Методы противодействия информационной войне

Шибаев Д.В.,
кандидат юридических наук,
заведующий кафедрой социально-гуманитарных дисциплин и правовой информатики
Северо-Западного института (филиала) Университета имени О.Е. Кутафина (МГЮА)
E-mail: 013600@inbox.ru

Аннотация. *Государству необходимо быть готовым к предупреждению и противодействию современным способам ведения войны — разработка методов противодействия информационному оружию, создание общества, невосприимчивого к методам информационной борьбы, формирование концепции противодействия информационной войне. Автор представляет анализ источников права, как иностранного, так и российского, определяющего требования к деятельности государства по противодействию информационным войнам, а также приводит точки зрения иностранных и отечественных исследователей, политических и общественных деятелей по понятию и особенностям таких политико-правовых конструкций, как информационная война и информационное оружие. В работе указываются отдельные положения, определяющие характеристики информационной войны и методы противодействия ей, как предложения к изменению национального законодательства, которые создадут условия для точного понимания этого политико-правового феномена. Кроме того, подчёркивается точка зрения, что внесение изменений только в Доктрину информационной безопасности недостаточно, необходимо выделить проблему информационной войны, как отдельную, крайне серьёзную угрозу и систематизировать понятия, требования и методы противодействия ей в самостоятельном документе, необходимы формирование отраслевого (информационная безопасность) законодательства и подготовка специалистов информационно-психологического противодействия и агрессии, формирование общественного мнения посредством подготовленных масс-медиа, проведение разъяснительной политики и т.д.*

Ключевые слова: *информационная война, информационное оружие, методы противодействия методы информационной войны, личность, общество, государство, оборона, модель безопасности.*

В настоящее время, особенно, в отношении стран с ядерным статусом, применение реального вооружения становится самой крайней мерой разрешения конфликта. Перспектива втянуться в широкомасштабные боевые действия, создать опасность для своих граждан — ни для одного государства это не является приоритетом. В то же время вопрос передела экономико-политических сфер влияния стоит достаточно остро — борьба за новые рынки сбыта, энергоресурсы, за политические «очки» создают крайне напряженную атмосферу в мире. Достаточно вспомнить грузино-осетино-российский конфликт, Египет, Сирию, Турцию, Ливию, Украину. Во всех этих случаях основу конфликта формировали информационные составляющие — недовольство действующим режимом, провоцируемый конфликт, применение социальных сетей для консолидации и управления протестом, формирование отрицательного образа легитимной власти посредством телевидения и радио. Все это, тщательно подготовленное, примененное вовремя, построенное на реальных или мнимых недостатках действующей власти, разрушает государственность гораздо эффективнее, нежели затратные (в части человеческих и экономических потерь) военные действия.

Применение методов информационной войны достаточно многообразно и все они опосредуются формированием протестных акций для осуществления государственных переворотов или сохранения действующей власти, но ее существенного ослабления в политико-экономическом и социальном плане. Именно информационное оружие (как составляющее информационных войн) используется для осуществления так называемых «цветных» революций[1].

Понятие и особенности дефиниции «информационная война»

На наш взгляд, необходимо определить два таких важнейших понятия, как информационная война и информационное оружие. В настоящее время самостоятельная характеристика этих дефиниций в Доктрине отсутствует, но словосочетание встречается два раза:

- п. 3 Доктрины — при перечислении внешних источников угроз информационной безопасности (разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним);
- п. 9 Доктрины — в качестве мероприятий по реализации государственной политики обеспечения информационной безопасности РФ (комплексное противодействие угрозам информационной войны).

[1] Dr. Gene Sharp «198 methods of non violent action» from The Politics of Nonviolent Action by Gene Sharp Boston, Porter Sargent, 1973 [Электронный ресурс] // URL: http://www.quakerquaker.org/profiles/blogs/dr-gene-sharps-198-methods-of (частично переводная версия — URL: http://philosophy.ru/library/vopros/met.html) (дата обращения: 19.11.2016).

В проекте новой Доктрины информационной безопасности РФ, основные положения которого были одобрены 5 октября 2015 г. рабочей группой Межведомственной комиссии Совета Безопасности РФ по информационной безопасности (сам проект разрабатывался в течение 2015 г.)[2], указания на информационную войну, как объект, не прослеживается. На наш взгляд, отсутствие дефиниции исключает все дальнейшие усилия по ее выявлению и противодействию ей.

Как целостное понятие «информационная война» содержится в распоряжениях Правительства РФ от 10.07.2014 № 1271-р[3] и от 17.09.2013 № 1672-р[4]. В них *информационная война* понимается как *противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны,* а *информационное оружие — как информационные технологии, средства и методы, применяемые в целях ведения информационной войны.*

В литературе очень часто можно увидеть соотношение понятий «информационная война» и «кибервойна»[5]. На наш взгляд, это не равнозначные, не подменяемые друг другом понятия. Они соотносятся как часть и целое, информационная война — целое, так как включает в себя действие, среду и орудие этого действия, в то время как кибервойна включает в себя только среду (исключительно электронную) и орудие (электронные средства коммуникации). В широком смысле информационное противостояние (война) может осуществляться (помимо самого популярного — электронного способа) посредством печатной пропаганды, телевидения и радио и др., хотя следует признать, что использование киберпространства (сети Интернет и альтернативных extranet и intranet-сетей) является не только самым дешевым, но и самым эффективным средством информационного противоборства.

