SWARMING-МОДЕЛЬ ОПЕРАТИВНОГО РЕАГИРОВАНИЯ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН

Проблемы обеспечения устойчивого развития общества и государства, сохранения социально-политической стабильности являются одними из наиболее актуальных как для России, так и ее ближайших соседей.

Наш анализ показывает – существующая сегодня в стране практика государственной внутренней и внешней пропаганды далеко не всегда является эффективной. Особенно в части превентивного воздействия на отдельные целевые группы, отработку перспективных тем, как в стране, так и за ее пределами.

Это ведет к тому, что в большинстве случаев официальные каналы, спикеры, провластные эксперты вынуждены комментировать уже оцененные оппонентами сюжеты, при этом, фактически, не имея времени на подготовку.

Достаточно проанализировать те проблемы, с которыми столкнулась Российская Федерация в августе 2008 года, когда фактически все западные (и не только) СМИ транслировали одну точку зрения на события в Абхазии. Позицию, которая была брошена американскими политтехнологами в первые часы конфликта и получившую максимальное распространение в сети.

Огромные усилия, приложенные российской стороной, смогли лишь отчасти скорректировать сложившуюся в глазах мирового сообщества оценку и «агрессивный» имидж России.

Безусловно, никто не умаляет проделанной тогда и осуществляемой сегодня работы. Однако в условиях постоянных конфронтаций, высокой скорости и эффективности информационных атак, спор о необходимости создания лабораторий, центров, способных разрабатывать технологии и готовить специалистов по сетевой контрпропаганде, осуществлять превентивные мероприятия в информационном пространстве и т.п., на наш взгляд, бессмысленен. Они нужны. Другой вопрос – на основе каких принципов они должны функционировать? Что должно являться их предметным полем? Какие стратегии, каналы и формы коммуникации должны быть использованы? И так далее.

Конечно, в рамках одной статьи невозможно сформулировать все ответы на существующие в этой сфере вопросы. В связи с этим, остановимся на тех, которые, как нам видится, являются одними из наиболее актуальных.

Для начала попытаемся сформулировать общую логику нашего анализа.

Технолог «цветных» революций Джим Шарп выделяет три основных этапа дестабилизации общества и государственных структур.

Первый этап – это акции протеста. Так проверяется уровень протестных настроений в обществе, готовность различных групп насе-

ТЕМЫ “АНАЛИТИКА”

- ИНФОРМАЦИОННАЯ ПОЛИТИКА
- НКО И ВЛАСТЬ
- ОБРАЗ ЖИЗНИ
- ПРОПАГАНДА
- МАРКЕТИНГОВЫЕ СТРАТЕГИИ
- ОБРАЗОВАНИЕ

Эта статья является частью результатов исследований специалистов Центра «Аналитик».

ления к социальному взрыву. С другой стороны – способность власти к его подавлению.

Второй этап – дискредитация государственного аппарата и силовых структур. Призывы к саботажу и вредительству.

Третий этап – свержение режима.

Нам хотелось бы добавить еще один «нулевой» этап, во время которого создаются условия (информационные, идеологические, организационные и т.п.) для обеспечения протестных акций.

Анализ факторов, влияющих на рост социальной напряженности в обществе, позволяет выделить три основных блока, концентрация на которых может детерминировать динамику общественных настроений. Это отношение \ доверие к экономическим институтам (начиная с уровня заработных плат и заканчивая лояльностью к отечественным банкам), отношение \ доверие к государственным институтам (начиная с президента и заканчивая оценкой работы главы своего муниципалитета) и общий эмоциональный настрой, существующий у населения.

Сам по себе рост социальной напряженности во многом носит информационную природу. При условии концентрации внимания целевых групп на блоке (и \ или отдельных элементах, его составляющих) могут формироваться эмоционально-оценочные конструкции, которые в свою очередь могут стать основой для зарождения протестных настроений.

Отметим, что именно на «нулевом» этапе происходит постоянная проверка потенциального «протестного градуса» и наличия «болевых точек». Если они находятся, то происходит концентрация воздействия, которая подкрепляется обострением эмоций (прежде всего, негативных).

