Д.П. Кафтанчиков

СОВРЕМЕННЫЕ УГРОЗЫ РЕГИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К началу XXI столетия в научных кругах актуализируется потребность в осмыслении феномена «информационной войны», непосредственно воздействующего на развитие современного политического процесса. Возникновение подобного явления целесообразно связывать с распространением за пределами военной организации государства принципов, методов и технологий, относящихся к сфере военного искусства и первоначально предназначенных для подготовки общества к реальной войне. В связи с этим в системе обеспечения национальной безопасности первостепенное значение приобретает проблема защиты информационной безопасности в регионах России.

По отношению ко многим новейшим военным технологиям, способам их распространения и внедрения пока не выработано эффективной системы государственного контроля, а многие из разработок осуществляются по инициативе и на средства негосударственных корпораций или частных лиц. Появление средств массового уничтожения поставили под сомнение целесообразность полномасштабных физических войн, приводящих к уничтожению ресурсов, населения, а также к невосполнимым потерям в лагере инициатора агрессии.

Определение «информационная война» впервые было сформулировано в 1976 г. американским исследователем Т. Рона[1].

В российской практике принято выделять такие виды противоборства как информационно-техническое и информационно-психологическое[2]. Исходя из этого в современной науке сложилось два основных подхода к сущности дефиниции «информационная война», в свою очередь детерминирующих определение сферы информационной безопасности[3].

---

[1] См.: *Требин М.*. Войны XXI века. М.,2005. С.398.

[2] См.: *Волковский Н.Л.* История информационных войн. Ч. 2. СПб., 2003. С.661.

[3] См.: *Лопатин В.Н.* Реальность – основа концепция информационной безопасности России // PS Week/RE. 1999. № 12. P. 19–21.

Первый из них трактует данный термин преимущественно с технократических позиций: «информационная война» понимается как комплекс действий, предпринимаемых для достижения превосходства путем воздействия на совокупность аппаратных и программных средств, обеспечивающих доступ, конфиденциальность, сохранность информации в современных телекоммуникационных и компьютерных сетях.

В рамках данного подхода абсолютизируется технологический аспект рассматриваемой проблемы, когда в качестве основного объекта защиты от противоправного воздействия определяется социотехнический феномен, в последней четверти XX в. именуемый «компьютерной безопасностью» либо «безопасностью данных». В 90-е гг. утвердился термин «информационная безопасность», под которой понимаются меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Таким образом, выделяются два объекта защиты – информация и информационная инфраструктура, которые должны быть гарантированы от случайных или преднамеренных воздействий естественного или искусственного характера.

Для реализации указанных задач применяется так называемое информационное оружие[1]. Большинство исследователей понимает под ним средства уничтожения, искажения или хищения информации; механизмы преодоления систем защиты; инструменты ограничения допуска законных пользователей; технологии дезорганизации функционирования телекоммуникационных и компьютерных систем. Инициаторы информационной агрессии стремятся принудить объект воздействия использовать имеющиеся у него средства поражения и обороны во вред собственным интересам. Главным фактором, стимулирующим использование информационного оружия, признается его небольшая стоимость по сравнению с другими видами вооружений.

Сегодня широко известен набор средств информационного оружия: компьютерные вирусы; логические бомбы (программные закладки); средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления; средства нейтрализации

[1] См.: *Шаравов И.* К вопросу об информационной войне и информационном оружии. // Зарубежное военное обозрение. 2000. № 10. С. 4.

тестовых программ; дисфункции, сознательно вводимые в программное обеспечение объекта.

Сторонники противоположного научного подхода склонны распространять термины «информационная война», «информационная безопасность» практически на все вопросы и отношения в информационной сфере. С этой точки зрения целью информационной войны является не столько разрушение коммуникаций и компьютерных технологий, сколько манипулирование мировоззрением и психологией объекта воздействия. В данном контексте возникает термин «информационно-психологическая война», стратегия проведения которой ориентирована на разрушения системы ценностей общества, его дестабилизации на духовном, политическом и экономическом уровне[1]. Одним из ее средств является мирная пропаганда достоинств собственного образа жизни. Для этого при помощи манипулятивных технологий реализуется задача разрушения психологической защиты общества. В ходе информационно-психологического воздействия стремятся достичь перемещения диссонирующих фактов и интерпретаций с периферии общественного сознания в центральное ядро духовного мира индивидов и социальных групп.

