Internet – джин, выпущенный из бутылки

"Кибервойна" – угроза национальной безопасности

Григорий Акопов,
кандидат политических наук,
член РАПН

С древнейших времен информация являлась важнейшей составляющей любых политически значимых действий. На протяжении всей истории цивилизации общественно-политические элиты плели интриги, проводили заговоры и манипулировали мнением окружающих. Что же касается непосредственно противоборств в сфере информации, то чем более развитым становилось общество, тем более изощренными были методы получения и распространения разнообразной политической информации и дезинформации, а также политической пропаганды. На современном этапе можно с уверенностью говорить об информационных баталиях и войнах, глобальных информационных противоборствах и локальных конфликтах.

Для военного "истеблишмента" становится очевидным, что современное общество зависимо от информационных систем, а наиболее современный способ воздействия на противника – воздействие на его граждан (манипуляция общественным сознанием). Эта стратегия наиболее эффективна для нанесения вреда противнику. Чем более развитым становится общество, тем более значимым фактором в этом обществе является информация.

Информационное противоборство присутствовало во всех войнах и проявлялось в различных формах, будь то ведение разведки, распространение дезинформации, либо проведение агитационных акций, захват средств получения и передачи информации и т.д. С появлением и развитием ядерного оружия перспектива реальных военных действий грозит трагедией для обеих сторон участников конфликта, именно поэтому для достижения своих целей выгоднее использовать информационное оружие, нежели традиционные вооружения.

Сегодня влияние армии и военных подразделений в решении политических споров и конфликтов сведено к минимуму, военная элита потеряла свое былое величие и влияние в обществе. 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.

Разработчики концепции информационной войны часто цитируют известный тезис древнекитайского военного теоретика и полководца Сун Цзы: "Подавить противника, не вступая в схватку с ним, есть величайшая мудрость военного искусства". Если конечная цель военного (и шире – политического) конфликта – навязать противнику свою волю и установить контроль над его экономическими, техническими и прочими значимыми ресурсами, вряд ли "мудро" достигать ее путем физического уничтожения значительной части этих ресурсов. Подавление политической воли и способности противника к сопротивлению посредством воздействия на его сознание, информацию об окружающем мире, безусловно, больше отвечает постулату китайского мудреца[1].

Первоначально термин "*информационная война*" использовал Томас Рона в отчете, подготовленном им в 1976 г. для компании "Боинг", и названном "Системы оружия и информационная война". Т.Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она становится и уязвимой целью как в военное, так и в мирное время.

Публикация отчета Т.Рона послужила началом активной кампании в СМИ. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься "секретными материалами". Военные аналитики США начали активно исследовать данное направление. Пик изучения данной проблематики, пришелся на период распада СССР. Если вспомнить развал Советского Союза, то без сомнения можно сказать, что он стал результатом информационной открытости и беззащитности, которая пришла в страну вместе с перестройкой. Возможно, причина кроется именно в новых формах ведения войн.

После окончания "холодной войны" термин "информационная война" был введен в документы Минобороны США. Он стало активно упоминаться в прессе после проведения операции "Буря в пустыне" в 1991 г., где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 г[2].

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 исследователи, и не только иностранные, но и отечественные[3] ученые начинают обращать внимание на данную проблему. Большинство современных исследователей рассматривают информационные войны и противоборства глобально, абстрагируясь от сетевой составляющей данного явления.

Проникновение материалов из сети "Интернет" в традиционные СМИ стало обычным явлением. Все чаще журналисты центральных и региональных изданий обращаются за оперативной и бесплатной информацией в сети "Интернет". Иногда информация из сетевых источников проходит в СМИ без ссылки, либо с пометкой "материал взят из Интернет". В случаях, когда ссылка все-таки есть, материал все равно не проходит должной проверки, несмотря на то, что в сети "Интернет", может быть опубликовано все что угодно. Имеется реальная возможность разместить нужный материал в сети "Интернет", а потом сослаться на Сеть в случае возникновения каких-либо проблем, а с "Интернета", как известно, "взятки гладки" (за исключением тех случаев, когда материал размещен на специально зарегистрированных информационных порталах).

