ВВЕДЕНИЕ

Цель современных сетевых войн, являющихся элементом так называемых гибридных войн, — получение одним из участников противоборства контроля над всеми другими участниками. Причем необязательна прямая оккупация, массовый ввод войск или захват территорий. Военные действия и огромные траты на традиционные вооружения излишни. Сеть — более гибкое оружие, она манипулирует насилием и военной силой только в крайних случаях, и основные результаты достигаются в контекстуальном влиянии на широкую совокупность факторов — информационных, социальных, когнитивных и т. д. [2].

Основой ведения сетевых войн являются операции, базирующиеся на эффектах ОБЭ. ОБЭ — совокупность скрытых действий, направленных на формирование требуемого поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны. Иными словами, ОБЭ — это такое качественное влияние на среду, при котором участникам ничего не навязывается прямым образом, но при этом они делают то, что хотят те, кто выстраивает эту модель управления [43].

Задачи сетевых войн заключаются [100] в следующем:

1) в преимущественном переходе от формы физического занятия обширного пространства к функциональному контролю над наиболее важными стратегическими его элементами;
2) в переходе к скрытым действиям во времени и пространстве, но с учетом нелинейных эффектов, в том числе — возможности сосредоточить критически важный объем сил в конкретном месте;
3) в усилении тесного взаимодействия разведки, операционного командования и логистики для реализации точных эффектов и обеспечения временного преимущества с помощью рассеянных сил.

В работах основоположника понятия сетевых воин Джорджа Карлина эти задачи формулируются следующим образом [42, 103, 130].

1. Заранее повлиять на стартовые условия войны, заложить в них такую структуру, которая заведомо приведет (американскую) сторону к победе.

2. Спровоцировать сочетание во времени и в пространстве ряда событий, которые призваны повлиять на потенциального противника и блокировать его ответную инициативу [103].

Современные конфликты развертываются в четырех смежных областях человеческой деятельности: в физической, информационной, когнитивной и социальной. Каждая из них имеет важное самостоятельное значение, но решающий эффект в сетевых войнах достигается синергией (однонаправленным действием) всех этих элементов [106].

1. Физическая область — это традиционная область войны, в которой происходит столкновение физических сил во времени и в пространстве. Эта область включает в себя традиционные среды ведения боевых действий (море, суша, воздух, космическое пространство), боевые единицы (платформы) и физические носители коммуникационных сетей. Этот аспект лучше всего поддается измерению и ранее служил основой при определении силы армии и ее способности вести боевые действия.
2. Информационная область — это сфера, где создается, обрабатывается и распределяется информация. Эта область покрывает системы передачи информации, базовые сенсоры (датчики), модели обработки информации и т. д. Это преимущественная среда эпохи сетевых войн, которая выделилась в самостоятельную категорию — информационную сферу (инфосферу) — наряду с физическими средами и приобрела важнейшее, если не центральное значение [43].
3. Когнитивной областью является сознание населения и бойца. Она является тем пространством, где преимущественно осуществляется ОБЭ. Все основные войны и битвы развертываются и выигрываются именно в этой сфере. Именно в когнитивной области располагаются такие явления, как намерение командира, доктрина, тактика, техника и процедуры. Таким образом, чуть шире — когнитивная сфера — сфера сознания боевой единицы. В сетевых войнах понятие солдата или боевой единицы — это, прежде всего интеллектуальная (с учетом дополненности) реальность.
4. Социальная область представляет собой поле взаимодействия людей. Здесь преобладают исторические, культурные, религиозные ценности, психологические установки, этнические особенности [43].

Войны информационной эпохи основаны на сознательной интеграции всех четырех областей. Путем их избирательного наложения и создается сеть, которая лежит в основе ведения военных действий.

Речь идет о том, что война в сетевом смысле выигрывается на четырех уровнях, из этого и складывается сетевое управление [101].

Сферы пересечения этих областей имеют принципиальное значение. Настройка всех факторов сети в гармоничном сочетании усиливает эффект от действий вооруженных сил, в то время как прямые действия, направленные против противника, хоть и расстраивают его ряды, но при этом разводят эти области между собой, исключая важнейший фактор превосходства. Сфера традиционного противоборства между наступательными и оборонительными системами была перенесена и в киберпространство, т. е. превратилось в глобальную сферу противоборства.

В этой связи важно отметить ряд принципиально новых особенностей такого противоборства [7, 49].

1. Область информационного противоборства изначально глобальна и не может быть ограничена ни отдельным театром военных действий, ни временем, ни системой оружия или военной техники.
2. Эта область не поддается контролю или ограничению за исключением крайне редких случаев (например, ограничений по развертыванию радиолокационных станций), т. е. не может стать предметом договоренностей.
3. Область информационного противоборства не имеет четких границ ни между формами использования («мягкой» или «жесткой») силы, ни между соответствующими средствами.
4. Информационные средства применительно к войскам военно-космической обороны (ВКО) фактически являются как частью стратегических ядерных сил, так и средств собственно ВКО. Не только военные, но и гражданские технологии становятся критически важными для ВКО.

Виртуальный характер сетевых войн меняет идентичность противника.