Со стороны институтов публичной власти, несмотря на декларативную приверженность ценностям демократии, нарастает стремление к поиску новых моделей манипулирования или доминирования над неправительственным сектором, заимствованных из арсенала военных технологий «непрямого действия» (информационно-психологической, кибервойны и т. д.) В распоряжении политических сил, ориентированных на достижение гегемонии в глобальных или региональных масштабах появились новые экономические возможности, специальные средства и методики для проведения подрывных психологических операций

Во многих странах как военные, так и штатские специалисты задействованы в разработке ряда проектов, на основе которых стали возникать совершенные технологии информационно-психологического воздействия. Одним из основных условий развертывания манипуляционной программы выступает препятствование получение альтернативных сведений об окружающем мире, ключевых политических событиях. В результате искусственно создается информационный вакуум, когда объекту воздействия при помощи

[1] См.*: Кара-Мурза С*. Манипуляция сознанием. М., 2000.

различных средств и методик навязывается только один вариант решения, преподносимый как безальтернативный и единственно приемлемый. Еще одним признаком манипуляции является создание ситуации искусственного дефицита времени. В этом случае цель считается достигнутой, если решение, противоречащее интересам объекта воздействия, принято без должного анализа альтернатив в чрезвычайно ограниченный период времени.

Таким образом, противодействие угрозам, возникающим в результате развертывания информационных войн, требует не только соответствующей реакции в отношении посягательств на информационные ресурсы личности, общества и государства, но и реализации системы мероприятий по противодействию акциям духовно-психологического (пропагандистского) воздействия.

Исследователями отмечается, что акции психологической войны с большим трудом могут быть подвернуты идентификации. В большинстве случаев они настолько замаскированы, что не кажутся действиями, направленными на политико-идеологическую, моральную и психологическую обработку населения. Эта особенность психологической войны приобретает все большее значение, когда ее методы переносятся в область политической борьбы мирного времени. Как отмечается в печати, психологической войне свойственно скорее «тихое, неприметное, полное недомолвок, двусмысленностей, дезинформации, воздействие длительное, непрерывное, въедливое»[1].

Задачи подрывных операций в гуманитарной сфере могут быть достигнуты, прежде всего, за счет девальвации мировоззрения и этических ценностей объекта воздействия, а также в навязывании ему идей, отражающих видение окружающей реальности, свойственное инициатору информационной или психологической агрессии. Сторона, подвергающаяся психологическому воздействию, также подспудно приготавливается к следованию целям, которые диаметрально противоположны ее интересам[2].

Специфической чертой информационно-психологической агрессии в настоящее время выступает отчетливо выраженная избирательность. Сегодня целью пропагандистского воздействия отнюдь не является манипулирование всей совокупностью черт индивидуального или группового сознания. Как правило, на прак-

[1] См.: *Морозов А.* Психологическая война. Киев, 1996.

[2] См.: *Панарин И.* Технология информационной войны. М., 2003.

тике имеет место подчинение одного из качеств личности, вследствие чего достигается не полное, а частичное моральное или интеллектуальное «зомбирование» личности, что не исключает сохранение ее способности в целом адекватно оценивать окружающий мир.

По нашему мнению, в начале XX1 столетия имеет место количественное и качественное нарастание реальных участников информационно-психологического противоборства. После крушения советского политического режима консолидация общественных сил, прежде обусловленная необходимостью противодействия равной по силе супердержаве, в значительной мере сменилась поляризацией политических настроений. В связи с исчезновением прежнего соперника, разрушением «образа врага», особое содержание начинают приобретать внутренние противоречия и конфликты, острота и значение которых ранее были нивелированы потребностями в достижении приоритета над основным идеологическим и геополитическим соперником.

Ввиду этого методология информационных и психологических войн все в большей степени осваивается субъектами негосударственного происхождения, которыми в условиях глобализации могут выступать не только институты государственной власти, но и различные неправительственные организации, группы интересов, лоббистские группы и неформальные бизнес-сообщества.

Инструментом является обращение конфликтности вовнутрь общества или цивилизации, социально-политической формации. Дефрагментация общества, атомизация, распыление для самоуничтожения, – цель политики порабощения общества, в контексте которых реализуется психологическая война. При этом боьшое значение имеет формирование в структуре объекта поражения антагонистических по отношению друг другу элементов или, по крайней мере, агрессивных меньшинств, открыто посягающих на моральные устои и традиционные духовные ценности большинства граждан. Под сомнение ставятся системные основы национального или социального самосознания, цементирующие человеческие агрегации, сплачивающих ее перед лицом вызовов и угроз окружающего мира. Наибольший эффект достигается, когда общество или система, подвергаемые внешнему пропагандистскому воздействию пребывают в состоянии системного кризиса.