"Интернет" упростил жизнь многим традиционным СМИ. Большинство газет превратились в своего рода дайджест "Интернета". Появились даже специализированные газеты и журналы, публикующие исключительно материалы из сети "Интернет". В газетах и журналах появляются материалы из Сети, на особенно популярные web-издания ссылаются центральные СМИ. Публикация в сети "Интернет" актуального и тем более сенсационного материала мгновенно находит отражение в прессе. Примеров этому существует множество. В 1999 г. в российском "Интернете" возникли ресурсы, обращенные, в первую очередь, к журналистской аудитории и специализирующиеся на регулярной публикации "сенсационных" фактов, как правило, это был разнообразный компромат. Распечатки этих сетевых изданий ложились на столы главных редакторов газет и журналов, а также руководителей различных пресс-служб.

Интернет-СМИ отличаются от обычных СМИ 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.

Хронологию этих провокаций в российском Интернете можно отсчитывать с ноября 1998 г., когда на российском сервере бесплатных web-страниц был размещён сайт "Коготь", содержащий список домашних адресов и телефонов многих известных чиновников, расшифровки телефонных переговоров, а также некоторые оперативные подробности. "Коготь" был прикрыт спецслужбами через пару часов после появления в сети.

Но появилась его вторая версия – "Коготь-2", – она продержалась гораздо дольше, так как была зарегистрирована в США. Как утверждают специалисты, так называемые "Когти" оказались репетицией. Скорей всего, политтехнологи проверили таким образом эффективность использования Интернета для "раскрутки" скандала. С приближением выборов Интернет становится похожим на систему для политических провокаций.

Примеров тому масса, можно вспомнить историю про сайты Ю.М.Лужкова в 1999 г., когда к группе сайтов, так или иначе связанных с именем мэра Москвы, добавился ещё один – www.lujkov.ru. По дизайну первой страницы он был почти идентичен личному сайту мэра. Но содержание для Лужкова было крайне неприятным. Спустя несколько часов после своего появления lujkov.ru был частично закрыт.

Или другой пример. Незадолго до выборов в Госдуму третьего созыва в Сети, помимо официального веб-сайта Г.А.Зюганова www.zyuganov.ru появился "паразитический" сайт www.zuganov.ru, на котором образ лидера российских коммунистов выглядел совсем не престижно. После выборов сайт перестал функционировать, очевидно, он был создан противниками КПРФ на предвыборный период для дискредитации имиджа руководителя КПРФ.

Наиболее распространенным приемом осуществления политических кибервойн может считаться вброс компромата посредством специализированных интернет-сайтов. В сети функционируют целые порталы планомерно вбрасываемого компромата.

Например, сайт "Compromat.ru" неизменно пользуется популярностью 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. Несмотря на это, сайт "Compromat.ru" является одним из самых популярных ресурсов российского политического Интернета, ежедневно его просматривают несколько тысяч человек, а общее количество просмотров данного ресурса превышает отметку в 50 млн.

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" (kavkaz.org), открыто выступавший не только против проведения контртеррористической операции в Чеченской Республике, но и призывающий бороться против федеральных властей.

Kavkaz.org неоднократно пытались ломать. В марте 2002 г. группа хакеров, скрывающаяся под псевдонимом "Сибирская сетевая бригада", смогла частично ликвидировать сайт. При попытке открыть электронную страницу на экране появлялись сообщения антитеррористической направленности. 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 возможно единственный адекватный ответ на акции сетевых провокаторов. Законодательные меры оказываются неэффективными.

Например, в сентябре 2003 г. суд Вильнюса признал незаконными действия литовского Департамента госбезопасности, который в июне 2003 г. закрыл сайт "Кавказ-Центр". Тогда создателей интернет-ресурса обвинили в пропаганде терроризма, национальной и религиозной розни. Были проведены обыски в офисе фирмы, которая размещала электронную страницу на своем сервере. Закрыть "Кавказ Центр" требовали от Литвы и российские власти. Однако интересы "Кавказ-Центра" защищала литовская комиссия по журналистской этике: она настаивает на том, что "опубликованные "Кавказ-Центром" материалы следует трактовать, как подстрекательство против оккупационных российских властей, однако подстрекательства против русских или христиан отсутствуют".

Другой, не менее интересный пример: в апреле 2003 г. руководство Эстонии ответило отказом на требование России запретить одной из коммерческих фирм этой 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".