Как известно, первым, кто использовал понятие «информационная война» был советник по науке министерства обороны Белого дома США Томас Рона. В 1976 г. он выделил признаки информационной войны в своем отчете «Системы оружия и информационная война» для компании Боинг[6]: увеличение объема собственной информации, затруднение для противника доступа к правдивой информации, размещение в информационных потоках противника кажущейся достоверной, но фальшивой информации, важность информационных потоков для действий противника.

Также свои подходы к определению понятия «информационная война» высказывали многие ученые. Как отмечает Г.Г. Почепцов, теория информационных войн прошла в своем развитии несколько этапов: на первом этапе (начало 1990-х гг.) группа ученых Авиационного университета ВВС США, изучая войны будущего, сформулировала требования к такой войне, подчеркивая, что самым слабым местом на поле боя останется мозг солдата. Например, Дж. Стейн в своей статье 1995 г. «Информационная война» указывает об информационной войне как о достижении национальных целей с помощью информации[7]. Р. Шафрански в 1994 г. подчеркивает важность ментального измерения и высших ценностей: зная систему ценностей противника мы можем общаться с его мозгом, и как следствие, навязывать свою волю[8].

Второй этап (конец 1990-х гг.) характеризуется деятельностью американского специалиста по международным отношениям Джона Аркилла, который первым фундаментально осветил проблемы информационной стратегии, кибервойны и сетевой войны, в том числе информационной[9]. Кибервойна и сетевая война являются разновидностями современного конфликта: кибервойна — это конфликты высокой и средней интенсивности, а сетевая война — конфликты низкой интенсивности и операции, отличные от войны. Термин «информационная война» для него слишком широк, так как пытается охватить все, но с другой стороны — слишком узок из-за отсылки к узким техническим вопросам уязвимости и безопасности киберпространства.

На третьем этапе (2000-е гг.) проявляют активность практики-военные, которые стали уделять

---

[2] Проект доктрины информационной безопасности РФ. [Электронный ресурс] // URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (дата обращения: 19.11.2016).

[3] Распоряжение Правительства РФ от 10.07.2014 № 1271-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // URL: http://www.pravo.gov.ru. (дата обращения: 19.11.2016).

[4] Распоряжение Правительства РФ от 17.09.2013 № 1672-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // URL: http://www.pravo.gov.ru (дата обращения: 19.11.2016).

[5] Crabb S. UK cyber security a top priority for UK Government [Электронный ресурс] // URL: https://www.gov.uk/government/news/uk-cyber-security-a-top-priority-for-uk-government (дата обращения: 19.11.2016).

[6] См.: Thomas P. Rona. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976, p. 14.

[7] Почепцов Г.Г. Информационная война: определения и базовые понятия [Электронный ресурс] // URL: http://psyfactor.org/psyops/infowar25.htm (дата обращения: 19.11.2016).

[8] Szafranski R. Neocortical warfare? The acme of skill. In Athena's camp. Ed. By J. Arquilla, D. Ronfeldt. Santa Monica, 1997, p. 309.

[9] Arquilla J., Ronfeldt D. The advent of netwar. Santa Monica, 2003, p. 21.

повышенное внимание операциям влияния вследствие прошедших в прошлом десятилетии войн, однако существенного расширения теоретической базы не произошло. Один из представителей данного этапа М. Либики определял информационную войну как атаку информации на информацию[10], т.е. когда противники стараются показать свою информацию правдивой, более правдоподобной, нежели информация, предлагаемая их соперником. Также Г.А. Атаманов понимает под «информационной войной» разновидность «противоборства социальных систем, в ходе которого допускается (предусматривается) физическое уничтожение элементов инфраструктуры противоборствующих систем, а главным средством ведения являются информационные технологии»[11].

Если обратиться к международному праву, то в нем понятие «информационная война» никак не закреплено, однако данный термин присутствует в национальном законодательстве некоторых стран.

Например, в китайской военной доктрине[12] указывается на информационную войну в широком и узком смысле. В узком смысле — боевые действия в сфере управления войсками, а в широком смысле — это боевые крупномасштабные действия с преобладанием информационной составляющей, характеризующиеся применением специально предназначенных для ее ведения воинских формирований и высокоточного оружия. Таким образом, в национальном праве Китая под информационной войной понимается один из способов ведения боевых действий.

