электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК. 316.47

Информационные войны: сущность и методы

***Слимов Н.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Автоматизированные системы обработки информации и управления»

Научный руководитель: Оплетина Н.В., к.с.н.,доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Социология и культурология»
dekan.fsgn@bmstu.ru

«Истинно тотальная война – это война посредством информации.
Ее незаметно ведут электронные средства коммуникации — это
постоянная и жестокая война, в ней участвуют буквально все.
Войнам в прежнем смысле слова мы отводим место на задворках вселенной»
Маршалл Маклюэн

XXI век — век высоких технологий, век информации. Главной ценностью считаются знания, то есть достоверная и истинная информация, а не представления, то есть информация, которая носит субъективный, индивидуальный характер. Возникает не только борьба за доступ к знаниям, но также и борьба за управление информацией. В связи с чем исследователи вводят понятия «информационная война», «информационное оружие», «информационное противоборство» и другие. Несмотря на то, что эти термины можно услышать в СМИ каждый день, не всегда понятно, что под ними подразумевается и какое влияние имеют информационные войны на современную жизнь.

В широком смысле информационная война — это открытое или скрытое целенаправленное использование информационных и коммуникационных технологий с целью получения преимущества над соперником. Из такой формулировки можно выделить основные ресурсы ведения войны — информация и коммуникации. Также определяется цель войны — получение преимущества над соперником. Так как война ведется в информационной сфере, то важными считаются качественные характеристики информации (доступность, целостность, авторство, полнота, актуальность, достоверность и т.д.). Соответственно, соперники стремятся получить своевременно достоверную

полную информацию без искажений и скрыть или исказить ту информацию, которую получат другие стороны.

Американские исследователи рассматривают информационную войну как «действия, предпринимаемые 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». [1] Можно отметить, что такая формулировка сужает понятие «информационная война» до контекста противодействия государств и достижения национальных целей.

Вместе с тем, примером такой информационной войны может служить вооруженный конфликт в Южной Осетии в 2008 году. Россия предприняла миротворческие действия для скорейшего решения конфликта, однако эти меры были восприняты отрицательно из-за общественного мнения, сформированного западными СМИ. Россия стала агрессором в глазах западных обывателей.

Другая группа определений раскрывает данное понятие на экономическом уровне: информационная война представляется как те виды конфликтов, где конкуренты преследуют целью достижение информационного превосходства, нанося урон информационным системам и процессам противника и защищая свои. [2]

Такое понимание информационной войны можно проиллюстрировать на примере конкурентных отношений в экономической сфере. Так, 2 декабря 2014 года между сервисами, предоставляющими услуги вызова такси онлайн, «Яндекс.Такси» и GetTaxi произошел конфликт в связи с распространением представителями первого сервиса недостоверной информации о тарифах второго. В распространенной информации тарифы GetTaxi были завышены, а цены на услуги «Яндекс.Такси» были указаны верно. Сравнительная таблица представляла GetTaxi в невыгодном свете, что усилило позиции «Яндекс.Такси». Однако пострадавшей компании удалось быстро восстановить свою репутацию и поставить под вопрос компетентность конкурента. [3]

В целом, можно выделить следующие характерные черты информационных войн:

- целенаправленность (обязательное наличие цели, конечного результата)
- непредсказуемость (невозможно однозначно предсказать результат войны)
- безграничность, масштабность (благодаря развитию информационных технологий и Интернета любую информацию можно передать мгновенно на тысячи километров, невзирая на границы)
- универсальность (возможность многовариантного использования)

- скрытность
- связь с другими типами противоборства и войн (часто информационная война является вспомогательным инструментом получения выгоды или нанесения ущерба)

В настоящее время в научной литературе информационные войны принято рассматривать, как социальные явления, которые не только несут определенное содержание, но и обладают структурными характеристиками. [4]

Во-первых, любая информационная война, проявляется в действиях участников: стороны, соперники, конкурирующие системы, которые могут быть представлены индивидами, компаниями, организациями, государствами, а также информационными системами или системами знаний и убеждений. Так как одной из сторон может выступать система знаний и убеждений, информационной войной можно считать манипуляции информацией государством для распространения определенных идеалов или так называемой «промывки мозгов».

