Курилкин А. В.

СОВРЕМЕННЫЕ ПОДХОДЫ К ВЕДЕНИЮ ИНФОРМАЦИОННЫХ ВОЙН

Аннотация. *После достижения ядерного паритета между СССР и США стало ясно, что крупномасштабные войны с применением больших армейских соединений и массовым использованием тяжелой бронетехники, авиации и пехоты между крупными державами стали практически невозможными, что побудило СССР и США искать иные способы вооруженного противостояния. Отчасти такое противостояние при сохранении биполярного мира вылилось в цепочку локальных конфликтов, где если одна из сверхдержав поддерживала одну из сторон, то с высокой долей вероятности противоположную сторону начинала поддерживать другая сверхдержава. Развитие электроники и науки позволило создать системы высокоточного вооружения или «умного» оружия, которое на современном этапе сравнилось по своей разрушительной мощи с оружием массового поражения, что позволило ускорить ведение конфликтов в несколько раз и одновременно усложнило их и сделало гораздо дороже. Однако, еще во время Первой и Второй мировой войны появились идея о том, что победа в войне достигается не сколько через уничтожение вражеских армий, сколько через воздействие на население противника с целью достижения такого состояния, когда население настолько деморализовано и устало от войны, что продолжение боевых действий становится невозможным.*
Ключевые слова: *международные отношения, внешняя политика, США, геополитика, конфликты, дипломатия, государство, информационная война, безопасность, ценности.*

Изменения стратегии ведения вооруженных конфликтов в современном мире

Интернет, зародившийся изначально в военных кругах, оказал большое влияние на развитие сетей управления государством, экономикой и вооруженными силами, но одновременно сделал систему управления более уязвимой.

Таким образом, на современном этапе развития основными «болевыми точками» являются системы управления и моральное состояние населения и армии противника, что породило в Соединенных Штатах новые концепции ведения войны, а именно «сетевой войны», «кибервойны» и «войны четвертого поколения». Рассмотрим данные концепции по отдельности.

«Сетевая война» и «кибервойна» являются довольно близкими терминами. Данные концепты ведения войны были предложены Дж. Аркиллой и Д. Ронфельдом в книге «В афинском лагере: подготовка к конфликтам информационной эры»[1].

Сетевая война определяется Дж. Аркиллой как завязанные на манипулирование информацией конфликты между народами или обществами. Сетевая война подразумевает под собой попытки уничтожения, повреждения или изменения информации цели о себе и положении в мире вокруг нее. Воздействие ведется прежде всего на мнение населения и/или элит. Воздействие ведется при помощи публичной дипломатии, пропаганды, психологических операций, политической и культурной подрывной деятельности, обмана или препятствия работе местных СМИ, инфильтрация компьютерных сетей и баз данных. Также в рамках данного конфликта могут использоваться военные методы, однако сетевая война не является «реальной войной» в ее традиционном понимании.

Кибервойна представляет собой проведение атак на вражеские информационные системы по управлению государством, экономикой и войсками, нарушению работы коммуникационных и информационных систем.

Р. Кларк, бывший советник Белого дома по безопасности, в своей книге «Кибервойна»[2] определяет данное как «действия одного национального государства с проникновения в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Однако, данное определение не совсем полное: не обязательно кибервойна будет вестить одним государством против

[1] Arquilla J., Ronfeldt D. Cyberwar is coming!/ In Athena's camp. Preparing for conflict in the information age. Ed. By J. Arquilla, D. Ronfeldt.— Santa Monica, 1997

[2] Clarke R.. Cyber War — HarperCollins, 2010

DOI: 10.7256/2305-560X.2014.1.10063

другого: известны случаи, когда кибератаки проводились негосударственными акторами, а именно независимыми группами хакеров (например, группа «Anonymous») либо же отдельными активистами. Стоит отметить, что на современном этапе развития Интернета, защита от кибератак является важной задачей: так, в своей статье «Обеспечение безопасности информационной магистрали»[1] Уэсли Кларк и Питер Левин приводят следующую статистику: «в 2007 г. было зарегистрировано почти 44 тыс. случаев злонамеренной киберактивности — это на треть больше, чем в предыдущем году, и более чем в 10 раз превышает уровень 2001 г.». Однако, кибервойна по отношению к информационным войнам имеет скорее вспомогательное значение, нежели основное: так, во время войны в Южной Осетии в 2008 году отдельные кибератаки силами активистов проводились на ряд грузинских сайтов, но в целом информационная война велась в СМИ и Интернете.

