УДК 341.1/8

КАТЕГОРИЯ «ИНФОРМАЦИОННОЙ ВОЙНЫ» В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Е.В. Калинина

Нижегородский государственный университет им. Н.И. Лобачевского, Н. Новгород

mikaella.evk@mail.ru

Поступила в редакцию 25.12.2019

Категория «информационная война» признана далеко не всеми доктринами международного права. Тем не менее ее проявления представляют реальную угрозу для безопасности государства и мирового сообщества в целом.

Ключевые слова: информационная война, кибервойна, международная информационная безопасность, кибербезопасность, киберпространство, информационное оружие.

Информационное воздействие на личность, общество, государство, мировое сообщество является неотделимой частью современной реальности. При этом следует помнить, что международная и внутригосударственная информационная безопасность различаются так же, как и международное и внутригосударственное право. А. Лукацкий поясняет, что, рассуждая о международной информационной безопасности, мы в первую очередь имеем в виду «свод вопросов, касающихся цифрового суверенитета, управления Интернетом, международного сотрудничества и т.п.» [1].

Плюрализм интерпретаций происходящих в стране и мире событий предполагает охват неограниченной по широте аудитории, и даже самые «стойкие» и невосприимчивые к влиянию чужого мнения порой неосознанно оказываются реципиентами и распространителями умело преподнесенных идей и суждений. Для каждой категории объектов информационного воздействия разработаны специальные технологии подачи материала.

Все это делает сообщества и государства уязвимыми перед актами, направленными на внутреннюю дестабилизацию и возможную реструктуризацию влиятельных акторов международного общения. Одним из основных вызовов информационного воздействия (как, впрочем, и одним из эффективных средств обеспечения информационной безопасности) является вынужденное ограничение суверенитета государств в информационном пространстве. В этой связи появляются новые категории: «информационный суверенитет» и «цифровой суверенитет». В.В. Бухарин полагает, что РФ для защиты национальных интересов в информационном обществе в первую очередь следует добиться независимости в области цифровых технологий. Исследователем перечислены приоритетные «компоненты цифрового суверенитета, технически обеспечивающие национальную безопасность: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платёжная система, собственные средства защиты, криптографические алгоритмы и протоколы, навигационная система» [2, с. 78].

В ноябре 2014 г. в журнале «Международная жизнь» (№ 11-2014) вышла в свет совместная статья специального представителя Президента РФ по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских и заместителя директора Института проблем информационной безопасности МГУ, профессора А.А. Стрельцова, в которой авторы формулируют основные вызовы использования ИКТ в международном информационном пространстве и, следовательно, размышляют о том, может ли сфера информационных технологий стать предметом регулирования международного права.

Профессор А.А. Стрельцов пошел дальше, предложив к обсуждению вопрос о применимости норм МГП к киберконфликтам в статье под названием «Применение норм международного гуманитарного права к вооруженным конфликтам в киберпространстве», опубликованной 25.04.2016 на сайте Digital.report [3]. Идея целесообразности использования норм МГП применительно к войне информационной, хоть и выглядит привлекательно, при более пристальном изучении оказывается надуманной, что определяется спецификой информационного воздействия, которое обладает следующими характер-

ными чертами: «информационную войну», как правило, не объявляют; целью атаки становится как компьютерная сеть, так и социально-политическая система; важной составляющей являются семантические атаки, вводящие противника в заблуждение посредством воздействия на него информации; имеет место относительная безответственность распространителей информации, обусловленная сложностью локализации и установления личности нарушителя; сложна процедура доказывания вины нарушителя; все существующие на данный момент средства борьбы с информационными угрозами отстают в развитии от интенсивно формирующихся способов воздействия на целевые объекты; плюрализм идей и политических теорий, с одной стороны, характеризует уровень свободы общества, но, с другой, в государстве с недостаточно развитым уровнем правовой культуры, правосознания и упадком ценностных ориентиров может привести не только к потере идентичности, но и к распаду страны; трансграничный характер воздействия (и в целом отсутствие установленных границ) делает установление факта агрессии практически невозможным; осуществляется неизмеримо больший охват территории, в сравнении с «театром военных действий» при классическом вооруженном конфликте (международного и немеждународного характера); как следствие, количество потенциальных жертв неисчислимо; в отличие от «физической» войны, влекущей в качестве побочного эффекта страдание мирного населения (гражданских), во время войны информационной гражданские используются в качестве основного средства воздействия на субъектов принятия решений. Как поясняют В.В. Кихтан и З.Н. Качмазова, в процессе информационной войны на объекты защиты производятся «интегрированные и динамические атаки», т.е. «воздействию может подвергаться один или сразу все элементы» [4, с. 230]. «Если мишенью предстают данные, то атакующее воздействие может приобретать следующие формы: отказ в получении данных; атаки на системы, содержащие данные, стирание данных; физическое уничтожение накопителей данных; кража данных с последующим их манипулированием для реализации преследуемых целей» [4, с. 230].

