МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Кафедра истории и правового регулирования массовых коммуникаций

КУРСОВАЯ РАБОТА

ИНФОРМАЦИОННАЯ ВОЙНА ЗАПАДНЫХ СМИ. ПУТИ РЕАЛИЗАЦИИ В СОВРЕМЕННОМ МИРЕ

Работу выполнил _____ Сарандук Н.С.

Факультет Журналистики

Направление 42.04.02 «Журналистика» (Правовая проблематика)

Научный руководитель
д.ф.н., профессор _____ А.В. Осташевский

Нормоконтролер
д.ф.н., профессор _____ А.В. Осташевский

Краснодар 2018

Содержание

Введение

Актуальность исследований в области информационных войн (ИВ), многогранность форм и методов этой работы в научном и практическом планах определяется тем, что сегодня любая страна мира нуждается в создании эффективной системы государственного противодействия операциям информационно-психологической войны (ИПВ). Не секрет, что в наше время многие государства рассматривают информационную войну как эффективный инструмент реализации внешней политики.

Информационно-психологическая война позволяет оказывать интенсивное воздействие на различные процессы практически на всех уровнях государственного и общественного устройства в любой стране или регионе.

Совокупность проблем в данной области объясняется несоответствием между объективной потребностью в создании такой системы и низкой степенью готовности современного общества оказывать активное сопротивление любым попыткам манипулирования общественным сознанием. Дело в том, что в массовом сознании граждан еще не совсем сформировалось понимание той угрозы, которую могут нести современные коммуникационные технологии при их скрытом информационно-психологическом воздействии. Особенно если использовать их в политических целях.

Еще одним нерешенным противоречием ИПВ является то, что при информационном противоборстве используются те же новейшие коммуникационные технологии и базовые элементы и способы коммуникации, что и в других социальных процессах. Таким образом, целенаправленное информационно-психологического воздействие НКТ на человека является разновидностью социальных отношений, в чем, по нашему мнению, таится особая опасность. ИВ приобретает все более скрытые формы.

Существует также еще одна проблема, мотивирующая наше

исследование. Речь идет о несоответствии темпов развития специальных технологий информационно-психологической агрессии и технологий психологической защиты сознания, системы ценностей и психического здоровья общества.

Целью данной работы является наиболее полное раскрытие значения новейших коммуникационных технологий при противостояниях и конфликтах в современном обществе с анализом их использования и применения в качестве оружия современных информационных войн.

Объектом исследования являются комплексные информационные потоки, представляющие основу такого явления как современные информационные войны.

Предметом изучения являются новейшие коммуникационные технологии используемые в качестве средства ведения информационных войн в современном обществе.

Для достижения поставленной в работе цели определяются следующие задачи:

1. Определить сущность понятия "информационная война".
2. Выявить способы применение НКТ как средства ведения информационной войны.
3. Изучить "линии фронта" информационной войны. В первой главе "Информационная война: истоки, виды и цели информационного противоборства" мы решаем первую задачу: даем определение информационным войнам, формулируем их основные цели, описываем способы ведения и виды, приводим примеры того, как информация становится оружием.

Во второй главе рассматриваются последствия информационной войны. Основная теоретическая база - книги Расторгуева С.П. "Информационная война", Почепцова Г.Г. "Информационные войны". Также мы рассматриваем зарубежные литературные источники: книги Тоффлера Э. "Третья волна", а также работа Czerwinski T. J. "The Third Wave: what the Tofflers never Told You", которые позволили нам лучшим образом понять и правильно интерпретировать истоки и предпосылки наступления информационной эры и, как следствие - информационного противоборства.

1. Информационная война: истоки, виды и цели информационного противоборства

1.1 Информационная война: определение и сфера деятельности

Человечество с незапамятных времен сталкивалось с проблемой информационных войн на всех уровнях, и лук, стрелы, мечи, пушки и танки, в конце концов, только завершали физический разгром сообщества, уже потерпевшего поражение в информационной войне.

Технологическая революция привела к появлению термина «информационная эра» из-за того, что информационные системы стали частью нашей жизни и изменили ее коренным образом. Информационная эра также изменила способ ведения боевых действий, обеспечив командиров беспрецедентным количеством и качеством информации. Теперь командир может наблюдать за ходом ведения боевых действий, анализировать события и доводить информацию.

