберпространство. В нём информация и коммуникационные системы (инфраструктура) играют обеспечивающую роль.

Информационное измерение – это то пространство, где информация создаётся, обрабатывается, распределяется и хранится. Оно связывает физическое и когнитивное измерения и служит для получения как входящей информации (стимулов, чувств), так и исходящей (намерений, решений и т.п.).

Когнитивное измерение существует в человеческом сознании. В нём поступающая информация в соответствии с теми или иными моделями восприятия обрабатывается, принимаются решения, формируются идеи и устремления.

Такая концептуальная модель может служить базой для определения сферы информационного противоборства конкурирующих субъектов и целей информационного доминирования (рис. 2).

Информация циркулирует в так называемой OODA-петле (*observation, orientation, decision, action* – наблюдение, ориентация,

---

непосредственное влияние на начало практических действий в этом направлении. Среди них – Д. Альбертс, на тот момент директор Управления исследований и стратегического планирования МО США, ранее – заместитель директора Национального института стратегических исследований, тесно связанного с Национальным институтом обороны; Дж. Гарстка – соавтор адмирала А. Цебровски, старший офицер Комитета начальников штабов, читавший курс лекций в Джорджтаунском, Гарвардском университетах и в Военно-морском колледже, офицер ВВС США в запасе; Р. Хайес – основатель корпорации Evidence Based Research, тесно сотрудничающий с различными структурами Министерства обороны и разведывательного сообщества США; Д. Сигнори – начальник направления проблем систем управления и информационных технологий корпорации РЭНД, тесно сотрудничает с Управлением перспективных исследований и МО.

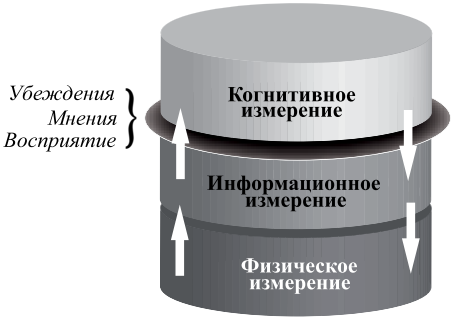

Рис. 1. Информационное окружение

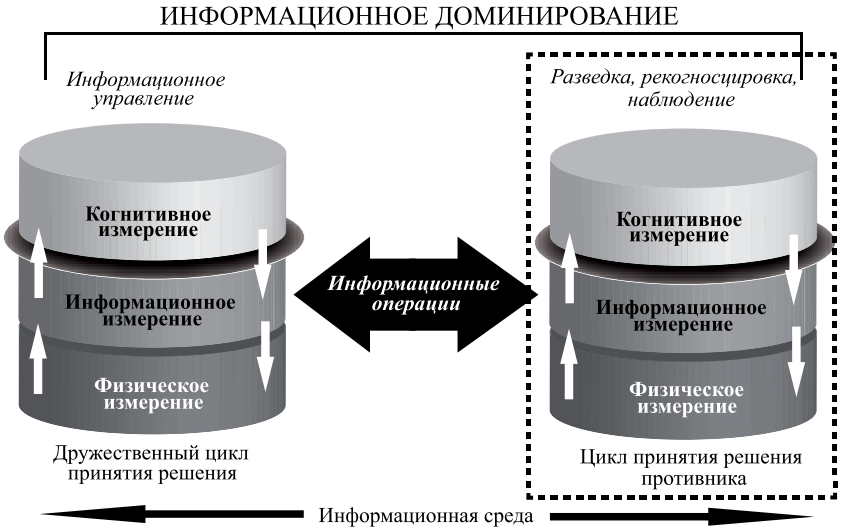

Рис. 2. Упрощённая модель информационного доминирования

принятие решения и действие). Решения принимаются с учётом информации, поступающей из физического окружения (разведка, рекогносцировка и наблюдение), и через информационное измерение оказывают влияние на реальный мир. Данное положение, в частности, означает, что когнитивная сфера не может быть объектом прямого воздействия, но ею можно манипулировать, воздействуя на физическое и информационное измерение (информационные операции), а также на восприятие противника. Соответственно, эффективность принятия собственных решений также будет зависеть от возможности получать и обрабатывать информацию (информационное управление). Таким образом, можно выделить два основных элемента, позволяющих достичь информационного доминирования:

– *информационный менеджмент,* или управление, включающее в себя системы управления, связи, компьютерного обеспечения, разведки и наблюдения, т.е. C^4ISR (эта проблематика рассматривается главным образом в рамках концепции сетевой войны);

– *информационные операции*, или действия, направленные на нарушение информационного управления противника и защиту собственного.

Концепция сетевой войны

Относительно новая концепция сетевой организации вооружённых сил, или сетевой войны [23], появилась в конце 90-х гг. прошлого века. Первоначально она представляла собой попытку осмыслить новые угрозы и возможности информационной эпохи в рамках военной теории. Затем термины "сетевая война" и "сетевая организация вооружённых сил" стали использоваться для описания широкого класса подходов к проведению военных операций с учётом как технических, так и организационных аспектов внедрения информационных технологий и сетевых принципов организации в военное дело.

Концепция сетевой войны, с одной стороны, является эволюционным продолжением теоретических разработок, посвящённых информационной войне и войне в информационную эпоху, а с другой – первой концепцией в этой области, которая стала основой программ развития Вооружённых сил Соединённых Штатов.

Разработка, испытания и развёртывание элементов информационной архитектуры (от систем управления, разведки и связи до высокоточного оружия) в вооружённых силах, происходившие на протяжении последних 10–15 лет, а также опыт вооружённых конфликтов этого периода демонстрируют необходимость и возможность функциональной интеграции боевых и разведывательных средств с системами управления, а также улучшения взаимодействия между разными видами вооружённых сил. Осознание необходимости такой функциональной интеграции привело к появлению теории сетевой организации ВС (*network-centric defense*), или сетевой войны (*network-centric warfare*).

