ГРАЖДАНСКИЕ СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ

Д.Б. Изюмов, нач. отд. ФГБНУ НИИ РИНКЦЭ, *izyumov@extech.ru*
Е.Л. Кондратюк, ст. науч. сотр. ФГБНУ НИИ РИНКЦЭ, *kel@extech.ru*

В статье рассмотрена концепция «гражданских сетецентрических войн», их цель и принципы ведения, основные черты и этапы проведения таких войн. Представлены взаимосвязи основных элементов и сред, порождающих «гражданские сетецентрические войны». Приведены результаты анализа терминологии «гражданской сетецентрической войны».

Ключевые слова: информация, сетецентрическая война, гражданская сетецентрическая война, концепция, информационно-коммуникационные сети, сетевая война, взаимосвязь информационной, когнитивно-социальной и физической сред сети.

CIVILIAN NETWORK-CENTRIC WARFARE

D.B. Izyumov, Head of Department, SRI FRCEC, *izyumov@extech.ru*
E.L. Kondratyuk, Senior Researcher, SRI FRCEC, *kel@extech.ru*

The article discusses the concept of «civil network-centric warfare», the aim and principles of management, basic features and stages of these wars. It presents the relationship of the main elements and environments, generating a «civic network-centric warfare». The article presents the results of the analysis of terminology, «civilian-centric warfare».

Keywords: information, network-centric warfare, network-centric civil war, the concept of information and communication network, the network war, the relationship of informational, cognitive, social and physical environments network.

В настоящее время существующее и довольно распространенное понятие «сетецентрическая война» – война, в которой увеличение боевой мощи группировки войск (сил) достигается за счет создания информационно-коммуникативной сети, связывающей источники информации (разведки), органы управления и средства поражения (подавления) – неразрывно связано с сетецентричными боевыми действиями (Network-Centric Warfare) и относится к сугубо военной терминологии [1]. В данном контексте сетецентризм способствует доведению до участников боевых операций достоверной и полной информации об обстановке практически в реальном масштабе времени.

Однако, помимо понятия «горячей» сетецентрической войны, связанной с организацией и проведением боевых действий, сетецентрические действия можно проводить и в рамках сугубо гражданских отношений, имеющих все признаки подобной войны, за исключением признаков среды и условий, в которой она проводится.

«Сетецентрическая война» в контексте невоенных взаимоотношений представляет собой мероприятия, проводимые в интересах повышения конкурентоспособности, обеспечения информационного превосходства различных организаций и институтов и объединения в единую сеть субъектов гражданских правоотношений, связанных общей целью.

В общем случае, сеть представляет собой не только объединенные в единый информационный комплекс компьютеры, но и информационно-технические «гражданские» сети, характеризующиеся устойчивостью и развитием сетевой архитектуры.

Анализ показывает, что к настоящему времени сетевые идеи были уверенно и успешно применены в широком спектре ряда практических вопросов. Например, при разработке

надежных масштабируемых сетей, объединяющих проводную и беспроводную связь, при анализе метаболических и генетических регуляторных сетей, в целях развития стратегии вакцинации в борьбе с болезнями, и других прикладных проблем. Однако при осуществлении государственного или корпоративного управления подобные идеи осознано и масштабно не применялись.

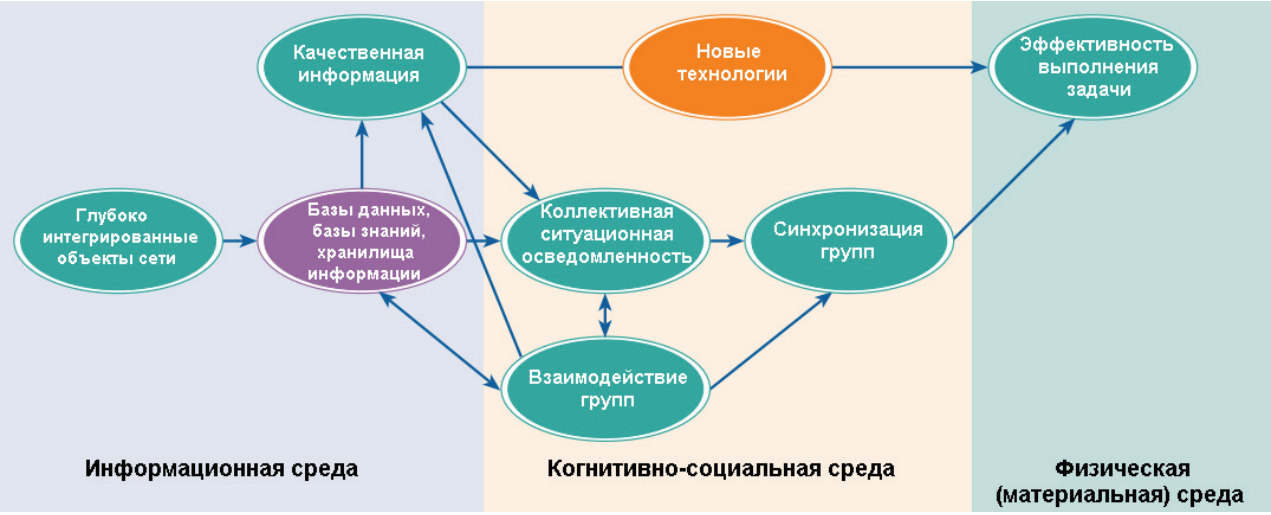

Рис. 1. Взаимосвязи основных элементов в рамках концепции «гражданских сетецентрических войн»