Что касается явных контрдействий органов власти, то, как показывает беглый анализ, они группируются, в основном, вокруг первого и второго этапов.

В частности, для первого этапа характерно

Активное применение законодательных регуляторов (например, регулирование и санкционирование проведения публичных акций – митингов, пикетов и т.п.). Быстрые санкции за нарушения. Введение санкций в отношении «оппозиционных» СМИ.

«Карнавализация» политических мероприятий и акций, когда друг за другом идут акции оппозиции и акции сторонников власти (например, контрмитинги сторонников «Единой России», направленные на поддержку государственных структур). Ввод «контрсимволики» (георгиевские ленты) и т.п.

Формирование «картины мира» и необходимой «повестки дня» через официальные каналы коммуникации (СМИ, сайты, провластные блогеры и т.п.).

На втором этапе к перечисленным выше методам, добавляется усиление администра-

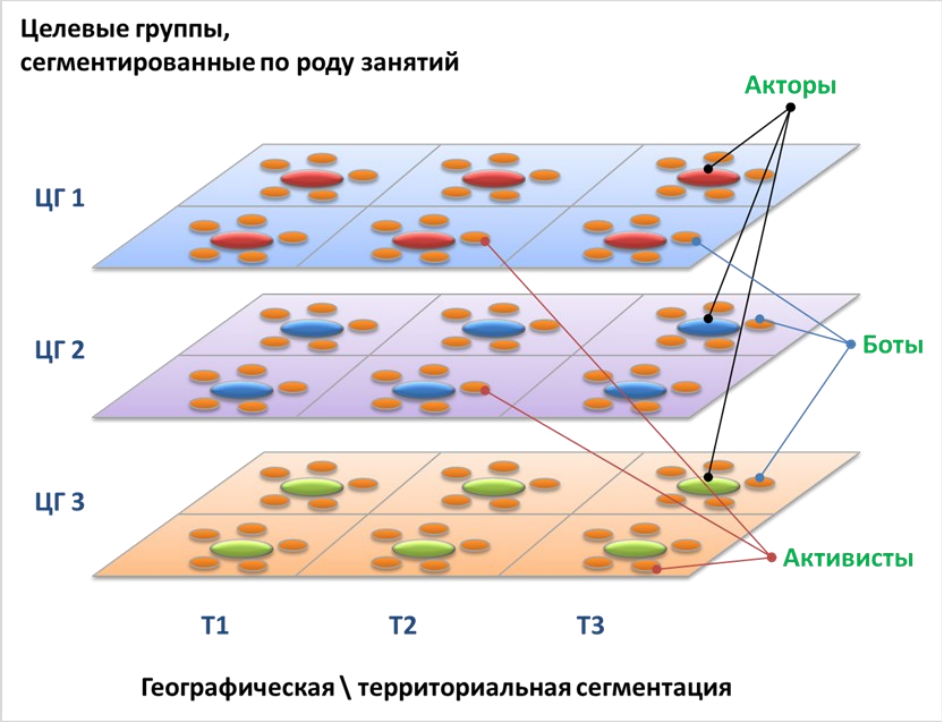

Рис. 1. Модель сегментирования интернет-пространства на сектора (основанием для дифференциации выступает географическая локализация и принадлежность к определенному роду занятий).

