УДК 32.019.51.57
ГРНТИ 81.93.29

ЦЕЛИ И ПОСЛЕДСТВИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ

С.В. ПОПОВА, кандидат экономических наук, доцент
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
В.Е. ФЕДОРИНОВ, доктор политических наук, профессор
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

В статье рассматриваются проблемы, связанные с формулировкой понятия «информационная война» отечественными и зарубежными исследователями, понимания ими целей информационной войны, признаки поражения в информационной войне.
Ключевые слова: информационная война; цели информационной войны; оружие информационной войны; победа в информационной войне; поражение в информационной войне.

PURPOSES AND EFFECTS OF THE INFORMATION WAR

S.V. POPOVA, Candidate of Economic Sciences, Associate Professor
MESC AF "N.E. Zhukovsky and Y.A. Gagarin Air Force Academy" (Voronezh)
V.E. FEDORINOV, Doctor of Political Sciences, Professor
MESC AF "N.E. Zhukovsky and Y.A. Gagarin Air Force Academy" (Voronezh)

The article deals with the problems associated with the wording of the concept of "information war" by domestic and foreign researchers, their understanding of the objectives of information warfare, signs of defeat in the information war.
Keywords: information war; information war aims; information warfare weapon; victory in information war; defeat in information war.

Введение. Явление информационной войны известно человечеству с древнейших времён. Возможность применения каких-либо сведений с целью дестабилизации ситуации, дезинформации противника и т.п. была известна человечеству давно. Из глубокой древности до нас дошли сведения о применении психологического воздействия на врага: запугивание, дезинформация, стремление успокоить или, наоборот, возбудить активность врага и т.д. Для этого активно использовались слухи, то есть недостоверная, но эмоционально насыщенная информация, активно влияющая на сознание людей.

Актуальность. В XX в. специальное и направленное использование информационных средств и технологий с целью воздействия на сознание людей и через него на содержание общественной ситуации в целом постепенно приняло форму особой войны, где средством поражения выступает «мягкое» информационно-психологическое оружие.

Сам термин «информационная война» появился в середине 1970-х годов, его автор – ученый-физик Т. Рон, который не только первым понял, но и научно обосновал, что именно информация является самым слабым звеном любой армии.

Понятие «информационная война» стало широко применяться в связи с бурным развитием информационных ресурсов, информационных и телекоммуникационных технологий, электронных средств массовой информации, которые в настоящее время рассматриваются как высокоэффективные средства для достижения превосходства в научно-технической, военной, политической, экономической, социальной и духовной сферах жизни общества. Информационные войны стали войнами «нового поколения», использующими специальное структурирование информации, организацию ее подачи, то есть, в конечном счёте – манипулирование информацией.

СОДЕРЖАНИЕ

Как любое оружие, технологии информационных войн могут применяться как во зло, так и на благо. Все зависит от того, с какой целью ведется информационная война:

- для самозащиты;
- для подготовки враждебных действий против другого государства.

В первом случае механизмы информационной войны помогают обществу и каждому отдельному человеку стабильно развиваться, становясь его надежной опорой в жизни, а во втором – приводят к полному социальному упадку и разрухе.

Для нас особую важность представляет тот факт, что современная информационная война может вестись постоянно, анонимно и незаметно, в любой точке информационного пространства, включая чужую территории. Объектом нападения здесь выступает культурное пространство противника, его сознание, и он долгое время может вообще не осознавать, что стал объектом нападения или управления извне. Все это обеспечивает значительную эффективность методов воздействия при минимизации потерь «агрессора», к тому же позволяя ему сохранять лицо мирного и цивилизованного государства.

Приемы информационных войн к XXI веку стали намного изощрённее, а потому опаснее в силу того, что специалисты, планирующие и осуществляющие информационные атаки, вооружены современными знаниями в области психологии и информационных технологий. Это позволяет им воздействовать на подсознание и таким способом управлять нашими поступками. То есть на смену приёмам давно известной традиционной пропаганде приходят психотехнологии, основанные на новейших достижениях психологических наук, отличающиеся высокой эффективностью информационного воздействия даже не на сознание, а на подсознание человека, который может и не осознавать не только цели воздействия, но и то, что оно вообще происходит.

