

ПРАВОВЫЕ ПРОБЛЕМЫ УКРЕПЛЕНИЯ РОССИЙСКОЙ ГОСУДАРСТВЕННОСТИ

Часть 23

Под редакцией доктора юридических наук

В.Ф. Воловича



ИЗДАТЕЛЬСТВО
ТОМСКОГО
УНИВЕРСИТЕТА
2005

НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

А.М. Барнашов

Проблема обеспечения информационной безопасности носит комплексный характер, т.е. является результатом взаимодействия и взаимопроникновения сферы информационных отношений и сферы обеспечения безопасности, и приобретает всё большую значимость как для отдельных государств, так и для международного сообщества в целом в связи с развитием информационных и коммуникационных технологий.

Актуальность обсуждения вопросов информационной безопасности и в рамках международных организаций, и на уровне государств обусловлена тем, что эти вопросы представляют собой как теоретическую проблему, так и самым тесным образом связаны с объективной международно-политической и внутригосударственной реальностью.

Манипулирование массовым сознанием, использование различных средств и технологий информационно-психологического воздействия стало достаточно обычным явлением в повседневной жизни, экономической конкуренции и политической борьбе. Таким образом, понимание угроз информационной безопасности общества, механизмов их действия и возможностей информационной защиты становится насущной потребностью практики международных отношений и жизни любого государства.

Появление проблемы информационной безопасности связано с одной из характерных особенностей современного этапа мирового научно-технического прогресса, с глобализацией информационного пространства, в результате чего происходит чрезвычайно быстрое и практически повсеместное распространение новейших информационных технологий и глобальных средств коммуникации, формируется своего рода глобальное информационное пространство международного сообщества. Тем не менее использование достижений прогресса в сфере информации возможно не только в позитивных целях, но и в целях, связанных с обеспечением превосходства отдельных государств на международной арене, с подавлением других государств, вмешательством в их внутренние дела. В связи с этим можно говорить о появлении принципиально

новой сферы международного противоборства, затрагивающей как интересы безопасности отдельных государств, так и общую систему международной безопасности на глобальном и региональном уровнях. Так, широко распространено в настоящее время использование информационных ресурсов в преступных целях. Растет число преступлений в сфере информации. Это касается как корыстных преступлений, так и терроризма, который использует насилие и угрозы насилием для достижения политических целей в очень широких масштабах.

Проблемы национальной безопасности государства, его международной безопасности, информационно-психологической безопасности общества, личности освещаются в работах И.Л. Бачило, Ю.Б. Кашлева, Ю.М. Колосова, В.А. Копылова, Б.В. Кристального, В.Н. Кудрявцева, В.Н. Лопатина, С.А. Малинина, М.А. Митюкова, И.Н. Панарина, М.А. Федотова, Р.В. Агеевой, В.Д. Аносова, Г.Н. Вачнадзе, М.С. Вершинина, А.Ф. Викторова, А.В. Кубышкина В.В. Мамонова, С.А. Модестова, А.А. Мухина, Ю.М. Нестерова, А.В. Старовойтова, Л.М. Стрельцова, А.Н. Сухова, Т.Э. Шуберт и др.

Информационное противостояние ранее присутствовало практически во всех войнах в таких основных формах, как ведение разведки и противодействие ей, распространение дезинформации, слухов и борьба с ними (в том числе при помощи цензуры) и т.п. С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне информационная составляющая в стратегии обеспечения национальной безопасности, по оценкам Совета Безопасности Российской Федерации, руководителей российских спецслужб и Минобороны России, вышла на первый план. По данным ФАПСИ, за последние 15 лет расходы на приобретение средств информационной борьбы увеличились в США в четыре раза и занимают сейчас там первое место среди всех программ по вооружению¹.

В ходе ведения обычной войны информационное противоборство начало переходить на новую, более высокую стадию – информационная война². Термин «информационная война» появился в середине 80-х гг. в связи с новыми задачами Вооруженных сил США после окончания «холодной войны» (разработка группы военных теоретиков США в составе Г. Экклз, Г. Саммерз и др.); начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средства веде-

¹ См.: *Шепотько И.* Борьба за информацию – реальность нынешнего дня // Красная звезда. 1997. 15 сент.

² См.: *Серебрянников В.В.* Войны России: социально-политический аспект. М.: Научный мир, 1998. С. 212–217.

