“Сетевая война” – новый вид противоборства

Александр Деньщиков,
помощник Министра иностранных дел

Концепция “сетевой борьбы”, несмотря на вполне “техническое” русское звучание, в наименьшей степени связана с собственно информационными технологиями, а охватывает полный комплекс проблем и аспектов информационного противоборства (организационные, доктринальные, стратегические, тактические и технические стороны ведения наступательных и оборонительных информационных операций).

Роль сетевой борьбы возрастает в конфликтах низкой интенсивности и при проведении так называемых “операций, отличных от войны”, а также в конфликтах, террористических и иных действиях, носящих невоенный характер. При этом понятие сетевой борьбы относится скорее к организационной форме противоборства, использующей информационные возможности, чем собственно к борьбе с информационными инфраструктурами про- тивника. Более того, концепция сетевой борьбы подразумевает использование информационных инфраструктур противника в своих целях. В этом отношении данный вид информационного противоборства (ИП) имеет много общего с ведением террористической борьбы, в которой главными действующими лицами выступают небольшие взаимосвязанные и координирующие свои действия группы, не имеющие единого командования. В таком случае можно говорить, что их структура строится не на иерархическом, а на сетевом принципе, и именно в этом заключается главное отличие информационно-ориентированной сетевой борь- бы от социальных конфликтов, в которых в качестве действующих лиц выступают разрозненные иерархические организации, имеющие жесткие и изолированные идеологии, доктрины и стратегии борьбы.

В качестве примеров, иллюстрирующих отмеченные различия иерархических и сетевых структур, можно привести особенности стратегий ряда экстремистских и террористических организаций.

Так, “Хамас”, по утверждению израильских источников, в значительно большей степени использует возможности сетевой борьбы, чем Организация освобождения Палестины.

То же самое можно сказать в отношении Американских христианских патриотов

и Ку-Клукс-Клана. А что касается мексиканского движения Запатисты, то оно полностью строится на сетевых принципах организации.

Список таких сравнений может быть продолжен, хотя следует подчеркнуть, что цели, преследуемые сравниваемыми организациями, лежат в целом в одной плоскости.

Характерная особенность сетевой борьбы состоит в том, что подавляющее большинство, если не все действующие лица, использующие методы такой борьбы, являются негосударственными организациями. Среди них могут быть: транснациональные террористические группы, нелегальные торговцы оружием, транснациональные преступные синдикаты, наркомафия, фундаменталисты, этнонационалистические движения, информационные пираты, контрабандисты и т.п.

Таким образом, на государственном уровне сетевая борьба сводится, прежде всего, к противодействию такого рода организациям, использующим сетевые организационные методы, то есть к антитеррористической борьбе.

Можно выделить две основные проблемы, возникающие при ведении государственной контрсетевой борьбы:

1. Иерархические государственные системы, как правило, оказываются малоэффективными при борьбе с сетевыми структурами. Это связано, прежде всего, с тем, что время, необходимое для принятия решений и адекватного реагирования на происходящие изменения обстановки, в иерархических системах значительно превышает аналогичные показатели сетевых структур.

2. Эффективная антитеррористическая борьба требует формирования антитеррористических подразделений, строящихся на сетевой основе и, следовательно, наделенных расширенными полномочиями в вопросах принятия решений.

Данное требование не подразумевает зеркального копирования структуры и методов террористических организаций, с которыми ведется борьба. Значительную роль в решении этой проблемы могут играть технические нововведения, выработка новых механизмов межведомственного координирования, а также развитие межгосударственной кооперации, включая, в том числе унификацию национальных законодательных систем.

После терактов в США 11 сентября 2001 г. появилось большое количество материалов об оценке ситуации в мире.

Рассмотрим один из опубликованных материалов в информационном бюллетене корпорации РЭНД – статью сотрудников этой организации Джона Арквилла и Дэвида Ронфельдта “Битва сетей”[1].

Работа основана на предположении, что если сеть “Аль-Каиды” Усамы бен Ладена является главным противником США на текущий момент, то Америка должна превзойти ее на всех 5 уровнях: структурном, мировоззренческом, доктринальном, технологическом и социальном.

