УДК 002.55/56

© Нежданов И.Ю.
Nezhdanov I.

АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ КОНФЛИКТОВ В ИНТЕРНЕТЕ

ANALYTICAL SUPPORT INFORMATIONCONFLICTS ON THE INTERNET

Аннотация. *Данная статья посвящена обоснованию положения о том, что в силу своих особенностей Интернет позволяет проводить воздействие гораздо эффективнее и с меньшими затратами. В настоящее время отработано достаточное количество алгоритмов, необходимых для создания комплекса «полного цикла» для ведения информационных войн.*

Annotation. *This article is devoted to the justification of the position that, because of their online features allows the impact is much more efficient and less costly. Currently worked out a sufficient number of algorithms needed to create complex "full cycle" information wars.*

Ключевые слова. *Аналитическое обеспечение, информационный конфликт, Интернет, эффективность, алгоритм, информационная война.*

Key words. *Analytical support, information conflict, Internet, efficiency, algorithm, information warfare.*

Современное противостояние держав не гарантирует оппонентам победу в случае полномасштабных военных действий с учетом ядерных сил. В то же время межгосударственные отношения обостряются по мере истощения ресурсов. Это стимулирует поиск альтернативных вариантов уничтожения противника. Таких вариантов, при которых риск получения ответного удара отсутствует или минимален. Одной из подобных альтернатив является информационно-психологическое воздействие на граждан противника или информационная война. Помимо победы в глобальной войне, такая альтернатива позволяет решать и локальные задачи. Например, повышение эффективности в локальных военных конфликтах, оказание давления на правительства, манипулирование рынками – есть масса вариантов применения методов информационной войны. При этом, если раньше основным инструментом информационных войн были СМИ, то сейчас основным инструментом стал Интернет. В силу своих особенностей Интернет позволяет проводить воздействие гораздо эффективнее и с меньшими затратами. Помимо этого, такие информационные войны агрессор может вести на любых территориях, находясь в удобном для него месте и в любое время, сохраняя свою анонимность.

С начала 2011 г. Пентагон развивает систему SMISC (Social Media in Strategic Communication в переводе - «социальные медиа в стратегической коммуникации»), которая отслеживает все политические дискуссии в Интернете и устанавливает, является ли это случайный спор или пропагандистская операция. Заявленные цели проекта таковы:

- обнаружение, классификация, измерение и отслеживание образования идей и концепций (мемов) и целенаправленного распространения сообщений и дезинформации;
- распознавание структур пропагандистских кампаний и операций влияния на сайтах и сообществах социальных медиа;
- идентификация участников и их намерений, измерение эффекта кампаний влияния;

Нежданов Игорь Юрьевич – эксперт по вопросам конкурентной разведки, Лаборатория перспективных разработок, tel. 8(495)543-36-76.

Nezhdanov Igor – expert on competitive intelligence, Laboratory promising developments, tel. 8 (495) 543-36-76.

• противодействие враждебным кампаниям влияния с помощью контрсообщений.

Фактически SMISC может быстро отмечать слухи и появляющиеся темы в соцмедиа, вычислять, кто и что за этим стоит и выстраивать противодействие. SMISC способна понять случайный ли это продукт коллективного разума или пропагандистская операция со стороны враждебной нации или группы. Как только SMISC улавливает, что была запущена операция влияния, она помогает бороться с ней, отправляя контрсообщения, или самостоятельно запускает манипулятивные процессы.

Параллельно с этим большим проектом развивается ряд вспомогательных, предназначенных для решения частных задач той же направленности автоматизация ведения информационной войны. Так, с 2010 г. DARPA финансирует две программы ICEWS и ADMS. Integrated Crisis Warning System (ICEWS) — информационная интегрированная система раннего предупреждения о возникновении кризисных ситуаций. ICEWS предназначена для мониторинга, оценки и выделения основных индикаторов, указывающих на нарастание социальной напряженности в обществе, в том числе и на основе данных из соцсетей. Anomaly Detection at Multiple Scales (ADMS) предназначена для выявления аномальных процессов, происходящих в обществе, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей. И вновь основным объектом наблюдения является Интернет.

Интернет стал инструментом манипулирования и естественно, что такой эффективный инструмент используется очень активно и совершенствуется. Эксперты утверждают, что уже в тунисских событиях использовались указанные технологии в полуавтоматическом режиме. Наши исследования показали, что и в России эти технологии активно применяются. Примером является интернет-деятельность «несистемной оппозиции», негативная активность по ряду высокопоставленных политиков и руководителей крупного бизнеса. Мы выделили ряд признаков, по которым с высокой достоверностью определяется подготовка к информационной войне, ее начало и активная фаза.