Благодаря возможностям системы электронных коммуникаций заинтересованные субъекты обретают возможность для достовер-

ной оценки ситуации в конкретном регионе России. Интенсивное распространение компьютерных сетей служит естественным каналом для проведения операций «информационной войны» в проблемных субъектах Российской Федерации. Так, благодаря возможностям Интернета могут передаваться указания, определяться цели и задачи, координироваться деятельность «внесистемной оппозиции», экстремистских организаций, транснациональным преступным сообществ. В результате инициаторы информационно-психологических войн против России на уровне субъектов федерации обретают возможность для определения социальных страт, воздействие на духовный мир и психологию которых может быть носить наиболее эффективный характер.

Как свидетельствует мировой и российский опыт, крупномасштабные реформы в сфере государственного строительства и управления неизбежно вступают в противоречие с интересами отдельных социальных слоев населения. Ввиду этого вдохновители и организаторы информационной агрессии стремятся абсолютизировать возникающие противоречия в области федеративной политики, стимулировать напряженность в проекциях «федеральный центр-регион» и «регион-регион», «муниципальная власть-регион», используя для этого возможности процесса информатизации.

Особую опасность для национальных интересов создает смещение приоритетов наступательных информационных действий с массированного воздействия на автоматические системы и средства вооружений, на психическую и духовную сферу личности, которое реализуется в условиях мирного времени. Ученые признают, что массовое сознание общества, служащее одним из основных объектов информационной безопасности, включает в себя несколько типичных моделей восприятия окружающей реальности. Именно на уровне подобных моделей происходит своего рода «просеивание» поступающих информационных потоков. Ввиду неоднородности общества, в том числе и в региональном аспекте, в социальной структуре существует иерархическая совокупность различных групповых ценностей, на основе которой и возникает система национальной ментальности. Наряду с архаическими представлениями она включает в себя и динамические элементы, привносимые в самосознание в том числе и посредством воздействия современных информационных технологий. В качестве наиболее уязвимых объектов манипуляции избираются так называемые фундаментальные ар-

хетипы, которые интенсивно разрушаются и заменяются новыми, привнесенными извне[1].

В интересах подрывных идеологических и психологических операций используются филиалы разведывательных служб, функционирующие под прикрытием институтов гражданского общества.

Отчасти современную ситуацию исправляет создание органов, предназначенных для противодействия экстремистским идеологиям, созданные в Федеральной службе безопасности и Министерстве внутренних дел. В июне 2007 г. в структуре российского Национального антитеррористического комитета была создана рабочая группа для противодействия идеологии терроризма. Ее задачей стал мониторинг ситуации в регионах, где возможно распространение экстремистских воззрений.

Представляется, что перечисленные структуры способны эффективно противостоять преимущественно очевидным подрывным идеологическим акциям. Изощренные меры косвенного воздействия, нацеленные на девальвацию традиционных духовных ценностей народа России, самобытности ее культурно-исторических регионов, по-прежнему не всегда распознаются органами охраны правопорядка и государственной безопасности. Последние зачастую не имеют соответствующей компетенции для идентификации подрывных акций в гуманитарной сфере и юридических оснований для привлечения к ответственности их исполнителей. Для исправления положения необходима продуманная государственная политика по защите духовного наследия российского общества. Оно должно предусматривать тесное сотрудничество органов публичной власти субъектов федерации, местного самоуправления и институтов гражданского общества, представителей творческой интеллигенции и журналистского корпуса, осознающих свою ответственность за сохранение самобытности отечественной культуры.

В России отсутствуют разработки единой концепции информационной войны, включающей как военный, так и финансовый, торговый, психологический, юридический и другие аспекты. В связи с этим на федеральном и региональном уровне необходимо предусмотреть: формирование специальных координирующих органов по контролю за созданием и применением технологий, способных

[1] См.: *Чалдини Р.* Психология влияния. СПб., 1999. С.24.

применяться в качестве информационного оружия; наращивание научных исследований в сфере информационно-психологической безопасности; разработку обоснованной юридической базы по обеспечению информационно-психологической безопасности; установление единой терминологии. Четкое распределение полномочий между федеральными ведомствами и институтами государственной власти субъектов федерации, наличие и исполнение единой концепции послужат гарантированной защите региональной информационной безопасности.