Информационная борьба в системе национальной безопасности

Василий Кириленко

Современные каналы массовой коммуникации всего мира становятся новой виртуальной силовой ареной геополитической борьбы и, в частности информационной. На первый взгляд информационная борьба является невидимой и бескровной, в действительности – жестокой и беспощадной. Промежуточные итоги информационной борьбы за пространство становятся зримыми и реальными после очередных так называемых "американских гуманитарных антитеррористических операций", в результате которых на карте мира исчезают целые государства.

В XXI в. судьба пространственных отношений между государствами определяется, прежде всего, информационным превосходством в виртуальном пространстве, что привело к возникновению новой информационной парадигмы геополитики. С учетом этого назрела объективная необходимость создания новой концепции обеспечения национальной безопасности государства, в основе базиса которой является информационное превосходство. Эта концепция позволила бы разработать современную геополитическую стратегию в интересах достижения роста боевой мощи государства с помощью информационных технологий.

Современное глобальное информационное пространство, в котором одно из важных мест занимает Интернет, в целом средства массовой коммуникации, – это виртуальный, невоспринимаемый сознанием человека мир, управляемый информацией. Невидимые человеку нити скрытого информационного воздействия формируют контуры будущего мира.

Эти новые приоритеты национальной безопасности в американской геополитической стратегии XXI в. обозначены следующим образом: "Наш принципиальный подход заключается в следующем:

– *во-первых*, мы должны быть готовы использовать все инструменты национальной мощи для оказания влияния на действия других государств и сил;

КИРИЛЕНКО Василий Иванович – кандидат юридических наук.

Ключевые слова: государственная информационная политика; информационная борьба; информационная война; информационное противоборство; информационное оружие.

– *во-вторых*, нам необходимо иметь волю и возможности для выполнения роли глобального лидера и оставаться желанным партнером для тех, кто разделяет наши ценности...

Лидирующая роль США подкрепляется силой демократических идеалов и ценностей. Вырабатывая стратегию, мы исходим из того, что распространение демократии укрепляет американские ценности и повышает нашу безопасность и благосостояние. Следовательно, тенденция к демократизации и распространению свободных рынков по всему миру способствует продвижению американских интересов"[1].

В этой связи значение информационной борьбы и ее составляющих форм: информационных войн и информационного противоборства, в современных условиях значительно возрастает для обеспечения национальной безопасности государства[2].

Как показало исследование научных разработок ученых и практиков, информационная борьба в рамках научного исследования может рассматриваться на различных уровнях познания:

– социальное явление;

– политические конфликты;

– особая форма политического конфликта;

– часть системы инструментов политического регулирования отношений[3].

На каждом из этих уровней информационную борьбу можно рассматривать через научные гипотезы.

1. Социологическая гипотеза информационной борьбы – это социальное явление и новая форма общественных отношений, порождаемая информационным обществом.

Информационная борьба рассматривается как новая форма социальных отношений (объект социологического анализа), а спектр конфликтных ситуаций, порождаемых информационной борьбой, – как внешнее проявление системных свойств данного объекта.

2. Статистическая гипотеза информационной борьбы – это поле политических конфликтов, находящихся в тесной взаимосвязи, взаимозависимости и взаимодействии.

Информационная борьба рассматривается как сложная высокодифференцированная система политических конфликтов, каждый из которых проявляется как единичная реализация конфликтных ситуаций, генерируемых или проявляемых полем информационной борьбы.

3. Конфликтологическая гипотеза информационной борьбы – система политических конфликтов для разрешения противоречий по вопросам власти и управления, в которых столкновение сторон осуществляется в форме информационных войн с применением информационного оружия[4].

В рамках конфликтологической гипотезы формы осуществления информационной борьбы рассматриваются как политические конфликты, имеющие самостоятельное значение в виде объекта исследования и управления, находящиеся во взаимодействии и взаимообусловленности друг с другом.

4. Системно-функциональная гипотеза информационной борьбы как часть системы политического регулирования, один из инструментов политических отношений.

Это часть системы политической борьбы как агрессора, так и жертвы агрессии, в рамках которой информационно-политические конфликты, порождаемые информационной борьбой, интегрируются в структуру политической системы конфликтующих сторон и ис-

пользуются ими в качестве инструментов политического регулирования[5].

Цель информационной борьбы – разрешение противоречий по вопросу власти и осуществления политического руководства в информационном обществе.