Во-вторых, в основе информационных противоборств, как правило лежит конфликт – разногласия сторон-участников, которые и определяют накал взаимодействия и предопределяют возможности достижения целей каждой из сторон. Сами цели участников, обычно не декларируются в связи со скрытым характером данного типа войны.

В-третьих, любое информационное противоборство характеризуется целым комплексом методов ведения информационной войны, особыми инструментами и способами достижения целей.

Важными элементами любой информационной войны выступают ресурсы – информация, коммуникация и связи соперников, обеспечивающих им влияние и достижение целей в ходе информационного противостояния.

Стратегия и тактика ведения информационной войны, безусловно, характерный элемент любых войн. В случае информационного противоборства можно рассматривать действия соперников с точки зрения применения методов ведения информационной войны в сложившейся ситуации, а так же реализацию разработанной стратегии в определенном пространстве и времени. Например, во время уже упомянутого вооруженного конфликта в Южной Осетии, кадры разрушений в местах боевых действий были показаны западными СМИ только после ввода миротворческих войск на территорию конфликта и были восприняты зрителями как разрушения в ходе именно миротворческой

операции, хотя кадры разрушений были сделаны задолго до конкретного времени трансляции данного материала.

В современном социальном пространстве информационные войны представлены как некий социальный феномен современности, характеризующийся достаточно широким спектром методов его осуществления, которые постоянно совершенствуются. Под методами мы понимаем инструменты и методики, которые применяются соперниками в условиях информационного противоборства для достижения своих целей. Рассмотрим некоторые из наиболее активных методов и постараемся представить их классификацию.

Программные методы

Такой вид методов включает в себя действия, направленные на нарушение работы аппаратуры, обрабатывающей информацию или предоставляющей доступ к ней. Задача таких действий состоит в поиске ошибок в программном обеспечении и создании условий для их порождения, т.е. перевод единичных ошибок на системный уровень. Программные методы включают в себя:

- воздействие на информационно-вычислительные сети, сети связи
- программные атаки на оборудование
- распространение компьютерных вирусов
- и другие.

Примером применения таких методов могут служить DDOS-атаки, распространенные в последнее время. Во время таких атак оборудование получает огромное количество запросов, с которым не способно справиться. Результатом атаки является временное прекращение работы оборудования. Так, весной в 2014 году DDOS-атакам подверглись сайты популярных СМИ (LifeNews, Первый канал, RussiaToday), сайты банков (Сбербанк, ГазпромБанк, ВТБ-24), сайты российских органов власти (Роскомнадзор, сайт Президент РФ) и другие. Эта атака была направлена на ограничение доступа к новостям, к онлайн-сервисам банков. Эксперты считают, что DDOS-нападение было связано с геополитической информационной войной против России (в связи с присоединением Крыма). [5]

Другим примером можно указать атаку хакеров на системы управления печами на металлургическом заводе в Германии 19 декабря 2014 года. В результате это привело к отказу оборудования, что нанесло прямой ущерб индустриальному предприятию. Также этот пример подтверждает скрытный характер информационной войны, так как в данном случае не удалось определить источник и организатора удаленной атаки. [6]

Физические методы

Такой вид методов представлен использованием средств, предназначенные исключительно для физического воздействия на элементы информационной системы: специализированные аккумуляторные батареи генерации импульса высокого напряжения, средства генерации электромагнитного импульса, графитовые бомбы, биологические и химические средства воздействия на элементную базу. [7] Такие средства также позволяют выводить из строя технику, обрабатывающую информацию, что приводит к ее полному или частичному отказу. По сравнению с программными методами данные имеют недостаток в необходимости близкого расположения к машинам (серверам и т.п.), то есть удаленные атаки невозможны.

Психологические методы

Цель информационных войн — получение преимущества с помощью воздействия на системы знаний, потребителем которых являются люди. Таким образом, психологические методы имеют своей целью воздействие на психологическое состояние человека или его сознание, передачу ему определенной информации, скрытие информации или ее искажение. [8] К психологическим относят следующие методы: пропаганда, сокрытие критически важной информации, погружение ценной информации в информационный мусор, подмена понятий и искажение их смысла, отвлечение внимания на незначительные события, ссылки на неавторитетные источники, создание «информационных бомб» — сенсационной информации (пример: организация WikiLeaks, создатели одноименного сайта, на котором публикуются секретные документы в открытом доступе; материалы сайта вызвали активное обсуждение после первых больших публикаций в ноябре 2009 года) и др.

