МОДЕЛЬ СНИЖЕНИЯ МОРАЛЬНО-ПОЛИТИЧЕСКОГО, ПСИХОЛОГИЧЕСКОГО СОСТОЯНИЯ, ПУТЕМ ВОЗДЕЙСТВИЯ НА ЧЕЛОВЕКА АГИТАЦИОННЫМИ МАТЕРИАЛАМИ, РАСПРОСТРАНЯЮЩИХСЯ С ПОМОЩЬЮ ОТКРЫТЫХ ТЕХНИЧЕСКИХ КАНАЛОВ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА WI-FI СЕТЕЙ

Лехачев Е.В.
Гусаров Ю.А.
Чернышов Д.В.

Аннотация*:* Рассмотрен вопрос разработки и программной реализации алгоритмов распространения агитационных материалов или любой другой информации, по средствам технических каналов передачи данных с использованием протоколов wi-fi сетей.

Пропаганда в военное время является оружием не менее мощным, чем танки, самолеты и боевые корабли. В период Великой Отечественной войны советское правительство старалось эффективно использовать пропагандистские рычаги, чтобы мобилизовать вооружённые силы и население для ведения тяжёлой войны, а также воздействовать на вражескую армию.

Популярными средствами пропаганды стали плакаты, листовки и радиопередачи.

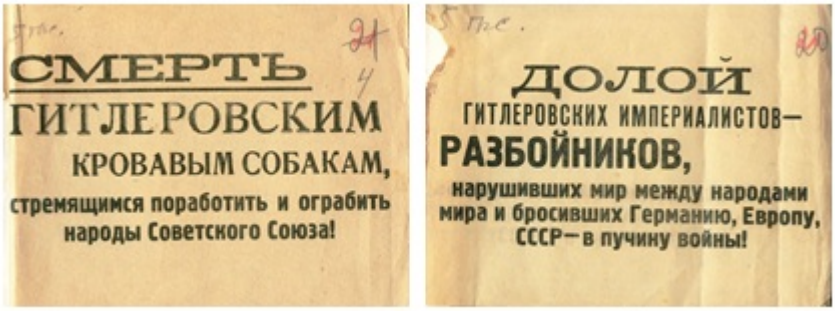
В газетах помещались материалы о зверствах, чинимых гитлеровскими войсками на оккупированных территориях, что должно было способствовать разжиганию ненависти к фашистским захватчикам.

Периодическая печать была ведущей формой советской пропаганды, отражавшей как точку зрения официальных властей, так и массовые настроения. В меньших масштабах были представлены устная пропаганда и наглядная агитация.

Во время Великой Отечественной войны 1941-1945 гг. неотъемлемым средством пропаганды служил плакат. Особенной популярностью пользовались сатирические плакаты художественного объединения Кукрыниксов. Нередко эти карикатуры сопровождались меткими стихотворениями С. Маршака.

Советскую пропаганду во время Великой Отечественной войны называли «третьим фронтом». Она подавляла врагов, воодушевляла бойцов Красной армии и восхваляла союзников. Она была гибкой и часто меняла курс, подстраиваясь под военные условия и внешнюю политику.

«Моральный фактор относится к материальному, как три к одному — говорил Напалеон». Одна пуля убивает одного солдата. Один паникер способен обратить в бегство весь взвод. Одна правильная листовка может оказаться самым эффективным оружием в пересчете на вес и стоимость.



а б

Рис. 1. Варианты агитационных материалов в период Великой Отечественной войны: а — Листовка, выпущенная в период ВОв с призывами уничтожить фашизм (1941г.); б — Лозунг ЦК ВКП(б) к XXV Годовщине Великой Октябрьской Социалистической революции.

Технологическая революция привела к появлению термина «информационная эра» [7] 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.

К информационной войне относятся две большие группы мероприятий:

— воздействие на военнослужащих и мирное население противника с целью внедрения массовое сознание определенных установок (пропаганда, «психологическая война»);

— поражение информации, информационных процессов и информационно-управляющих систем противника, независимо от применяемых средств (и высокоточная ракета, и компьютерный вирус могут выступать оружием информационной войны).

