Центр стратегических оценок и прогнозов

www.csef.ru

Сетевые войны как новая доктрина вооруженной борьбы

МАТЕРИАЛ ОН-ЛАЙН ЛЕКЦИИ ДЛЯ ФОНДА «НОРАВАНК»
ЛЕКТОР, Д.Т.Н. СЕРГЕЙ ГРИНЯЕВ
14 ДЕКАБРЯ 2012 Г.

СОДЕРЖАНИЕ

1. Сетевое общество. Стратегическое информационное противоборство

Разработки в области информационных технологий резко изменяют характер взаимодействие как целых народов, так и отдельных людей. Быстрое распространение информации ставит под вопрос уместность привычных и обычных организационных и управленческих начал. Глобализация сетевой связи создает новые уязвимости ключевым национальным информационным инфраструктурам.

Общество сейчас переживает распространение сетевой организационной культуры, которая до сих пор не претендовала на роль доминирующей, но, тем не менее по эффективности стоит выше нынешней, иерархической. "Кирпичик" иерархической культуры - институт, сетевой - личность. Если институт основан на централизации, вертикальной субординации, штатном расписании и постановке формальных целей, то сетевая организация - на относительной автономии частей, аутсорсинге и распределении рисков. Сетевые сообщества (и террористические в частности) формируются из личностей, которые несут собственное концептуальное целеполагание, создавая временные виртуальные организации. Если выдвинутая идея содержит вызов, то заразившиеся ею люди собираются в своего рода кластеры. Даже если один кластер сети разрушен, остальные могут продолжать функционировать. (Применительно к террористическим организациям это означает, что арест даже большой группы террористов может не затронуть работоспособности всей сети.)

Глобализующийся мир требует качественно нового подхода к проблемам принятия решений. Все более настойчиво ставится вопрос о ***сетевой природе управления***: перехода от жестко иерархичной вертикальной системы управления (где четко разделены центральное «ядро», в котором и принимаются решения, и «периферия», обязанная эти решения беспрекословно выполнять) к распределенной, т.е. сетевой системе, когда полномочия по принятию решений делегируются от центрального «ядра» к структурным подразделениям. Сетевая форма организации позволяет ей быстро адаптироваться к изменяющимся внешним условиям, отмечал один из главных теоретиков "сетевого общества" Мануэль Кастельс. И, кстати, именно так уже действуют многие крупные транснациональные корпорации, приспосабливаясь к изменчивой геометрии глобальной экономики, легче других выдерживая конкуренцию

Изменения в общественно-политической жизни ряда государств, вызванные быстрыми темпами информатизации и компьютеризации общества, ведут к пересмотру геополитических взглядов руководства, к

возникновению новых стратегических интересов (в том числе и в информационной сфере), следствием чего является изменение политики, проводимой этими странами. Развивая для новых условий глобализирующегося мира определение войны, данное Клаузевицем («война есть продолжение политики другими средствами»), можно сказать, что глобальные противоречия требуют новых средств и методов их разрешения - стратегического информационного противоборства.

2. Сетецентрические войны: подходы, доктрины, практика

Террористические акты в США 11 сентября 2001 г. открыли эпоху «мятежевойны» (в ряде трактовок этот термин звучит как «мятежвойна»), наступление которой предсказал еще в начале 60-х гг. XX в. русский военный ученый-эмигрант, полковник царской армии Евгений Месснер (1891—1974 гг.). Им были определены принципиальные особенности этого явления: отсутствие линий фронта и четких границ между противниками, превращение общественного сознания в основной объект воздействия, пространство войны становится четырехмерным (к трем традиционным добавляется информационно-психологическое измерение). Примером мятежвойны могут служить афганская компания бывшего СССР, обе чеченские компании, война в бывшей Югославии, война коалиционных сил в Афганистане и Ираке.

Однако Месснер был крайне скуп в описании методов борьбы с противником, избравшим стратегию "мятежевойны". Первыми попытку восполнить этот вакуум предприняли политики и военные США. Теракты заставили американцев активизировать эти усилия. Ответом на стратегию "мятежевойны" стала концепция "сетевого противоборства", лежащая в основе стратегии проведения «***сетецентрических войн***».