1. Сетевые операции ведутся не только против врагов, но и против нейтральных сил или друзей. Контролировать надо всех, а значит, алгоритм ведения операций скрывается от всех (включая союзников).
2. Сеть — явление динамическое, и сегодняшний союзник может превратиться в завтрашнего противника (и наоборот), поэтому распределение ролей в сетевой войне носит отчасти условный характер. Так как они все равно ведутся против всех, поэтому «образ врага» становится все более и более гибким и динамичным.
3. Враг сам становится все более и более виртуальным. В каком-то смысле его может и не быть, и сетевая война может

вестись с фиктивным противником, причем боевые действия и последствия войны могут быть реальными.

Изучив и проанализировав опыт стран — участниц сетевого противостояния, можно однозначно сказать, что основная цель — контроль государства над личностью, обществом и по возможности над другой страной. Это, кстати, показательный момент сетевого подхода — реальность сформирована, запрограммирована заранее [32].

Именно по этой причине сетевая война столь эффективна — она не дает возможности найти и покарать ответственных, установить прямую связь между источником принятия решения и исполнителем. Тем не менее, она дает широкие возможности для действий, дает возможность осуществить что-то, а потом не понести за это ответственности. Это действительно эффективная стратегия [43].

Рассмотрим средства проведения сетевых атак [95, 98].

1. **Физическая сфера.** Ярчайшим примером сетевой атаки в физической сфере являются действия США в войне с Ираком. Американцам удалось подавить системы ПРО и ПВО противника, в дальнейшем, нанеся авиаудары по стратегическим объектам обороны, они фактически нейтрализовали иракскую армию. Средством проведения сетевой атаки явились стратегические бомбардировщики, а также системы РЭБ и РЭП американских вооруженных сил [94].
2. **Информационная сфера.** Гегемония США и Европы в общемировом информационном пространстве — BBC, CNN, CNBC. Россия достойно отвечает на этот вызов, проведя успешную реализацию проекта телеканала Russia Today [98].
3. **Когнитивная сфера.** Широкое распространение получили блоги известных и влиятельных людей. Запад использует «заряженных» блогеров, чтобы влиять на сознание индивида. В России эта сфера пока слабо развита, но есть положительные тенденции [98].
4. **Социальная сфера.** Огромное количество некоммерческих организаций прозападного толка функционирует во всем мире, в том числе и России. Руководство РФ вынуждено решать вопрос по регулированию их деятельности на самом высоком уровне [95].

Увы, идея мирового господства не умерла вместе с Наполеоном и Гитлером. Ее продолжают вынашивать и сегодня траснациональные корпорации (ТНК), претендующие на управление всем миром. Перешагнув государственные границы и накопив капитал, соизмеримый с национальными бюджетами развитых стран, владельцы ТНК заявили о своих амбициях в Бильдербергском клубе, который фактически отражает интересы Запада.

Сетевое устройство современных ТНК открывает широкие перспективы для управляющего воздействия на страны и народы, прежде всего в информационной сфере. Однако, заявить о своей исключительности (как это делают США) и успешно решать мировые проблемы — это далеко не одно и то же. Несостоятельность свою в этом аспекте американская «сверхдержава» демонстрировала неоднократно.

Груз глобальных проблем (перенаселение, незаконная иммиграция, продовольственная, экологическая, энергетическая безопасность и защита от террористических угроз) настолько велик, что их разрешение не под силу не только США, но и всему «золотому миллиарду». Возможно, чувствуя свою несостоятельность, американцы запустили стратегию «управляемого хаоса», стремясь в многочисленных азиатских и африканских конфликтах отвлечь «не золотые миллиарды» от вышеуказанной проблематики и сохранить свое лидерство. Однако хаос по определению имеет минимальную управляемость, и в результате был запущен дестабилизирующий механизм мирового масштаба, ввергнувший в кровавые междоусобицы многие страны. Следствием этого стало процветание международного (также сетевого) терроризма, миллионные миграционные потоки.

В этой турбулентности очевидно стремительно возрастают риски. Причем увеличиваются не только размеры возможных ущербов, но и вероятность их наступления. «Черные лебеди» прилетают все чаще... В этом контексте актуальность сетевого риск-анализа и управления рисками становится первостепенной проблемой международного масштаба.

К сожалению, современная теория сетей [11, 128, 148, 156, 173] не может служить полноценной основой для данного анализа. Она, как правило, за редким исключением, ориентирована на так называемые невзвешенные сети, т. е. на сетевые структуры, в которых весами вершин и дуг (физическими параметрами хранимого и распространяющегося по сети наполнителя) можно пренебречь. Однако такой подход не применим для случая, когда возникает необходимость оценки вероятных ущербов, объективно необходимого в риск-анализе.

В этой связи необходимо развитие теоретических основ описания и функционирования сетей в контексте учета взвешенности их элементов для анализа процессов сетевого противоборства, что и предлагает настоящая монография.

Авторы выражают благодарность Ю.Н. Гузеву, Е.Ю. Чапурину, В.А. Кургузкину и К.С. Коряковцеву за помощь в подготовке и оформлении материалов.