В информационной войне существуют три основные цели:

— контроль информационного пространства и обеспечение защиты своей информации от вражеских действий;

— использование контроля над информационным пространством для проведения информационных атак на врага;

— повышение общей эффективности вооруженных сил путем повсеместного внедрения военных информационных функций.

В настоящее время уровень развития информационных технологий стер границы между государствами в информационном пространстве и создал беспрецедентные возможности для подавления противника без использования традиционных средств поражения. Целями воздействия в нем являются объекты противника, выбираемые по принципу «пяти колец» [1] (по мере убывания важности):

— политическое и военное руководство страны;

— системы жизнеобеспечения;

— инфраструктура; население;

— вооруженные силы.

Рис. 2 Пример информационной войны в современном сетевом пространстве.

Поскольку воздействие на указанные объекты осуществляется с помощью сетевых технологий и методов, такое противоборство получило название «информационно-сетевая война» [2]. Основой ее является массированное воздействие на морально-психологическое состояние руководства и население страны-противника.

Причем, зачастую даже сам факт такого воздействия заблаговременно не может быть выявлен ее спецслужбами. Информационно-сетевая война предусматривает проведение комплекса мероприятий в отношении противника:

— создание атмосферы бездуховности и безнравственности, что автоматически создает благоприятную атмосферу для нагнетания конфликтной обстановки внутри страны-противника и падению авторитета государственной власти;

— манипулирование общественным мнением и политической ориентацией социальных групп с целью создания обстановки политической напряженности и хаоса;

— дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания атмосферы недоверия и подозрительности;

— обострение политической борьбы, провоцирование репрессий против оппозиции;

— развязывание в обществе гражданской войны; снижение уровня информационного обеспечения органов власти и управления с целью затруднения принятия важных решений;

— дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;

— провоцирование социальных, политических, национальных и религиозных столкновений;

— инициирование массовых протестных акций, забастовок, массовых беспорядков;

— подрыв международного авторитета государства; нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

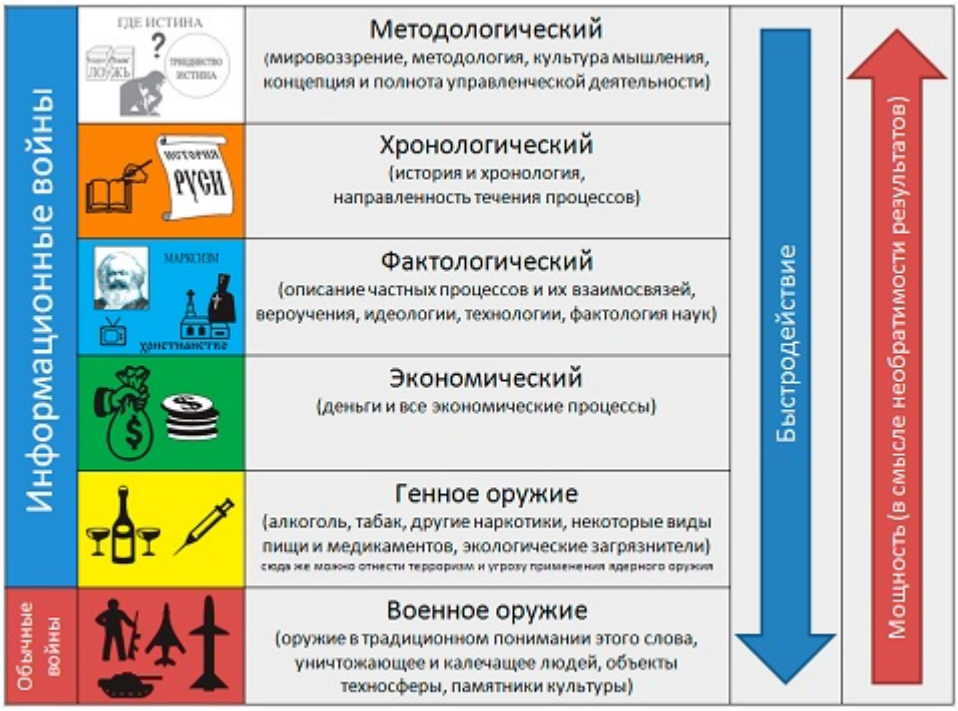


Рис. 3 Сравнительные характеристики традиционных и информационных войн.