Прорыв в сфере информационных технологий в средине 1990-х гг. заставил военно-политическое руководство США заняться исследованиями их влияния на военную безопасность США и НАТО не только в мятежвойнах, носящих, как правило, местный, локальный характер, но также в глобальных конфликтах, в которых с обеих сторон участвуют регулярные войска. В декабре 1995 г. МО США поручило RAND провести комплексный анализ аспектов информационной войны, оценить их влияние на ход и исход глобальных вооруженных конфликтов, сформулировать требования и исходные данные, необходимые для решения проблемы информационной безопасности страны в обозримой перспективе. В интересах решения указанных задач RAND была разработана и проведена специальная исследовательская командно-штабная военная игра (КШВИ) с участием высших должностных лиц страны и бизнеса, получившая название «На

следующий день после....»(«The Day After....»). Результатом игры стало появление нового понятия в области военного искусства — «стратегическая информационная война». Стратегическая информационная война (по мнению американских специалистов) — область конфликта, в которой киберпространство используется для оказания воздействия на ход и исход стратегических военных операций и нанесения ущерба национальной информационной инфраструктуре противостоящей стороны.

В проводимой КШВИ акцент был сделан, прежде всего, на оборонительной стороне, связанной с обеспечением информационной безопасности территории США и союзников по НАТО от враждебных кибератак. В ходе исследования, вопросы информационной безопасности в основном сводились к ее технической стороне. В ходе проведения КШВИ была выявлена высокая степень уязвимости «киберпространства» США от информационных воздействий со стороны большого числа плохо идентифицируемых противников.

По итогам было признано, что единое «киберпространство» США и их союзников по НАТО характеризуется настолько динамичным развитием, что проблема снижения его уязвимости, требует создания на национальном и межнациональном уровне специальных «иммунных систем», которые бы были предназначены для заблаговременного выявления и устранения уязвимых мест в системе информационной безопасности.

Новая концепция позволяет в рамках единого подхода охватить все три уровня информационно-силового противоборства: *стратегический* — уровень, охватываемый понятием «стратегическая информационная война», *оперативный* и *тактический*—уровни, охватываемые понятием «мятежвойна».

Внедрение сетевых технологий в военную сферу является действительно революционным шагом, направленным на повышение боевых возможностей вооруженных сил, но уже не только за счет повышения огневых, маневренных и других характеристик индивидуальных платформ, а в первую очередь за счет сокращения цикла боевого управления в операции (бою). Сейчас можно говорить о фундаментальном сдвиге от того, что называлось «платформоцентрической» войной, к тому, что называется «сетецентрической» войной.

Введение понятия «сетецентрическая война», авторами которого считаются вице-адмирал ВМС США Артур Себровски и Джон Гарстка, определяет новые принципы управления войсками и силами. Успех современных операций будет зависеть в первую очередь от объединения всех участников боевых действий в рамках информационного пространства.

Главной особенностью развертывания новых цифровых сетей является то, что они могут повысить темп операции, сократив время фазы Observation-Orientation (разведка – оценка).

Основу новой концепции ведения информационной войны составляет понятие «сеть», а ее базовым принципом является принцип «сетецентризма». Принцип сетецентризма, в его широком понимании, содержит три основных положения.

Первое положение. В новом глобализирующемся мире не транспортные коммуникации («коридоры») с циркулирующими по ним потоками материальных ресурсов и услуг, а опоясывающие весь земной шар глобальные информационно-коммуникационные сети, в том числе, с использованием средств космического базирования, с передаваемыми по ним потоками информации, составляют *несущий каркас* будущего глобального «сверхобщества».

Второе положение. Мировой исторический процесс это единый глобальный процесс борьбы, взаимопомощи, нейтрального сосуществования человеческих сообществ организованных как по иерархическому («вертикальному»), так и по сетевому («горизонтальному») принципу, при этом сетевой («горизонтальный») принцип со временем может стать доминирующим. Другими словами, здесь сетецентризм исходит из того, что как *субъектами,* так и *объектами* мирового исторического процесса в современном мире являются различные по своему происхождению, предназначению, численности, географическому и временному масштабу, правовому статусу, способу взаимодействия «горизонтальные» и «вертикальные» сетевые структуры, осуществляющие непрерывные процессы внутри сетевой и межсетевой дивергенции и конвергенции.