В дальнейшем теория кибервойны была интегрирована в концепцию сетецентрической войны, где первым (и, пожалуй, самым важным) является завоевание киберпространства путем уничтожения соответствующих структур и средств управления противника при защите своих и широкое использование информационных технологий в управлении войсками.

Четвертое поколение войн
(4 generation warfare)

Впервые данный термин появился в 1989 году, в статье «Изменяющееся лицо войны: 4 поколение»[2] за авторством коллектива военных США. Согласно их мнению, война на современном этапе ведется не только по схеме «государство-государство», но и «государство-неправительственный актор» с широким привлечением таких методов как терроризм, информационная и кибервойна. Война четвертого поколения ассиметрична; целью является не сколько силовое разрушение государства, сколько моральное разложение и смена или изменение моральных и культурных ценностей. Победа в такой войне невозможна чисто военными методами, что показывает опыт Иракской и Афганской операций или войны в Чеченской республике — требуется лишить негосударственного актора (допустим, террористическую группировку) поддержки местного населения, изменить отношение к противнику и «завоевать умы» мирового сообщества для лишения противника международной поддержки и получения поддержки для себя.

Подводя итог, стоит сказать, что во всех вышеуказанных концепциях важное место отводится не только военным способам ведения войны, сколько информационным и психологическим операциям, что означает необходимость вести исследования в данном направлении и интегрировать их в военные концепции государств для противостояния угрозам на современном этапе.

Информационные операции

В современной российской политической науке отсутствует общепринятое определение информационных войн, что вызывает некоторые трудности в исследовании данного явления. Определений одной информационной войны существует несколько десятков, причем зачастую они довольно сильно отличаются друг от друга. Если брать за основу разбор термина «информационная война» в русском языке, то можно вывести довольно широкую трактовку: информационная война — ограниченный по времени конфликт между государствами, ведущийся с помощью информационного оружия. Существует и второй подход — рассмотреть данный термин в английском языке (information warfare), калькой с которого является термин «информационная война» в русском языке. При переводе с английского возникает два значения information warfare: информационная война и информационное противоборство. Для данной работы более интересен термин «информационное противоборство», поскольку противоборство подразумевает под собой сочетание как агрессивных (характерных для войны), так и довольно нейтральных; противоборство может идти довольно длительное время (по мнению отдельных авторов, примером информационного противоборства является Холодная война) с разным уровнем интенсивности без применения вооруженных сил.

Организационно информационно-психологическая война, и как самостоятельное явление, и как средство сопровождения конфликта, состоит из последовательности специальных операций, делится на информационную и психологическую составляющую. Единая по замыслу операция прописывается по этим двум направлениям: психологическому, акцентирующему внимание на объект воздействия — индивидуальное, массовое сознание, и информационному, указывающему на инструменты воздействия, применяемые в такого рода операциях.

[1] Кларк У., Левин П. Обеспечение безопасности информационной магистрали.— М.: Россия в глобальной политике, 2010

[2] Lind W. S., Nightengale K., Schmitt J. F., Sutton J. W., Wilson G. I. The Changing Face of War: Into the Fourth Generation.— Marine Corps Gazette, October 1989

DOI: 10.7256/2305-560X.2014.1.10063

Стоит также отметить, что в западной литературе отмечается, что «информационная война» является публицистическим термином — военные данный термин не используют, заменяя его на термин «информационная операция». Данная замена выглядит довольно логичной, так как война представляет собой открытую конфронтацию двух государств (или аналогичный конфликт с участием негосударственных акторов), в то время как операция является довольно скоротечной и не ставит перед собой целью одержать полную победу над противником.

Информационная составляющая является важной частью информационной войны — именно по информационным каналам доводится психологическая составляющая, направленная на достижение нужных результатов.

Согласно «Объединенной доктрине информационных операций»[1], принятой в США в 1998 году, «информационная операция — это действия, предпринимаемые с целью затруднить сбор, обработку, передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем». Данное определение подходит больше к кибервойне и контрразведке, нежели к операциям информационной войны. В 1999 году данное упущение было исправлено и в руководящих документах НАТО информационная операция трактовалась как «действия, предпринимаемые с целью оказания влияния на принятие решений в поддержку собственных политических и военных целей путем воздействия на информацию, информационные процессы и системы управления противника, при одновременной защите собственной информации и информационных систем».