Как правило, методами информационной войны является вброс дезинформации, или представление информации в выгодном для себя ключе. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие. Мы постоянно держим телефон в руках, выкладываем на стол в кафе и прячем под подушку во время сна. Смартфон стал неотъемлемой частью жизни. Не обязательно использовать тонны бумаги для воздействия на подсознание противника, достаточно использовать технические каналы передачи данных с протоколом wi-fi сетей, как открытых, так и закрытых для передачи информации, деморализующей сознание противника.

В целях реализации алгоритма распространения информации по средствам wi-fi сетей, возможно использование портативных роутеров (маршрутизаторов) с подготовленной начальной страницей, так называемым Captive portal на котором пользователя подключившегося к нашей wi-fi сети будет автоматически перенаправлять на страницу с материалами агитационной направленности или любой другой информации, которую мы хотим передать в целях информационно-психологического воздействия на необходимый объект. Объектом является как массовое сознание, так и индивидуальное. Индивидуального воздействия «удостаиваются» лица, от решения которых зависит принятие решений по интересующим противоборствующую сторону вопросам (президент, премьер-министр, глава МИД, диппредставители, главы воинских формирований, военнослужащие всех видов и родов войск).

Все пользователи, которые хотят подключиться к публичной Wi-Fi-сети и выйти в интернет, вначале проходят через шлюз, который представляет собой устройство с несколькими сетевыми интерфейсами. Шлюз действует как маршрутизатор и брандмауэр, а для возможности авторизации пользователя при помощи браузера он содержит еще и веб-сервер. Для аутентификации клиентов может использоваться внутренняя база данных или внешний RADIUS-сервер. Все пакеты от «неавторизованных» пользователей помечаются на брандмауэре, и посетитель переправляется на специальную веб-страницу (Captive Portal), где мы и предлагаем размещать необходимые материалы в целях информационно-психологического воздействия. На рисунке 3 представлена реализация данной модели.

Рис. 4 Разработанная модель (вариант) информационно-психологического воздействия.

В результате сравнительного анализа традиционных и информационных войн (представлен на рисунке 2), негативное информационное воздействие на противника в современной войне рассматривается в качестве важного и эффективного средства достижения тактических, оперативных и стратегических целей. Они могут осуществляться как самостоятельно, так и в комплексе со средствами боевого поражения. Новое «несмертельное психологическое» оружие используется как эффективный способ достижения политических, экономических, военных целей еще до этапа применения военной силы. Оно представляет собой самостоятельный, эффективный и сравнительно дешевый вид оружия современной и будущей войны.

Таким образом, разработана модель снижения морально-политического, психологического состояния, путем воздействия на человека агитационными материалами, распространяющихся с помощью открытых технических каналов с использованием протокола WI-FI сетей. Показано, что использование современных способов ведения информационного воздействия, является неотъемлемой частью информационно-психологического противоборства.

Список литературы

1 Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно психологической войны. 3-е изд. М.: Горячая линия — Телеком, 2012.

2 Расторгуев С.П. Информационная война http://evartist.narod.ru/text4/54.htm.

3 Волкогонов Д.А. Психологическая война: Подрывные действия империализма в области общественного сознания. М. Воениздат, 1983.

4 Гриняев С.Н. Поле битвы — киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Мн.: Харвест, 2004.

5 Лисичкин В. А., Шелепин Л. А. Третья мировая информационно-психологическая война. М.: Академия социальных наук, 1999.

6 И.И. Завадский. "Информационная война — что это такое?«//Защита информации.

«Конфидент». № 4, 1996 г.

7 А.В. Хомков методы и цели информационных войн // Материалы VIII Международной студенческой научной конференции «Студенческий научный форум» https://scienceforum.ru/2016/article/2016023722