Авторы считают, что на структурном уровне глобальная конфронтация сегодня бушует между иерархическими (государственные игроки) и сетевыми структурами (негосударственные игроки). Еще не ясно, имеет ли сеть “Аль-Каиды” единственный узел коммуникаций и управления, центром которого является бен Ладен, или же у нее множество таких узлов.

Первый вариант наиболее прост. Если она имеет единственный узел, то смерть бен Ладена или его захват американскими войсками указал бы на поражение его сети.

Однако большинство сетей имеет архитектуру типа “*сети паука*”. Это может быть и в случае с “Аль-Каидой”.

Будучи гораздо более избыточной и гибкой, такая структура обладает большей устойчивостью, что затруднит ее окончательное уничтожение. В этой ситуации, считают авторы статьи, Соединенные Штаты и их союзники должны совместно изучать особенности сетевых архитектур. Частично такой подход уже работает на примере взаимного обмена разведданными.

Подобные изменения являются большой и сложной работой для громоздкой американской бюрократии, которой необходимо развернуть широкие, хорошо организованные сети военных и юридических структур, элементов разведки. Следует отметить, что американские антитеррористические агентства развивались в этом направлении уже в течение ряда лет, но взаимная конкуренция и недоверие часто замедляли продвижение к намеченной цели.

Второй аспект противоборства касается мировоззренческого уровня.

Западные идеи распространения свободных рынков, свободных народов и открытых обществ сталкиваются с мусульманским убеждением относительно эксплуатационной, агрессивной и высокомерной природы западного присутствия в исламском мире. США еще больше ужесточили свою позицию, считая террористические атаки "действиями войны" против "цивилизованного мира", а американское общественное мнение гальванизировалось возрождением метафоры Перл Харбора.

Сегодня больше чем когда-либо важно овладеть искусством "информационной стратегии", реализуемой бригадами "специальных информационных сил", которые могли бы обобщать и распространять необходимую информацию. И везде, где США используют группы войск, нужно остерегаться порождения неприятия этого присутствия со стороны мирного населения, которое чревато невоенным поражением. Все это необходимо, чтобы быть неуязвимыми к встречному обвинению в создании "государственного террора".

Третий аспект заключается в доктрине.

Сеть "Аль-Каиды", очевидно, организует атаки по множеству направлений рассеянными подразделениями. Бен Ладен и его когорты, похоже, следуют доктрине "пчелиного роя". При этом различными узлами сети инициируется ряд эпизодических пульсирующих атак в ряде мест, распределенных в глобальном пространстве и времени.

Против этой доктрины США пока еще немногое могут противопоставить. Наступательная часть американской военной доктрины все еще основана на стареющих понятиях стратегической бомбардировки, которая вряд ли будет правильным подходом в борьбе с терроризмом.

В этих условиях должна быть развита новая доктрина, основанная *на принципе "роения" малых мобильных и хорошо вооруженных подразделений*, которая бы подчеркивала особую роль специальных сил и ограниченного применения авиации. ВВС использовались бы главным образом для огневого обеспечения подразделений на земле.

В-четвертых, на технологическом уровне Соединенные Штаты обладают массой очень передовых систем, в то время как "Аль-Каида" таковых не имеет или имеет очень немного.

Однако только малая часть таких высокотехнологических систем может быть полезна против рассеянных сетевых структур террористов.

В-пятых, на социальном уровне сеть "Аль-Каиды" демонстрирует тесные религиозные и родственные связи среди людей, которые разделяют племенное, родовое представление "мы" против "них".

В этом отношении США стоят перед сложной дилеммой. Если метафора Перл Харбора поддерживается, и если американские действия приводят к успешным ранним контрударам, то может иметься необычная общественная сплоченность, чтобы поддерживать войну против терроризма. В случае, когда встает вопрос: должны ли контрудары следовать как элемент "войны" или "исполнения закона", возможно появление различных социальных реакций в США и Европе.