ния войны; (официально впервые закреплена в директиве Министерства обороны США от 21 декабря 1991 г. и в директиве Комитета начальников штабов Вооруженных Сил США Т9 3600. 1 (декабрь 1992 г.); детально разъяснена в Меморандуме №30 (1993 г.) заместителей министра обороны и председателя Комитета начальников штабов Вооруженных сил США.) В военных кругах США под информационной войной понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

Понятие «информационная война» достаточно сложное, поэтому существуют различные подходы к его определению, нашедшие отражение, например, в исследованиях Института углубленного изучения информационной войны (США), Международного аналитического центра безопасности колледжа Кинга в Лондоне, Центра стратегических и международных исследований (США), а также в работах многих зарубежных и отечественных авторов.

Информационное пространство как часть геополитического пространства формируется через протекающие через него информационные процессы. Это пространство становится тем более развитым и обжитым, тем более совершенным и комфортным как среда обитания того или иного геополитического субъекта, чем более оно (это пространство) оказывается опосредованным разнообразными средствами передачи данных, их обработки, хранения, чем более совершенны технологии использования этих средств (например, скорость обработки и передачи данных, криптологические их защиты, создающие особую структуру информационного, а значит, и геополитического пространства и т.п.)¹.

Авторы В.Ф. Комарович и И.Б. Саенко дают такое определение информационной войны: «Комплекс взаимосвязанных действий, предпринимаемых для достижения информационного превосходства путем нанесения ущерба информационной сфере противника при обеспечении собственной информационной безопасности»². По их мнению, «информационная сфера – это сфера общечеловеческой деятельности, связанная с получением, переработкой, распределением и использованием информации»³.

¹ См.: *Модестов С.А.* Информационное противоборство как фактор геополитической конкуренции. М., 1999. С. 35.

² *Комарович В.Ф., Саенко И.Б.* Компьютерные информационные войны // *Защита информации.* 2002. Конфидент № 4–5. С. 84.

³ Там же.

Информационная война ведётся с помощью манипулирования знаниями, охватывает СМИ, влияет на образование и разрушает традиционные «старые» культуры. При сверхмалом сроке реализации военных действий (иногда это занимает доли секунды) нет возможности немедленно противостоять агрессии¹.

Вместо того чтобы вводить в стан противника танки, можно ослабить его более эффективно, подавляя (военное время) элементы инфраструктуры государственного управления, поражая центры военного командования, ведя радиоэлектронную разведку, «хакерскую» войну, распространяя дезинформацию для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения².

В последнее время на Западе получило хождение понятие «глобализация озабоченности», смысл которого в том, что информационные операции должны проводиться не только при объявлении войны. Если в военное время их цель – парализация информационной инфраструктуры противника при обеспечении устойчивого функционирования своей, то в мирные дни задача заключается в том, чтобы склонить политическое руководство противоположной стороны к принятию решений, выгодных для их организаторов. Такие операции могут проводиться против любых государств, в том числе и не являющихся потенциальными противниками³. Информационная война будет представлять собой бескомпромиссную борьбу в информационной сфере. Она охватит всю совокупность военных, политических и экономических аспектов человеческой жизнедеятельности. Люди, участвующие в информационной войне, могут принимать стратегические решения в качестве персонала так называемых мозговых центров, основа которых – специалисты высочайшей квалификации в области информационных технологий⁴.

¹ См.: Информационное общество: Информационные войны. Информационное управление. Информационная безопасность / С.М.Виноградова, Н.А.Войтович, М.А. Вус; и др. Под ред. М.А. Вуса. СПб.: Изд-во С.-Петерб. ун-та, 1999. С. 45.

² См.: Шиллер Г. Манипуляторы сознанием: Пер. с англ. М., 1980. С. 23; Кубышкин А.В. Международно-правовые проблемы обеспечения информационной безопасности государства: Автореф. дис. ... канд. юрид. наук. М., 2002. С. 18–19; Доронин А. Дезинформация: война в королевстве кривых зеркал // БДИ. 2002. № 1 (41). С. 26; Грачев Г.В. Личность и общество: Информационно-психологическая безопасность и психологическая защита. М., 2003. С. 84.

³ См.: Коновалов А.М. Информационная безопасность: кто – за, кто – против? // Современная Европа = Contemporary Europe. М., 2003. № 2. С. 71.

⁴ Гулаев С. Новые параметры угроз и безопасности // Ориентир. 2002. № 1; Информационное пространство как мишень оружия будущего // БДИ. 2002. № 2. С. 29.

