I. ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО. АКТУАЛЬНЫЕ ПРОБЛЕМЫ. ТЕОРИЯ

УДК 517.929

© Раскин А. В., Тарасов И.В.
Raskin A., Tarasov I.

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В СОВРЕМЕННОЙ ВОЙНЕ

INFORMATION ANTAGONISM IN MODERN WAR

Аннотация. *В статье рассмотрены подходы военно-политического руководства США к определению информационного противоборства. Показано, что на современном этапе информационное противоборство стало составной частью национальной безопасности любого государства. Особое внимание уделяется анализу информационному противоборству первого и второго этапа, а также трансформации его форм. Исследуются основные виды информационных войн.*

Annotation. *In article approaches of the military-political leadership of the USA to definition of information antagonism are considered. It is shown that at the present stage information antagonism became a component of national security of any state. The special attention is paid to the analysis to information antagonism of the first and second stage, and also transformation of its forms. Main types of information wars are investigated.*

Ключевые слова. *Информационное противоборство, психологическая война, кибервойна, сетевая война.*

Key words. *Information antagonism, war of nerves, cyberwar, netwar.*

Информационная война – это
целенаправленное обучение врага тому,
как снимать панцирь с самого себя.
Притча о Черепахе.

Информационное противоборство (манипулирование информацией) не является чем-то новым для человеческой цивилизации. Ещё античные авторы в подробностях повествуют об изощрённых агитационных кампаниях, при помощи которых политики древности пытались деморализовать своих противников, ввести их в заблуждение, заставить подчиниться своей воле.

В современном мире информация играет важную роль в жизни не только общественных и государственных институтов, но и каждого человека. В настоящее время понятие «информация» присутствует во всех сферах знания человечества: философии, экономики, науке и техники. Очевидно, что нынешний век является веком информационных технологий. Информатизация ведет к созданию единого мирового информационного пространства, создаваемого информационными и телекоммуникационными системами, которые стали неотъемлемыми компонентами систем управления государством, экономикой, финансами и обороной. Однако необходимая степень информатизации может быть достигнута только при условии высокого научно-технического и промышленного потенциала, а также соответствующего культурно-образовательного уровня общества.

Очевидно, что чем большими информационными возможностями обладает одна из взаимодействующих (противодействующих) сторон, тем эффективнее она достигает своих целей. В то же время, страны – аутсайдеры процесса информатизации могут оказаться в условиях социальной и экономической нестабильности. Подобная ситуация может привести к противостоянию развитых государств и остального мира. Именно поэтому в эпоху многополярного мира ведущие зарубежные страны используют технологии информационного противоборства для достижения мирового господства. Сегодняшние события на Украине яркий тому пример.

Проведенный анализ войн и вооруженных конфликтов убедительно показывает, что информационная инфраструктура противника является одной из основ-

Раскин Александр Владимирович – доктор военных наук, начальник отдела Командования Войск Воздушно-космической обороны, тел. 8-(495)–333-93-20;
Тарасов Игорь Викторович – кандидат технических наук, доцент, ведущий научный сотрудник, ФКГУ «4 ЦНИИ МО РФ».

Raskin Alexander –Doctor of Military Science, head of the division of Command of the Air and space defense Forces, tel. 8-(495)–333-93-20;
Tarasov Igor – Cand.Tech.Sci., the senior lecturer, the leading research assistant, FKGU «4 TSNII MO the Russian Federation.»

ных целей при ведении боевых действий, а сторона, проигравшая информационное противоборство, неизбежно терпит поражение не только в современной высокотехнологической войне, но и в локальных вооруженных конфликтах.

В этой связи информационная безопасность становится неотъемлемой частью национальной безопасности любого государства, а информационное противоборство составной частью вооруженной борьбы.

В настоящее время ведущие государства мира уделяют большое внимание развитию теории и практики информационного противоборства, созданию сил и средств информационной борьбы.