Третье положение. Жесткость несущему сетевому информационному каркасу будущего глобального «сверхобщества», основу которого в настоящее время составляют естественные глобальные психосоциальные сети межличностного общения, придают динамично развивающиеся *искусственные* (электронные) сети, которые, переплетясь и взаимодействуя с психосоциальными сетями, создают качественно новое социальное явление, для обозначения которого в сетецентрической концепции информационной войны используется термин «сегментированная, полицентрическая, идеологизированная сеть» (Segmented, Polycentric, Ideologically integrated Network — SPIN).

Важнейший вывод из сетецентрической концепции для обеспечения военной безопасности США и их союзников по НАТО состоит в признании того, что в обозримом будущем основные угрозы их национальным интересам будут исходить не от регулярных армий, а от террористических, криминальных, экстремистских и других преступных сообществ, способных

объединяться в региональные или глобальные транснациональные сетевые структуры.

Понимая, что с сетецентрическими структурами можно бороться только с помощью других сетецентрических структур, военно-политическое руководство США отдает предпочтение *невоенным операциям* (Operation Other Then War), что требует организации тесного сетевого взаимодействия между подразделениями ВС с гражданскими государственными и негосударственными организациями, осуществляющими наступательные и оборонительные акции в сфере организационного и информационного противоборства.

Главным объединительным мотивом сетевой организации являются мнения, установки и убеждения ее членов и источники финансирования.

Объединяясь в небольшие группы, через горизонтальные связи, поддерживаемые с другими сетевыми структурами, они могут превращаться на короткий срок в локальные, региональные и даже в глобальные сетевые структуры, а после достижения своих целей, опять становиться локальной сетевой группой или полностью прекращать свое существование. Выявить и уничтожить такую сетевую структуру достаточно сложно, поскольку она, как правило, не имеет четко очерченных географических и исторических границ, однозначного центра, а значит — выраженной устойчивой иерархии, уничтожением которой можно было бы разрушить всю систему. Более того, если даже центральный орган, будет все-таки локализован или уничтожен, лидерство в сети автоматически переходит к другому центру.

Взаимодействия членов сообщества в такой сетевой структуре, как правило, организованы по принципу «стаи». В повседневной жизни отношения членов сетевого сообщества носят спонтанный, чисто символический характер. В определенный момент времени члены сетевого сообщества, мотивированные общей целью на то или иное совместное действие, собираются в условленном месте в «стаю», участвуют в теракте, нападении, бандитской вылазке. Сразу после ее завершения «стая» прекращает свое существование. Ее члены вновь превращаются в законопослушных, мирных граждан. Подвергнутая нападению «стаи» сторона часто не может идентифицировать, кем, откуда и с какой целью была проведена такого рода акция, а потому не способна нанести ответный удар, чтобы наказать виновных и, тем самым, не допустить повторения аналогичных действий в будущем. Именно в этом заключается высокая живучесть и целевая эффективность организованного по сетецентрическому принципу противника.

Сетецентрические войны по принципу «стаи» могут вестись не только криминальными, террористическими и экстремистскими организациями, но и легитимными, в том числе финансовыми и другими неправительственными национальными и транснациональными организациями (например, захват

чужого имущества с помощью механизма рейдерства). Для успешного проведения таких акций на временной или постоянной основе в состав членов сетевой структуры включаются их представители, внедренные в законодательные и исполнительные органы власти. Благодаря этому, государство превращается в политический инструмент, который отдельные легитимные и теневые сетевые структуры используют для достижения своих целей в ущерб национальным интересам.

По этой причине процесс глобализации, инициатором которого выступают США — процесс формирования и постоянного реконфигурирования глобальных транснациональных горизонтальных сетевых из локальных национальных организационных сетевых структур, игнорирующих национальный суверенитет государств и национальную самобытность народов и, которые в этот миллиард не попали.