Следует различать войну информационной эры и информационную войну. Война информационной эры использует информационную технологию как средство для успешного проведения боевых операций. Напротив, информационная война рассматривает информацию как отдельный объект или потенциальное оружие и как выгодную цель. Технологии информационной эры сделали возможной теоретическую возможность - прямое манипулирование информацией противника.

Информация появляется на основе событий окружающего мира. События должны быть восприняты каким-то образом и проинтерпретированы, чтобы стать информацией. Поэтому информация результат двух вещей - воспринятых событий (данных) и команд, требуемых для интерпретации данных и связывания с ними значения.

Отметим, что это определение абсолютно не связано с технологией. Тем не менее, что мы можем делать с информацией и как быстро мы можем это делать, зависит от технологии. Поэтому введем понятие информационной функции - это любая деятельность, связанная с получением, передачей, хранением и трансформацией информации.

Качество информации - показатель трудности ведения войны. Чем более качественной информацией владеет командир, тем большие него преимущества по сравнению с его врагом [6, с. 138].

Так в ВВС США анализ результатов разведки и прогноза погоды является основой для разработки полетного задания. Точная навигация увеличивает эффективность выполнения задания. Все вместе они являются видами военных информационных функций, которые увеличивают эффективность боевых операций.

Поэтому дадим определение военным информационным функциям - это любые информационные функции, обеспечивающие или улучшающие решение войсками своих боевых задач.

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю или возможности вести борьбу. Поэтому дадим определение информационной войне - это любое действие по использованию, разрушению, искажению вражеской информации

и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций. Это определение является основой для следующих утверждений.

Информационная война – это комплексное совместное применение сил и средств информационной и вооруженной борьбы.

Информационная война – это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.

Информационная война – только средство, а не конечная цель, аналогично тому, как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Первым использовал термин «информационная война» американский эксперт Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война» [3, с.37].

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года.

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 составе Г.Е. Экклз, Г.Г. Саммерз и др. 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.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Публикация определяет борьбу с системами контроля и управления как «объединенное использование приемов и методов

безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое» [17, с.165].

Наиболее важным является то, что эта публикация определила понятие войны с системами контроля и управления. И это было впервые, когда Министерство обороны США определило возможности и доктрину ИВ.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину «кибермaневра», которая должна явиться естественным дополнением

традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «human network»).

В октябре 1998 года, Министерство обороны США вводит в действие "Объединенную доктрину информационных операций". Первоначально эта публикация называлась «Объединенная доктрина информационной войны». Позже она была переименована в «Объединенную доктрину информационных операций». Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны. Они были определены, следующим образом:

информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем; информационная война: 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.

Сейчас существует довольно много разных определений ИВ и с техникотехнологической точки зрения. В коридорах Пентагона ходит, например, такое шутливое определение «Информационная война - это компьютерная безопасность плюс деньги» [7, с.106].

А если серьезно, то военные подходят к ИВ так, как это было сформулировано еще в Меморандуме N30 (1993 г) заместителей Министра Обороны и Комитета начальников штабов Вооруженных Сил США [4, с.21].

Под информационной войной здесь понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

В гуманитарном смысле «информационная война» понимается как те или иные активные методы трансформации информационного пространства. В информационных войнах этого типа речь идет об определенной системе (концепции) навязывания модели мира, которая призвана обеспечить желаемые типы поведения, об атаках на структуры порождения информации, процессы рассуждений.

Основными формами ведения технической ИВ являются радиоэлектронная борьба, война с использованием средств электронной разведки и наведения, нанесения удаленных точечных ударов с воздуха, психотропная война, борьба с хакерами, кибернетическая война.

Прежде чем всерьез анализировать различные определения информационной войны с технической точки зрения отметим присущее ей важное свойство:

ведение информационной войны никогда не бывает случайным или обособленным, а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле боя, либо в экономической, политической, социальной сферах.

Поэтому в качестве основного и наиболее общего определения ИВ предложу следующее:

«Информационная война - это всеобъемлющая целостная стратегия, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики» [9, с.49]. 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, действуют 150.000 военных компьютеров, и 95% военных линий связи проходят по открытым телефонным линиям [11, с.114].

Какой бы смысл в понятие «информационная война» ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями.

Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психотронная война, информационнопсихологическая война, кибернетическая война и т.

Итак, информационная война – это такая форма конфликта, в которой происходят прямые атаки на информационные системы для воздействия на знания или предположения противника.