Термин «информационная война» впервые был использован в директиве министра обороны США от 21 декабря 1992 года DOD S 3600.1. Здесь данное понятие употреблялось в узком смысле слова и рассматривалось как разновидность радиоэлектронной борьбы. В январе 1995 года корпорации RAND получила заказ на проведение исследования по определению роли и места информационного противоборства (ИП) в национальной военной стратегии США. Результаты этих работ были изложены в отчетах MR-661-OSD «Strategic information Warfare. A new face of War» (1996 год), MR-963-OSD «The Day After ... in the American Strategic infrastructure» (1998 год) и MR-964-OSD «Strategic information Warfare Rising» (1998 год) [1]. В них впервые появился термин – «стратегическая информационная война (информационное противоборство)», которая определялась как война с использованием государственного глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и укрепления влияния на собственный информационный ресурс.

В отчете MR-661-0SD указывалось, что вызванные быстрыми темпами информатизации общества изменения в политической жизни ряда государств ведут к пересмотру геополитических взглядов военно-политического руководства, к возникновению новых стратегических интересов (в том числе и в информационной сфере), следствием чего является изменение политики, проводимой этими странами. Авторы подчеркивают, что, учитывая определение войны, данное Клаузевицем («война – это продолжение политики другими средствами»), глобальные противоречия требуют новых средств и методов их решения – стратегического информационного противоборства.

Ключевым понятием, введенным в отчете MR-964-OSD, является деление стратегической информационной войны на первое и второе поколение. Стратегическое ИП первого поколения включает в себя основные методы информационной войны, которые США реализуют в настоящее время и от которых не планирует отказываться в ближайшем будущем.

Информационная война (противоборство) второго поколения в перспективе может привести к полному отказу от использования военной силы. По нашему мнению, речь идет о воздействии на процесс принятия решения противником с целью заставить его действовать в соответствии с замыслом воздействующей стороны. В конечном итоге сторона – агрессор может добиться от противника полного отказа от достижения своих целей.

В настоящее время в США действуют полевые уставы 100-6 «Информационные операции», 33-1 «Психологические операции», 31-20 «Операционная техника специальной борьбы» [1]. Для ведения ИП Пентагон осуществляет подготовку специалистов в области информационного противоборства как в военно-учебных заведениях Минобороны, так и в гражданских учебных заведениях.

В общем виде информационное противоборство можно определить как борьбу в информационной сфере, представляющую собой деструктивное воздействие на когнитивную сферу ЛПР, информацию, циркулирующую в различных информационных системах, на сами информационные системы и информационную инфраструктуру противодействующей стороны, а также защиту когнитивной сферы ЛПР, собственной информации и информационной инфраструктуры от подобного воздействия.

В широком смысле под информационным противоборством следует понимать борьбу сторон за достижение превосходства над противником в своевременности, достоверности, полноте получения информации, скорости и качестве ее переработки и доведении до исполнителей.

По мнению американских специалистов, ИП представляет собой не просто вид обеспечения операций вооруженных сил путем нарушения процесса управления войсками, радиоэлектронного подавления, морально-психологического воздействия и так далее, но имеет более глобальное значение. Основное – это внедрение в сознание населения противостоящей стороны своих ценностных ориентиров. Например, в результате попытки внедрения в сознание россиян прозападных русофобских идей Запад сумел извлечь из информационной войны против России ряд выгод, таких как приобретение природных ресурсов по заниженным ценам; господство на российском рынке; податливость во внешней политике; отток из России интеллектуальной элиты; одностороннее разоружение России и так далее.