Ввиду изложенного, концепция «гражданских сетецентрических войн» предполагает задействование цифровых сетей с целью обеспечения и вертикальной, и горизонтальной интеграции (экономической, торговой, научной, производственной и пр.) всех участников такой войны. Концепция основывается на информационном превосходстве или же приоритете информационно-когнитивной сферы деятельности организации (групп организаций) над физической средой функционирования конкурирующих групп (рис. 1).

Проведение «гражданской сетецентрической войны» подразумевает обязательное наличие трех составляющих: информационно-телекоммуникационной, социально-когнитивной и материально-физической (рис. 2).

Информационно-телекоммуникационная составляющая предполагает наличие совокупности подходов, инструментов и методов обработки структурированных и неструктурированных данных больших объемов и многообразных по своему содержанию, в условиях их непрерывного прироста, распределения по многочисленным узлам сетей, альтернативных традиционным системам управления базами данных и решениям уровня «конкурентной разведки» (Business Intelligence).

Материально-физическая составляющая представлена вычислительной сетью физических предметов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, предполагающая организацию сетей как явление, способное перестроить экономические и общественные процессы. Зачастую материально-физическая составляющая «гражданской сетецентрической войны» исключает из части процессов необходимость вовлечения человека.

В свою очередь, *когнитивно-социальная составляющая* связана с процессами познания моделей поведения, психологии, нейрофизиологии, когнитивной лингвистики и основными постулатами теории искусственного интеллекта.

При детальном анализе рис. 2, авторами которого являются военные специалисты США, можно видеть возникновение промежуточных сфер.

Информационно-когнитивная сфера деятельности участников «гражданских сетецентрических войн» включает информационную (базы данных, базы знаний, хранилища информации, качественно обработанную и проанализированную информацию) и когнитивно-социальную среды (непосредственно взаимодействующие группы контрагентов). Заинтересованные в подобных сетях контрагенты нацелены на повышение коллективной ситуационной осведомленности, тесном взаимодействии и самосинхронизации. Последнее предполагает единую терминологию, достижение единого (общего, одинакового) понимания внешних и внутренних факторов в любой момент времени и обеспечение рационального, синергетического взаимодействия в своей сфере деятельности.

Рис. 1. Взаимосвязи основных элементов в рамках концепции «гражданских сетецентрических войн»

Результатом взаимодействия информационной и физической сфер является координация действий внутри сети в соответствии с поступающими информационным «сигналами», что вызывает оперативную реакцию системы (побуждает к конкретным, материализованным действиям).

Взаимосвязь когнитивной и физической сфер подразумевает планирование и организацию деятельности, всестороннее обеспечение и поддержку элементов сети, конечной целью

которой является максимально эффективное оперативное управление. Данная деятельность во взаимосвязи с информационно-когнитивной и информационно-физическими сферами внутри сети позволяет привести все механизмы системы «гражданской сетецентрической войны» в действие. Отсутствие любого из этих элементов приводит к дисбалансу и будет представлять собой обычную информационную войну, рекламу, процесс оперативного управления организацией или что-либо иное.

Таким образом, концепция «гражданских сетецентрических войн» предусматривает увеличение потенциала организации или гражданского института за счет образования информационно-коммутационной сети, объединяющей всевозможные источники информации (в том числе информацию, получаемую средствами технической, экономической и иных видов разведки), органы управления и принятия решений (мозговые центры и пр.) и средства подавления конкурентов, а также обеспечивающих доведение до участников сети достоверной и полной информации об обстановке в режиме, максимально приближенному к реальному времени.

Осуществление данного процесса предполагает объединение различных субъектов (организаций, НИИ, производств, некоммерческих организаций и пр.), функционирующих в определенных сферах и областях деятельности, в единые концерны, корпорации, кластеры и платформы в целях:

– повышения своих конкурентных преимуществ;

– рентабельности производственной или иной деятельности организаций, вовлеченных в такие «войны»;

– промышленного, коммерческого, научного, кадрового и иного шпионажа;

– активизации усилий в области создания перспективных технологий, новой продукции и/или оказании качественно новых услуг;

– объединения дополнительных ресурсов для проведения научных исследований и разработок;

– организации эффективного взаимодействия всех заинтересованных сторон.

В определенной степени, примером может послужить объединение организаций в технологические платформы – коммуникационные площадки для взаимодействия бизнеса, науки, потребителей и государства по вопросам модернизации и научно-технического развития по определенным технологическим направлениям.