Информационная война может проводиться как часть большего и более полного набора военных действий.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести «бесконтактную» войну, в которой количество жертв (в прямом значении слова) сведено до минимума. «Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, - сказал один из руководителей Пентагона. - Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума» [16, с. 171].

Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами оружием массового поражения.

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 атаковали информацию врага косвенно. То есть, 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.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить, но не до нуля эту уязвимость.

1.2 Составные части информационной войны

К составным частям информационной войны относятся:

1) психологические операции – использование информации для воздействия на аргументацию солдат врага.

2) электронная война – не позволяет врагу получить точную информацию

3) дезинформация – предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение – может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности – стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки – прямое искажение информации без видимого изменения сущности, в которой она находится.

Как ранее говорилось, существует два способа повлиять на информационные функции врага – косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

Пусть нашей целью является заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.

Косвенная информационная атака: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и противник будет наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению [20, с.204].

Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение – производить переброску войск
через другие коммуникации.

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию - не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность - типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

2. Пути реализации информационных войн в современном мире

2.1 Цели информационной войны

Существуют три цели информационной войны:

- контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация).
- использовать контроль за информацией для ведения информационных атак на врага
- повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

Приведем наглядный пример применения информационной атаки при выполнении ВВС стратегической атаки.

Предположим, что мы хотим ограничить стратегические возможности врага по переброске войск путем уменьшения запасов топлива. Сначала мы должны выявить нефтеперегонные заводы, которые будут наиболее подходящими целями при этой атаке. Потом нужно установить, какие заводы производят больше всего топлива. Для каждого завода нам надо выявить местоположение перегонных емкостей. Мы организуем атаку и, при значительной экономии сил, выводим заводы из строя, взрывая их только перегонные емкости, и оставляя все остальное оборудование нетронутым. Это классический пример стратегической атаки [19, с.29].

Теперь посмотрим, как надо добиться той же цели в информационной

войне. Все современные нефтеперегонные заводы имеют большие автоматизированные системы управления. Эти информационные функции являются потенциальной целью в информационной войне. На ранней стадии конфликта мы выполнили разведывательную информационную операцию по проникновению и анализу системы управления нефтеперегонным заводом. В ходе анализа мы обнаружили несколько уязвимых информационных зависимостей, дающих нам средства воздействия на работу нефтеперегонного завода в нужное нам время. Позднее, в ходе конфликта, в ходе одной из операций по блокированию вражеской группировки мы использовали одно из уязвимых мест. Мы просто остановили эти заводы. Это, тоже классический пример стратегической атаки.

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки [6, с.109]. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий – будь то на реальном поле брани, либо в экономической, политической или социальной сферах. Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах.

Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или «штабной войны». Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых

действий – война в Персидском заливе и вторжение на Гаити. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

Атаки инфраструктуры наносят удары по жизненно важным элементам, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками, или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

Промышленный шпионаж и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных [13, с.43]. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого,

уже имеются спутниковые системы слежения, имеющие разрешающую способность в несколько сантиметров.

Конфиденциальность все более уязвима по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны, таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин «информационная война» обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее. Следующее определение вышло из стен кабинета Директора информационных войск Министерства обороны:

«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» [15, с.47]. Информационная война представляет собой всеобъемлющую, целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах. Объектом внимания становятся информационные системы (включая соответствующие линии передач,

обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений. 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.

Многие ведущие стратеги полагают, что противостояние армий, погибающих на полях генеральных сражений, очень скоро займет свое место на свалке истории рядом со шпорами и арбалетами. Высшая форма победы теперь состоит в том, чтобы выигрывать без крови. В то же время довольно трудно представить боевые действия как игру на видеоприставке без страха и боли.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести «бесконтактную» войну, в которой количество жертв (в прямом значении слова) сведено до минимума. «Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, - сказал один из руководителей Пентагона. Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума» [22, с.201].

Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами оружием массового поражения. Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Поскольку такая война связана с вопросами информации и коммуникаций, то если смотреть в корень, это есть 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.

По определению С.П. Расторгуева, информационная война – это «целенаправленное широкомасштабное оперирование субъектов смыслами; создание, уничтожение, модификация, навязывание и блокирование носителей смыслов информационными методами для достижения поставленных целей» [5, с.102]. Речь идет, по сути, о работе по созданию той или иной модели мира.