Для анализа сферы информационного противоборства в данном ракурсе особый интерес представляют высказывания бывшего директора ЦРУ Аллена Даллеса, произнесенные им сразу после окончания Великой Отечественной войны: «Мы бросим все, что имеем, все золото, всю материальную мощь и ресурсы на оболванивание, и одурачивание людей... Посеяв в России хаос, мы незаметно подменим их ценности на фальшивые... Мы найдем своих единомышленников, своих помощников и союзников в самой России. Эпизод за эпизодом будет разыгрываться грандиозная трагедия гибели самого непокорного на земле народа, окончательного угасания его самосознания... Литература, театр, кино – все будет изображать и прославлять самые низменные человеческие чувства. Мы будем всячески поддерживать и поднимать так называемых художников, которые станут насаждать и вдалбливать в сознание культ секса, насилия, садизма, предательства – словом, всякой безнравственности. В управлении государством мы создадим хаос, неразбериху. Мы будем незаметно, но активно и постоянно способствовать самодурству чиновников, взяточников, беспринципности. Честность и порядочность будут осмеиваться и станут никому не нужны, превратятся в пережиток прошлого. Хамство и наглость, ложь и обман, пьянство и наркомания, животный страх друг перед другом и беззастенчивость, предательство, национализм и вражда народов, прежде всего вражда и ненависть к русскому народу, – все это мы будем ловко и незаметно культивировать... Мы будем расшатывать, таким образом, поколение за поколением... Мы будем драться за людей с детских, юношеских лет, будем всегда главную ставку делать на молодежь, станем разлагать, развращать, растлевать ее. Мы сделаем из них космополитов». Что-то добавить к сказанному трудно. Именно такая «незаметная, кропотливая» работа привела к развалу Советского Союза, хаосу девяностых годов прошлого века, братоубийственным войнам в республиках бывшего СССР. Результаты этой деятельности мы наблюдаем на Украине сегодня, где культивирование среди молодежи национализма и вражды народов, прежде всего вражды к русскому народу, дало свои результаты.

В широком смысле слова целью ИП является завоевание и удержание превосходства в информационной сфере путем информационного воздействия (ИВ). Она является частью идеологической борьбы.

Главная задача ИП заключается в манипулировании сознанием людей. Цель такой манипуляции заключается в следующем:

• навязывании общественному и индивидуальному сознанию чуждых идей и взглядов;

• дезориентации и дезинформации населения;

• раскачивании убеждений, устоев государства;

• запугивании своего народа образом врага;

• демонстрации противнику своего могущества.

Объектами ИП могут выступать:

• процесс принятия решения, через когнитивную сферу ЛПР;

• информационные системы и информационная инфраструктура.

К воздействиям на первый тип объектов ИП можно отнести когнитивное и информационно-психологическое воздействие. При этом информационно-психологическое воздействие производится по социуму государства, подвергшегося нападению. Оно «переворачивает» массовое сознание населения и вооруженных сил – патриотизм заменяется на космополитизм, способность поставить общественное выше личного на потребительскую идеологию.

Когнитивное воздействие осуществляется по ЛПР и специалистам, обеспечивающих процесс принятия решения (в условиях вооруженной борьбы на офицеров органов военного управления). Его целью является подмена их идеологических ориентиров, деквалификация, что приводит к воздействию на механизм принятия решений.

К воздействиям на второй тип объектов ИП можно отнести поражение информационно-технических систем (систем связи, телекоммуникационных систем, систем передачи данных, радиоэлектронных средств, систем защиты информации и т. д.). Это может быть как программно-математическое воздействие, так и физическое уничтожение информационных систем.

Очевидно, что при трансформации ИП происходит изменение ее форм. На рис. 1 показаны формы ИП первого и второго поколения.

На рис. 2 показаны виды информационных войн.

Конечно, назвать ИП информационной войной можно весьма условно. В отличие от классической войны информационная война ведется во все периоды военно – политической обстановки. Она не имеет основного атрибута войны – вооруженной борьбы. Вооруженная борьба ведется оружием. Информационная война ведется информационным оружием, определение которого сегодня не определено однозначно. Поэтому представляется более корректным употреблять термин информационное противоборство.

Раскроем некоторые виды информационных войн.