Кроме психологической составляющей, информационная война может иметь другую важную сторону – техническую, связанную с противоборством в области поиска, выделения и соответствующей обработки необходимой для использования в противоборстве информации. Поэтому в современных условиях часто под информационной войной понимается состояние противоборствующих сторон, при котором осуществляется активное информационное воздействие на информационные ресурсы друг друга с целью получения определенного выигрыша в материальной и интеллектуальной сфере.

В литературе встречаются различные определения информационной войны, базирующиеся на понятиях «информационное оружие», «информационная пропаганда», «информационное воздействие», «информационная агрессия» и др.

С военной точки зрения термин «информационная война» в наше время был употреблен в середине 80-х годов XX в. в связи с новыми задачами Вооруженных сил США после окончания «холодной» войны. Это явилось результатом работы группы американских военных теоретиков. В дальнейшем термин начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г. в Ираке, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года [1], где он толковался как комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника [2].

Директор информационных войск Министерства обороны США В. Лакер определяет информационную войну несколько иным образом: «Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информационных систем» [3].

СОДЕРЖАНИЕ

По мнению специалистов поле действия информационных войн при таком определении оказывается достаточно широким и охватывает следующие области:

1) инфраструктуру систем жизнеобеспечения государства – телекоммуникации, транспортные сети, электростанции, банковские системы и т.д.;

2) промышленный шпионаж – хищение патентованной информации, искажение или уничтожение особо важных данных, услуг; сбор информации разведывательного характера о конкурентах и т.п.;

3) взлом и использование личных паролей VIP-персон, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;

4) электронное вмешательство в процессы командования и управления военными объектами и системами, «штабная война», вывод из строя сетей военных коммуникаций;

5) всемирная компьютерная сеть Интернет, в которой, по некоторым оценкам, действует большое количество военных компьютеров, и подавляющее количество военных линий связи проходят по открытым телефонным линиям [4].

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую врагом, косвенно, путем восприятия, они и атаковали информацию врага косвенно. Для того, чтобы хитрость была эффективной, враг должен был сделать три вещи: наблюдать обманные действия, посчитать обман правдой, действовать после обмана в соответствии с целями обманывающего. В целом, эти же цели должны достигаться и в современных условиях, но уже в соответствии с современными способами получения и обработки информации.

С точки зрения специалистов, в современных условиях выделяются следующие цели информационной войны:

1) контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация);

2) использовать контроль за информацией для ведения информационных атак на врага;

3) повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

То есть на первый взгляд информационная война – это применение технических устройств и предоставляемых ими возможностей для беспрепятственного использования информационных ресурсов «своими» и препятствование их использования условными «чужими», врагами в военных целях. Но, например, специалисты американского Института компьютерной безопасности считают, что информационная война нацелена на мировую экономику. А потому, в Университете национальной обороны в Вашингтоне создана специальная группа студентов с целью подготовки специалистов по ведению компьютерной войны. Оружием в этом случае становятся компьютеры, с помощью которых на расстоянии можно вывести из строя неприятельские коммуникации, манипулировать средствами информации и связи, разрушать финансовые системы [4].

Следовательно, цели информационной войны в таком понимании совершенно иные, нежели войны в «традиционном» понимании: не физическое уничтожение противника и ликвидация его вооруженных сил, не уничтожение важных стратегических и экономических объектов, а широкомасштабное нарушение работы финансовых, транспортных, коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и подчинение населения атакуемой страны воле страны-победителя. Более того, в эпоху информационных войн планы боевых операций разрабатываются военными вместе с гражданскими специалистами, причем нередко последние играют ведущую роль в этом. То есть армия вынуждена вначале овладевать новыми информационными технологиями, а уже потом изыскивать пути их использования.