Авторами этой концепции в её сегодняшнем понимании считаются бывший директор Управления трансформации сил МО США вице-адмирал А. Цебровски и Дж. Гарстка. Хотя эта теория появилась относительно недавно, она уже усиленно внедряется в практику, тем более что информационное насыщение вооружённых сил и "интеллектуализация" боевых платформ создали для этого все предпосылки.

Концепция сетевой организации ВС базируется на использовании информационных технологий и в первую очередь означает тотальную интеграцию сети сенсоров (разведывательных спутников, самолётов ДРЛО, разведывательных БЛА, сонаров и т.п.), компьютерных и коммуникационных систем, систем управления (ответственных за принятие решения) и боевых платформ. Как отметил А. Цебровски, "концепция сетевой войны говорит не о технологиях. Она является продолжением военной теории" [24].

Если говорить в самом общем виде, то предлагается сместить приоритеты с создания тех или иных боевых платформ (танков, самолётов, кораблей) к их интеграции в единую структуру для совместного использования. А. Цебровски выделяет следующие основные принципы сетевой войны [25]:

– создание мощных вооружённых сил с сетевой структурой распределения информации, обладающих расширенными возможностями информационного обмена;

– повышение качества поступающей информации и получение более точного представления об общей боевой ситуации, что достигается улучшенным информационным обменом между всеми задействованными элементами;

– наличие у этих элементов (даже на тактическом уровне) возможности "самосинхронизации", т.е. расширенных прав принятия

решения, что придаёт им большую боевую устойчивость даже при нарушении центрального управления, а также повышает скорость боевого реагирования.

Комбинация этих принципов качественно улучшает эффективность боевых действий за счёт происходящих синергетических (взаимовлияющих) процессов в упомянутой выше OODA-петле. По мнению авторов данной концепции, её практическое осуществление позволит повысить боевую эффективность войск путём синхронизации совместных действий разнородных сил на поле боя, улучшения качества командования и скорости реагирования в быстро меняющейся боевой обстановке.

Сетевая интеграция, по мнению Дж. Гарстки, должна осуществляться на всех трёх уровнях принятия решения: физическом, информативном и когнитивном [26]. На *физическом* уровне необходимо наладить тесное непосредственное взаимодействие между всеми участвующими в операции подразделениями. На *информационном* уровне войска должны обладать такими возможностями доступа к информации, её распределения и защиты, которые необходимы для достижения и удержания информационного превосходства над противником. Для этого они должны пользоваться всем информационным массивом, независимо от того, кем и как была добыта информация. На *когнитивном* уровне подразделения должны максимально полно представлять себе ситуацию на театре военных действий или поле боя. В этом случае командные структуры всех уровней управления смогут не просто владеть необходимой информацией и эффективно осуществлять свои функции, но и понимать при этом намерения вышестоящего командования. А это, в свою очередь, сделает возможной самосинхронизацию сил непосредственно в ходе боевых действий.

Принцип функциональной интеграции является основополагающим как при проектировании технических систем, так и при проведении организационных преобразований в вооружённых силах. Предпосылкой для этого послужила отмеченная экспертами смена приоритетов при создании военной техники и вооружений: предпочтение стали отдавать не повышению боевых характеристик разрозненных платформ ("платформно-ориентированная" модель), а развитию средств управления, разведки и связи (так называемая

"интеллектуальная" модель) [27]. Для первой модели характерно развитие военной техники, оснащённой нестандартизованными сенсорными системами, что не позволяет свободно распределять и совместно использовать получаемую с их помощью информацию. Вторая модель тоже предполагает установку на боевых платформах собственных сенсоров, однако получаемые с их помощью данные поступают в централизованные системы хранения и обработки информации и открыты для всех пользователей. В этом случае сеть сенсоров, размещённых как на специализированных носителях, так и непосредственно на боевой технике, позволяет получить полную картину района боевых действий и на её основе принимать решения об использовании того или иного оружия.

Практическая реализация концепции сетевой войны требует комплексного внедрения в вооружённые силы информационных систем: различных средств сбора информации и сенсоров для повышения разведывательных возможностей и точности наведения оружия (а значит, для быстрого и гарантированного поражения противника); средств связи для обеспечения взаимодействия и управления войсками; систем обработки информации для эффективного командования. Исходя их этого, Дж. Гарстка определяет сетевые силы как вооружённые силы, связанные единой информационной инфраструктурой [28].

Данная инфраструктура в самом общем виде включает в себя следующие восемь элементов [29].

1. *Сбор информации.* Обеспечивается сетью сенсоров космического, воздушного, наземного и морского базирования, которые собирают на ТВД разноплановую информацию о противнике.

2. *Доступность собранной информации.* Все участвующие в боевых действиях подразделения и командиры разных уровней должны иметь доступ к получаемой информации. При этом даже на самом низком уровне управления войсками командиры имеют возможность получать ту информацию, которую считают необходимой для принятия решения (сфера их компетенции при этом расширяется), а не только ту, которую считает нужным предоставить им вышестоящее руководство.

3. *Предоставление информации пользователям.* Пользователи должны получать информацию в наиболее наглядной и удобной

форме. Например, географические координаты не только в виде цифр, но и в виде отметки на электронной карте. Это требует предварительной обработки и систематизации получаемой информации.

4. *Информационная сеть*. Доступ к информации зачастую определяется возможностями коммуникационных линий: скоростью передачи информации, устойчивостью связи и помехозащищённостью линий. Таким образом, создание и внедрение соответствующих коммуникационных средств является одной из важнейших задач построения оборонной информационной архитектуры.

5. *Распределение информации и управление информационными потоками.* Значительные объёмы информации и динамичность боевой обстановки предъявляют повышенные требования к системам оценки поступающей информации, делают необходимой постоянную фильтрацию дублирующих и устаревающих данных.

6. *Система безопасности.* В задачи системы безопасности входит проверка авторизации пользователя и его прав на доступ, редактирование и удаление той или иной информации, а также своевременное обнаружение возможных информационных атак (взлом системы, проникновение вирусов и т.п.), быстрое устранение источников угрозы и минимизация возможных негативных последствий.