В соответствии с названной целью можно выделить следующие задачи информационной борьбы:

– достижение и сохранение мирового информационного превосходства в собственных интересах и установление контроля над международной информационной сферой;

– оказание влияния на политических, государственных и общественных деятелей зарубежных стран;

– создание благоприятного для государства общественного мнения в зарубежных странах, в частности за счет проведения пропагандистских и контрпропагандистских мероприятий;

– достижение военно-политического превосходства и безусловного лидерства в сфере международных отношений; осуществление полувоенных (специальных) акций для поддержки или свержения существующих в зарубежных странах режимов в собственных интересах;

– установление контроля над информационным пространством противостоящей стороны, который может быть полным, частичным или локальным (над одной или несколькими системами);

– оказание в явной или скрытной форме выгодного целенаправленного информационного воздействия, обеспечивающего управление действиями противостоящей стороны в соответствии с заявленными интересами;

– защита собственного информационного пространства от упреждающих или ответных действий;

– обеспечение благоприятных условий для перехода собственной национальной системы социально-политических отношений на новый, более высокоразвитый и высокотехнологичный этап эволюционного развития.

Необходимо отметить, что информационная борьба является также частью системы информационной политики, поскольку для агрессора такая форма информационной борьбы как информационная война – средство достижения политических целей, для жертвы агрессии – средство нанесения ответного информационного удара и восстановления военно-политического баланса.

Таким образом, информационная борьба – социальное явление, являющееся частью системы политического регулирования отношений между государствами и находящееся в тесной взаимосвязи и взаимозависимости от политических конфликтов для разрешения противоречий и получения определенного выигрыша в политической, военной, материальной и других сферах, в которых столкновение сторон осуществляется для оказанная выгодного влияния, подчинения и (или) разрушения систем управления (социальных и технических) противостоящей стороны.

Анализ закономерностей ведения войн, различного рода конфликтов, противоборств между спецслужбами, организациями и даже личностями свидетельствует о том, что ход и исход разведывательных, боевых и иных действий любого масштаба в современном мире определяются искусством ведения информационной борьбы. В информационную борьбу вовлечены, как правило, все государственные структуры, в том числе люди и общество в целом.

Рассматривая такую форму информационной борьбы как информационное противоборство, необходимо отметить, что в информационном противоборстве участвуют в основном меха-

низмы обеспечения национальной безопасности государства, в которых одна из основных ролей должна отводиться спецслужбам.

Цель информационного противоборства – не допустить захвата информационной сферы государства противоборствующей стороной и одновременно взять под контроль информационную сферу другого государства в интересах достижения политических, экономических и иных целей своего государства[6].

В соответствии с законодательной базой *информационное противоборство* осуществляется в мирное время и определяется как форма ведения информационной борьбы государств с использованием как специальных (разведывательных и оперативно-розыскных), так и обычных (политических, экономических, дипломатических, военных и иных) методов, способов и средств воздействия на информационную среду противостоящей стороны для достижения политических, экономических и иных целей и защиты собственных интересов.

Информационное противоборство можно подразделить на сферы его ведения:

– в сфере развития и функционирования информационной инфраструктуры и информационных ресурсов Российской Федерации;

– в сфере противоправной деятельности национальных органов иностранных государств в информационном пространстве, а также использования возможностей и достижений информатизации этими органами и организациями, террористическими, экстремистскими и иными организациями и отдельными лицами для осуществления деятельности в ущерб безопасности Российской Федерации;

– в сфере иной деятельности национальных органов иностранных государств в информационном пространстве, а также использования его возможностей антироссийскими и другими силами для нанесения ущерба политической системе общества, оказания негативного информационно-психологического воздействия на органы власти и управления, политические партии и движения, СМИ, широкие общественные слои и отдельных граждан.

При осуществлении противоборства *в первой сфере* его ведения одним из основных объектов воздействия и защиты являются информационные ресурсы (отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в том числе в архивах, фондах, библиотеках, банках данных, других информационных системах): государственные и негосударственные, открытые и закрытые, а также информационная инфраструктура.

Во второй сфере его ведения – специальная деятельность, заключающаяся в применении системы оперативно-розыскных и иных мер российских правоохранительных органов, направленная на выявление, предупреждение угроз информационной безопасности России со стороны противоправной деятельности национальных органов и организаций иностранных государств, террористических и иных преступных и экстремистских организаций и отдельных лиц, наносящих ущерб безопасности Российской Федерации, их локализацию и нейтрализацию, парирование этих угроз.

В третьей сфере его ведения – защищенность от манипулятивных воздействий на личность, на ее представления и эмоционально-волевую сферу, на групповое и массовое сознание, которые осуществляются с применением инструмента психологического давления (различных видов информационного оружия) для явного или срытого по-

буждения индивидуальных и социальных субъектов к действиям в ущерб собственным интересам в интересах отдельных лиц, групп или организаций, осуществляющих эти воздействия; защита психики высшего руководства страны, силовых ведомств и спецслужб противостоящих сторон, системы формирования общественного мнения и принятия решений и так далее.

Вместе с тем, все сферы информационного противоборства между собой тесно взаимосвязаны и образуют единую систему ведения информационного противоборства государства.