Отличие информационной операции от психологической заключается в разном подходе к информации и разных путях восприятия этой информации. Если целью информационных операций является манипулирование какой-либо информацией в целях захвата медиапространства, то целью психологической операции является изменение установок, мнения и симпатий при помощи информации, получаемой из медиапространства. Но, информационные и психологические операции довольно тесны переплетены и в итоге можно говорить о единых информационно-психологических операциях. Как показывает опыт войны в Ливии и Сирии, зачастую в целях информационной войны создается качественная дезинформация — например, заранее снимаются видеоролики, которые позже транслируются в эфир под видом новостных либо выкладываются в Интернет и создающаяся в результате шумиха может служить основанием для международных санкций и даже интервенции.

Информационные операции можно разделить на три больших группы (данное разделение было предложено полковником французской армии Жан-Люком Молине в статье ««La guerre de l›information vue par un opérationnel français»)[2]

Война за информацию: целью является получить информацию о средствах противника, возможностях и стратегии для того, чтобы защитить себя

Война против информации: задача состоит в одновременном защите собственных информационных систем и нарушением или уничтожением аналогичных систем противника

Война с помощью информации: путем дезинформации или хитрости ввести противника в заблуждение для достижения информационного доминирования.

Стоит отметить, что подобное деление включает в себя и кибервойну (война против информации), но при этом содержит важное разделение информационной политики на две составляющие: оборонительную и наступательную. Оборонительная (война за информацию) представляет собой разведдеятельность по сбору данных о возможностях потенциального противника в сфере информационных войн и стратегию их применения, что позволяет нейтрализовать угрозы для государства. Наступательная (война с помощью информации) ставит перед собой задачи одержать верх над противником путем дезинформации и хитрости, то есть при помощи манипуляции информацией.

Психологические операции

Психологическая борьба издревле была частью военного дела: так, еще древнеегипетские жрецы умели проводить «психологические операции» для поддержки своей власти в глазах населения. Однако, понятие психологической войны как средства обработки населения и армии, начало складываться только во время Первой Мировой войны и окончательно сложилось в конце Второй Мировой. Термин «психологическая война» ввел в оборот Поль Лайбаджер, назвав свою книгу «Психологическая война»[3], вышедшую в 1948 году. Постепенно термин

[1] Joint Pub 3–13 «Information Operations», DOD US, December 1998

[2] Moliner Jean-Luc La guerre de l'information vue par un opérationnel français.— L'Armement, No. 60, Dec. 1997-Jan. 1998

[3] Лайнбарджер. П. Психологическая война.— М.: 1962

DOI: 10.7256/2305-560X.2014.1.10063

«психологическая война» трансформировался в западной военной мысли в термин «психологическая операция» («psychological operation» или сокращенно psyop). В Советском союзе аналогом психологических операций являлась т.н. «спецпропаганда». В отличие от информационных операций, направленных на захват информационного пространства и информационное доминирование, перед психологическими операциями стоит задача по изменению мнения противника при помощи инструментов психологии.

Для начала необходимо выделить определение психологической операции. Согласно полевому уставу Армии США FM 33–1[1], психологические операции — это проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные враждебные, дружественные иди нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных национальных целей США. Психологические операции подразделяются на стратегические, оперативные и тактические.

Стратегические психологические операции осуществляются в интересах достижения долгосрочных целей, призванных создать благоприятную психологическую обстановку для ведения военных действий и проведения внешней и внутренней политики. Такие операции обычно носят глобальный характер.

Оперативные психологические операции осуществляются в интересах достижения среднесрочных целей, в поддержку военных кампаний и проводимой региональной политики. Объектом таких операций обычно является население определенного региона.

Тактические психологические операции осуществляются в интересах достижения краткосрочных целей, в поддержку командиров тактического звена. Объектом таких операций обычно является противостоящая группировка войск противника.