"Аль-Каида" на сегодняшний день, отмечают авторы, обладает преимуществами на структурном, доктринальном и социальном уровнях, что серьезно осложняет борьбу с ней. Соединенные Штаты и их союзники, возможно, имеют преимущества только на мировоззренческом и технологическом уровнях. Поставленный в сложную ситуацию Запад сегодня должен строить собственные сети и изучать роящиеся вражеские. Ключом к разрешению противоречия является понимание того, что в современном сетевом или информационно-ориентированном конфликте между сетями информационной эпохи гораздо большее значение имеет структурное и доктринально превосходство, чем технологическое.

Вице-президент по внешним связям РЭНД, директор Вашингтонского офиса корпорации Брюс Хоффман в одном из своих выступлений перед конгрессом США очертил круг задач, которые предстоит решить американской администрации в ходе борьбы с терроризмом.

Прежде всего, он отметил, что США нуждаются в объединенном федеральном усилии, повседневных оценках угрозы и трансформации всей структуры национальной безопасности.

Множество федеральных агентств и программ, занимающихся антитеррористической деятельностью, остаются сильно фрагментированными и нескоординированными, с взаимно пересекающимися обязанностями, но без ясной цели. Сейчас, по его мнению, необходимо, всесторонне усилие, чтобы связать воедино под более чутким руководством то огромное число возможностей и средств, которые Соединенные Штаты могут использовать в борьбе против терроризма.

Предварительными условиями для формирования национальной стратегии, отмечает Хоффман, являются регулярные оценки террористической угрозы как внешней, так и внутренней.

Последняя всесторонняя оценка внешней террористической угрозы в США была предпринята во время войны в Персидском заливе в 1990–1991 гг. Хотя после этого и разрабатывался ряд оценок, но они не учитывали те глубокие изменения в природе, действиях и мышлении террористов, которые стали очевидны в последние годы. Как только будет установлено ясное понимание термина "*новый терроризм*", его мотивы, намерения и имеющиеся возможности определить способ, позволяющий, прогнозировать, предотвращать и сдержать террористические атаки.

Хоффман особо отмечает, что необходимо трансформировать все американское разведсообщество, чтобы иметь возможность противостоять террористическим угрозам не только сегодня, но и завтра. Он считает, что архитектура национальной безопасности США – реликт, символ "холодной" войны. Она создавалась более 50 лет назад, чтобы противостоять специфичным угрозам от отдельных стран с иной идеологией.

Архаичность этой архитектуры, ориентированной в основном на военные угрозы и, следовательно, на военную разведку, была доказана разрушительными атаками

11 сентября негосударственными, невоенными противниками.

Основа американской архитектуры национальной безопасности существенно не изменялась, начиная со времени Второй мировой войны.

Так, около 60% усилий разведсообщества сосредотачивается на военной разведке, имеющей отношение к регулярным вооруженным силам конкретных суверенных государств.

8 из 13 американских агентств, отвечающих за сбор развединформации, докладывают ее непосредственно министру обороны, а не руководству ЦРУ. Это неудивительно, ведь, по мнению Хоффмана, американская *HUMINT* (агентурная разведка) сегодня практически не дееспособна из-за того, что военная ориентация разведсообщества США основывается на технологической разведке типа *ELINT* (электронная разведка) и *SIGINT* (разведка средствами связи), осуществляемой, как правило, с использованием спутников на околоземной орбите.

Увеличивающееся поражающее действие межнациональных, негосударственных и невоенных противников, объединенных в открытые сети, а не в жесткие иерархии "командования и управления", требует перераспределения сбора разведывательных сведений от традиционных военных противников на спектр противников скрытых, которые теперь представляют угрозу национальной безопасности США.

Бюджет американского разведсообщества оценивается примерно в 30 млрд. долл., что уже больше, чем бюджеты национальной обороны многих стран мира (за исключением 6 высокоразвитых государств Запада).

Хоффман считает, что необходимо перераспределить персонал и ресурсы так, чтобы США могли адекватно реагировать на текущие и, возможно, будущие террористические угрозы. Анахроничная архитектура разведки создала опасный разрыв в обороноспособности страны.