Сама по себе Олимпиада это очень яркое и разрекламированное мероприятие, а потому всё, что было связано с ней, появлялось в ТОПе новостных агентств и на первых полосах газет. Очень удобно для разгона нужной информации, в том числе и информации негативной. Злоумышленники готовились к Олимпиаде по нескольким направлениям. Создавались виртуальные личности, от имени которых распространялась негативная информация. Подбирались живые распространители информации и «генераторы контента» и объединялись в виде групп в социальных сетях. Разгонялась негативная информация и готовилась информация, которая использовалась для дальнейших вбросов. Проведенный анализ показывает ,что основными разгоняемыми темами являлись следующие:

• ФСБ прослушивает всех иностранцев на Олимпиаде;

• в России ущемляются права сексуальных меньшинств;

• оккупации Россией Осетии и Абхазии;

• геноцид кабардинцев;

• уничтожение уникальной природы в местах проведения Олимпиады;

• национальная нетерпимость в России.

А после событий в Бирюлево и Волгограде темы «оккупации Россией Осетии и Абхазии» и «геноцид кабардинцев» начали конвертировать в тему «национальная нетерпимость в России», которая и стала основной. Видимо, эта тема активно использоваласть в дискредитации Олимпиады.

Информационная война, как и раньше, имеет своей целью разрушение. Но в отличие от недавнего прошлого ее реализация стала значительно проще – появился новый инструмент для ее ведения – Интернет. Этот инструмент сделал информационную войну более эффективной. Понимая это, ведущие мировые державы прикладывают немало усилий для еще большего проникновения Интернета – цель взять под контроль и управление как можно больше людей в разных уголках планеты.

Весь цикл информационной войны состоит из нескольких этапов. Первым шагом является поиск уязвимостей у той группы людей, которой планируется манипулировать, – уязвимостей, которые позволяют управлять поведением людей. Такими уязвимостями, если нужно подтолкнуть к насильственному свержению власти, могут быть недовольство низким уровнем жизни или коррупцией, проблемами ЖКХ или ГИБДД. Если уязвимостей нет или они недостаточно сильны, то их создают искусственно или создают видимость их наличия. Затем эти уязвимости эксплуатируются – осуществляется их усиление и привязка к некому действию, например, к активным уличным акциям. Обычно после этого делается вброс катализирующей информации – повода для начала активных действий. Где-то самосожжение, где-то стычка с полицией и погибшие, но всегда нужен яркий символ – «ритуальная жертва». После такого вброса все усилия направляются на разгон катализирующей информации – доведения ее до каждого члена выбранного соци-

ума. После чего начинается хаос – восстание, гражданская война, свержение.... Цель информационной войны достигнута.

Выявление подготовки к информационной войне возможно по вторичным признакам. По тем самым признакам, которые сопутствуют поиску уязвимостей социума-цели или подготовки к началу самой агрессии.

Поиск уязвимостей сопровождается не только пассивным наблюдением за дискуссиями на разных площадках, но и тестированием – пробными локальными вбросами (разведка боем) для определения уровня напряженности, для выявления «непримиримых», лояльных и неопределившихся. Такая активность имеет конкретные признаки и вполне детектируется. А подготовка к агрессии сопровождается созданием плацдармов – аккаунтов на тематических площадках, виртуальных личностей с соответствующим имиджем, их внедрение в нужные группы и т.п.. Такая деятельность также имеет характерные признаки и определяется с помощью мониторинга.

Противодействие информационным войнам подразумевает несколько направлений. Часть их (удаление контента, блокирование аккаунтов, площадок и т.п.) находится в ведении соответствующих госструктур. А программно реализуемы такие направление, как дискредитация информации, распространяемой агрессором, или источника этой информации, отвлечение внимания целевой аудитории на яркое событие или ресурсов оппонента на защиту, размытие негативной информации и т.п.. Все эти варианты противодействия реализованы и в нашем комплексе противодействия информационным войнам.

Используя те же самые методы, что и при отражении агрессии, можно организовать ответное воздействие на граждан противника, используя принцип бумеранга, либо конструируя новые информационные поводы. Такое воздействие подразумевает поиск уязвимостей противника, подготовку контента для удара и собственно воздействие. Мало того, информационное воздействие может быть и упреждающим, если выявлена подготовка к удару со стороны оппонента.

В настоящее время нами отработаны все алгоритмы, необходимые для создания комплекса «полного цикла» для ведения информационных войн, от мониторинга активности оппонента и поиска уязвимостей до выработки сценария воздействия и его реализации в автоматическом или полуавтоматическом режимах. Часть элементов системы уже работает и проходит испытания на реальных задачах.

Материал поступил в редакцию 22. 02. 2014 г.