В этом случае главной целью информационной войны является получение не только политического и военного, но и экономического и социального выигрыша за счет принуждения противной стороны принять решение, соответствующее намерениям другой стороны.

Для достижения своих целей противоборствующие стороны активно используют весь арсенал средств, которые способны воздействовать на информационный и интеллектуальный ресурс противной стороны и позволяют манипулировать данными и знаниями. Информационная война в таком понимании – это всеобъемлющая, целостная стратегия, призванная отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов не только вооруженными силами, но и реализации национальной политики в целом. В этом случае в целях информационная война будет нацелена на все возможности и факторы уязвимости, которые неизбежно возникают в условиях возрастающей зависимости от информации, а также на использовании информации (и возможности манипуляции ею) в конфликтах. Объектом внимания становятся информационные системы, включая линии передач данных, обрабатывающие центры и человеческие факторы этих систем, а также информационные технологии, используемые в системах вооружений.

Как и традиционная война, информационная война имеет наступательные и оборонительные составляющие, но начинается с целевого проектирования и разработки своей «архитектуры командования, управления, коммуникаций, компьютеров и разведки, обеспечивающей лицам, принимающим решения, ощутимое информационное превосходство во всевозможных конфликтах». Как видим, это определение практически не затрагивает содержательных аспектов, а направлено на техническое обеспечение информационной составляющей армии. Таким образом, информационная война – только средство, а не конечная цель.

Тем не менее, оружие информационной войны уже «стреляет»: достаточно часто средства массовой информации сообщают о состоявшихся хакерских атаках банки, офисы крупных фирм, государственные учреждения и т.д. Современная практика показывает, что в условиях ведущихся военных действий атаки информационных ресурсов противника – обычное дело, как например, попытки проникнуть в системы безопасности водоочистной системы Донецка со стороны Украины или взлом сайта руководителя ДНР А. Захарченко с искажением размещённой на нём информации [5], хакерская атака на пенсионный фонд ДНР и др. [6].

Результатом «боёв» информационной войны должно, по мнению специалистов, стать изменение расстановки сил в обществе, снижение готовности населения страны-противника активно сопротивляться врагу. Гораздо дешевле не убивать солдат врага, рискуя жизнями своих военнослужащих, а убедить врагов сдаться без сопротивления. В современных условиях это «война за знания – за то, кому известны ответы на вопросы: что, когда, где и почему и насколько надежными считает отдельно взятое общество или армия свои знания о себе и своих противниках» [7] с целью использовать это знание для достижения своей победы. Следовательно, в ходе информационной войны надо иметь способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое [8]. Тем самым война выводится из сферы прямых силовых столкновений и переводится главным образом в сферу противоборства информационных систем, способных как получать «чужую» информацию, так и защищать «свою».

Встаёт вопрос – какое состояние общества соответствует поражению в информационной войне? Специалисты считают, что поражение в ней характеризуется рядом признаков, присущих поражению в обычной войне:

1) гибель и эмиграция части населения;
2) разрушение промышленности и выплата контрибуций;
3) потеря части территории;
4) установление политической зависимости от победителя;
5) полный роспуск, многократное сокращение армии или запрет на собственную армию;
6) вывоз из страны наиболее перспективных и наукоёмких технологий.

Одновременно для информационной системы общества, проигравшей информационную войну, это означает:

1) сокращение информационной ёмкости системы, гибель элементов и подструктур, что делает её безопасной для победившей стороны;

2) включение информационной системы проигравшей стороны в решение задач в интересах победителя, который определяет входные данные;

3) информационная система проигравшей стороны поглощается структурой победителя и начинает работать в его интересах.

То есть особой разницы для страны, проигравшей войну – обычную или информационную – в целом нет. Но проблема для проигравшей стороны усугубляется тем, что информационная война не имеет финала – нет причин, по которым агрессор прекратил бы свое воздействие на жертву.