Один из видных теоретиков в области информационного противостояния В.И. Цымбал[13] отмечает, что информационная война имеет широкий и узкий смысл. В широком смысле — это *один из способов противостояния между двумя государствами, которое осуществляется главным образом в мирное время, где объектом воздействия являются наряду с вооруженными силами и гражданское население, общество в целом, государственные административные системы, структуры производственного управления, наука, культура и т.д.* В узком смысле *информационная война — один из способов боевых действий или непосредственной подготовки к ним, имеющий целью достичь подавляющего преимущества над противником в процессе получения, обработки, использования информации для выработки эффективных административных решений, а также успешного осуществления мероприятий по достижению превосходства над противником на этой основе.*

В.С. Пирумов[14] определил информационную войну как *новую форму борьбы двух и более сторон, которая состоит в целенаправленном использовании специальных средств и методов влияния на информационные ресурсы противника, а также защиты собственного информационного ресурса для достижения назначенных целей*. По его мнению, в мирное время информационная война носит преимущественно скрытый характер. Ее основной задачей является ведение политико-психологических действий по отношению к противнику, а также осуществление мероприятий по собственной информационной безопасности. В ситуации реального противостояния государств силы и средства информационной войны решают такие задачи, как массированное воздействие на информационный ресурс противника и предотвращение снижения боевых возможностей своих сил; проведение мероприятий по снижению уровня морально-психологической устойчивости войск противника и обеспечение нейтрализации информации, воздействующей на морально-психологическое состояние своего личного состава; ведение разведывательной деятельности и обеспечение скрытности важнейших мероприятий своих войск и т.д.

Профессор С.П. Расторгуев[15] определяет понятие *информационной войны как открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере.* Прекрасное определение, в котором верно указаны два основных признака информационной войны. Основной задачей информационной (информационно-психологической) войны на тактическом уровне является получение определенного материального выигрыша (преимущества), при этом в процессе информационной войны одни участники противоборства эти преимущества получают, а другие их утрачивают. Для тех, кто преимущества утрачивает, эти потери могут служить количественным выражением материального ущерба, нанесенного войной.

Ряд иностранных ученых[16] определяет исследуемое понятие как *класс методов, в том числе сбора, транспортировки, охраны, отрицания, нарушения и искажения информации, используя*

[10] Libicki M. Conquest in cyberspace. National security and information warfare. Cambridge, 2007, p. 114.

[11] Атаманов Г.А. Информационная война: экспликация понятия. [Электронный ресурс] // URL: http://www.naukaxxi.ru/materials/254/ (дата обращения: 19.11.2016).

[12] Ministry of national defense the people republic of China [Электронный ресурс] // URL: http://eng.mod.gov.cn (дата обращения: 19.11.2016).

[13] Цымбал В.И. О концепции информационной войны // Информационный сборник «Безопасность». 1995. № 9. С. 35.

[14] Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 44–47.

[15] Расторгуев С.П. Информационная война. М.: Радио и связь. 1998. С. 35–37.

[16] См., напр.: Martin C. Libicki, What is Information Warfare? (Washington DC: Institute for National Strategic Studies, 1996), p. 11; John Arquilla and David Ronfeldt, The Advent of Netwar, (Santa Monica: RAND, 1996), p. 3; Winn Schwartau, Information Warfare, (New York: Thunder's Mouth Press, 1996), p. 216.

которые поддерживается преимущество над своими противниками[17]. Как видим, зарубежные исследователи в большей части не противоречат мнению российских ученых, расширяя определение методами информационной войны.

Отдельные предложения по совершенствованию законодательства в сфере информационной безопасности

На наш взгляд, логично было бы внести изменения в Доктрину информационной безопасности, дополнив п. 2 раздела 1 характеристикой понятия «информационная война» в следующей терминологии:

Информационная война — это противоборство, т.е. открытое и скрытое целенаправленное информационное воздействие между двумя или более государствами в информационном пространстве, осуществляемое главным образом в мирное время с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Имеющееся в распоряжениях Правительства РФ понятие автор расширяет важными на его взгляд положениями, отмеченными С.П. Расторгуевым и В.И. Цымбалом:

1) указанием на особенности (в частности, латентность) информационного воздействия, что создает возможность идентифицировать отдельные информационные потоки, как элемент информационной войны и своевременно их пресечь или исказить;

2) уточнением на мобилизационный фактор — преимущественно мирное время, когда силы и средства противодействия (не только государственного, но и общественного сектора) не находятся в боевом положении (не проводится массированная пропаганда, не введено военное положение, цензура и т.д.).

Также необходимо расширить раздел 2 Доктрины характеристиками и угрозами информационной войны и методами ее противодействия.

I. Должны быть определены основные способы достижения информационного превосходства в информационной войне.

1. Скрытое управление деятельностью органов власти государства-противника информационными (в том числе информационно-психологическими) процессами, определяющими облик системы общественных, политических, экономических, духовных отношений государства-соперника.

Наиболее актуальным и действенным способом управления является применение «агентов влияния», т.е. лиц, наделенных определенной властью (сотрудники органов государственной власти) или способных влиять на представителей власти посредством материальной или моральной заинтересованности.