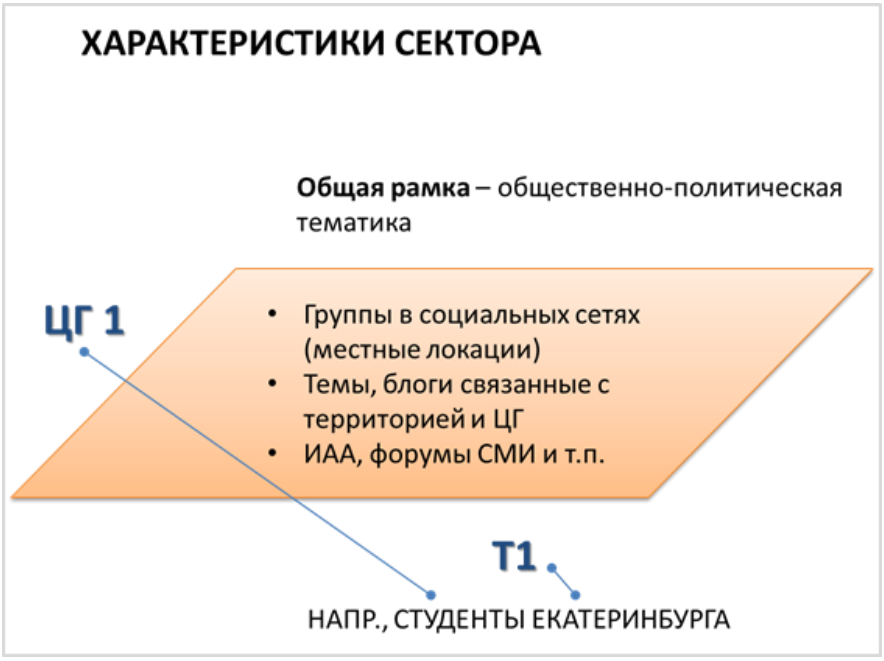

Рис. 2. Пример сектора в интернет-пространстве.

тивных и силовых методов, направленных на стабилизацию ситуации (разгон демонстраций, аресты оппозиционеров и т.д.).

Безусловно, это далеко не полный перечень. Нам хотелось бы отметить лишь одно - данные шаги, как правило, являются результатом реагирования на уже сложившийся факт. Говорить о превентивных, опережающих действиях здесь не приходится.

Вслед за Дж.Шарпом, мы можем отметить, что одной из основных слабостей любого государственного аппарата, которая наиболее ярко проявляется в условиях информационных войн, является его неповоротливость.

Низкая скорость реагирования на угрозы, обусловленная сложной иерархической структурой госаппарата, невозможностью одновременного централизованного мониторинга всех проблемных зон, зачастую сводит на нет имеющиеся у государства ресурсы. Особенно, когда речь заходит об атаках в интернете.

Одним из возможных тактических решений данной проблемы для успешного противостояния в современных информационных войнах является использование концепции «swarming» (роение).

Ее реализация предполагает использование небольших автономных высококвалифицированных групп (единиц), рассредоточенных в интернет-пространстве, ведущие свой мониторинг угроз и перспектив. Из этих единиц могут формироваться сети, способные в течение короткого промежутка времени сконцентрировать всю свои усилия на конкретной цели противника, напасть с различных сторон, нанести ему максимальный урон и снова рассредоточиться. Их активность определяется набором основных правил, что позволяет им не только оперативно реагировать на ситуации, но и быть максимально инициативными.

На наш взгляд, эти правила могут формироваться, например, на основе стратегии непрямых действий, разработанной Б.Х. Лидделл-Гартом и предполагающей, в качестве цели, нарушение устойчивости противника.

Если воспользоваться военной терминологией, то нарушение устойчивости является результатом действий, которые приводят: а) к нарушению диспозиции противника и, вынуждая его неожиданно изменить фронт, к нарушению организации и группировки его войск; б) к расчленению сил; в) к созданию опасности для системы снабжения; г) к созданию угрозы коммуникациям, по которым противник мог бы в случае необходимости отступить и снова закрепиться на промежуточных рубежах или в стратегическом тылу. Как показывается практика, данные правила достаточно легко адаптируются для разработки конкретных тактик превентивной деятельности в интернете.

Приведем в качестве примера несколько возможных стратегий, основанных на данном подходе.