Кроме того, ведение информационной войны искажает реальность в массовом общественном сознании, а ее результат может существенно отличаться от итогов вооруженного столкновения. То есть, если одна из сторон конфликта может понести военное поражение, то в информационной сфере она же может считаться победителем, рассчитывать на благоприятное общественное мнение различных стран и международных организаций, которые сами не участвуют в этом конфликте. Так, специалисты отмечают, что в августе 2008 года, пока Россия не вмешивалась в ход грузино-осетинского конфликта, большинство мировых СМИ писали именно о нападении Грузии на Южную Осетию, не привязываю каким-либо образом к событиям Россию. Но с началом входа в Южную Осетию войск РФ Грузия начинает информационную атаку на Россию и те же СМИ обвиняют Россию в агрессии против Грузии. То есть журналисты этих изданий не видят ничего дурного в том, чтобы фактически моментально диаметрально изменить точку зрения на одно и то же событие.

В целом, специалисты приходят к выводу, что Россия в 2008 г. оказалась неготовой к массированной информационной агрессии противника, и, одновременно делают вывод о том, что в информационном противостоянии наша страна выступала в одиночестве, в то время как Грузия действовала в ней единым фронтом с США, НАТО, Евросоюзом. Даже сам факт своего военного проигрыша Грузии для России стал поражением, поскольку информационная война, точнее, победа в ней, имеет совершенно конкретный, денежно выражаемый результат. Так, электронный вестник «Государственное управление» показал, что «отток иностранного капитала из России в результате войны [*с Грузией – авт.*] составил около $7 млрд., российские компании испытывают серьезные затруднения на фондовом рынке, многим из них пришлось отложить выход на IPO на неопределенный срок. Позиции рубля по отношению к доллару заметно пошатнулись. Кроме того, Россия испытывает серьезные затруднения в политико-дипломатических отношениях с рядом государств, международных режимов и организаций: ВТО, G8 и другими. Для России обострились угрозы размещения американской ПРО на территории Польши, а также вступления Грузии в блок НАТО» [9].

Компьютер и средства глобальной телекоммуникации изменили наш мир – оперировать информацией стало быстрее, проще и дешевле, чем оружием (что не отменяет возможного применения этого оружия, но угроза применения иногда эффективнее, чем само применение). При этом следует не забывать о чисто технической составляющей проблемы: качественная работа с информацией требует современной высокопроизводительной аппаратуры, качественного программного обеспечения, высококвалифицированного персонала, знакомого с последними достижениями науки, что, естественно, требует больших финансовых затрат. В то же время, страна, рассчитывающая на результативное участие в информационной войне, не должна останавливаться перед этими расходами.

Таким образом, мы подходим к вопросу о возможности противостоять угрозам информационной войны. Государство может эффективно себя защищать в сфере информационного противоборства, но с соблюдением одного обязательного условия – эта защита должна быть актив-

СОДЕРЖАНИЕ

ной, с применением всех средств информационного воздействия, с выявлением всего спектра внешних и внутренних врагов, наращивая мощности информационных систем, выявляя и используя сильные и слабые стороны противника. Поэтому, без сомнения, в текущей ситуации необходимо восстанавливать тот богатый опыт спецпропаганды, который накопила наша страна в ходе вооружённых конфликтов и войн.

Выводы. Человечество стоит на пороге постиндустриальной, информационной эры, что существенно изменило давно свойственные человечеству информационные взаимодействия. С одной стороны, давно известные методы пропаганды активно используются и сегодня, но в современных условиях происходит переход к информационно-психологической войне. Широкое внедрение информационных технологий, использование новейших технических изобретений даёт возможность широчайших манипуляций информацией в военных целях. В то же время, широкая общественность зачастую не воспринимает факт, что информационные войны уже активно ведутся, причём не единичными хакерами-любителями, стоящими вне закона или популярными блогерами-энтузиастами, а на государственном уровне и для достижения целей государств.