7. *Совместимость элементов системы.* Совместимость элементов системы имеет два уровня: аппаратный и программный. Первый подразумевает возможность совместной работы оборудования, второй – программную совместимость и стандартизацию форматов предоставления информации.

8. *Интеграция элементов системы.* Основное отличие интеграции от совместимости в данном случае заключается в том, что совместимость предполагает главным образом разработку единых стандартов оборудования, программного обеспечения и передачи данных, а интеграция – неизбыточность и функциональную полноту системы в целом. Наиболее ярким примером могут служить разработка и внедрение на флоте и в авиации боевых информационно-управляющих систем, выполняющих функции навигационно-пилотажного комплекса и системы управления оружием. Такая интеграция позволяет оптимизировать процессы управления боевыми системами, а также избежать дублирования отдельных модулей.

Построение такой военной информационной инфраструктуры, по мнению экспертов, требует развития ряда ключевых технологий [30]:

Сетевая архитектура. Общая эффективность сетевых вооружённых сил в первую очередь зависит от полной совместимости используемого информационно-коммуникационного оборудования, поэтому внедрение единых стандартов передачи и хранения информации является приоритетной задачей, без решения которой реализация сетевых принципов становится невозможной. Учитывая современное положение дел, когда в ВС используются различные несовместимые или малосовместимые друг с другом системы передачи данных (например, оптоволоконная, космическая, радиосвязь и т.п.), решение данной задачи представляется весьма сложным делом, требующим перехода на единые цифровые стандарты хранения и передачи информации и единые протоколы передачи цифровой информации.

В настоящее время наиболее известными американскими военными протоколами передачи данных являются стандартные сетевые интернет-протоколы пакетной передачи NIPRNET (для несекретных данных) и SIPRNET (для секретных данных). Различие между ними состоит в том, что SIPRNET представляет собой изолированную от посторонних пользователей интранет-сеть, а NIPRNET использует открытые интернет-каналы. До недавнего времени многие военные использовали специальные технологии кодирования для передачи секретных данных по обычным гражданским каналам. По мнению экспертов, в дальнейшем военные пользователи полностью перейдут на изолированный SIPRNET.

Спутники. Использование спутников является жизненно необходимым условием обеспечения связи в удалённых районах, навигации, снабжения картографической и метеорологической информацией, а также раннего предупреждения системы ПРО. Орбитальная группировка США включает в себя 28 спутников навигационной системы GPS, 6 орбитальных разведывательных комплексов, 1 спутник раннего предупреждения ПРО, 2 – объектовой разведки и 3 спутника радиоперехвата. Однако, несмотря на столь значительную группировку, по данным Управления информационных систем МО (DISA), в ходе операции "Свобода Ираку" 84 % радиочастот,

использовавшихся коалиционными силами, обеспечивали коммерческие спутники.

Рабочие радиочастоты. Перевод связи на цифровые стандарты передачи данных лежит в основе практически всех программ трансформации ВС. Цифровые технологии позволяют использовать рабочий диапазон частот более эффективно, чем аналоговая связь, поскольку при этом в одном диапазоне количество каналов связи увеличивается в 6–10 раз.

Беспилотные аппараты. Беспилотные аппараты (БА), к которым относятся летательные (БЛА), наземные (БНА) и подводные аппараты (БПА), в основном используются для ведения разведки, однако в последнее время рассматривается возможность придать им ударные функции. Кроме этого, БА могут использоваться как узлы-ретрансляторы информационной сети при проведении сетевых операций. Перспективы массового использования БА являются одной из причин расширения диапазона частот связи.

Компьютерные процессоры. Ставший классическим закон удвоения производительности компьютерных процессоров каждые 1,5 года был сформулирован Г. Муром и положен в основу американской инвестиционной политики в области компьютерных технологий. Поэтому в значительной части проектов, связанных с реализацией концепции сетевых вооружённых сил, тоже учитывается постоянная эволюция компьютерных систем, и они изначально ориентируются на перспективу.

Нанотехнологии. В настоящее время МО США использует ряд материалов, созданных с помощью нанотехнологий, для изготовления лопаток корабельных турбин, а также для улучшения показателей ракетного топлива. Однако предполагается, что этими методами можно получить новые материалы, которые смогут радикально улучшить параметры многих систем. В частности, ожидается появление более лёгких материалов, обладающих повышенной твёрдостью и гибкостью, которые могут использоваться для создания средств индивидуальной защиты и в элементах силовых установок, испытывающих повышенные нагрузки. Также в перспективе могут быть разработаны миниатюрные сенсоры, которые будут способны с высокой точностью обнаруживать, идентифицировать,

сопровождать возможные цели противника и объединяться в информационные сети.

Ввиду актуальности проблемы в июне 2003 г. на базе Массачусетского технологического института был открыт Институт армейских нанотехнологий (Institute for Soldier Nanotechnologies). Решение об этом было принято в марте 2002 г., и тогда же от Сухопутных сил был получен первый грант в 50 млн дол. на разработку переносных детекторов химического и биологического оружия, а также на разработку гибкого экзоскелета со встроенными сенсорами и датчиками, который весит на 15 кг меньше, чем современная амуниция пехотинцев.

Программное обеспечение. Программное обеспечение (ПО) является одним из важнейших компонентов всех информационных систем. Главное ревизионное управление рекомендовало МО США использовать в качестве базовых компонентов специализированного ПО коммерческие разработки. В соответствии с этими рекомендациями Министерство обороны заключает субконтракты на разработку программного обеспечения с коммерческими (в ряде случаев с офшорными) фирмами. Правда, существуют опасения, что ПО, созданное ими по заказу Пентагона, может содержать в себе коды и фрагменты для несанкционированного использования информации или вывода из строя компьютерных сетей. По мнению Р. Ленца, директора Управления информационной безопасности МО США, эти опасения во многом преувеличены, поскольку у военных имеются достаточно эффективные методы повышения безопасности информационных систем. Однако эксперты относятся к этим методам довольно скептически, так как обнаружить программу-вирус до того, как она начала работать, практически невозможно [31].