Факты наличия указанных лиц присутствуют в современной России. Так, на пресс-конференции «Прямая линия с Владимиром Путиным» наш Президент прямо заявил, что «в окружении ... Чубайса ... в период его работы в правительстве, в качестве советников, как выяснилось сегодня, были кадровые сотрудники ЦРУ США»[18]. Наличие такого рода агентов влияния создает не только проблемы защиты государственной тайны, но и нарушает режим национальных интересов;

2. Открытая информационно-психологическая агрессия.

Наиболее ярким современным примером агрессии является показ телешоу «Третья мировая война: в командном пункте» (World War Three: Inside the War Room) на BBC-2, в которой смоделирована ситуация нападения РФ на Латвию. По мнению посла РФ в Латвии А. Вешнякова данное событие является опасной провокацией. Он отмечает, что сценарий абсолютно надуманный, преследующий политические цели: во-первых, включиться в информационную войну по демонизации России; во-вторых, оправдать запросы военно-политических лобби на увеличение расходов НАТО в Европе более чем в 4 раза; в-третьих, дискредитировать любые политические силы в Латвии, в Европе, которые относятся к России непредвзято, выступают с прагматических позиций по отношению к ней[19].

Указанная информационная провокация не является единичной. Осенью 2015 г. норвежское телевидение транслировало сериал «Оккупация», в котором показывалась не менее гипотетическая ситуация оккупации Норвегии Россией «в целях защиты энергетической безопасности ЕС». Этот сериал также вызвал протесты со стороны некоторых российских политиков и посольства России в Норвегии. Российское посольство в Норвегии заявило, что авторы сериала решили в худших тра-

[17] В частности указанное определение дает Ajay Singh, Research Fellow, IDSA (Институт оборонных исследований США), в работе Information Warfare: Reshaping Traditional Perceptions [Электронный ресурс] // URL: http://www.idsa-india.org/an-mar-4.html (дата обращения: 19.11.2016).

[18] Прямая линия с Владимиром Путиным [Электронный ресурс] // URL: http://kremlin.ru/events/president/news/17976 (дата обращения: 19.11.2016).

[19] Посол РФ в Латвии: Телешоу на BBC-2, моделирующее нападение на Латвию, демонизирует Россию [Электронный ресурс] // URL: http://www.rosbalt.ru/world/2016/02/04/1486561.html (дата обращения: 19.11.2016).

дициях «холодной войны» попугать норвежского зрителя несуществующей угрозой с Востока. «Хотя авторы сериала старательно подчеркивают вымышленность сюжета, якобы не имеющего ничего общего с действительностью, речь в этом фильме идет о вполне реальных странах, причем России, к сожалению, отведена роль агрессора», — отмечалось в комментарии посольства[20].

Интересны сами технологии информационно-психологических атак, как правило, они направлены не на атакуемое государство, а на население атакующего, чтобы сформировать у последнего чувство тревоги и недоверия, мобилизовать перед внешним врагом. Результатом такой атаки является существенное изменение общественного мнения населения атакующего государства против атакуемого. Атакуемый же становится агрессором и какие-либо оправдания и доводы его не принимаются к рассмотрению.

II. Должны быть указаны основные технологии информационного противоборства.

1. Информационная асимметрия — осуществление контр-дезинформации или пропаганды.

После каждого информационного репортажа противника (непринципиально, направлен он против вас или нет, лучше на подавляющее количество новостей в эфире) должно последовать его опровержение или существенное понижение важности, переквалификация из положительного в несущественное. Крайне важно, чтобы использовалась так называемая «информационная волна», т.е. публикация опровержения происходит со ссылкой на эксперта — известного политика, общественного деятеля, иного известного человека, издание, орган. Другие издания осуществят его перепечатку на своих информационных площадках уже со ссылкой на указанного известного субъекта, издание, орган. На третьем-четвертом шаге перепечатки информация уже будет индексирована не от вашего имени, а от имени известных изданий или этого эксперта. Ее опровержение (если оно последует) произойдет через 1–2 дня и сможет перекрыть только меньшую часть волны дезинформации. Использование указанного метода не является желательным, так как подрывает значение государства и государственных институтов (министерство иностранных дел, министерство внутренних дел, службу внешней разведки, от лица которых действительно идет дезинформация), но учитывать «информационную волну» как способ атаки на вас необходимо.

Более корректные способы информационной ассиметрии применяются в виде контрпропаганды и разъяснения своих действий и действий противника посредством информационного доминирования.

2. Информационное доминирование — наличие в инфосфере государства-противника ему неподконтрольных масс-медиа, общественных объединений, политических сил.

Умение сформировать общественное мнение, в том числе не только в отдельно взятой стране, но и трансгранично, позволяет политической силе манипулировать населением (например — перед выборами, иными социально-значимыми событиями) и посредством недовольства населения государственной властью, желающей остаться на своем месте. Способы манипулирования достаточно широки, включая заявления в масс-медиа о фактах коррупции высших лиц государства или их близких.