СПИСОК ЛИТЕРАТУРЫ

1. Черноморский флот-2017. Досье – Информационная война URL http://flot 2017. com/item/file/15444

2. Дела давно минувших дней №4. Информационная война: история, день сегодняшний и перспектива URL https://cont.ws/@exelenc/530654

3. Персональный сайт Николая Баранова. Курс «Информационная война в системе политических отношений». Лекция 1. Предмет и особенности учебного курса URL http://nicbar.ru/politology/study/kurs-informatsionnaya-vojna-v-sisteme-politicheskikh-otnoshenij/108-lektsiya-1-predmet-i-osobennosti-uchebnogo-kursa

4. Что такое информационная война? История термина «информационная война» URL http://pandia.ru/text/77/425/15462.php

5. Сайт «Прямой линии» Главы ДНР подвергся хакерской атаке URL http://s mdnr.ru/sajt-translyacii-pryamoj-linii-glavy-dnr-podvergsya-xakerskoj-atake/;

6. Хакерская атака на пенсионный фонд ДНР URL http://novorossia-tv.ru /news/ nrus/khakerskaya-ataka-na-pensionnyy-fond-dnr-/

7. Информационная война URL http://poznayka.org/s68642t1.html

8. Информационная война. Глава 13(8). Последствия информационной войны URL http://bookap.info/psywar/infowar/gl25.shtm

9. Михайленко Т.А. Особенности информационной войны в современном мире. На примере грузино-южноосетинского конфликта в августе 2008 года // Государственное управление. Электронный вестник Выпуск № 19. Июнь 2009 г. URL http://e-journal.spa.msu.ru/uploads/vestnik/2009/vipusk__19._ijun_2009_g._/mikhaylenko.pdf

REFERENCES

1. CHernomorskij flot-2017. Dos'e – Informatsionnaya vojna URL http://flot 2017. com/item/file/15444.

2. Dela davno minuvshikh dnej № 4. Informatsionnaya vojna: istoriya, den' segodnyashnij i perspektiva URL https://cont.ws/@exelenc/530654.

СОДЕРЖАНИЕ

3. Personal'nyj sajt Nikolaya Baranova. Kurs «Informatsionnaya vojna v sisteme politicheskikh otnoshenij». Lektsiya 1. Predmet i osobennosti uchebnogo kursa URL http://nicbar.ru/politology/study/kurs-informatsionnaya-vojna-v-sisteme-politicheskikh-otnoshenij/108-lektsiya-1-predmet-i-osobennosti-uchebnogo-kursa.

4. CHto takoe informatsionnaya vojna? Istoriya termina «informatsionnaya vojna» URL http://pandia.ru/text/77/425/15462.php.

5. Sajt «Pryamoj linii» Glavy DNR podvergsya khakerskoj atake URL http://s mdnr.ru/sajt-translyacii-pryamoj-linii-glavy-dnr-podvergsya-xakerskoj-atake.

6. KHakerskaya ataka na pensionnyj fond DNR URL http://novorossia-tv.ru /news/ nrus/khakerskaya-ataka-na-pensionnyy-fond-dnr-/

7. Informatsionnaya vojna URL http://poznayka.org/s68642t1.html.

8. Informatsionnaya vojna. Glava 13(8). Posledstviya informatsionnoj vojny URL http://bookap.info/psywar/infowar/gl25.shtm.

9. Mikhajlenko T.A. Osobennosti informatsionnoj vojny v sovremennom mire. Na primere gruzino-yuzhnoosetinskogo konflikta v avguste 2008 goda // Gosudarstvennoe upravlenie. EHlektronnyj vestnik Vypusk № 19. Iyun' 2009 g. URL http://e-journal.spa.msu.ru/uploads/vestnik/2009/vipusk__19._ijun_2009_g._/mikhaylenko.pdf.

Попова Светлана Владимировна, кандидат экономических наук, преподаватель кафедры гуманитарных и социально-экономических дисциплин, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, svpbravo@mail.ru

Федоринов Вадим Евгеньевич, доктор политических наук, профессор, профессор кафедры гуманитарных и социально-экономических дисциплин, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, vadtek@vmail.ru