Реализация рассмотренных выше принципов и создание единой информационной архитектуры на базе перспективных технологий, по мнению сторонников концепции сетевой войны, позволят повысить общую эффективность вооружённых сил, в частности:

– усилится взаимодействие сил, участвующих в комплексных воздушно-наземно-морских операциях;

– сетевые вооружённые силы будут состоять из более компактных, мобильных подразделений, что упростит их снабжение в боевых условиях и снизит стоимость содержания в целом;

– будет создана новая тактика ведения военных действий;

– упростится общая система командования и управления, в ряде случаев (например, в сложной боевой обстановке) решение можно будет принимать на более низком уровне;

– сократится время реагирования на действия противника (от момента обнаружения цели до принятия решения о её поражении).

Что касается новой тактики, то некоторые её черты уже просматриваются. Например, в ходе операции США против Ирака (2003 г.) применялась "тактика роёв", которая заключалась в том, что части быстро продвигались вперёд, не дожидаясь полного развёртывания системы тылового обеспечения [32]. Налаженная информационная сеть позволяла поддерживать тесный информационный обмен, что давало возможность быстро перемещать по территории противника компактные независимые подразделения и избегать избыточной концентрации войск. Каждое подразделение получало целостную картину поля боя: информацию о местоположении других подразделений и получаемых ими данных о противнике. В случае упорного сопротивления противника на одном из участков командир всегда имел возможность направить туда дополнительные подразделения.

Дальнейшее развитие тактики "боевых роёв", по мнению её сторонников, позволит сократить численность ВС и количество техники, а значит, снизить расходы на оборону; ограничить возможности противника противодействовать компактным дисперсным подразделениям (в частности, сделает неэффективным использование тяжёлых вооружений и ОМП); снизить вероятность поражения от "дружественного огня"; избегать боестолкновений с тяжеловооружёнными, но менее мобильными частями противника и быстро ликвидировать его командные структуры, парализуя сопротивление.

Информационные операции

Особый интерес к информационным операциям как к элементу ведения информационной войны проявляет прежде всего Министерство обороны США[1]. Этот интерес обусловлен стремлением достичь

[1] Интересно, что термин "информационные операции" постепенно заменяет термин "информационная война". Это не означает, что комплексная проблема ведения

информационного превосходства над противником путём оказания воздействия на его информационные ресурсы и системы, а также путём защиты собственной информации и информационных систем. Для этого могут использоваться любые имеющиеся в распоряжении военные и технические силы и средства при условии формального соблюдения правовых, моральных, дипломатических, политических и военных норм.

Основные принципы ведения информационной войны применительно к ВС были сформулированы в Директиве министра обороны США № TS 3600.1 "Информационная война". В ней перед объединённым штабом Комитета начальников штабов (КНШ) и штабами видов вооружённых сил ставились задачи по разработке военного аспекта новой концепции. Эта работа была завершена к концу 1993 г. и нашла своё отражение в Директиве председателя КНШ МО № 30-93. В ней достаточно аморфные исходные положения концепции информационной войны были трансформированы в концепцию "борьбы с системами управления", которая определялась как "комплексное проведение по единому замыслу и плану психологических операций и мероприятий по оперативной маскировке, радиоэлектронной борьбе и физическому уничтожению пунктов управления и систем связи противника с тем, чтобы лишить его информации, вывести из строя или уничтожить его системы управления, одновременно защитив свои от аналогичных действий" [33]. Позднее военное руководство было вынуждено существенно расширить изложенный в Директиве перечень целей проведения информационных операций.

В настоящее время под информационными операциями понимают операции, цель которых – повлиять на процесс принятия решений противником методами радиоэлектронной и психологической борьбы, нарушения работоспособности компьютерных сетей,

---

информационной войны потеряла своё значение. Скорее несколько сужается сфера действия Министерства обороны, поскольку при переводе вопроса в практическую плоскость теоретические концепции неизбежно корректируются в соответствии с целями и задачами государственных институтов, ответственных за реализацию тех или иных замыслов. В дальнейшем эта специализация ведомств будет описана более подробно. (Об отказе от термина "информационная война" в МО США см.: Information Operations // Joint Publication 3–13. – 2006. – February 13.)

дезинформации и мерами по обеспечению безопасности, а также вспомогательными и обеспечивающими действиями, нарушающими или защищающими информационные ресурсы и системы. То есть в рамках информационных операций объединяются ранее разрозненные виды боевых и обеспечивающих действий.

Судя по этому определению, весь спектр информационных операций разрабатывался с учётом практически всех основных теоретических направлений 90-х гг. в области информационной войны.

Информационные операции являются одним из элементов государственной мощи (наряду с дипломатическими, военными и экономическими), использование которых для обеспечения стабильного развития государства определяется Стратегией национальной безопасности и военной стратегией США. Учитывая, что информационные операции в силу их специфики могут осуществляться на любом этапе конфликта, в том числе и в мирное время, то вооружённые силы проводят их в тесном взаимодействии с другими государственными институтами.

В мирное время целями ИО являются формирование безопасного стратегического окружения, подготовка к кризисному периоду или войне. Важным элементом такой подготовки в мирное время являются сбор и анализ информации о потенциальных противниках и главных международных игроках. При этом основное внимание должно уделяться сбору сведений о:

– политическом руководстве той или иной страны;

– возможностях и уязвимых точках её информационной сферы, включая военные и гражданские информационные и коммуникационные сети и СМИ;

– военном руководстве, системе военного планирования, инфраструктуре и уязвимых точках на стратегическом, оперативном и тактическом уровнях;

– экономических факторах, определяющих потенциальные возможности подготовки и ведения войны, влияющих на моральное состояние населения и руководства страны (в том числе и данные об инфраструктуре, необходимой для поддержания экономической активности);

– этнических, расовых и исторических предпочтениях и фобиях, которые проявляются на социальном уровне.