С другой стороны, исследователи выделили характерную особенность человеческого восприятия, заключающуюся в том, что человек лучше усваивает ту информацию, которая похожа на уже существующие у него представления.

Основные средства ИВ ориентированы на этот феномен. Любые манипуляции и пропагандистские компании основаны на «эффекте резонанса», когда «имплантируемая» информация, направленная на изменение поведения общности, маскируется под знания и стереотипы, уже существующие в конкретной социальной общности, на которую направлена пропагандистская компания.

Целью манипуляции является асихронизации представлений группыадресата с помощью «эффекта резонанса» и перевод ее на другие модели поведения, ориентированные на совершенно иную систему ценностей.

«Эффект резонанса» достигается, когда тому или иному факту, проблеме или психологической установке придается искусственно преувеличенное значение, которое по мере продвижения в культурное ядро, диссонирует и разрушает существующую в обществе систему ценностей [18, с.138]. Диссонанс достигается при раздувании одной из уже существующих

моральных норм, которые в определённых рамках сами по себе помогают обществу.

Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Как указывают американские военные эксперты, ИВ состоит из действий, предпринимаемых с целью достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Информационное превосходство определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях [14, с. 76].

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и дает интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок, состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационное противоборство осуществляется путем проведения мероприятий направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается путем проведения психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц, принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Вообще, по словам некоторых экспертов, попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет его деревом; тот, кто ощупывает хвост, называет его канатом и так далее. Можно ли так получить более верное представление? Возможно, слонато и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом [4, с.58].

Однако проблема поиска надлежащего определения этому явлению весьма серьезная и требует, на наш взгляд, детальнейшей и серьезной проработки. В противном случае можно вполне разделить незавидную участь черепахи из басни С.П. Расторгуева, которая «не знала и уже никогда не узнает, что информационная война – это целенаправленное обучение врага тому, как снимать панцирь с самого себя» [5, стр.4].

Взрыв нескольких гранат нельзя назвать войной, кто бы их не бросал. Взрыв нескольких водородных бомб – это уже и начатая и завершенная война.

Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина «холодная война».

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно «запрудить» конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. «Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю. В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность – защиту от информации» [15, с.126].

Почему надо защищать информационную систему от информации? Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война – это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия – алгоритмы генерации алгоритмов.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны.

Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

1) включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);

2) полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

3) полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности /разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);

4) разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;

5) сокращение функциональных возможностей побежденной

системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие @степень поражения информационным оружием@, оценив ее через информационную

емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие даст максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления [11, с.174]. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению се безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Заставить противника изменить свое поведения можно с помощью явных и скрытых, внешних и внутренних информационных угроз.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы, обеспечивающие системе допустимый режим существования.

Причины внутренних угроз – в появлении внутри система множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Скрытая угроза – это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

В информационной войне наибольший приоритет отдается скрытым угрозам, так как именно они позволяют взращивать внутренние угрозы и целенаправленно управлять системой извне. Информационную самообучающуюся систему назовем тотально управляемой, а поведение ее полностью прогнозируемым на интервале времени [8, с. 267], если известен алгоритм информационного воздействия (например, методика обучения), позволяющий привести систему в любой момент времени [12, с. 134] к требуемому от нее результату (поступку).

Возможно, ли и с какой точностью спрогнозировать поведение ИСС в условиях непредсказуемости ее входных данных? Ответ на этот вопрос и представляет собой в каждом частном случае конкретный результат информационного моделирования поведения конкретной системы. Мощностью и качеством подобных моделей оцениваются "информационные мускулы» любой ИСС. Основными исходными данными для решения задачи по прогнозированию поведения ИСС в условиях информационного внешнего управления ею являются знания о ее знаниях и целях. В заключение еще раз подчеркну, что информационная война – это война алгоритмов и технологий; это война, в которой сталкиваются именно структуры систем, как носители знаний. Это значит, что информационная война – это война базовых знаний и ведется она носителями этих самых базовых знаний. На современном этапе, когда базовые знания человечества аккумулированы в рамках различных современных цивилизация, информационная война олицетворяет собой войну цивилизаций за место под солнцем в условиях все сокращающихся ресурсов. Открыто говорить о приемах и методах информационной войны сегодня необходимо потому, что, во-первых, осмысление того или иного приема информационной войны позволяет перевести его из разряда скрытых угроз в

явные, с которыми уже можно бороться, во-вторых, факт наличия теории информационной войны должен предостеречь потенциальную жертву от идеалистически наивного восприятия как внешнего, так и собственного внутреннего мира.