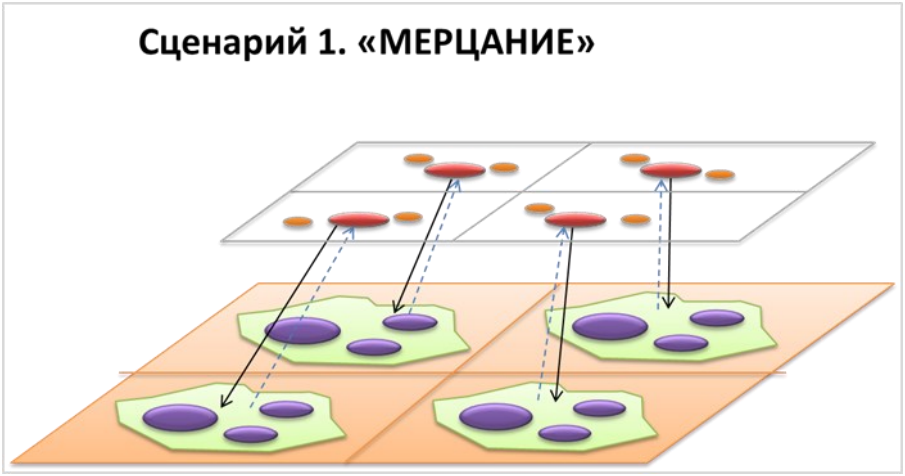

Рис. 3. Сценарий фонового присутствия.

Этот сценарий (Рис. 3.) носит, по сути, подготовительный, фоновый характер. Основные задачи акторов в рамках его осуществления направлены на создание «репутационной истории» и сбор информации об основных субъектах (блогеры, активисты), присутствующих в данном секторе.

В том числе, в эти функции входит:

1. Поддержание видимости присутствия \ минимальной активности актора и ботов;
2. Формирование френд-лент;
3. Мониторинг тематики и актуальных проблем;
4. Сбор и анализ информации по потенциальным носителям угрозы.

Следующий сценарий (Рис. 4.) предполагает самостоятельную оценку акторами серьезности потенциальной угрозы со стороны основных субъектов сектора и \ или новых участников. Речь идет о появлении негативной информации или фейков, связанных с теми объектами, защиту которых и призваны осуществлять акторы. При этом, защита строится не на прямом нападении на те темы и смыслы, которые формулируют «оппозиционные субъекты», а на их «болевые точки» в других сферах.

Добавим, что при необходимости, акторы одного сектора могут самостоятельно инициировать усиление необходимых тем с помощью акторов других секторов.

Основные функции, которые выполняются на уровне этого сценария состоят в следующем:

1.Выявление потенциально опасных субъектов и тем;

2.Сбор и анализ информации по возможным «болевым» точкам;

3.Принятие решения о необходимости превентивной атаки;

4.Превентивное воздействие;

5.Принятие решения о необходимости привлечения дополнительных акторов.

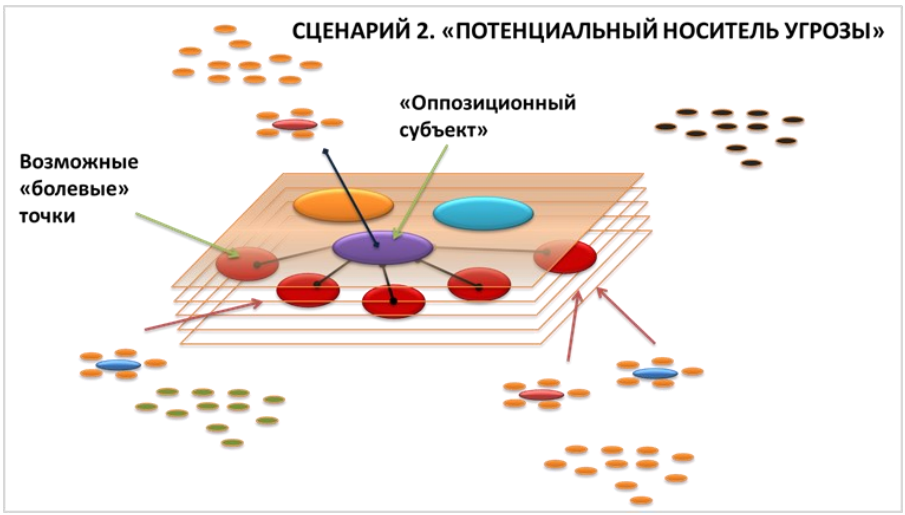

Рис. 4. Сценарий действий при возникновении потенциальной угрозы

Безусловно, использование описанных подходов не является единственным средством противодействия информационным атакам.

На наш взгляд, только создание оптимальных организационных и технологических структур, адекватных специфики каждого этапа дестабилизации общества, позволит разработать эффективную систему информационного противодействия.