Первые четыре фактора (политический, информационный, военный и экономический) являются категориями государственной мощи и относительно легко формализуются. Последний, социальный, более неопределённый, но для успешного осуществления информационных операций может иметь важное значение.

Наибольший интерес представляет целевая информация о:

– наиболее влиятельных государственных и негосударственных деятелях и движениях;

– государственных и негосударственных деятелях, принимающих решения (руководителях);

– лицах и группах, симпатизирующих США или подверженных американскому влиянию, а также враждебно настроенных по отношению к ним;

– темах, которые можно свободно обсуждать в различных целевых аудиториях;

– государственных учреждениях, поддерживающих те или иные целевые группы или противодействующих им;

– государственных и негосударственных игроках, принимающих или отвергающих экономическую или военную поддержку США;

– религиозных, этнических и культурных ценностях, обычаях и нормах;

– коммуникационной инфраструктуре;

– военной системе связи и управления;

– уровне военного профессионализма и системе подготовки кадров, военно-гражданских отношениях;

– системе образования;

– об отношениях между этническими и языковыми группами.

Осуществление информационных операций в мирное время зачастую требует принятия решения на высшем стратегическом уровне, но при этом оценка окружения, планирование, подготовка и тренировки являются постоянным процессом, необходимым для поддержания боеготовности. К этой деятельности привлекаются военные, правительственные и ряд неправительственных учреждений и институтов. Такой подход позволяет координировать межведомственную активность и планирование в этой сфере.

В кризисный период информационные операции проводятся в соответствии с разработанными планами действий. Однако непредвиденные ситуации или сама возможность их возникновения могут потребовать дополнительной информации для уточнения этих планов. Вообще кризисный период является наиболее сложным и динамичным этапом конфликта, когда командирам приходится проявлять б**о**льшую инициативу и принимать самостоятельные решения. Особенно это касается региональных командований, которые на этом этапе пользуются расширенными полномочиями. В связи с тем, что в кризисный период ситуация может развиваться как в направлении мира, так и в направлении войны, наиболее эффективным видом информационных операций считается воздействие на целевые группы политической, экономической, военной и общественной систем управления противника.

Другими важными направлениями в кризисный период являются контрразведывательные и контрпропагандистские мероприятия, а также выявление реальных планов противника.

В ходе *войны* информационные операции являются неотъемлемым элементом боевых действий. При этом используется весь спектр наступательных и оборонительных ИО. Боевое планирование и проведение таких операций осуществляются в соответствии с планами, доктринами и схемами взаимодействия, разработанными в мирное время. Считается, что хорошо скоординированные и синхронизированные наступательные информационные операции способны не только нейтрализовать военную силу противника, но и лишить его возможности осуществлять общее политическое руководство.

В настоящее время в США основными методами ведения информационных операций считаются психологические операции, активные мероприятия или дезинформация (MILDEC, Military Deception), контрразведка или операции по обеспечению безопасности (OPSEC, Operations Security), электронная борьба и операции в компьютерных сетях (CNO, Computer Network Operations) [34]. В той или иной степени эти методы были предметом теоретических дискуссий в американском экспертном сообществе на протяжении 90-х гг. прошлого века и подробно рассматривались выше. Здесь же представляется необходимым вкратце описать современную

понятийную базу и классификацию основных методов информационных операций.

1. *Психологические операции* – спланированное информационно-психологическое воздействие на зарубежную аудиторию с целью вызвать у неё желаемую эмоциональную реакцию, изменить мотивацию и целевые установки, скорректировать в нужном направлении поведение правительств, организаций, групп и индивидуумов. Конечной целью психологических операций является формирование общественного мнения и поведения в соответствии с задачами организаторов психологических операций.

2. *Дезинформация* – преднамеренные действия, вводящие в заблуждение (прежде всего лиц, ответственных за принятие решения), тем самым побуждая противника предпринимать шаги, которые соответствуют целям США или дружественной им страны.

3. *Контрразведка или операции по обеспечению безопасности* – выявление информации, критически важной для осуществления военных операций (или других действий, включая политическую и экономическую сферы), прежде всего:

– участков, уязвимых для разведывательных систем и действий противника;

– факторов, способствующих успешному ведению разведывательной деятельности противником.

На основе полученных данных выбираются и применяются конкретные меры, направленные на срыв разведывательной активности противника или снижение её до приемлемого уровня.

4. *Электронная борьба* – военные действия с использованием электромагнитного излучения или направленной энергии для установления контроля над электромагнитным диапазоном или поражения противника. Американские эксперты выделяют три основных направления электронной борьбы:

– электронные атаки – использование электромагнитной и направленной энергии и подавление источников излучения[1] для нанесения ущерба личному составу, оборудованию и оснащению

[1] Электронные атаки включают в себя радиоэлектронное подавление систем противника и применение оружия прямого действия (лазеров, радиочастотного и пучкового оружия).

противника для снижения, нейтрализации или полной ликвидации его боевых возможностей;

– электронная защита – использование пассивных и активных мер, направленных на защиту собственных войск, оборудования и оснащения от средств ведения электронной борьбы;

– обеспечивающие действия – перехват, идентификация и определение координат источников преднамеренного или непреднамеренного излучения электромагнитной энергии с целью определения степени угрозы, целеуказания, планирования и осуществления боевых операций.

5. *Операции в компьютерных сетях* включают в себя сетевые атаки, защиту компьютерных сетей и мероприятия содействия.

Сетевые атаки предпринимаются через компьютерные сети для перехвата, искажения или уничтожения информационных ресурсов противника, выведение из строя его компьютерных систем и сетей.

Защита собственных компьютерных сетей должна эффективно противостоять сетевым атакам противника, для чего необходимо создать систему защиты от несанкционированного проникновения и обеспечить постоянный мониторинг, анализ и обнаружение угроз, а также реагировать на них.