Хотя аналогия применимости норм МГП и права вооруженных конфликтов к информационной войне неубедительна, она, безусловно, не только явилась изощренным способом привлечения внимания теоретиков и практиков к проблеме активного информационного противоборства, но и вынудила признать факт утверждения в современной политико-правовой практике новой категории «информационная война», наряду с уже имеющимися – «война», «холодная война». Можно согласиться лишь с использованием категории «информационная война» в контексте политического противоборства государств и, в этой связи, с применением понятия «театр военных действий» в отношении информационного пространства.

Отсюда – назревшая необходимость не только глобального признания правил поведения государств в информационном пространстве, но и ограничения по применению технологий воздействия, аналогично тому, как в современном мире ограничивается и даже запрещается использование определенных видов оружия.

Хотя следует признать, что идея «информационной войны» вошла в политический и медийный обиход гораздо раньше: И.Н. Панарин утверждает, что впервые данный термин был упомянут в 1967 г. в книге А. Даллеса «Тайная капитуляция» [5]; а В.В. Кихтан и З.Н. Качмазова [4, с. 228] полагают, что термин был впервые использован в докладе Т. Рона «Системы оружия и информационная война» в 1976 г. [6].

К сожалению, политические амбиции и конфликт интересов ведущих держав до сих пор препятствуют достижению компромисса в формулировании универсальных организационно-правовых средств обеспечения безопасности международного информационного пространства.

Так, до сих пор не выработано единообразного определения понятия «информационная война». Г. Вирен считает, что «информационная война – это комплекс мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им целей, которые не входят в число их интересов, а также защита от подобных воздействий» [7, с. 6–7].

В.В. Кихтан и З.Н. Качмазова представляют информационную войну как конфликт репутаций между различными коалициями [4, с. 228–235].

Мартин Либики, один из исследователей искомой категории, понимает под информационной войной воздействие, направленное на манипулирование, искажение и опровержение информации [8]. Он также выделяет 7 форм информационного воздействия: 1) командно-управленческая (Command-and-Control Warfare); 2) разведывательная (Intelligence-Based Warfare); 3) электронная (Electronic Warfare); 4) психологическая (Psychological Warfare); 5) хакерская (Hacker Warfare); 6) экономико-информационная (Economic Information Warfare); 7) кибервойна.

С.П. Расторгуев трактует информационную войну как открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения

определенного преимущества в материальной сфере [9].

Г.Г. Подчепцов определяет информационную войну как коммуникативную технологию, которая воздействует на получателя с кратковременными или долговременными целями. Объектом таких воздействий всегда является массовое сознание.

Большинство авторов, таким образом, характеризует данное явление как *воздействие*, т.е. не состояние, а именно действие. Существенным его признаком следует считать направленность на массовое сознание, как справедливо отметил Г.Г. Подчепцов.

Профессор Н.И. Костенко выявил 3 подхода к пониманию феномена информационной войны: 1) информационная война имеет исключительно военный характер и применяется только в боевых действиях; 2) информационная война – это явление, сопутствующее человеку со времен общинно-племенного строя; 3) информационная война суть информационно-пропагандистские операции. Третий подход, как более комплексный, гораздо точнее отражает реалии современных внешних и внутренних отношений обществ и государств.

В российской и зарубежной правовой науке использование понятий «информационная война» и «кибервойна» различно: за рубежом чаще всего встречается термин «кибервойна» (Cyber Warfare), в российской – «информационная война».

