Г. Л. Акопов,
к. п. н., член РАПН, ст. преп. СКАГС

«КИБЕРВОЙНА» – УГРОЗА НА ПУТИ ФОРМИРОВАНИЯ СТАБИЛЬНОЙ ПОЛИТИЧЕСКОЙ СИСТЕМЫ

С древнейших времен информация являлась важнейшей составляющей любых политически значимых действий. Чем более развитым становится общество, тем более значимым фактором в этом обществе является информация. Грозным оружием современной эпохи стало слово, а наибольшее влияние и власть получает информационная элита. Именно поэтому органы государственной власти должны уделять такое пристальное внимание информационным ресурсам (в том числе и информационно-коммуникационным сетям общего пользования), какое в былые времена уделялось Вооруженным силам. Особо пристального внимания заслуживают теории информационных войн, разрабатываемые западными теоретиками.

Американские теоретики в большинстве случаев под информационной войной понимают форму агрессивной борьбы сторон, представляющую собой использование специальных методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах реализации поставленных целей и задач. В трактовке отечественных ученых информационная война – это действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственной информации, процессов, основанных на информации, и информационных систем.

Сегодня к проблемам информационных войн все чаще обращаются не только иностранные, но и отечественные[1] ученые. Большинство современных исследователей рассматривают информационные войны и противоборства глобально, абстрагируясь от сетевой составляющей данного явления. Наибольший интерес для нас представляет лишь отдельная площадка ведения информационных войн, которая, по нашему мнению, заслуживает особого внимания. Речь идет о всевозрастающем информационном противоборстве с использованием компьютерных сетей общего пользования. Очевидно, что уже сегодня мировое сообщество стоит на пороге новой эпохи информационных противоборств, эпохи кибервойн. Понятие кибервойны развивается и уточняется. Мы проводим свое исследование, определяя кибервойну как информационное противоборство с использованием информационно-коммуникационных компьютерных сетей общего пользования для достижения поставленных целей и задач[2].

Цели и задачи при осуществлении кибервойн преследуются разнообразные. для большей ясности назовем наиболее распространенные:

– размещение в сети «Интернет» заведомо ложной или провокационной информации для ее последующего распространения в средствах массовой информации и сетевом сообществе;

– манипулирование общественным сознанием, навязывание необходимой идеологии (влияние на общественное мнение);

– вербовка сторонников и единомышленников;

– несанкционированный доступ к информационным ресурсам с последующим их искажением или хищением;

– подрыв международного авторитета государства;

– влияние на принятие политически значимых решений;

– создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию;

– дестабилизация политических отношений в обществе;

---

[1] Расторгуев С. П. Информационная война, М., 1998; Прокофьев В. Ф. Тайное оружие информационной войны. М., 1999; Мухин А. А. Информационная война в России. М., 2000; Панарин И. Н. Информационная война и выборы. М., 2003 и др.

[2] Акопов Г. Л. Глобальные проблемы и опасности сетевой политики: Монография. Ростов-на-Дону. ООО «Ростиздат», 2004, стр. 39

– распространение компромата и иных сведений, порочащих честь и достоинство политической элиты страны;

– создание атмосферы напряженности между партиями, общественными объединениями и движениями;

– политический либо иной шантаж;

– разжигание межнациональной розни и расовой нетерпимости;

– воздействие на экономическую инфраструктуру государственного образования;

– инициирование массовых беспорядков и иных протестных акций.

Далее мы попробуем на основе примеров проиллюстрировать методы осуществления перечисленных выше задач.

Сегодня становится очевидным тот факт, что сугубо информационная направленность сети «Интернет» постепенно заменяется явно выраженным агитационным, популистским, а иногда и агрессивным подходом. Проникновение материалов из сети «Интернет» в традиционные средства массовой информации стало обычным явлением, несмотря на то, что в сети «Интернет» может быть опубликовано все, что угодно. Интернет-СМИ отличаются от обычных средств массовой информации тем, что там можно публиковать новости не только дешево и оперативно, но и, что самое примечательное, анонимно. Это делает их идеальным инструментом для различного рода политических провокаций.