2.2 Сочинская Олимпиада в освещении западных СМИ

Крупнейшие информагентства и газеты Запада, создающие так называемую мировую информационную повестку, среди первых сообщили о взрывах, которые произошли в Волгограде. Причем акценты в освещении терактов ставились на зимнюю Олимпиаду в Сочи, до открытия которой осталось сорок дней. «Опасения по поводу волны атаки, безусловно, появляются в России, поскольку страна готовится к проведению зимних Олимпийских игр 2014 года в Сочи», - пишет французская газета Figaro, напоминая, что буквально в пятницу произошел взрыв заминированного автомобиля в Пятигорске, в результате которого погибли три человека. Волгоград уже был местом взрыва в переполненном автобусе два месяца назад, – пишет британская Guardian. – Волгоград является железнодорожным узлом на маршруте, соединяющем европейскую часть России с Центральной Азии. Это что-то вроде шлюза на Кавказ, в 430 километрах от Сочи, черноморского города, где 7 февраля планируется начать зимние Олимпийские игры. Российские власти настаивают, что не будет никаких угроз безопасности в ходе Олимпиады, несмотря на то, что город лежит к западу от беспокойного Северо-Кавказского региона. В июле Доку Умаров, лидер остальных чеченских джихадистов, предупредил, что боевики будут пытаться саботировать игры». «Подготовка России к проведению зимних Олимпийских игр в Сочи была поставлена под угрозу взрывом бомбы в одном из крупнейших городов на юге России», – утверждает Telegraph. Доку Умаров в своем

видеообращении призвал своих сторонников сорвать игры. И, похоже, это были не пустые слова, пугает газета. По заявлению другого западного издания New York Times, взрыв в Волгограде увеличивает угрозу волны терроризма накануне Олимпиады в Сочи. Газета пишет, что от российских властей потребуются чрезвычайные усилия, чтобы сохранить в безопасности Сочи, город-курорт на Черном море, который будет хозяином зимних Олимпийских игр. Сможет ли Кремль обеспечить безопасность, которая оказалась под угрозой после взрывов в Пятигорске и Волгограде? – задается вопросом Reuters. И сразу добавляет, что теракт может усилить озабоченность по поводу способности правительства обеспечить проведение Олимпийских игр-2014 в черноморском курортном городе Сочи. «Игры, которые открываются через 40 дней, являются одним из основных проектов престижа для Путина, который хочет показать, как далеко продвинулась Россия после распада Советского Союза в 1991 году», – пишет Reuters.

Заключение

Связи с общественностью играют важную роль в жизни общества. Изначально созданные для информирования общественности о ключевых событиях в жизни страны и властных структур, они постепенно стали выполнять еще одну не менее важную функцию - воздействие на сознание своей аудитории с целью формирования определенного отношения к сообщаемым фактам, явлениям действительности. Это воздействие осуществлялось при помощи методов пропаганды и агитации, разрабатываемых на протяжении не одной тысячи лет.

В скором времени связи с общественностью заняли важное место в жизни государств, а с развитием техники и технологии стали активно использоваться и на международном уровне с целью приобретения каких-либо преимуществ контролируемым им государством. В наши дни особое внимание следует уделить роли связей с общественностью в международных конфликтах, в том числе и геополитического характера, поскольку в последние годы наряду с классическими видами оружия все чаще применяется информационно-пропагандистское, в основе которого - работа с различными средствами массовой информации.

Таким образом, в ходе проделанной работы мы получили ответы на все поставленные задачи.

1. Наступление информационной эры привело к тому, что информационное воздействие, существовавшее испокон веков во взаимоотношениях между людьми, в наши дни все более очевидно приобретает характер военных действий.

2. В настоящее время накоплен значительный опыт научных исследований в области информационного противоборства и

информационнопсихологических войн. Какой бы смысл в понятие «информационная война» ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину ИВ, отчетливо представляют себе отдельные ее грани и виды. Гражданское же население пока не готово в силу причин социального и психологического характера в полной мере ощутить всю опасность неконтролируемого применения НКТ в информационной войне.

3. Информация действительно стала реальным оружием. Пример с февральской атакой китайцев, затронувшей корневые серверы Интернет, стала чем-то большим, чем забавы нескольких хакеров. Этот инцидент мог стать «первым залпом» в глобальной информационной войне.