Мероприятия содействия направлены на сбор и анализ разведывательной информации о компьютерных системах противника, его планах и возможностях проведения сетевых атак.

Пять перечисленных методов ведения информационных операций дополняются восемью сопутствующими, пять из которых (информационная и физическая безопасность, физические атаки, контрразведка и боевая визуализация) носят скорее технический характер, а три остальных (организация связей с общественностью, налаживание военно-гражданских и военно-дипломатических отношений) призваны влиять на сознание и формировать восприятие человека.

1. *Информационная безопасность* – меры по защите информации и информационных систем путём обеспечения их целостности, идентификации пользователей, конфиденциальности и безотказности.

2. *Физическая безопасность* обеспечивает физическую защиту персонала, направлена на предотвращение несанкционированного

доступа к оборудованию, материалам и документам, включая такие действия, как шпионаж, саботаж, похищение и уничтожение.

3. *Физические атаки* – нарушение работоспособности, повреждение или уничтожение информационных систем противника методами физического воздействия.

4. *Контрразведка* – сбор информации о возможных противниках (государствах, организациях, зарубежных гражданах, террористах) и срыв их разведывательной и диверсионной деятельности.

5. *Боевая визуализация* – применение методов компьютерной визуализации для более лёгкой, полной и быстрой передачи необходимой информации персоналу.

6. *Связь с общественностью* – предоставление информации внутренним и зарубежным СМИ, общественным организациям, учреждениям и частным лицам в интересах Министерства обороны.

7. *Военно-гражданские отношения* – действия по установлению, поддержанию, формированию и использованию отношений между военным ведомством и государственными и негосударственными организациями, влиятельными лицами и гражданским населением на дружественной или нейтральной территории, а также в районах боевых действий для облегчения ведения войны и достижения её политических целей.

8. *Военно-дипломатические отношения* – действия Министерства обороны, поддерживающие общеполитические усилия руководства США.

В обобщённом виде основные и обеспечивающие мероприятия, используемые при проведении информационных операций, представлены в таблице.

Такое деление даёт основания представить информационные операции также в виде двух больших классов: один охватывает преимущественно действия технического характера в сфере информации и информационных систем, а второй касается воздействия непосредственно на общественное сознание и социально-политические институты. Естественно, что рассматривать эти классы операций следует несколько шире, не ограничиваясь исключительно анализом концептуальных построений и доктрин Министерства обороны США.

Таблица

Классификация методов информационных операций, принятая МО США

	Методы информационных операций	
	Основные	*Обеспечивающие*
Технические	Операции по обеспечению безопасности Электронная борьба Операции в компьютерных сетях	Информационная безопасность Физическая безопасность Контрразведка Боевая визуализация Физические атаки
Воздействие на сознание	Психологическая борьба Активные мероприятия или дезинформации	Связи с общественностью Военно-гражданские отношения Военно-дипломатические отношения

Защита информационных инфраструктур

Обеспечение безопасности собственных информационных инфраструктур, на первый взгляд, кажется отдельной темой. Отчасти это обусловлено тем, что она слабо соотносится с сугубо военными вопросами. Однако, учитывая проблему безопасности всех государственных и общественных институтов, её, безусловно, необходимо рассматривать в общем контексте современных концепций информационной войны.

Развитие информационных технологий приводит к быстрому и подчас трудно прогнозируемому изменению информационных инфраструктур. Это обстоятельство вносит элемент неопределённости в любую сферу деятельности, где они используются. Поэтому помимо чисто технической задачи обновления парка оборудования часто возникает необходимость пересмотреть основные концептуальные и организационные вопросы, связанные с использованием нововведений. Поскольку обновление информационных систем, как правило, приносит значительную выгоду всем звеньям

организационной структуры в целом (например, и банковско-финансовой, и оборонной сферам), время и ресурсы, которые будут расходоваться на внедрение новшеств и обучение персонала для работы с ними, будут постоянно возрастать.

Особую остроту вопрос о защите информационных инфраструктур приобретает из-за относительной новизны проблемы. Бурное развитие информационных сетей во второй половине XX в. в короткие сроки привело к появлению новой инфраструктуры, которая наряду с традиционными стала играть важную роль в государственном и экономическом управлении. Это потребовало пересмотра некоторых базовых принципов построения организационных структур. В связи с этим возникает потребность согласовать основные связанные с этой сферой понятия, найти единую трактовку их содержательной стороны и функциональной нагрузки. Основные определения в рассматриваемой области, представленные ниже, были даны в опубликованном в октябре 1997 г. докладе президентской комиссии "Критические основы. Защита американских инфраструктур" [35].

Критические инфраструктуры – жизненно важные инфраструктуры, вывод которых из строя или разрушение наносит ущерб обороноспособности или экономической безопасности страны.

Уязвимость – характеристика принципа построения, реализации и функционирования критической инфраструктуры, которая описывает степень её восприимчивости к разрушающим воздействиям, способность или неспособность противостоять угрозам.

Угроза – воздействие внутреннего или внешнего характера, которое либо возникает из-за уязвимости критической инфраструктуры, либо является злонамеренным актом, представляющим опасность для обороноспособности или экономической безопасности страны (такой угрозой могут быть действия отдельной личности, организации или нации).

Оценка уязвимости – регулярная проверка критической инфраструктуры и связанных с ней систем, от которых зависит работоспособность инфраструктуры, сохранность информации или продукции. В ходе оценки выявляются слабые звенья в системе безопасности, ведётся поиск альтернативных вариантов защиты и проверяется адекватность предпринимаемых мер.

Информационная или "кибернетическая" безопасность – действия, направленные на снижение системного риска, особенно возможностей возникновения угрозы для критической инфраструктуры из-за уязвимости электронных, высокочастотных или компьютерных систем.

Защита инфраструктуры – действия по предотвращению угроз уничтожения или выведения из строя критических инфраструктур (например, сдерживание угрозы и защита уязвимых звеньев).