Кроме того, данные термины не эквивалентны по своему содержанию: «информационная война» представляется шире, поскольку предполагает не только использование технических средств для осуществления противоборства между сторонами, но и психологическое воздействие технологий подачи информации на целевые социальные группы, которые в результате и становятся основными инструментами влияния на субъектов принятия политических решений. Такое понимание позволяет утверждать, что примитивные формы информационной войны возникли за тысячелетия до появления кибервойны.

В аналитической статье, посвященной попыткам РФ и ШОС добиться принятия в ООН проекта Правил поведения в информационном пространстве (еще в версии 2016 года), ее автор – И. Дылевский – критикует идею «информационного устрашения», формулируя тезисы, опровергающие сопоставимость угрозы, например, ядерного оружия и использования компьютерных технологий в военных целях: 1) применение информационных технологий не влечет, в отличие от применения ядерного оружия, «явной угрозы взаимного гарантированного уничтожения» [10], что исключает элемент взаимного сдерживания; 2) идея «ядерного устрашения» [10] воплощалась двумя основными ядерными державами: СССР и США, а в информационном пространстве действует множество негосударственных акторов, в силу чего односторонней доброй воли к прекращению эскалации информационного противоборства будет явно недостаточно; 3) разработать, произвести, приобрести и распространить «информационное оружие» легче, чем технологии создания ядерного оружия, что затрудняет достижение существенного превосходства над соперниками; 4) как отмечалось ранее, «источник информационной атаки» выявить сложно по причине «его анонимности и комплекса специальных мер, принимаемых для «запутывания» следов» [10], а значит, получить достоверные доказательства вины для обоснования актов «справедливого возмездия» не удастся; 5) крайне сложно «обеспечить баланс военных информационных потенциалов на основе достоверного знания основных характеристик системы информационного вооружения сторон» [10]. Распространение сведений о «разработке новых систем вооружения» должно привести «к совершенствованию средств и способов противодействия им, т.е. к нарушению баланса» [10]. Но и любая неконтролируемая скрытая разработка таких систем также будет нарушать искомый баланс, и дестабилизировать военно-политическую обстановку [10].

В процессе поиска оптимальных подходов к обеспечению коллективной информационной безопасности обнаруживаются следующие дилеммы:

1) для поддержания коллективной безопасности в целом и для информационной безопасности в частности необходимо сотрудничество всех заинтересованных сторон, поскольку в открытом информационном пространстве государству защитить себя индивидуально, без содействия других субъектов международных отношений, гораздо сложнее, что порождает необходимость компромиссов, ставящих под сомнение полноту внешнего суверенитета государства (пример – Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 2001 г.), которую Российская Федерация не поддержала именно по причине наличия в документе положений, позволяющих соответствующим учреждениям вмешиваться во внутренние дела государств, под благовидным предлогом совместной борьбы с киберпреступностью);

2) под удар будут поставлены атрибуты государственной тайны;

3) взаимное недоверие субъектов международного киберпространства (единственным способом укрепления доверия, в данной сфере, могла бы стать открытость и предоставление доступа к государственным базам данных в целях оптимизации противодействия киберугрозам, чем не преминули бы воспользоваться отдельные державы для реализации определенных политических амбиций, что возвращает нас к предыдущим дилеммам);

4) обеспечение безопасности предполагает порой тотальный контроль поступающей информации и ее цензуру, а значит, и ограничение свобод личности в информационном пространстве, сопровождаемое сомнительной (временной) защищенностью персональных данных.

5 декабря 2018 г. был представлен на голосование Проект резолюции ГА ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», ставший результатом российской инициативы от 9 ноября 2018 г. (Проект резолюции I, содержащий правила ответственного поведения государств в киберпространстве). Проект был поддержан подавляющим большинством участников голосования: «за» – 119, «против» – 46, «воздержались» – 14. Это была далеко не первая попытка российской дипломатии добиться межгосударственного компромисса в сфере безопасности информационных технологий. В недавнем прошлом, в 2011 г. и в 2015 г., РФ и ШОС представляли на рассмотрение ГА ООН проект «Правила поведения в области обеспечения межнациональной информационной безопасности», не получивший, однако, поддержки в связи с противодействием США.