Задачей психологических операций является изменение в нужную сторону мнений, установок, мировоззрения, позиций населения и/или элит (культурных, политических, научных, военных, экономических) путем психологических манипуляций в различные временные отрезки и в количественно разных группах, но единых целей для всех уровней психологических операций нет. Если говорить про тактический уровень, то задачей является психологическое давление на подразделение противника с целью прекращения последним сопротивления, если рассматривать стратегический уровень — то задачей является изменение мнения целого народа с целью прекращения войны или же создания необходимой реакции для принятия политических решений. Поскольку нам наиболее интересны в рамках данной работы стратегический и оперативный уровень ввиду масштабности и возможности экстраполировать военный опыт на политическую сферу жизни общества (хотя зачастую в этом нет необходимости, т.к. зачастую оперативный и стратегический политический и военный уровень тесно переплетены). Если принять подобное ограничение, то можно сказать, что целью психологических операций является создание необходимого мнения или принятия какого-либо решения элитами объекта воздействия для достижения собственных политических, экономических и военных целей.

Заключение

В конце XX века огромное влияние приобрели компьютерные системы управления государством, Интернет и СМИ, что вкупе с переходом ядерного оружия из разряда тактических и стратегических вооружений в разряд «последнего довода» заставило военных крупных держав разрабатывать новые методы ведения войны, основываясь на опыте Второй Мировой и Холодной войны. Однако, на сегодняшний день, только Соединенным Штатам Америки удалось разработать полноценную теорию информационно-психологической войны и, более того, провести ряд испытаний и о встроить новые методы в военную концепцию; разработки в других странах (прежде всего, в Китае и в России) не привели к созданию единой концепции ведения информационно-психологической войны и на сегодняшний день и КНР, и РФ отстают от Соединенных Штатов в данном вопросе и не применяли собственные наработки комплексно для отражения атак на собственные информационные системы.

Концепция информационной войны включает в себя два крупных направления и одно «поднаправление», а именно: информационные операции, психологические операции и кибероперации. Использование термина «война» является не совсем корректным; более уместном в глобальном плане было бы применение термина «информационное противостояние», а при разборе отдельных операций наиболее удачным и научным является использование терминов «информационная операция», «психологическая операция» и «информационно-психологическая операция», однако проведение данной диверсификации по направлениям требует выработки

[1] Полевой устав армии США FM 33–1. Психологические операции.— М.: ГШ ВС СССР, 1988

DOI: 10.7256/2305-560X.2014.1.10063

определенной общепризнанной теории информационной войны в российском научном дискурсе.

Различия между информационными, психологическими и информационно-психологическими операциями проявляются в используемых методах. Основным инструментом информационных операций является, прежде всего, манипуляция информацией, дезинформация и технические методы борьбы с информационной инфраструктурой противника. К инструментам психологических операций относятся пропаганда, манипуляция общественным сознанием и отдельные акции воздействия. Однако, по отдельности на оперативном и стратегическом уровне информационные и психологические операции проводятся редко, поскольку для достижения поставленных целей приходится комбинировать и соединять методы информационных и психологических операций, что приводит к появлению такого вида операций как информационно-психологические, которые представляют собой отдельный тип операций; именно к термину «информационно-психологическая операция» с элементами кибервойны наиболее близко российское понимание информационной войны.