Устойчивость инфраструктуры – превентивные и реактивные действия, которые позволяют сохранить работоспособность критической инфраструктуры в случае, если ей нанесены повреждения и ущерб (например, периодическое архивирование, случайные выборки).

Информация и телекоммуникации – критическая инфраструктура, целиком зависящая от компьютерного и телекоммуникационного оборудования, программного обеспечения, процессов и людей, которые обеспечивают:

– производство, хранение и передачу данных и информации;

– преобразование данных в информацию, а информации – в знания;

– данные и информацию в целом.

К концу 90-х гг. прошлого века в США была разработана следующая классификация угроз критическим инфраструктурам по степени воздействия и интенсивности [36].

"Инфраструктурный шум". Термины "шум" или "помехи", принятые в физике, оказались очень удобными для описания побочных эффектов, возникающих при функционировании самих инфраструктур. К ним можно отнести:

– различные сбои программного обеспечения, текущие поломки оборудования, нарушение электропитания, перебои в сети и т.п.;

– периодические ошибки в сетевой адресации, переполнение сетевого трафика и т.п;

– ошибки в работе обслуживающего персонала;

– периодические правонарушения.

Основным показателем, по которому оценивается эффективность инфраструктуры, является отношение уровня её нормальной работы к частоте возникновения побочных эффектов (данная

характеристика носит, естественно, только оценочный, качественный характер).

Задачей защиты от "информационного шума" является снижение его уровня за счёт оптимизации организационной структуры. Сам по себе "шум" может и не представлять опасности, но его появление нередко сигнализирует об атаке на информационные инфраструктуры или служит маскирующим фоном для неё. Это, например, происходит при применении "логических бомб", при шифровании путём преднамеренного создания "ошибочных данных" или проведении замаскированных хакерских атак.

Следовательно, при такой угрозе важно установить, является ли "шум" реальной угрозой или умышленной атакой, возникающей на "шумовом фоне", и соответствующим образом отреагировать на них. С другой стороны, "инфраструктурный шум" можно использовать в качестве маскировки для собственных мероприятий по обеспечению безопасности.

Низкоуровневые и умеренные атаки и проникновения. Низкоуровневые атаки по своему влиянию на работоспособность инфраструктуры сопоставимы с нормальными возмущениями и вызываются, как правило, фоновыми событиями (например, периодическими ошибками эксплуатации или случайными проникновениями). Их полное устранение невозможно, и роль защиты в данном случае сводится к минимизации последствий: к выявлению источников такого рода угроз, созданию условий, при которых проведение низкоуровневых атак становится невозможным, и к устранению их возможных последствий.

При повышении уровня атак до умеренного используется специально созданный для таких случаев ответный механизм. Однако при этом чрезвычайные меры не должны носить тотального характера. На большей части территории страны функционирование коммуникаций и инфраструктур будет продолжаться в нормальном режиме. Даже при поражении отдельных функциональных звеньев остальные должны сохранять работоспособность, в противном случае нельзя будет оперативно локализовать зоны, подвергшиеся нападению, и устранить его последствия. То есть сохранение нормальной жизнедеятельности государственных учреждений и всех

сфер бизнеса в таких условиях само по себе уже является механизмом предотвращения умеренных атак.

Атаки и вторжения чрезвычайно высокого уровня. К ним относятся атаки и вторжения, интенсивность которых может нарушить функционирование, разрушить или даже парализовать целые сферы государственной или экономической жизнедеятельности, например основные производства или банковскую систему. Такие атаки требуют немедленной реакции со стороны государственных структур вплоть до введения чрезвычайного положения на территории страны. При этом будет приостановлена работа ряда служб и ограничены некоторые свободы. Например, будут запрещены частные полёты, ограничен доступ в информационные сети. В условиях чрезвычайной ситуации могут быть резко ограничены потребление некоторых национальных ресурсов частными лицами (в том числе электроэнергии и информации), свобода СМИ, прежде всего телевидения и радиовещания (вплоть до введения элементов цензуры).

Однако, по мнению американских экспертов, при решении задач защиты информационных инфраструктур такие экстраординарные вызовы не следует рассматривать как приоритетные, поскольку они мало вероятны. Необходимо сосредоточить внимание на мероприятиях, которые предпринимаются для снижения риска умеренных атак и ликвидации их последствий, и именно эти мероприятия должны служить базой для разработки адекватных мер ответа на более масштабные угрозы.

Следует оговориться, что теракты 11 сентября 2001 г. внесли определённые коррективы в такие оценки.

Интересно также отметить, что в процессе обсуждения проблем защиты информационных инфраструктур акценты с технических вопросов постепенно смещались в сторону организационных. Таких взглядов придерживались, например, эксперты РЭНД Ф. Фукуяма и А. Шульски [37]. По их мнению, для основных инфраструктур критически важной темой являются именно организационные вопросы, поскольку от технических инноваций эти инфраструктуры зависят в меньшей степени. (Однако, с нашей точки зрения, не следует забывать, что технические инновации могут служить толчком к более быстрым и радикальным организационным изменениям не только

самой инфраструктуры, но и тех областей, которые она обслуживает.)

Таким образом, были выработаны три основные стратегии обеспечения безопасности информационных инфраструктур: защита, сдерживание и предупреждение атак.

Защита – это комплекс мероприятий, направленных на уменьшение уязвимости за счёт снижения эффективности атак и минимизации наносимого ими ущерба, а также совершенствование методов быстрого восстановления атакованных систем.

Сдерживание подразумевает ограничение способности вероятного противника осуществлять информационное воздействие путём демонстрации собственных возможностей адекватно отвечать на него.

Предупреждение атак – меры, ограничивающие возможности противника создавать, разворачивать или успешно использовать информационное оружие и технику против национальных инфраструктур.

Все эти стратегии тесно взаимосвязаны, и их применение обусловлено степенью и характером возникающей угрозы.