Другим примером организации сетей «гражданских сетецентрических войн» могут служить создаваемые в настоящее время в Пентагоне межфункциональные группы («Cross-functional teams» – CFTs) [2]. Данные группы создаются с целью оптимизации системы принятия решений, выработки эффективного и молниеносного решения возникшей проблемы, в интересах создания временного запаса и обеспечения доминирующих позиций в любом возникающем кризисе. Данная концепция уже широко применяется бизнесом и гражданскими органами управления США.

Организации, объединенные в рассматриваемые сети, обладают значительными преимуществами благодаря единым базам данных, единому электронному документообороту, высокой скорости передачи и объема обмениваемой между собой информации (например, раскрытие своим партнерам коммерческой тайны, передача прав интеллектуальной собственности и др.). В конечном итоге, «гражданские сетецентрические войны» направлены на завоевание монополистических позиций групп/объединений организаций в определенных областях и сферах деятельности.

Концепция «гражданских сетецентрических войн» предполагает проведение интеллектуальных разработок и мозговых штурмов, экспериментов и моделирования, направленных на дальнейшее совершенствование в информационно-телекоммуникационном пространстве с применением информационно-коммуникационных технологий.

Таким образом, *принципами ведения* «гражданских сетецентрических войн» являются:

– возможность качественно нового порядка и уровня обмена профильной информацией между организациями, объединенными высоко надежными защищенными сетями;

– организация обмена информацией в целях повышения ее качества и уровня общей информированности организаций о происходящем;

– высокоэффективное взаимодействие и сотрудничество организаций, объединенных в такую сеть.

Концепция предполагает перевод преимуществ, присущих отдельным инфокоммуникационным технологиям, в конкурентное преимущество за счет объединения в устойчивую сеть географически рассредоточенных и информационно обеспеченных сил. Такая сеть, соединенная с новыми технологиями и новым уровнем организации процессов и взаимодействия людей, предполагает новые формы и принципы организации.

Основные черты «гражданской сетецентрической войны»:

– широкая возможность использования географически распределенных субъектов. Ранее из-за различного рода ограничений предусматривалось расположение всех элементов системы в непосредственной близости к друг к другу. Концепция «гражданской сетецентрической войны» снимает эти ограничения;

– «гражданскую сетецентрическую войну» способны вести только высокоинтеллектуальные, технологически оснащенные и развитые субъекты. При задействовании знаний, полученных из всевозможных источников и расширенном понимании обстановки, они способны к большей эффективности, чем отдельная организация, осуществляющая автономные, сравнительно разрозненные действия;

– наличие эффективных высокозащищенных и надежных коммуникаций между субъектами. Это дает возможность географически распределенным субъектам проводить совместные действия, а также динамически распределять весь объем ответственности, наиболее эффективно адаптируясь к любой ситуации. Этому способствует постоянно растущая пропускная способность каналов связи для передачи информации.

Основные фазы (этапы) ведения «гражданской сетецентрической войны»:

– достижение информационного превосходства посредством дестабилизации, дезорганизации, опережающего подавления конкурента, его системы информационного обеспечения, а зачастую и проведение мероприятий по дискредитации конкурентов (завоевания господства в киберпространстве, СМИ и формирование негативного облика конкурента в массовом сознании);

– потеря конкурентом деловой репутации, финансирования, имеющихся контактов и пр. (промежуточная фаза «уничтожения» конкурента);

– уход конкурента с рынка, его банкротство и пр. (окончательное «уничтожение» конкурента).

Успешное осуществление каждой из фаз основывается на значительно меньшей продолжительности временных затрат, чем в рамках ведения честной конкурентной борьбы, подразумевающей создание инновационного (лучшего) продукта и, как следствие, ведет к существенному снижению затрат материальных и человеческих ресурсов.

Таким образом, целью статьи было выявление основных признаков концепции «гражданских сетецентрических войн» для дальнейшего обнаружения и анализа недобросовестных действий конкурентов или, наоборот, применения данной схемы в интересах развития российских элит, бизнеса и представителей науки и производства на мировой арене, с точки зрения завоевания ими доминирующих и лидирующих позиций в своих сферах деятельности.

Работа выполнена в ФГБНУ НИИ РИНКЦЭ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках Государственного задания по проекту № 2.39.2016/НМ.

Список литературы

1. Office of Force Transformation. The Implementation of Network-Centric Warfare. January, 2005.

2. Lamb C.J. (2016) Cross-Functional Teams in Defense Reform: Help or Hindrance? STRATEGIC FORUM. National Defense University. August, 2016. Avialable at: http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-298.pdf?ver=2016-08-30-123820-727.

References

1. Office of Force Transformation. The Implementation of Network-Centric Warfare. January, 2005.

2. Lamb C.J. (2016) Cross-Functional Teams in Defense Reform: Help or Hindrance? STRATEGIC FORUM. National Defense University. August, 2016. Avialable at: http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-298.pdf?ver=2016-08-30-123820-727.