Информационное противоборство всегда было и есть в самых различных областях межгосударственных отношений. Однако благодаря появлению новейших видов информационного оружия возникла новая возможность более продуктивного, но вместе с тем и опасного для общества, воздействия на информационную сферу того или иного государства, вплоть до ее захвата или уничтожения. Появилась новая форма информационной борьбы – *информационная война*, которая осуществляется в интересах уничтожения телекоммуникационных систем или взятие их под свой контроль, нанесения психологического удара по населению и личному составу вооруженных сил и т.п. с возможным последующим ведением боевых действий на суше, морском и воздушном пространствах для достижения политических, экономических и иных целей и защиты собственных интересов.

Средством реализации концепций информационных войн служит информационное оружие.

Стратегические тайные операции США в ряде стран (Югославия, Ирак, Афганистан) показали возможности информационного оружия по воздействию на личный состав вооруженных сил и массы людей из виртуальной реальности с последующим захватом информационных пространств государств и их территорий и подчинением людей в своих целях.

Объектами воздействия могут являться:

– информационно-технические и информационно-аналитические системы;

– информационно-технические и информационно-аналитические системы, включающие человека;

– информационные ресурсы;

– система формирования общественного мнения, базирующаяся на средствах массовой информации и пропаганды;

– психика человека.

Анализ научной и специальной литературы, в том числе зарубежных источников, показал, что, как правило, информационная война против другого государства осуществляется накануне войны (возможно локального конфликта) с применением традиционных сил и средств. Ее планирование и осуществление ведется специальными подразделениями вооруженных сил с привлечением других силовых структур и спецслужб.

В результате информационной борьбы между государствами возникают внешние угрозы безопасности Российской Федерации[7].

Вместе с тем, внутренние угрозы в этой сфере способствуют реализации внешних угроз. Проповедуемые Западом теории “справедливого глобального мира”, единого постиндустриального общества, равноправного партнерства, идеи общечеловеческих ценностей, концепции “открытого общества” и “открытых дверей” на современном этапе все чаще заменяются новыми (или лучше сказать – модернизированными старыми) взглядами об избранничестве, “золотом миллиарде” населения мира, этнокультурном мировом барьере, особой миссии западной циви-

лизации, исключительной роли США и т.п. Однако противоречий между этими идеями и основанными на них геополитическими прогнозами нет, так как "справедливый новый мировой порядок" лишь прикрывает старую гегемонистскую цель достижения глобальной монополии США и их союзников.

В 50-е годы XX в. в США был принят Закон о порабощенных народах, в соответствии с которым на территории бывшего СССР проживало 22 порабощенных народа. Соответственно на 22 государства и должен был распасться Советский Союз. С его распадом в Закон были внесены уточнения: на территории Российской Федерации проживает 8 порабощенных народов. Соответственно вместо Российской Федерации должно образоваться 8 новых государств. Таким образом, информационная борьба продолжается.

На основании проведенного анализа можно сделать несколько выводов:

– государство должно взять на себя ответственность за формирование и реализацию государственной информационной политики в сфере информационной борьбы;

– для достижения информационной независимости и национальной самодостаточности нашему государству, прежде всего, требуется определиться с выработкой и закреплением четких национальных приоритетов. Это и будет являться базовым элементом государственной информационной политики при сохранении свободы слова, плюрализма мнений, но в рамках правового законодательства и законов этики и нравственности;

– государственная информационная политика в области ведения информационной борьбы должна базироваться на научных и методологических разработках, систематизированных и объединенных в единую концепцию. Она может быть представлена как совокупность национальных целей, интересов и ценностей; стратегии и тактики управленческих решений и методов их реализации, разрабатываемых и реализуемых государственной властью для регулирования и совершенствования как непосредственно процессов информационного взаимодействия во всех сферах жизнедеятельности общества и государства, так и процессов (в широком смысле) технологического обеспечения такого взаимодействия.

Примечания

[1] Цит. по: Зарубежное военное обозрение. 1997. № 8.

[2] *Почепцов Г.Г.* Информационные войны. М.: "Рефл-бук", 2000. С. 476.

[3] *Манойло А.В.* Управление психологической войной в системе государственной информационной политики // Сб. материалов 4-й международной конференции "Информационные технологии и безопасность". Киев, 2004. Вып 7. С. 48–66.

[4] *Манойло А.В.* Государственная информационная политика в особых условиях. М.: МИФИ, 2003. С. 30–35.

[5] *Манойло А.В., Петренко А.И., Фролов Д.Б.* Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия-Телеком, 2003. С. 124.

[6] *Стрельцоы А.А.* Обеспечение информационной безопасности России. Теоретические и методические основы / Под ред. А.А.Садовничего, В.П. Шерстюка. М.: МЦНМО, 2002. С. 78.

[7] Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. 28 сентября.