Информационная война идет уже в третьем поколении. Сергей Гриняев, доктор технических наук даёт следующую классификацию:

1-е поколение информационной войны – это РЭБ (радиоэлектронная борьба). Проводная, частотная, сотовая связь, подслушки, глушилки, блокировки, помехи и т.д.;

2-е поколение информационной войны – это РЭБ плюс партизанская и контрпартизанская пропаганда. Так было в Чечне в 90-х. У сепаратистовбоевиков были свои пропагандистские сайты в Интернете, они распространяли газеты и боевые листки, организовывали интервью для сочувствующих им западных журналистов. Контрпропаганда велась доступными федеральному центру средствами как на территории конфликта и смежных территориях, так и на более широкую общественность.

3-е поколение информационной войны – это глобальная информационная война, специалисты называют её так же «войной на эффектах».

Информационная войны вокруг событий в Южной Осетии - именно война третьего поколения.

Формирование вокруг России «санитарного пояса» из стран-соседей происходит политическими средствами - проведением цветных революций, формированием органов власти и парламентского большинства из проамериканских сил, и экономическими средствами - скупкой национальных бирж, наращиванием американского капитала в ключевых государственных отраслях и компаниях. Но в эпоху информационного общества ключевое значение приобрели СМИ, Интернет-каналы и контроль над информпотоками. Из представленного материала очевидно, что Россия в этом отношении значительно отстает от США. Для формирования нового многополярного мирового порядка России необходимо предпринимать решительные действия для прорыва в информационной сфере.

Список использованной литературы

1. Абрамов В. С. Методика работы журналистов в особых условиях / В. С. Абрамов. - Москва: Аспект-Пресс, 2005. - 286 с.
2. Амиров В. М. Журналистика экстремальных ситуаций: конспект лекций / В. М. Амиров; Гос. федеральное образовательное учреждение, Урал. гос. ун-т им. А. М. Горького, Фак-т журналистики, Каф. периодической печати. - Екатеринбург: 2008. - 51 с.
3. Афанасьев В. Социальная информация и управление обществом. - М.: Знание, 2005, - 119 с.
4. Блэк С. Паблик рилейшнз. Что это такое? М.: Наука, 2007, - 256 с.
5. Вершинин М.С. Политическая коммуникация в информационном обществе. М.: Ягуар, 2006, - 256 с.
6. Зверинцев А.Б. Коммуникационный менеджмент: Рабочая книга менеджера PR: 2-е изд., испр. - СПб.: Союз, 2007, - 288с.
7. Каландаров К.Х. Управление общественным сознанием. Роль коммуникативных процессов. М.: Наука, 2006, - 154 с.
8. Корконосенко С.Г. Основы журналистики: учебное пособие / С.Г. Корконосенко. - М.: КНОРУС, 2016. - 272 с.
9. Крутских А., Федоров А. О международной информационной безопасности. М.: Слово, 2008, - 234 с.
10. Малькова Т.В. Массы. Элита. Лидер. М.: Яуар, 2006, - 232 с.
11. Массовая информация в советском промышленном городе: Опыт комплексного социологического исследования / Под общей редакцией Б.А. Грушина, Л.А. Оконникова. - М.: 2006, - 347 с.

12. Почепцов Г.Г. Информационные войны. М.: ИЦ Гарант, 2008, - 453 с.
13. Расторгуев С.П. Информационная война. М.: Наука, 2008, - 235 с.
14. Рютингер Р. Культура предпринимательства. - М.: Лидер, 2006, 672 с.
15. Сергеев И., Кирсанова Н., Кирсанова И. – Развитие социальной сферы: приоритеты регулирования // Экономист - 2007 - №1. с. - 47.
16. Тоффлер Э. Третья волна. М.: Палея, 2007, - 458 с.
17. Танскотт Д. Электронно-цифровое общество. Плюсы и минусы сетевого интеллекта. М.: Прогресс, 2006, - 673 с.
18. Техника дезинформации и обмана. - М.: Слово, 2008, - 139 с.
19. Фирсов Б. Телевидение глазами социолога. - М. Слово, 2008, - 418 с.
20. Хаббард Л.Р. Проблемы работы. - СПб.: Знание, 2008, - 342 с.
21. Хейне П. Экономический образ мышления. - М.: Слово, 2006, - 457 с.