ЦРУ ответственно за внешнюю разведку и прогноз развития внешнеполитической обстановки. В соответствии с законом, ЦРУ не может работать в пределах Соединенных Штатов.

Антитеррористические действия внутри страны падают на Федеральное бюро расследований. Однако ФБР – это, прежде всего, агентство, занимающееся расследованием уголовных преступлений, а не спецслужба. Его зона интересов перекрывает очень широкий спектр, который включает похищения, грабежи банков, контрразведку, серийные убийства и другие, более прозаические, преступления в дополнение к терроризму.

Новое Управление внутренней безопасности потенциально дает идеальный шанс устранить этот промежуток между ЦРУ и ФБР, создавая новую аналитическую возможность раскрытия внутренних террористических угроз. Однако, по мнению Хоффмана, такую аналитическую возможность нужно укрепить новой организационной структурой, в которой должны быть скоординированы антитеррористические усилия всех агентств. Пока еще нет полной ясности в том, будет ли предоставлено достаточно полномочий и ресурсов Управлению внутренней безопасности для выполнения этой задачи.

По мнению Хоффмана, подобно тому, как задача борьбы с наркоторговлей в свое время расценивалась как серьезная задача в обеспечении национальной безопасности США и были созданы специализированные агентства по борьбе с наркотиками, необходимо создание подобных агентств, занимающихся исключительно борьбой с терроризмом.

Получение преимущества в сетевой борьбе в значительной степени определяется тем, насколько эффектив-

но используются возможности, предоставляемые сетевой организацией и информационными сетями (Интернет).

В частности, с решением всех этих проблем пришлось столкнуться американским специалистам при создании специального контртеррористического Центра, функционирующего при ЦРУ.

С одной стороны, в работе этого Центра используются функциональные принципы сетевой организации, а *с другой* – осуществляется активное взаимодействие с традиционными военными и государственными иерархическими институтами.

15 августа 2001 г. президент США Буш предложил министру обороны Дональду Рамсфелду подготовить стратегическое представление о том, как американская армия "должна выглядеть сегодня и как она должна выглядеть завтра".

Но тут грянули события 11 сентября, и в одном из выступлений, прозвучавшем сразу после терактов, Рамсфелд отметил, что в связи с совершенными в Нью-Йорке и Вашингтоне нападениями "мы наблюдаем появление нового поля боя... конфликтов иного типа".

Он заявил, что в ближайшем будущем Америке предстоит решить две важные задачи: одержать победу в борьбе с терроризмом путем ликвидации сети террористических организаций, а также осуществить подготовку к совершенно другой войне – войне, разительно отличающейся не только от войн прошлого столетия, но и от той войны с терроризмом, которую США ведут в настоящее время.

В ноябре 2001 г. в статье "За рамками войны с террором" Рамсфелдом[2] были обозначены контуры новой стратегии.

Он подчеркивает, что в свете последних событий в США подготовка к внезапному нападению – подготовка быстрая и решительная – должна стать одним из слагаемых военного планирования в XXI в. Для того, чтобы отражать внезапные удары, военные стратеги США должны перенести центр тяжести в системе оборонного планирования с модели, в которой отправным моментом является угроза и которая до сих пор доминировала в теории обороны, на модель, опирающуюся на силы и средства, необходимые в будущем.

Вместо того, чтобы искать очередного противника и планировать крупномасштабные войны на точно определенных ТВД, считает Рамсфелд, необходимо предвидеть появление новых и разнообразных врагов, которые будут полагаться на фактор внезапности, обмана и на применение асимметричного оружия для достижения своих целей.

Согласно определению Института национальных стратегических исследований Национального университета обороны Соединенных Штатов, под "асимметричными" угрозами понимаются "использование фактора неожиданности во всех его оперативных и стратегических измерениях, а также использование оружия такими способами, которые не планируются США".

Как заявил Рамсфелд, подготовка к такому развитию событий стала целью проводящегося раз в четыре года анализа состояния и перспектив развития обороны.

В точном соответствии с тезисами Рамсфелда, операция американских войск в Афганистане во многом является полигоном испытания принципиально новой оперативной концепции ведения противоборства, известной из зарубежных источников как "сетевая война" (*network-centric warfare – NCW*).