Библиография

1. Бернейс Э. М.: Пропаганда.— М., Hippo Publishing LTD, 2010
2. Бодрияр Ж. Симулякры и симуляция [эл. ресурс] http://simulacra-and-simulation.blogspot.com
3. Вепринцев В. Б., Манойло А. В., Петренко А. И., Фролов Д. Б.. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник.— М.: Горячая линия— Телеком, 2005.
4. Кара-Мурза С. Г. Манипуляция сознанием.— М.: Алгоритм, 2004.
5. Кларк У., Левин П. Обеспечение безопасности информационной магистрали.— М.: Россия в глобальной политике, 2010
6. Лайнбарджер. П. Психологическая война.— М.: 1962
7. Манойло А. В., 2003 г.: Государственная информационная политика в особых условиях, монография.— М.: Изд. МИФИ, 2003
8. Полевой устав армии США FM 33–1. Психологические операции.— М.: ГШ ВС СССР, 1988
9. Почепцов Г. Г. Психологические войны.— М.: «Рефл-бук», 2000
10. Arquilla J., Ronfeldt D. Cyberwar is coming!/ In Athena's camp. Preparing for conflict in the information age. Ed. By J. Arquilla, D. Ronfeldt.— Santa Monica, 1997
11. Arquilla J., Ronfeldt D. The emergence of noopolitik. Toward an American information strategy.— Santa Monica, 1999
12. Clarke R.. Cyber War — HarperCollins, 2010
13. Denning D. E. Information warfare and security.— Reading etc., 1999
14. Ehlers V.J Information warfare and international security — NATO Parliamentary Assembly, NATO PA. 45th annual session. Science and Technology Committee, STC, 1999
15. Lind W. S., Nightengale K., Schmitt J. F., Sutton J. W., Wilson G. I. The Changing Face of War: Into the Fourth Generation.— Marine Corps Gazette, October 1989
16. Libicki MC Conquest in cyberspace. National security and information warfare.— Cambridge, 2007
17. Moliner Jean-Luc La guerre de l'information vue par un opérationnel français.— L'Armement, No. 60, Dec. 1997-Jan. 1998,
18. Szafranski R. Neocortical warfare? The acme of skill / / In Athena's camp. Preparing for conflict in the information age. Ed. by J. Arquilla, D. Ronfeldt.— Santa Monica, 1997
19. Байректаревич А.. Future of Europe (of Lisbon and generational interval) // NB: Международные отношения.— 2013.— 4.— С. 16–26. URL: http://www.e-notabene.ru/wi/article_9399.html

References (transliterated)

1. Berneis E. M.: Propaganda.— M., Hippo Publishing LTD, 2010
2. Bodriyar Zh. Simulyakry i simulyatsiya [el. resurs] http://simulacra-and-simulation.blogspot.com
3. Veprintsev V. B., Manoilo A. V., Petrenko A. I., Frolov D. B.. Operatsii informatsionno-psikhologicheskoi voiny: kratkii entsiklopedicheskii slovar'-spravochnik.— M.: Goryachaya liniya— Telekom, 2005.
4. Kara-Murza S. G. Manipulyatsiya soznaniem.— M.: Algoritm, 2004.

DOI: 10.7256/2305-560X.2014.1.10063

5. Klark U., Levin P. Obespechenie bezopasnosti informatsionnoi magistrali.— M.: Rossiya v global'noi politike, 2010
6. Lainbardzher. P. Psikhologicheskaya voina.— M.: 1962
7. Manoilo A. V., 2003 g.: Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh, monografiya.— M.: Izd. MIFI, 2003
8. Polevoi ustav armii SShA FM 33–1. Psikhologicheskie operatsii.— M.: GSh VS SSSR, 1988
9. Pocheptsov G. G. Psikhologicheskie voiny.— M.: «Refl-buk», 2000
10. Arquilla J., Ronfeldt D. Syberwar is coming!/ In Athena's camp. Preparing for conflict in the information age. Ed. By J. Arquilla, D. Ronfeldt.— Santa Monica, 1997
11. Arquilla J., Ronfeldt D. The emergence of noopolitik. Toward an American information strategy.— Santa Monica, 1999
12. Clarke R.. Cyber War — HarperCollins, 2010
13. Denning D. E. Information warfare and security.— Reading etc., 1999
14. Ehlers V.J Information warfare and international security — NATO Parliamentary Assembly, NATO PA. 45th annual session. Science and Technology Committee, STC, 1999
15. Lind W. S., Nightengale K., Schmitt J. F., Sutton J. W., Wilson G. I. The Changing Face of War: Into the Fourth Generation.— Marine Corps Gazette, October 1989
16. Libicki MC Conquest in cyberspace. National security and information warfare.— Cambridge, 2007
17. Moliner Jean-Luc La guerre de l'information vue par un opérationnel français.— L'Armement, No. 60, Dec. 1997-Jan. 1998,
18. Szafranski R. Neocortical warfare? The acme of skill / / In Athena's camp. Preparing for conflict in the information age. Ed. by J. Arquilla, D. Ronfeldt.— Santa Monica, 1997
19. Bairektarevich A.. Future of Europe (of Lisbon and generational interval) // NB: Mezhdunarodnye otnosheniya.— 2013.— 4.— C. 16–26. URL: http://www.e-notabene.ru/wi/article_9399.html

DOI: 10.7256/2305-560X.2014.1.10063