К сожалению, в настоящее время в международном и национальном праве отсутствуют нормы, прямо разрешающие проблемы, связанные с таким явлением, как информационная война. Так, нет ясности в вопросе о соотношении между трансграничным характером информационных сетей и принципом государственного суверенитета. Каковы условия для ввода «военного» положения со всеми его атрибутами (ограничениями некоторых демократических ценностей, запретительными нормами в отношении свободы слова, введением цензуры и т.п.)¹. Следовало бы нормативно определить рамки начала «военных действий» и их конца, а также основания применения норм международного гуманитарного права к действиям в период «информационной войны», в частности возмещения ущерба за разрушения правительственных или частных баз данных как составной части культурных ценностей участников конфликта.

Для разрешения указанных проблем в международном праве необходимо было бы провести разграничение таких понятий, как информационное нападение, применение силы, акт агрессии и др., чтобы определить статус нападений и допустимых ответов на них в рамках информационной войны. Целесообразно также использовать достаточно широкое международно-правовое понятие «информационное воздействие». Так, по мнению А.В. Кубышкина, «информационное воздействие» представляет собой любые действия государства с использованием информационных средств, направленных на критические структуры государства, а также на другие объекты информационной структуры государства в случае, если воздействие на указанные объекты повлекло значительный ущерб деятельности жизненно важных структур государства, а также причинило ущерб национальной безопасности².

Существующие международно-правовые документы, формулирующие принципы, на которых должна основываться информационная безопасность, еще, к сожалению, весьма неполны. Актуальная проблема на сегодняшний день – принятие новых всеобъемлющих соглашений, уточняющих и усиливающих международно-правовые принципы трансграничного распространения информации. Одним из таких документов могла бы стать международная конвенция, которая, во-первых, установила бы зоны национальной юрисдикции в Интернете, во-вторых, такая конвенция должна была бы установить общие правила дозволения, обя-

¹ Киришин Ю. // Новая эра: международные отношения после 11 сентября 2001 года: Материалы международной Интернет-конференции, проходившей 15 апреля – 28 июня 2002 года на информационно-образовательном портале www.auditorium.ru. М., 2003. С. 165.

² Кубышкин А.В. Цит. соч. С. 30–31.

зывания и запрета в отношении деятельности в трансграничных компьютерных сетях. Опыт формирования международного космического права был бы весьма полезен в качестве образца при создании актов международного и национального права, призванных регулировать деятельность в киберпространстве.

По справедливому мнению В.А. Копылова, «в Интернет отсутствуют географические и геополитические границы государств-участников ТИТС (трансграничных информационно-телекоммуникационных сетей), происходит «столкновение» и «ломка» национальных законодательств стран в этих сетях. На этой основе возникает проблема формирования нового международного правового пространства и национального информационного законодательства»¹.

К сожалению, для урегулирования этого вопроса международным правом потребуется немало времени. Для того чтобы информационный обмен в Интернете соответствовал политическим, правовым и моральным устоям, признанным человечеством, на универсальном уровне должны быть выработаны и закреплены в многосторонних международных договорах правовые предписания по охране информации. Прежде всего, необходимо заключение многостороннего договора, в котором были бы зафиксированы общие запреты на распространение определенной информации, сформировавшиеся обычно-правовым путем, а также организационные и технические меры по их реализации. Текст такого договора было бы целесообразно разработать в рамках ООН с привлечением компетентных экспертов для обсуждения технических вопросов. Это может обеспечить тесную связь правового регулирования использования компьютерных сетей с регулированием других научно-технических достижений в интересах всего человечества.

В заключение хотелось бы привести важную мысль из Доктрины информациологического развития человечества в XXI в., которая провозгласила следующее: «Чем выше информациологический уровень человеческой цивилизации, тем с более грандиозными проблемами ей приходится сталкиваться; наступает информациологический переход от частных проблем к глобальным и от глобальных – к глобально-космическим. В этих условиях слишком высока цена конфликтов и размежевания, и лишь международное, межнациональное, межгосударственное единение людей на информациологической основе способно обеспечить дальнейший прогресс и само существование человечества»².

¹ Копылов В.А. Информационное право. М.: Юристъ, 2002. С. 235.

² «Доктрина информациологического развития человечества в XXI веке»: Материалы всемирного информациологического форума 2002 г. М., 2002. С. 11. 198