За множеством таких сетевых структур, в том числе и сетей, элементами которых являются отдельные государства, стоят надгосударственные международные сетевые структуры — *инициаторы процесса глобализации*, государственные и негосударственные сетевые структуры — проектировщики и генеральные директора, управляющие глобальными сетевыми ресурсами, а также сетевые структуры — доноры, которые несут всю тяжесть последствий глобализации. При этом в различные моменты истории одни и те же сетевые структуры могут занимать различное положение в общей иерархии, выстраиваемой инициаторами процесса глобализации: из разработчиков и сетевых менеджеров могут превращаться в исполнителей, распорядителей и даже сетевых доноров.

Международные сетевые структуры — инициаторы процесса глобализации, которые принято называть «мировой закулисой», представлены закрытой для посторонних сетью влиятельных *неправительственных организаций* (НПО). Их сетевая структура также не имеет четкой иерархии, географической привязки, устава, постоянного членства, функционирует по принципу «стаи». Эти сетевые структуры способны через своих представителей в сетевых структурах более низкого международного статуса оказывать влияние на всю мировую политику, финансовую систему, экономику, принимать и проводить решения о смене политических режимов, изменению курса развития той или иной страны и др.

За счет мобилизации сетевых ресурсов, находящихся под контролем этих представителей, мировое сообщество может в «мягкой» форме направляться на решение, широкого круга четко фиксируемых и координируемых задач в сфере внутренней и внешней политики. Благодаря формированию такой пространственно разнесенной и иерархически упорядоченной мета-сетевой организации, верхние этажи которой занимают сети, принадлежащие западному сверхобществу, реализуется фарисейский по своей сути принцип

управления миром, когда управляемый либо не понимает, что им управляют, а если и понимает, то не может определить, из какого центра происходит это управлении и кто несет за него ответственность.

Между тем, известно, что современное противостояние в информационной сфере ведется не только между государствами, но и между негосударственными (неправительственными) организациями и государством. Роль НПО в организации и проведении т.н. «цветных революций» хорошо известна.

Это особый, в основном для частных случаев, метод является необычайно мощным средством как нападения, так и защиты. В нападении сетевые организации, как правило, очень гибки, легко адаптируемы к различным условиям, универсальны и предоставляют многочисленные возможности взаимодействия. Особенно это характерно для случаев, где субъекты используют тактику так называемого «роения».

Как и практически любое новое явление, концепция военного и информационного противоборства и сдерживания пережила определенное смысловое перерождение. О том, что **СЦВ зачастую становятся не механизмом борьбы с терроризмом и иными ассиметричными угрозами** (в качестве которого они изначально рассматривались), а **инструментом самого терроризма и транснациональной преступности, а также способом решения определенных политических задач,** говорят многие факты. Межнациональные террористические группы, черный рынок оружия массового поражения, нарко- и иные преступные синдикаты, фундаменталистские и этнонационалистические движения, пираты в сфере IT-технологий и иной интеллектуальной собственности, контрабандисты, беженцы и нелегальные мигранты по-прежнему остаются составной частью сетевых войн. Однако к этой же концепции обращаются и радикалы нового поколения, начинающие создавать свои идеологии на основе достижений века информации, в которых акценты от отдельного государства смещаются в сторону межнационального уровня «глобального гражданского общества». При этом действия всех указанных групп могут носить как национальный, так и транснациональный характер. Естественно, целью некоторых субъектов является уничтожение, но целями большинства является подрывная деятельность и дезориентация. Сетевая форма организации позволяет ей быстро адаптироваться к изменяющимся внешним условиям, отмечал один из главных теоретиков "сетевого общества" Мануэль Кастельс.

Кроме того, при иерархическом и сетевом подходах значительно различаются цели проведения деструктивных управляющих воздействий, направленных на получение контроля над информационными системами,

входящих в контур управления ключевыми объектами информационной инфраструктуры страны.

Следует отметить, что адекватное понимание проблем сетевого информационного противоборства естественным образом вытекает из **общесистемных представлений противоборства** любых двух систем с противоположными интересами и целями, в нашем случае, систем защиты и нападения, каждая из которых представляет собой многофакторную, иерархическую, многоцелевую, сложноорганизованную многоэлементную систему. В этом плане целесообразно рассматривать информационное противоборство исходя из **общей задачи противоборства двух динамических развивающихся сложных систем**, теоретический базис которого сегодня достаточно полно разработан.

Использованные источники