Ярким примером создания политической напряженности является «дело Лизы»[21]. Факт возможного изнасилования русской девочки мигрантами (на волне событий в Кельне[22]) не способствовал снятию напряженности в немецком обществе, создал факт дополнительных политических проблем для руководства Германии. Этот и другие факты внедрения в информационное пространство зарубежных государств мнения, которое идет вразрез с принятым и допустимым, повлекли за собой заявление вице-президента Фонда поддержки демократии (National Endowment for Democracy, NED) Кристофера Уолкера о том, что «американским и европейским медиа необходимо более активно бороться с российскими каналами RT и LifeNews, а также другими СМИ из государств, представляющих угрозу для США»[23].

Деятельность России в части доминирования в медиапространстве является весьма успешной: во-первых, RT и LifeNews являются важнейшими средствами массовой информации на целом ряде языков и, как признают зарубежные журналисты, создают серьезную конкуренцию проправительственным зарубежным СМИ на их территории. По мнению журналиста Джоша Кучеры (Josh Kucera), освещающего события в России и на постсоветском пространстве, RT рассказывает о США точно так же, как американские СМИ рассказывают о России, делая упор на отрицательных тенденциях

[20] По материалам Русской службы BBC [Электронный ресурс] // URL: http://www.bbc.com/russian/international/2016/02/160203_world_war_three_war_room_bbc (дата обращения: 19.11.2016).

[21] Бедная Лиза [Электронный ресурс] // URL: http://www.rg-rb.de/index.php?option=com_rg&task=item&id=17640&Itemid=13 (дата обращения: 19.11.2016).

[22] Нападения в Кельне: беззащитность и ярость немцев [Электронный ресурс] // URL: http://www.bbc.com/russian/international/2016/01/160110_germany_cologne_vulnerable (дата обращения: 19.11.2016).

[23] Январский доклад Фонда поддержки демократии (National Endowment for Democracy, NED), опубликованный в Journal of Democracy [Электронный ресурс] // URL: http://www.ned.org/wp-content/uploads/2016/01/January-2016-JOD-Hijacking-of-Soft-Power-Christopher-Walker.pdf (дата обращения: 19.11.2016).

и публикуя интервью с диссидентами. В целом RT занимает в США ту же нишу, что и Democracy Now или «Аль-Джазира», т.е. освещает темы и мнения, в которых слишком много критики США, чтобы они могли попасть в ведущие СМИ. Как выразился в своем замечательном отзыве на программу Ассанжа Кевин Гостола (Kevin Gosztola), «критикам пора смириться с тем, что, хоть этот канал и пристрастен, некоторые его программы обеспечивают резкую и необходимую критику нашего правительства, которую трудно увидеть на американских каналах»[24].

Во-вторых, защита внутреннего информационного пространства Россией определена на законодательном уровне. В конце 2014 г. в ст. 19.1 Федерального закона «О средствах массовой информации» были внесены изменения, ограничивающие размер иностранного капитала в уставном капитале СМИ не более 20% (ранее было 50%, что давало существенную возможность определения принципов и тематики издания или канала). Кроме того, лицензирование вещательных СМИ дает возможность государству ограничивать количество нежелательных масс-медиа без претензий об ограничении свободы СМИ.

3. Информационно-правовое доминирование — присутствие и наличие голоса в максимально большом количестве международных организаций для возможности быстрого реагирования на информационные вызовы и разъяснения международной общественности собственной точки зрения.

Это крайне важный элемент технологии информационного противоборства, в первую очередь, из-за своей легитимности и публичности. Присутствие на большинстве политических и экономических площадок (Организация объединенных наций, Совет безопасности ООН, Парламентская ассамблея Совета Европы, Шанхайская организация сотрудничества и др.), хотя и требует определенных материальных затрат, но создает площадку для высказывания собственного мнения на межгосударственном уровне. Ограничительные действия ПАСЕ в отношении России являются, по сути, способом информационного противоборства, так как при наличии голоса Россия смогла бы аргументировать свою точку зрения на Крым и связанные с ним события, на ситуацию на Донбассе. Отсутствие России в ПАСЕ возводит информационную войну против РФ на новую ступень, на данном уровне мы не можем защищаться и переходить в информационное наступление. Мнения ряда экспертов об отсутствии необходимости членства и голоса РФ в ПАСЕ, на наш взгляд, в корне неверны.

4. Латентность процессов информационной борьбы, т.е. скрытность и анонимность оперирования информационно-психологическими воздействиями, возможность проведения их «под чужим флагом» и с любой точки инфосферы, в связи с чем возникает сложность обвинения государства в намеренном проведении контр-информационной деятельности.

В данном случае часто используются агенты влияния, которые внедрены в государственные структуры и способны действовать от имени государства в интересах атакующего. Кроме того, использование коалиции при информационных атаках создает комплексность противоборства и обвинить какое-либо конкретное государство в атаке достаточно сложно.

5. Использование отсутствия четких юридически закрепленных в международных и национальных правовых нормах определений информационно-психологической агрессии и информационно-психологической войны в целях развязывания вооруженной агрессии и нанесения ущерба национальным интересам противников в мирных условиях.