Важно отметить, что психологические методы широко используют СМИ. С помощью особых техник изменения информации, журналисты, репортеры могут передавать информацию в той форме, которая вызовет требуемую предсказуемую реакцию у потребителя информации, зрителя. К таким методам относят «будничный рассказ» (диктор без эмоций говорит о негативно воспринимаемых зрителями событиях, приучая их к спокойному восприятию, например, крови, насилия или убийств), «анонимный авторитет» (представления неправдоподобной информации под видом экспертного мнения, часто без указания источника) и многие другие. [9]

Также к психологическим методам относят создание мифов, сплетен и слухов. Данные действия вызывают особо оживленное обсуждение, а значит, такая даже неправдоподобная информация получит свое быстрое распространение, что может быть выгодно одному из соперников в войне.

Примером слухов в информационных войнах могут являться спекуляции на фондовых биржах. С их помощью игроки могут манипулировать поведением друг друга и влиять на стоимость акций. Например, 3 октября 2008 года слух о госпитализации главы компании Apple С. Джобса привел к падению стоимости акций компании на 5 %. [10]

Методы ведения информационных войн постоянно пополняются новыми, поскольку войны такого типа бесконечны и масштабны и ограничиваются только коммуникациями и возможностями соперников. Современные возможности, которые открывает динамичное развитие технологий и техники, так же способствуют интенсивному появлению новых методов.

В связи с развитием техники, средств связи, вычислительной техники и коммуникаций, в современном обществе возрастает роль информации. Борьба за доступ к информации и управление ей проявляется именно в информационных войнах. Они уверенно вошли в нашу жизнь, примеры новых противоборств можно видеть регулярно в выпусках новостей. Эффективность их методов превзошла все виды оружия, поскольку они позволяют скрыто оказывать влияние на противника, управлять большими группами людей. Каждый день появляются новые методы ведения такого вида войн.

Перед современным человеком и обществом в целом возникают вопросы информационной безопасности: как определять достоверность получаемой информации, как противодействовать влиянию соперников в информационных войнах, как определить и предотвратить информационные атаки и многие другие. Для решения таких вопросов необходимо изучать информационные войны, их инструменты и методы противодействия.

Список литературы

1. Панарин И.Н. СМИ, пропаганда и информационные войны. М.: Поколение, 2012. 169 с.
2. Дроботенко О.Н. Информационная безопасность России в условиях глобализации: внешнеполитический аспект: дис. … канд. полит. наук. Пятигорск, 2014. 209 с.
3. Панфилов К.: Основатель GetTaxi Шахар Вайсер обвинил «Яндекс.Такси» в публикации ложной информации. Режим доступа: http://siliconrus.com/2014/12/gettaxi-vs-yandex-taxi/ (дата обращения 24.04.2015).
4. Почепцов Г.Г. Информационные войны. Электр. Книга. Режим доступа: http://www.telecomlaw.ru/studyguides/Pocheptsov_inwars.pdf (дата обращения 24.04.2015).

5. Михайлов А. Российские компании подверглись самой масштабной DDoS-атаке в рунете. Режим доступа: http://www.vedomosti.ru/tech/news/26998611/ukrainskij-rekord (дата обращения 24.04.2015).
6. Степанов В. Хакеры вывели из строя печи на металлургическом заводе в Германии. Режим доступа: http://tjournal.ru/paper/iron-plant-attack (дата обращения 24.04.2015).
7. Шеховцев Н.П., Кулешов Ю.Е. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник АВН. 2012 №1(38). С. 35–40.
8. Матвиенко Ю.А. Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе Режим доступа: http://media.wix.com/ugd/ec9cc2_a1ef5c460da54f21746aac788b9b2c21.pdf (дата обращения 24.04.2015).
9. Слухи о госпитализации главы Apple опустили акции компании. Режим доступа: http://korrespondent.net/business/companies/604363-sluhi-o-gospitalizacii-glavy-apple-opustili-akcii-kompanii (дата обращения 24.04.2015).
10. Сороченко В.А. Энциклопедия методов пропаганды. Режим доступа: http://psyfactor.org/propaganda.htm (дата обращения 24.04.2015).