13 сентября 2004 г. после ряда террористических актов МИД России вновь потребовало прекращения работы сайта чеченских боевиков "Кавказ-Центр".

Требования российских властей вполне обоснованы. Специализированные сайты террористов наносят ощутимый информационный урон государственной политике. На подобных сайтах боевики пишут о готовящихся терактах, выдвигают различные условия, запугивая общественность и шантажируя власти.

Все чаще террористы берут на себя ответственность через интернет-сайты или вывешивают на своих сайтах фотографии жертв, взрывов и даже видеоролики отснятых терак-

эти сетевые ресурсы наносят не малый вред и способны не только внедрять идеи сепаратизма в массовое сознание, но и рекрутировать новых членов террористических организаций.

Как сообщила газета *"Washinfton Times"* за 29 июня 2004 г., наиболее активным пользователем "всемирной паутины" среди террористов является возглавляющий ячейку "Аль-Каиды" в Ираке Абу Мусаб аль-Заркави. Он использует сеть "Интернет" для вербовки сторонников и сбора средств на проведение террористических актов, направленных против сил коалиции и нового иракского правительства.

Газета приводит слова представителя коалиционных сил: "Аль-Заркави продолжает широко использовать интернет и СМИ, чтобы обмениваться информацией с другими террористическими группами, а также для того, чтобы запугивать страны коалиции и любые другие силы, поддерживающие восстановление Ирака". В частности, аль-Заркави и его боевики разместили на исламистских сайтах видеосюжеты с казнью американца Ника Берга и южнокорейского гражданина Ким Сон Ира.

Американцы пытаются оперативно закрывать сайты, на которых "засветился" известный террорист. Однако аль-Заркави каждый раз ухитряется найти новый способ публиковать в Сети факты своих деяний.

Террористы также широко используют электронную почту, чтобы связаться со своими сторонниками в других странах. С помощью почты проходит и вербовка новых участников террористических группировок. Сейчас, по данным американцев, у аль-Заркави "несколько сот сторонников" и он собирает добровольцев по всему исламскому миру.

Как известно из многих источников, связь с членами экстремистских группировок также осуществляется с помощью сети "Интернет".

Например, Мухаммад Наим Нур-Хан (*Muhammad Naeem Noor Khan*), задержанный в Пакистане по подозрению в связях с террористами, рассказал следователям, что для связи члены "Аль-Каиды" использовали веб-сайты и электронную почту в Турции, Нигерии и областях, занятых пакистанскими племенами.

Администрации многих стран в меру сил пытаются бороться с проявлением кибертеррора. В конце 2003 г. США, впервые внесли в свой список "иностранных террористических организаций" несколько интернет-сайтов.

Список, опубликованный Госдепартаментом США в Федеральном регистре, включает сайты newkach.org, kahane.org, kahane.net, kahanetzadak. com в качестве другого названия еврейской организации "Кахане Хай" или "Ках", которая подозревается в организации нападений на палестинцев.

Согласно американскому законодательству, эти сайты теперь вне закона и запрещена любая их материальная поддержка, 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.

Например. В середине декабря 2003 г., после оглашения предварительных результатов думских выборов, в сети "Интернет" появился интернет-сайт www.fairgame.ru с параллельным подсчетом голосов на думских выборах.

После официального оглашения итогов выборов, председатель Центризбиркома РФ А.Вешняков говоря о появившемся в Интернете сайте, заметил, что: "Следы этого сайта ведут в Лондон, но кто конк-

ретно стоит за этим – пока неизвестно". По словам Вешнякова, попытка уточнить, кому принадлежит сайт, не дала результатов. Только через технические каналы удалось выяснить, что он заполняется из Великобритании.

Как ранее сообщал NEWSru.com и некоторые другие издания, альтернативная система голосования, о которой идет речь, была создана КПРФ.

9 декабря создатель этой системы, руководитель ИТЦ КПРФ Илья Пономарев, сообщил следующее: "Это действительно альтернативная "ГАС-Выборам" система. Наши наблюдатели на местах собирают точные данные с участков и сообщают их в наш информационно-аналитический центр". По данным Fairgame на 19 декабря: единороссы набрали 34,2% голосов; КПРФ – 12,54%; ЛДПР – 11,56%; Блок "Родина" – 10,49%; Российская демократическая партия "Яблоко" – 5,2%; Союз правых сил – 4,61%; блок РПП и ПСС – 3,16%; Аграрная партия России – 3,35%; Число голосов избирателей, поданных против всех федеральных списков кандидатов – 5,19%[6].