На современном этапе Россия не является в достаточной мере защищенной национальным правом в части квалификации информационной войны, методов противоборства ей и санкций за противоправные действия. Изменение действующей Доктрины информационной безопасности или доработка и принятие проекта новой Доктрины, внесение изменений в Уголовный кодекс РФ в части ответственности за осуществление, посредничество или организацию информационной агрессии являются крайне необходимыми мероприятиями на настоящий момент. Но нельзя ограничиваться только национальным правом, на уровне Президента, Правительства РФ, Министерства иностранных дел необходимо предлагать соответствующие изменения в основополагающих международных актах ООН, ШОС, ОДКБ, СНГ и др. для обеспечения международного сотрудничества и унификации национальных законодательств в вопросах противоборства информационной войне.

6. Принцип возможности сочетания информационно-психологической борьбы, ведущейся участником борьбы в составе коалиции, с информационно-психологической борьбой, ведущейся этим же членом коалиции против других ее членов, в отношении достижения тех или иных частных преимуществ (как правило, посредством подкупа или обещания политико-экономических преимуществ перед противниками).

Коалиционный принцип является наиболее значимым в процессе развязывания информационной войны. Использование союзников или агентов влияния в государственных органах, от имени которых будут осуществляться совместные информационные действия, создают достаточные условия для успешного проведения опе-

[24] Нападки на RT и Ассанжа многое говорят о самих критиках [Электронный ресурс] // URL: http://inosmi.ru/world/20120420/190851187.html (дата обращения: 19.11.2016).

рации по информационному противоборству, пропаганды, информационной диверсии и др. Противодействие коалиции возможно созданием собственной коалиции и использованием контр-пропаганды целым рядом собственных и коалиционных иностранных масс-медиа, охватывающих максимально большую территорию. Примером подобной коалиции и применения приемов пропаганды является ситуация в отношении России в ПАСЕ. Резолюция о лишении голоса российской делегации в ПАСЕ первоначально не была принята единогласно. Ряд стран Евросоюза были против подобной меры и, наоборот, настаивали на предоставлении большего времени России для создания возможностей дискуссии с ней. Но польская, английская и ряд других делегаций создали коалицию и с требованием сохранения единства мнений стран Евросоюза по этому вопросу, убеждая и применяя иные методы (как правило — экономические), добились принятия этой резолюции. Похожим примером (менее цивилизованным) является пример попыток признания России страной-агрессором. В ряде областей Украины с первого раза это не удалось, но под нажимом ультраправых националистических сил была сформирована коалиция, запуганы инакомыслящие и решение было принято. Подобные примеры формирования коалиционных сил для проведения информационной войны необходимо учитывать, и в целях их недопущения или снижения эффективности заблаговременно проводить контрпропаганду. Ее примером может являться широко освещенное в масс-медиа мероприятие по поставке российского природного газа в Геническ (Украина) зимой 2016 г.

7. Создание в информационном пространстве системы органов государственной власти и управления государства-противника атмосферы недоверия, настороженности и враждебности по отношению ко всем остальным направлениям, предложениям и вариантам решения данного вопроса.

Умение «поставить в тупик» органы государственной власти в атакуемой стране достаточно сложно и, как правило, для этого используются «агенты влияния». Но внедрение указанных лиц достаточно трудоемкая задача и чаще всего для исключения альтернативных путей деятельности государства в ситуации информационной войны используются международные соглашения, заключенные в невыгодных для атакуемого условиях. Как правило, на атакуемую сторону оказывается международное давление для принятия завуалированного и в будущем невыгодного документа. В дальнейшем ссылка на указанный документ является элементом (оружием) этой войны, ссылаясь на который, атакующая сторона регулярно указывает на невыполнение стороной своих обязательств. Для создания атмосферы враждебности и недоверия ко всем остальным направлениям, предложениям и вариантам решения данного вопроса также используется дезинформация. Информация, исходящая от авторитетного субъекта о скором изменении экономической, политической, общественной обстановки, способна заставить атакующую сторону принять ошибочное решение.

8. Информационная зависимость государства-противника от непрерывного поступления внешних или альтернативных информационных ресурсов.

На данный момент в мире нет ни одного государства, которое бы напрямую зависело от поступления информации извне. Но создать информационную зависимость государства все-таки возможно. Как правило, это осуществляется посредством регистрации достаточно большого количества средств массовой информации в стране, проведении их массированной рекламы, стимулирования их использования посредством розыгрышей, лотерей, ток-шоу, формирование имиджа этих СМИ как объективных и актуальных. Также одним из связанных методов зависимости является популяризация исследования культуры и особенностей другого государства. Наиболее ярким примером в данном случае являются каналы RT и LifeNews, транслируемые в США и др. странах. Эти каналы рассказывают о России, ее политической, экономической, общественной и культурной жизни, тем самым поддерживая интерес жителей этих государств к получению информации от негосударственных каналов, которые не предоставляют подобный пакет информации. Еще одним примером явился факт показа фильма «Украина: Маски революции» режиссера Поля Морейра на французском канале Canal+. Учитывая, что государственные каналы не предоставляют подобной информации, французы вынуждены искать альтернативные источники. Учитывая высокую заинтересованность в альтернативном мнении, Canal+ несколько раз ретранслировал этот фильм[25]. Отсутствие на официальных каналах и других информационных источниках альтернативного мнения создает условия для его поиска.