Операции влияния

Действия, направленные на формирование общественного мнения и изменение системы восприятия противника, которые в итоге заставляют его действовать в выгодных для США направлениях, называются операциями влияния. Это операции стратегического уровня, поскольку предпринимаются с целью изменения общественного мнения и политики другого государства, организаций и социальных групп.

Некоторые исследователи даже выделяют операции влияния (или управление восприятием) в отдельный вид действий вне рамок информационной войны [38]. Очевидно, что проведение операций влияния в наименьшей степени зависит от технических инноваций. Они базируются главным образом на достижениях в области социальной психологии, поэтому рассмотренные выше принципы психологической борьбы в целом сохраняют свою актуальность. Хотя на протяжении 90-х гг. концепция операций влияния и не претерпела существенных изменений, но зато она обрела новое

звучание в связи с появлением компьютерных сетей, Интернета и повышением оперативности традиционных каналов СМИ (телевидение, радио), которые стали возможны с внедрением систем спутниковой и сотовой связи.

Оперативная связь вкупе с новыми цифровыми возможностями обработки звука, изображения и их последующего монтажа позволяет создавать практически любой желаемый образ событий, отличить который от реального можно только после тщательной экспертизы. Такое манипулирование сознанием активно использовалось в качестве инструмента информационно-пропагандистского обеспечения в ходе всех военных конфликтов с участием США, начиная с первой войны в Заливе. Тогда из коалиционного пресс-центра поступали видеоизображения, снятые с головок самонаведения ракет или бортовых систем теленаведения самолётов. Даже эксперты не были до конца уверены в том, какие конкретно объекты поражались и насколько реальной (или смонтированной) была "картинка". Между тем передача таких изображений помогла решить целый комплекс задач психологической обработки общественного мнения.

Прежде всего, передаваемые "реальные" кадры поражения иракских объектов удовлетворили существовавший информационный голод и позволили "переиграть" альтернативные каналы массового вещания, которые не обладали аналогичными возможностями для создания подобных "доказательств".

Кроме того, американским военным удалось убедить общественность в своём "всеведении" и неограниченных возможностях получения информации, что должно было послужить актом устрашения для потенциальных противников.

И, наконец, американская пропаганда сформировала виртуальный образ некоего "супероружия", которым якобы обладают США и которое способно поражать любые объекты противника с первого раза и со стопроцентной гарантией. Во многом именно передача таких кадров помогла создать миф о том, что высокоточное оружие – это своего рода абсолютное оружие, хотя тогда, в 1991 г., лишь 10 % общего количества применённых боеприпасов относились к высокоточным, а многие комплексы, включая широко разрекламированный "Пэтриот", продемонстрировали недостаточную боевую эффективность.

Безусловно, каждое внешнеполитическое решение, принятое в США на государственном уровне, так или иначе оказывает определённое психологическое воздействие на заинтересованные стороны. Например, выдвижение ударной авианосной группировки в кризисный регион вызывает прямой психологический эффект в странах, непосредственно прилегающих к нему. Однако воздействие становится глобальным только тогда, когда СМИ имеют возможность транслировать информацию в реальном масштабе времени на весь мир. Не случайно бывший председатель КНШ Дж. Шаликашвили как-то заметил: "Мы не побеждаем до тех пор, пока CNN не говорит, что мы побеждаем". То есть подобная пропагандистская операция становится частью стратегической кампании по оказанию влияния, в которой используются самые разные средства, и отдать приоритет какому-либо из них очень сложно. Однако принципы межведомственного взаимодействия при этом прослеживаются достаточно чётко: решение принимается высшим политическим руководством США, исполняется Министерством обороны, обеспечивается дипломатической поддержкой со стороны Государственного департамента и освещается СМИ.

Сегодня ключевыми компонентами стратегических операций влияния являются общественно-политические отношения, политическая борьба, политическая пропаганда, государственная дипломатия и психологические операции. Следует особо отметить, что стратегические операции влияния нельзя сводить к какому-то одному методу. Они включают в себя полный набор средств информационно-психологического воздействия, согласованно применяемых различными ведомствами.

Некоторые эксперты подчёркивают, что эффективность целого ряда стратегий, взятых на вооружение Соединёнными Штатами (сдерживание, проецирование силы и др.), во многом зависит от их способности влиять на восприятие и решения правительств других стран [39]. Таким образом, операции влияния должны рассматриваться как один из основных инструментов формирования благоприятной для США внешнеполитической среды в мирное время и эффективное средство предотвращения акций, которые могут принести ущерб США и их союзникам в периоды кризисов.

Обычно принято считать, что операции влияния носят деструктивный характер (впрочем, как и любые другие боевые действия). Это следует из традиционного определения информационной войны как воздействия на информационные системы противника и информацию, что само по себе подразумевает её объективность. Однако при планировании операций по управлению восприятием этот тезис не имеет решающего значения, поскольку в данном случае собственно информация служит только инструментом для формирования у противника "правильного" восприятия ситуации и для влияния на выработку им "правильных" решений. То есть гораздо важнее знать, *как противоположная сторона воспринимает наши действия, поскольку именно это даёт нам возможность контролировать её реакцию.* Различия в восприятии сторон не делают позицию одной из них правильной, а другой – ошибочной, но формируют у обеих разные поведенческие стереотипы [40]. Задачей управления восприятием, таким образом, становится не разрушение психологии или моральных устоев противника, не искажение информации и не выведение из строя его информационных систем, а формирование такого восприятия, которое позволило бы направлять его действия в русло интересов стороны, проводящей операцию влияния. (В этом ключе можно рассматривать и череду "цветных революций" в республиках СНГ.) Естественно, что с этой точки зрения управление восприятием является совершенно самостоятельной областью информационного противоборства.

Библиографические ссылки

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

2. Ibid. – P. 275.

3. *Stein G. J.* Information Attack: Information Warfare In 2025 / Research paper presented to 'Air Force 2025'. – 1996. – August.

4. *Szafranski R*. Harnessing Battlefield Technology: Neocortical Warfare // The Acme of Skill, Military Review. – 1994. – November; *Szafranski R.* Parallel