Резолюция 2018 г. включает только правила, одобренные Группой правительственных экспертов ООН по международной информационной безопасности в 2015 году [11]. Основной целью документа является мирное использование глобального информационного пространства, предотвращение военного использования информационных технологий.

В свете вышеизложенного можно было бы предложить к обсуждению нижеследующие пути противодействия потенциальному внешнему информационному воздействию.

1. Учитывая закономерности ведения войны, не только физической, с прямым использованием вооруженных сил, но и «холодной войны», а также характерные тенденции гонки вооружений, разработать средства, обеспечивающие защиту государства в международном информационном пространстве (как прямо, так и гипотетически), например, оптимизировать мероприятия по разработке программ, не только обеспечивающих кибероборону жизненно важных объектов, но и, в случае необходимости, «атакующих».

2. Создать при ООН совещательный орган, уполномоченный рассматривать и формулировать проекты решений по проблемам информационной безопасности.

Заместитель директора Центра международной информационной безопасности и научно-технологической политики МГИМО Е.С. Зиновьева сообщает о предложении РФ по формированию Группы открытого состава ООН, призванной стать «площадкой» для обсуждения направлений дальнейшего сотрудничества в целях обеспечения международной информационной безопасности [11]. Ранее, до 2017 г., в рамках ГА ООН функционировала созданная благодаря российским инициативам Группа правительственных экспертов ООН. На данный момент представляется необходимым наличие международного механизма, способного оптимизировать переговорный процесс в исследуемой сфере и компетентно оценивать поступающие предложения по «оздоровлению» обстановки в информационном пространстве.

3. Способствовать широкому распространению на внутригосударственном уровне аналитических ситуационно-кризисных центров обработки данных, поступающих через открытое информационное пространство. Уже существующие центры, имеющие существенный опыт работы, следует наделить новыми функциями с целью расширения их функциональности. В штат таких учреждений можно включить специалистов по созданию «киберпреград» активного свойства, т.е. способных разработать программы, атакующие субъектов несанкционированного доступа.

4. Создать на базе ведущих вузов междисциплинарные подразделения по подготовке кадров, необходимых для поддержания как национальной, так и международной информационной безопасности. Ввиду того что деятельность в указанном направлении требует серьезной подготовки в сфере информатики, программирования и компьютерной безопасности, юриспруденции, политологии, экономики, военной стратегии, национальной безопасности и проч., для преподавания в таких подразделениях следует привлекать теоретиков и практиков всех указанных и иных соответствующих областей.

5. Поощрять использование зарубежного опыта, как в области практических мероприятий по обеспечению стабильности и защищенности государственных интересов в информационном пространстве, так и в сфере реализации имеющихся программ и методик преподавания с целью подготовки кадров широкого

профиля, способных к пониманию и решению проблем, вызванных непониманием и, как следствие, невозможностью сотрудничества между прежними узкопрофильными специалистами: программистами и юристами, политологами и военными и проч.

6. Способствовать развитию информационной грамотности у пользователей, включающей не только способность использовать широкие «просторы» киберпространства, но и устойчивость к информационным манипуляциям и воздействию на сознание. Для реализации данной цели недостаточно включения курсов информационной безопасности в образовательные программы вузов даже для непрофильных специальностей. Необходимо участие специально подготовленных психологов, помогающих целевой аудитории осознать персональные уязвимости каждого перед манипуляционными технологиями подачи материала, причисляющими их к тем или иным группам риска.

Список литературы

1. Лукацкий А. В международной ИБ грядет передел. Режим доступа: https://www.securitylab.ru/blog/personal/Business_without_danger/135155.php (дата обращения: 10.11.2017).

2. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6(51). С. 76–91.

3. Стрельцов А.А. Применение норм международного гуманитарного права к вооруженным конфликтам в киберпространстве. Режим доступа: https://digital/report/konflikt-v-kiberprostranstve/ (дата обращения: 29.09.2019).

4. Кихтан В.В., Качмазова З.Н. Информационная война: понятие, содержание и основные формы проявления // Вестник Волжского университета им. В.Н. Татищева. 2018. № 2. Т. 2. С. 228–235.

5. Панарин И.Н. Информационная война: крепкий щит и острый меч. Режим доступа: http//www.panarin.com/comment/16/?sphrase_id=9391 (дата обращения: 10.09.2019).