Наиболее распространенным приемом осуществления политических кибервойн может считаться вброс компромата посредством специализированных Интернет-сайтов. В сети функционируют целые порталы планомерно вбрасываемого компромата. Соответствующие сайты чрезвычайно популярны среди пользователей, желающих получить соответствующую информацию. Причем в отличие от ряда подобных ресурсов здесь компромат базируется, создается своего рода библиотека компромата, однако достоверность данных, разумеется, никто не гарантирует.

Существуют в сети и сайты, дискредитирующие не только политику партий или индивидов, но и политику целых государств, осуществляя тем самым информационные атаки не на те или иные политические институты, а на государственный суверенитет. Так, в сети на протяжении нескольких лет существовал сайт чеченских сепаратистов, открыто выступавший не только против проведения контртеррористической операции в Чеченской республике, но и призывающий бороться против федеральных властей. На следующий день после теракта в ДК на Дубровке пропагандистский сайт был ликвидирован группой российских программистов.

Исходя из мировой практики, создается впечатление, что действия программистов – это возможно единственный адекватный ответ на акции сетевых провокаторов. Законодательные меры оказываются неэффективными. Например, в сентябре 2003 года суд Вильнюса признал незаконными действия литовского Департамента госбезопасности, который в июне 2003 года закрыл один из сайтов чеченских сепаратистов как содержащий пропаганду терроризма, национальной и религиозной розни. Закрыть сайт требовали от Литвы и российские власти. Однако уже в конце сентября 2003 года суд Вильнюса вынес решение в пользу создателей сайта. Интересы создателей страницы защищала литовская комиссия по журналистской этике – они настаивали на том, что «опубликованные на сайте материалы следует трактовать как подстрекательство против оккупационных российских властей, однако подстрекательства против русских или христиан отсутствуют». Суд, как ни странно, с этими доводами согласился[1]. Другой, не менее интересный пример: в апреле 2003 года руководство Эстонии ответило отказом на требование России запретить одной из коммерческих фирм этой прибалтийской страны сотрудничать с чеченскими террористами. Как сообщала телекомпания НТВ, данная компания предоставляла чеченским экстремистам услуги по размещению Интернет-сайта боевиков. По словам эстонского премьер-министра, «сайт находится не на сервере правительства Эстонии, поэтому кабинет в его деятельность вмешиваться не станет, несмотря на то, что Россия требует его закрыть». 19 сентября власти Литвы (только после теракта в Беслане) временно заблокировали чеченский информационный сайт, публиковавший за-

[1] www.ntv.ru Суд Вильнюса разрешил деятельность сайта чеченских экстремистов. 01. 10. 2003

явления лидеров чеченских боевиков. Кстати, одной из последних публикаций этого сайта было заявление чеченского полевого командира Шамиля Басаева, в котором тот взял на себя ответственность за захват заложников в Беслане.

Специализированные сайты террористов наносят ощутимый информационный урон государственной политике. На подобных сайтах боевики сообщают о готовящихся терактах, выдвигая различные условия, запугивая общественность и шантажируя власти. Все чаще террористы берут на себя ответственность через Интернет-сайты или, еще чего хуже, вывешивают на своих сайтах фотографии жертв, взрывов и даже видеоролики отснятых терактов и казней. Нередко посредством своих сайтов боевики отчитываются о проделанной работе или обращаются с посланиями к определенной категории граждан. Наибольший эффект эти заявления получают благодаря массовому цитированию новых сообщений от террористов всевозможными средствами массовой информации.