9. Дестабилизация ситуации внутри государства (геополитического субъекта) с целью навязывания внешнего антикризисного управления.

Наиболее ярким примером является практика так называемых «цветных революций» или иной дестабилизирующий фактор, который ставит в зависимость экономический или политический суверенитет государства от внешнего управления. Современные примеры указывают на отработан-

[25] Французский канал в третий раз покажет фильм «Украина: Маски революции» [Электронный ресурс] // URL: http://rian.com.ua/culture/20160208/1004885647.html (дата обращения: 19.11.2016).

ную практику подобных действий. Защитой от такого дестабилизирующего действия может быть только устойчивость государственного аппарата, в том числе военная, полицейская, экономическая, нормативно-правовая.

10. Информационно-психологическая экспансия — деятельность по достижению национальных интересов методом бесконфликтного проникновения в сферу социальных и духовных отношений общества с целью постепенного, плавного, незаметного для общества изменения системы социальных отношений по образцу системы источника экспансии, вытеснения положений национальной идеологии и национальной системы ценностей и замещение их собственными ценностями и идеологическими установками, увеличения степени своего влияния и присутствия, установления контроля над стратегическими ресурсами, информационно-телекоммуникационной структурой и национальными средствами массовой информации (СМИ), наращивание присутствия собственных СМИ в информационной сфере объекта проникновения.

11. Возрастное зомбирование посредством масс-медиа — использование, как правило, телевидения для растления или изменения сознания недостаточно социализированной части общества — детей и подростков. Использование фильмов, мультфильмов, тематических программ, нацеленных на отторжение отечественного, традиционного и принятие иностранного (чаще — именно ценностей государства-противника)[26].

Средства и методы борьбы между государствами за последние десятилетия изменились, приобрели латентный характер (противодействие в информационном пространстве), и в связи с данным фактом следует законодательно определить термин «информационная война», на уровне национального права закрепить меры ответственности, направленные на предотвращение и недопущение информационной войны в отношении РФ, а также проводить соответствующие изменения в основополагающих международных актах — Шанхайской организации сотрудничества, Организации договора о коллективной безопасности, Соглашении о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности, в базовых документах ООН.

[26] См. напр. Ловцов Д.А. Канал 2х2: юмор, сарказм… экстремизм? // Закон. № 11. 2008. С. 28–29.

Список литературы

1. Атаманов Г.А. Информационная война: экспликация понятия [Электронный ресурс] // URL: http://www.naukaxxi.ru/materials/254/ (дата обращения: 19.11.2016).
2. Доклад Фонда поддержки демократии. Январь 2016 (National Endowment for Democracy, NED), опубликованный в Journal of Democracy [Электронный ресурс] // URL: http://www.ned.org/wp-content/uploads/2016/01/January-2016-JOD-Hijacking-of-Soft-Power-Christopher-Walker.pdf (дата обращения: 19.11.2016).
3. Ловцов Д.А. Канал 2х2: юмор, сарказм… экстремизм? // Закон. № 11. 2008. С. 28–29.
4. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 44–47.
5. Почепцов Г.Г. Информационная война: определения и базовые понятия [Электронный ресурс] // URL: http://psyfactor.org/psyops/infowar25.htm (дата обращения: 19.11.2016).
6. Проект доктрины информационной безопасности РФ [Электронный ресурс] // URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (дата обращения: 19.11.2016).
7. Распоряжение Правительства РФ от 10.07.2014 № 1271-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // URL: http://www.pravo.gov.ru (дата обращения: 19.11.2016).
8. Распоряжение Правительства РФ от 17.09.2013 № 1672-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // URL: http://www.pravo.gov.ru (дата обращения: 19.11.2016).
9. Расторгуев С.П. Информационная война. М.: Радио и связь, 1998.
10. Цымбал В.И. О концепции информационной войны // Информационный сборник «Безопасность». 1995. № 9.
11. Ajay Singh, Research Fellow, IDSA (Институт оборонных исследований США), в работе Information Warfare: Reshaping Traditional Perceptions [Электронный ресурс] // URL: http://www.idsa-india.org/an-mar-4.html (дата обращения: 19.11.2016).
12. Arquilla J., Ronfeldt D. The advent of netwar. Santa Monica, 2003.
13. Arquilla J., Ronfeldt D. The Advent of Netwar (Santa Monica: RAND, 1996).
14. Crabb S. UK cyber security a top priority for UK Government [Электронный ресурс] // URL: https://www.gov.uk/government/news/uk-cyber-security-a-top-priority-for-uk-government (дата обращения: 19.11.2016).
15. Gene Sharp Dr. «198 methods of non violent action» from The Politics of Nonviolent Action by Gene Sharp Boston, Porter Sargent, 1973 [Электронный ресурс] // URL: http://www.quakerquaker.org/profiles/blogs/dr-gene-sharps-198-methods-of (частично переводная версия [Электронный ресурс] // URL: http://philosophy.ru/library/vopros/met.html) (дата обращения: 19.11.2016).
16. Libicki M. Conquest in cyberspace. National security and information warfare. Cambridge, 2007.
17. Martin C. Libicki, What is Information Warfare? (Washington DC: Institute for National Strategic Studies, 1996.
18. Ministry of national defense the people republic of China [Электронный ресурс] // URL: http://eng.mod.gov.cn (дата обращения: 19.11.2016).
19. Szafranski R. Neocortical warfare? The acme of skill // In Athena's camp. Ed. By J. Arquilla, D. Ronfeldt. Santa Monica, 1997.
20. Thomas P. Rona. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976.
21. Winn Schwartau, Information Warfare, (New York: Thunder's Mouth Press, 1996).