6. Гриняев С. Концепция ведения информационной войны в некоторых странах мира. Режим доступа: http://www.soldiering.ru/psychology/conception_psywar.php (дата обращения: 15.09.2019).

7. Вирен Г. Современные медиа: Приемы информационных войн. М.: Аспект Пресс, 2013. 126 с.

8. Либики М. Что такое информационная война? Режим доступа: https://pluriversum.org/opinion/strategy/chto-takoe-informatsionnaya-vojna/ (дата обращения: 07.09.2019).

9. Расторгуев С.П. Информационная война. Режим доступа: http://log-in-ru/books/rastorguev-s-p-informatsionnaya-voiyna-rastorguev-s-p-voennoe-delo/ (дата обращения: 02.09.2019).

10. Дылевский И. Правила поведения в информационном пространстве – альтернатива гонке информационных вооружений. Режим доступа: https://digital.report/pravila-povedeniya-v-informatsionnom-prostranstve/ (дата обращения: 25.11.2017).

11. Зиновьева Е.С. Дипломатическое наступление России в области информационной безопасности. Режим доступа: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/ (дата обращения: 28.09.2019).

THE CATEGORY OF «INFORMATION WARFARE» FROM THE PERSPECTIVE OF NATIONAL AND INTERNATIONAL SECURITY

E.V. Kalinina

Despite the fact that the category of «information warfare» was not recognized by every doctrine of international law, information warfare manifestations constitute real threat for state and international security in general.

Keywords: information warfare, cyber warfare, international information security, cybersecurity, cyberspace, information weapon.

References

1. Lukackij A. V mezhdunarodnoj IB gryadet peredel. Rezhim dostupa: https://www.securitylab.ru/blog/personal/Business_without_danger/135155.php (data obrashcheniya: 10.11.2017).

2. Buharin V.V. Komponenty cifrovogo suvereniteta Rossijskoj Federacii kak tekhnicheskaya osnova informacionnoj bezopasnosti // Vestnik MGIMO-Universiteta. 2016. № 6(51). S. 76–91.

3. Strel'cov A.A. Primenenie norm mezhdunarodnogo gumanitarnogo prava k vooruzhennym konfliktam v kiberprostranstve. Rezhim dostupa: https://digital/report/konflikt-v-kiberprostranstve/ (data obrashcheniya: 29.09.2019).

4. Kihtan V.V., Kachmazova Z.N. Informacionnaya vojna: ponyatie, soderzhanie i osnovnye formy proyavleniya // Vestnik Volzhskogo universiteta im. V.N. Tatishcheva. 2018. № 2. T. 2. S. 228–235.

5. Panarin I.N. Informacionnaya vojna: krepkij shchit i ostryj mech. Rezhim dostupa: http//www.panarin.com/comment/16/?sphrase_id=9391 (data obrashcheniya: 10.09.2019).

6. Grinyaev S. Koncepciya vedeniya informacionnoj vojny v nekotoryh stranah mira. Rezhim dostupa: http://www.soldiering.ru/psychology/conception_psywar.php (data obrashcheniya: 15.09.2019).

7. Viren G. Sovremennye media: Priemy informacionnyh vojn. M.: Aspekt Press, 2013. 126 s.

8. Libiki M. Chto takoe informacionnaya vojna? Rezhim dostupa: https://pluriversum.org/opinion/strategy/chto-takoe-informatsionnaya-vojna/ (data obrashcheniya: 07.09.2019).

9. Rastorguev S.P. Informacionnaya vojna. Rezhim dostupa: http://log-in-ru/books/rastorguev-s-p-informatsionnaya-voiyna-rastorguev-s-p-voennoe-delo/ (data obrashcheniya: 02.09.2019).

10. Dylevskij I. Pravila povedeniya v informacionnom prostranstve – al'ternativa gonke informacionnyh vooruzhenij. Rezhim dostupa: https://digital.report/pravila-povedeniya-v-informatsionnom-prostranstve/ (data obrashcheniya: 25.11.2017).

11. Zinov'eva E.S. Diplomaticheskoe nastuplenie Rossii v oblasti informacionnoj bezopasnosti. Rezhim dostupa: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/ (data obrashcheniya: 28.09.2019).