По данным исследования, проведенного институтом United States Institute for Peace (USIP), террористы адресуют свои сайты трем типам аудитории: активным членам и сочувствующим, международной общественности для формирования соответствующего мнения, противникам с целью их деморализации. Все более или менее серьезные представители экстремистских организаций располагают не только веб-сайтами, но и форумами, и досками объявлений, где могут пообщаться их сторонники. Террористы также широко используют электронную почту, чтобы связаться со своими сторонниками в других странах. С помощью почты проходит и вербовка новых участников террористических группировок.

Администрации многих стран в меру сил пытаются бороться с проявлением кибертеррора. В конце 2003 года США впервые внесли в свой список «иностранных террористических организаций» несколько Интернет-сайтов. Согласно американскому законодательству эти сайты теперь вне закона и запрещена любая материальная поддержка этих сайтов, их сотрудникам запрещен въезд на территорию США, а американские банки должны заморозить их счета. Однако, как сообщило агентство Reuters, даже сам Госдепартамент пока не понимает, каким образом это будет сделано.

Свободное распространение информации в Интернете не на шутку беспокоит спецслужбы, осознавшие свою слабость перед лавинообразно увеличивающимся потоком информации и, что не менее важно, дезинформации.

Единственный метод, которым можно, с точки зрения официальных лиц, остановить появление террористов-самоучек – это цензура. Нечто подобное после 11 сентября 2001 года практиковали США. Тогда из общего доступа были удалены многие ресурсы, представляющие хоть какую-то ценность для потенциальных террористов. Цензура введена и на территории Китая, где, помимо всего прочего, ограничен доступ к зарубежным СМИ.

Подобные меры, принимаемые в ряде стран, востребованы, хотя и не всегда являются популярными. Возможно, что с течением времени образуются учреждения, предсказываемые М. Кастельсом «On-line полицейские патрули»[1] – специальные полицейские подразделения, в задачи которых входят расследование он-лайн-преступлений и слежка за распространением запрещенных публикаций в киберпространстве. Структуры, следящие за содержанием сети «Интернет», безусловно, востребованы уже сегодня.

Совсем не случайно Ю. М. Лужков опубликовал 16 мая 2004 года в газете «Известия» статью «О темной стороне Интернета». Основной смысл названной публикации сводился к тому, что необходим специальный закон об Интернете. Кому, как не мэру столицы, неоднократно подвергавшемуся сетевым нападкам, говорить об этом. И с ним трудно не согласиться.

Но нужно четко понимать, что борьба за содержание киберпространства представляется крайне сложной задачей. Прежде всего потому, что всемирная сеть, как известно, не имеет границ. Если в одной стране принято законодательство, жестко регулирующее публикации в национальном сегменте сети «Интер-

---

[1] Кастельс Мануэль. Информационная эпоха. Экономика. Общество и культура. Пер. с англ. Под науч. ред. профессора О. И Шкаратана М., Государственный университет – высшая школа экономики, 2000, стр. 510

нет», сами жители этой страны без труда будут размещать свои сайты на зарубежных серверах.

Однако все больше цивилизованных государств задумываются о необходимости контроля над всемирной компьютерной сетью, поскольку угрозы информационной безопасности государства, общества и личности носят реальный, угрожающий характер. На протяжении столетий контроль над информацией являлся одной из важнейших функций государственной власти и потеря этой функции в связи с массовым распространением неконтролируемой информации из Всемирной паутины (которую все чаще называют всемирной информационной свалкой) может обернуться трагедией.

Но несмотря на этот факт, ряд исследователей все еще считают проблемы информационных противоборств надуманными, а исследования информационных войн в области компьютерных сетей в нашей стране практически не ведется, лишь в последнее время можно встретить эпизодические заметки по данной проблеме. Считается, что воздействие сетевых атак и информационных противоборств по средствам глобальной компьютерной сети иллюзорно. Как мы можем судить, исходя из обозначенных выше фактов, такое мнение является ошибочным. Кибервойна – явление, безусловно, виртуальное, но имеющее реальное влияние не только на сетевое сообщество, но и на все общество в целом.