Methods to Counter Information War

Shibaev D.V.,
PhD in Law, Associate Professor,
Head of Department of Social Science,
Humanities and Legal Computer Science of North-Western Institute (branch)
of Kutafin Law University (MSLA)
E-mail: 013600@inbox.ru

Abstract. *The government should be prepared to prevent and counteract state of the art techniques of warfare, viz.: to work out measures to oppose enemy's information weapons; to gain information superiority; to develop a society that is immune to information; to establish a concept of counteraction to information warfare. The authors have examined both foreign and Russian sources of law defining the requirements for the government activities to confront the information war. They also refer to the viewpoints of foreign and Russian researchers, politicians and public figures who have narrated their opinions on the concept and features of such political and legal constructs as information war and information weapons. The problem of information warfare must be identified as a profoundly serious and damaging threat. The paper expands on some provisions defining the characteristics of information warfare and methods to resist it as well as the proposals to amend the domestic legislation to create conditions for an accurate understanding of this political and legal phenomenon. In addition, it emphasizes the view that amending the Information Security Doctrine is not enough to counterbalance the threat of IW. In a separate document it is necessary to recount all notions, requirements and methods for the government actions to bring about a gradual change in the situation, inter alia, developing sectoral (information security) legislation, training specialists in informational and psychological counter aggression, shaping public opinion through the government-run media, pursuing advocacy policy, etc.*
Keywords: *information war, information weapons, methods to counteract information warfare techniques, individual, society, state, defense, security model.*

References

1. Atamanov G.A. Informacionnaya voina: eksplikaciya ponyatiya [Elektronnyi resurs] // URL: http://www.naukaxxi.ru/materials/254/ (data obrasheniya: 19.11.2016).
2. Doklad Fonda podderzhki demokratii. Yanvar' 2016 (National Endowment for Democracy, NED), opublikovannyi v Journal of Democracy [Elektronnyi resurs] // URL: http://www.ned.org/wp-content/uploads/2016/01/January-2016-JOD-Hijacking-of-Soft-Power-Christopher-Walker.pdf (data obrasheniya: 19.11.2016).
3. Lovcov D.A. Kanal 2h2: yumor, sarkazm ekstremizm? // Zakon. № 11. 2008. S. 28–29.
4. Pirumov V.S., Rodionov M.A. Nekotorye aspekty informacionnoi bor'by v voennyh konfliktah // Voennaya mysl'. 1997. № 5. S. 44–47.
5. Pochepcov G.G. Informacionnaya voina: opredeleniya i bazovye ponyatiya [Elektronnyi resurs] // URL: http://psyfactor.org/psyops/infowar25.htm (data obrasheniya: 19.11.2016).
6. Proekt doktriny informacionnoi bezopasnosti RF [Elektronnyi resurs] // URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (data obrasheniya: 19.11.2016).
7. Rasporyazhenie Pravitel'stva RF ot 10.07.2014 № 1271-r «O podpisanii Soglasheniya mezhdu Pravitel'stvom Rossiiskoi Federacii i Pravitel'stvom Respubliki Kuba o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informacionnoi bezopasnosti» [Elektronnyi resurs] // URL: http://www.pravo.gov.ru (data obrasheniya: 19.11.2016).
8. Rasporyazhenie Pravitel'stva RF ot 17.09.2013 № 1672-r «O podpisanii Soglasheniya mezhdu Pravitel'stvom Rossiiskoi Federacii i Pravitel'stvom Respubliki Belarus' o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informacionnoi bezopasnosti» [Elektronnyi resurs] // URL: http://www.pravo.gov.ru (data obrasheniya: 19.11.2016).
9. Rastorguev S.P. Informacionnaya voina. M.: Radio i svyaz', 1998.
10. Cymbal V.I. O koncepcii informacionnoi voiny // Informacionnyi sbornik «Bezopasnost'». 1995. № 9.