За последние годы резко возрос интерес к реализации проекта создания глобальной информационной сети Минобороны США, известном как проект *Defense Information Grid*, который координируется Агентством информационных систем МО (*DISA*). Именно она является основой ведения "сетевой войны".

С сентября по октябрь 2001 г. тематика "сетевой войны" так или иначе обсуж-

далась практических на всех конференциях и семинарах, проходивших с привлечением специалистов Пентагона. Наряду с этим, только за несколько последних лет анализу различных аспектов данной оперативной концепции был посвящен ряд исследований ведущих аналитических центров Министерства обороны США.

Данное направление в развитии оперативного искусства было положено в основу концепции строительства американских вооруженных сил "Единая перспектива 2010" ("*Joint Vision 2010*")[3] и связано с трансформацией взглядов на характер угроз в новом веке.

Новый взгляд на угрозы XXI столетия заключается в том, что в будущем основная угроза будет исходить не от регулярных армий разных стран, а от всевозможных террористических, криминальных и других организаций, участники которых объединены в некие сетевые структуры. Подобные организации не имеют четкой иерархической подчиненности, зачастую у них нет единого руководства, они координируют свою деятельность с использованием средств глобальных коммуникаций. Отличительной особенностью таких структур является наличие единой стратегической цели и отсутствие четкого планирования на тактическом уровне. Для обозначения подобных структур появился специальный термин "сегментированная, полицентрическая, идеологически интегрированная сеть" (*Segmented, Polycentric, Ideologically integrated Network – SPIN*).

В условиях воздействия подобных угроз изменяются роль и место вооруженных сил. В большей степени акцент делается на проведение невоенных операций (*Operation Other Then War*), что требует тесного взаимодействия с негосударственными организациями и структурами.

Американцы определяют "сетевую войну" как оперативную концепцию, базирующуюся на информационном превосходстве и позволяющую достичь увеличения боевой мощи войск за счет ориентации на сеть датчиков, штабов и исполнительных подразделений. Это дает возможность достичь широкой осведомленности, увеличить скорость доведения приказов, более высокого темпа проведения операции, большего поражающего действия, большей живучести и степени самосинхронизации.

Есть несколько ключевых понятий, которые в основном отличают "сетевую войну" от войны традиционной:

Первое заключается в использовании географически распределенной силы. Как указывают эксперты, ранее из-за разного рода ограничений было необходимо, чтобы подразделения и элементы тылового обеспечения располагались в одном районе в непосредственной близости к противнику или к обороняемому объекту. Новая концепция снимает эти ограничения.

Второе ключевое понятие состоит в том, что силы, участвующие в "сетевой войне" высокоинтеллектуальны. Пользуясь знаниями, полученными от всеохватывающего наблюдения за боевым пространством и расширенного понимания намерений командования, эти силы будут способны к самосинхронизации деятельности, станут более эффективными при автономных действиях.

Третье ключевое понятие – наличие эффективных коммуникаций между объектами в боевом пространстве. Это дает возможность географически распределенным объектам проводить совместные действия, а также динамически распределять ответственность и весь объем работы, чтобы приспособиться к ситуации.

В сущности, "сетевая война" переводит информационное превосходство в боевую мощь, эффективно связывая

интеллектуальные объекты в единое информационное пространство театра военных действий.

Происходит трансформация понятия поле боя в понятие боевого пространства. В него помимо традиционных целей для поражения обычными видами вооружений включены также и цели, лежащие в виртуальной сфере: эмоции, восприятие и психика противника.

Воздействие на новые классы целей достигается за счет тесной интеграции сетевых структур Министерства обороны и сетевых структур гражданского общества (как совокупности общественных объединений, отвечающих за выработку "общественного мнения").

Примечания

[1] *Arquilla J., Ronfeldt D.* The Advent of Netwar. Santa Monica, Calif., RAND, 1996.

[2] *Rumsfeld D.* Beyond This War on Terrorism // Washington Post. 01.11.2001.

[3] Joint Vision 2010. Washington, 1995.