Единственный метод, которым можно, с точки зрения официальных лиц, остановить появление террористов-самоучек – это цензура. Нечто подобное после 11 сентября 2001 г. 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"[7]. Первые прототипы подобных организаций появились в августе 2004 г. во Вьетнаме, там было сформировано специальное полицейское подразделение, в задачи которого входит расследование онлайн-преступлений и слежка за распространением запрещенных публикаций в киберпространстве[13]. Структуры, следящие за содержанием сети "Интернет", безусловно, востребованы уже сегодня.

Это связано с тем, что в сети масса вредных и провокационных сайтов, помимо того, что с их помощью экстремисты распространяют свои идеи и вербуют сторонников, с помощью специализированных сайтов можно овладеть многими опасными навыками (научиться взламывать сетевые ресурсы). В сети можно встретить и сайты, содержащие или даже продающие различные тайны, в том числе и государственные. В сети открыто пропагандируются, а порой и продаются запрещенные товары (наркотики или оружие). А специализированные сайты научат, как это все грамотно использовать.

Все больше 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 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 последние время можно встретить эпизодические заметки по данной проблеме. Считается, что воздей-

Наибольший интерес для нас представляет всевозрастающее информационное противоборство с использованием компьютерных сетей общего пользования. Еще в конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции "*Force XXI*"). В ее основу было положено разделение всего театра военных действий на две составляющих – традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Особенно с учетом перспективы распространения ИКТ. Очевидно, что уже сегодня мировое сообщество стоит на пороге новой эпохи информационных противоборств, эпохи кибервойн.

Понятие кибервойны развивается и уточняется. Однако уже сегодня можно обозначить два направления развития трактования данного термина.

Согласно *одному направлению* кибервойны исследуются как развитие и распространение информационных технологий в военной области, подразумевая под собой высокоточное оружие, технологии "стелс", боевые и разведывательные радиоэлектронные средства и, даже, футуристические разработки в области роботизации и автоматизации.

Другое направление исследований понимает кибервойны как элемент информационных войн, осуществляемый посредством всемирной паутины.

Именно в этом направлении мы и сконцентрируем свое исследование, определив **кибервойну** как – **информационное противоборство с использованием информационно-коммуникационных компьютерных сетей общего пользования для достижения поставленных целей и задач**[4].

Цели и задачи при осуществлении кибервойн преследуются разнообразные.

Назовем наиболее распространенные:

- размещение в сети "Интернет" заведомо ложной или провокационной информации для ее последующего распространения в СМИ и сетевом сообществе;
- манипулирование общественным сознанием, навязывание необходимой идеологии (влияние на общественное мнение);
- вербовка сторонников и рекрутирование 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;
- 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.

Сегодня становится очевидным тот факт, что сугубо информационная направленность сети "Интернет" постепенно заменяется явно выраженным агитационным, популистским, а иногда и агрессивным подходом.

ствие сетевых атак и информационных противоборств по средствам глобальной компьютерной сети иллюзорно. Приведенные факты говорят об ошибочности такого мнения. Кибервойна явление, безусловно, виртуальное, но имеющее реальное влияние не только на сетевое сообщество, но и на все общество в целом.

Примечания

[1] *Турунок С.* Информационно-коммуникативная революция и новый спектр военно-политических конфликтов // Полис. 2003. № 1.

[2] *Гриняев С.Н.* Информационная война: история, день сегодняшний и перспектива. http://www.agentura.ru/equipment/psih/info/war/

[3] *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.

[4] *Акопов Г.Л.* Глобальные проблемы и опасности сетевой политики: Монография. Ростов-на-Дону: ООО "Ростиздат", 2004. С. 39.

[5] *Шалоумов Е., Баусин А.* "Аль-Каида" завоевывает интернет. Известия. № 144. 2004. 28 апреля. 2004. 10 августа.

[6] NEWSru.com. 19.12.2003.

[7] *Кастельс М.* Информационная эпоха. Экономика. Общество и Культура. Пер. с англ. Под науч. Ред. проф. *О.И Шкаратана* М.: Государственный университет – высшая школа экономики, 2000. С. 510.