Психологическая война – это совокупность це-

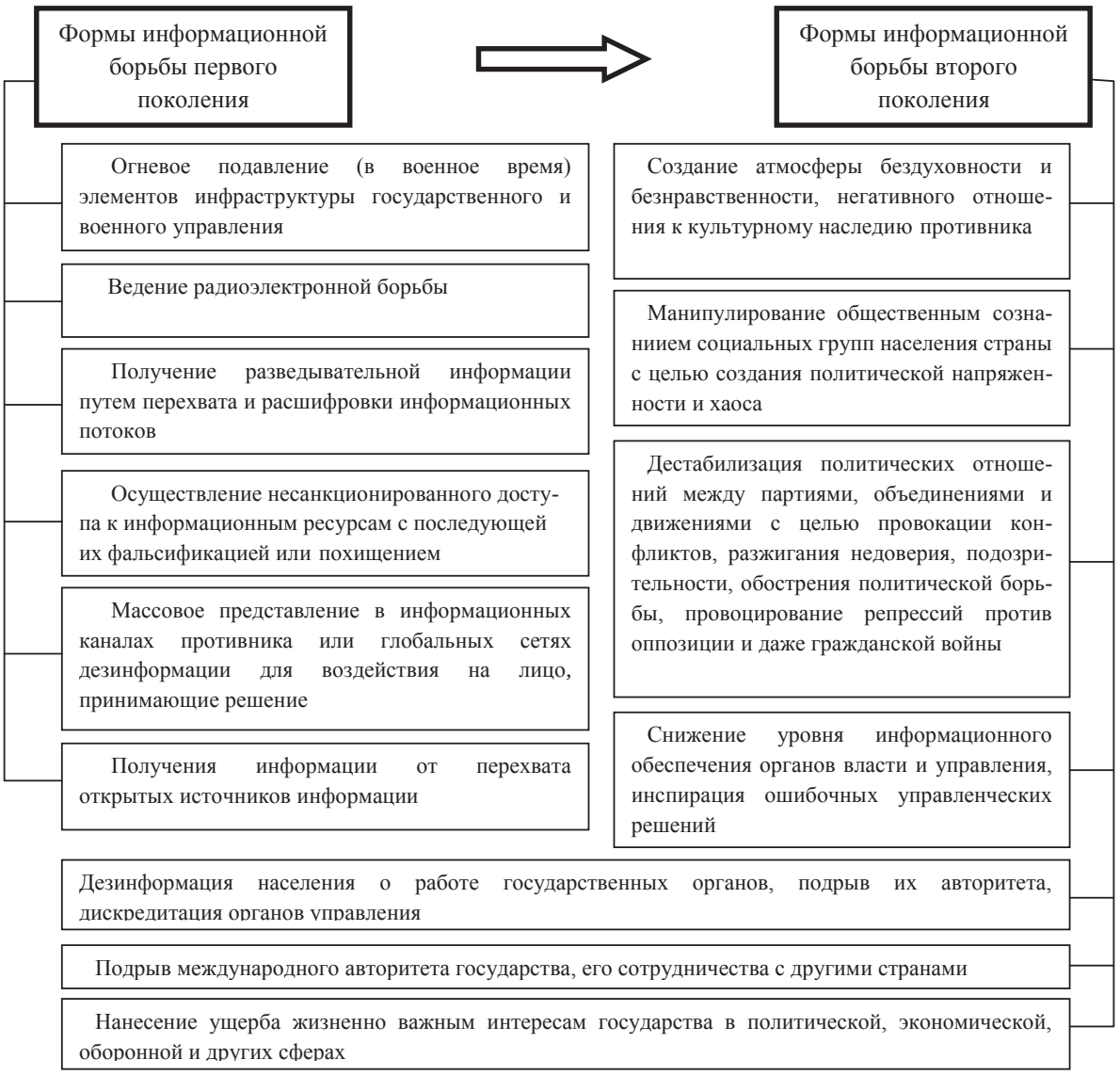

Рис. 1. Трансформация форм информационной борьбы

Рис. 2. Виды информационных войн

ленаправленных, проводимых по единому замыслу действий, направленных на пропагандистское, экономическое, дипломатическое давление, проведение разведывательно-диверсионных актов, провокаций, маневров вооруженных сил и локальных вооруженных операций, рассчитанных на воздействие на сознание и поведение населения и военнослужащих противодействующего государства.

Кибервойна (от англ. *Cyber-warfare*) — компьютерное противостояние в пространстве Интернета. Имеет целью нарушение функционирования компьютерных систем и доступа к Интернету государственных учреждений, финансовых и деловых центров, а также создание хаоса в жизни населения стран, которые используют Интернет в повседневной жизни. Кибервойна может являться продолжением межгосударственных отношений в виде пропаганды, шпионажа и непосредственных атаках на компьютерные системы и серверы.

Термин «кибервойна» может звучать следующим образом — использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информацион-

ной безопасности и суверенитету другого государства».

Появление термина «*сетевая война*» стало также возможным благодаря информационной эпохе и информационным технологиям.

Согласно определению Пентагона, сетецентричная война (СЦВ) направлена на перевод информационного преимущества по средствам информационных технологий в боевое превосходство географически распределенных сил и средств.

Цели СЦВ состоят в преобразовании военной структуры в такую конфигурацию, которая сделает войска наиболее эффективными: они будут более оперативными; рассредоточенными; понизят коэффициент смертности, в то же время уменьшая зависимость от применения оружия; будут иметь возможность предвидеть, а также интегрировать новые технологии в сеть для производства информации и получения преимущества в скорости по сравнению с будущими оппонентами [2].

Средствами ведения информационной войны могут быть: компьютерные вирусы; «логические бомбы», «программы-оборотни», «программы-убийцы информации»; программы несанкционированного доступа к информационным ресурсам противника с целью завладения разведывательной информацией; средства подавления информационных систем противника; биотехнологические средства; средства внедрения вирусов, логических бомб, программ-оборотней, программ-убийц информации, программ воздействия на персонал («зомбирование») и другие.

Таким образом, приведенные выше определения «информационного противоборства», «информационной войны» не являются универсальными. Дело в том, что полномасштабных информационных войн, изучая которые можно вывести стройную теорию, было очень мало. Поэтому пока не существует единого, всеми признанного определения этого понятия. В одних исследованиях понятие информационной войны дается слишком широко. Например, «информационная война – это стратегия, операции, тактические действия, проводимые в мирное время, во время кризиса, конфликта, войны, в период восстановления мира между соперниками, конкурентами, врагами с использованием современных информационных технологий, чтобы достигать своих целей». Очевидно, что это определение слишком многозначно, так как предполагает почти все виды человеческой деятельности. Другие определения информационной войны, наоборот, слишком ограничены, они рассматривают какой-то узкий аспект, называя, например, информационной войной только компьютерные преступления. В качестве базового определения представляется удобным использовать определение Г. Почепцова: «Информационная война – коммуникативная технология по воздействию на массовое сознание с кратковременными и долговременными целями. Целями воздействия является внесение изменений в когнитивную структуру, чтобы получить соответствующие изменения в поведенческой структуре» [3].

Очевидно, что информационная война это война нового типа, ее объектом является сознание людей. Она основана на возможности управления и манипулирования общественным сознанием, подчинения воли человека. Это чаще всего происходит неосознанно для тех, кто подвергается информационно-психологическому воздействию

Дальнейшее развитие теории информационного противоборства, на наш взгляд, должно проводиться в направлении дальнейшего формирования понятийного аппарата, вскрытия законов и закономерностей информационной борьбы, а также принципов его ведения.

Литература.
1. Антонович П. Ключевые аспекты информационной войны/ Армейский сборник. - №1, 2014.
2. Tisserand III J. Network Centric Warfare Case Study. US. V Corps and Third Infantry Division during Operation Iraqi Freedom Combat Operations (Mar-Apr 2003). US. Army War College. Carlisle, 2006. P. 175.
3. Почепцов Г.Г. Информационные войны. – М., 2000. – С.20.

Материал поступил в редакцию 17. 08. 2014 г.