Безопасность критических информационных инфраструктур в международном гуманитарном праве

А.В. Коротков, Е.С. Зиновьева

Информационная безопасность выходит на передний план международной повестки дня вследствие осознания возрастающей зависимости всех сфер жизни личности, общества и государства от информационных инфраструктур и их уязвимости - как информационной, логической, так и физической. В статье рассматривается вопрос применимости международного гуманитарного права к информационной сфере.

Информационная безопасность выходит на передний план международной повестки дня вследствие осознания возрастающей зависимости всех сфер жизни личности, общества и государства от информационных инфраструктур и их уязвимости как информационной, логической, так и физической. Подтверждение тому - последние события, получившие широкое освещение в СМИ, - атаки вируса Stuxnet на ядерные объекты Ирана, публикация конфиденциальной дипломатической переписки сайтом WikiLeaks, массовая волна протестов в странах арабского Востока, получившая в прессе название «революции Facebook».

Аналитические материалы по проблемам информационной безопасности публикуют ведущие зарубежные и российские издания, издаются научные труды и монографии. Создаются специализированные исследовательские центры, такие, как Институт проблем информационной безопасности МГУ, Центр исследований безопасности Университета Цюриха. Проблема информационной безопасности находит отражение в официальных документах и практической деятельности ведущих международных организаций - ООН, ОБСЕ, СНГ, ОДКБ, НАТО.

Несмотря на то, что к информационной безопасности приковано внимание международного сообщества, данная сфера фактически не регулируется нормами международного права. Единственным договором является Европейская конвенция о киберпреступности 2001 г. В настоящее время к конвенции присоединились 42 страны, в том числе 38 стран-членов Совета Европы, а также США, Канада, Япония и ЮАР. Россия не ратифицировала Конвенцию.

В феврале 2011 г. на Мюнхенской конференции по безопасности были представлены результаты исследования группы российских и американских ученых под руководством профессора МГИМО (У) А.В. Короткова и ведущего научного сотрудника Института Восток-Запад (East-West Institute, EWI) К. Раушера «Выработка правил регулирования кибер-конфликта: применимость Женевских и Гаагских конвенций в информационной сфере»[1]. Российско-американские эксперты, таким образом, стали инициаторами обсуждения вопросов правового регулирования новой высокотехнологичной области безопасности, что особенно актуально и перспективно в контексте «перезагрузки» отношений между государствами.

Коротков Андрей Викентьевич – д.э.н., профессор, заведующий кафедрой мировых информационных процессов и ресурсов МГИМО(У) МИД России. E-mail: vestnik@mgimo.ru
Зиновьева Елена Сергеевна – к.полит.н., преподаватель кафедры мировых политических процессов МГИМО(У) МИД России. E-mail: vestnik@mgimo.ru

Международная информационная безопасность. Развитие информационных технологий преобразует современный мир. Формируется глобальное информационной пространство, которое создает новые возможности для экономического роста, политической модернизации, культурного развития. Но оно также формирует новые угрозы и разделительные линии на международной арене. Одно из негативных последствий бурного развития Интернета и других информационно-коммуникационных технологий - возникновение новых форм международных конфликтов, включая информационные войны, сетевые противоборства, хакерские атаки и т.п.

По мнению отечественного исследователя, научного сотрудника Центра политических исследований России А.В. Федорова, «в результате распространения информационно-коммуникационных технологий изменяется характер социума, следовательно, изменяется характер возникающих в нем противоречий и их разрешения»[2]. Все большее число государств вовлекаются в создание программ информационных средств воздействия, а также ведения информационных войн. Террористические и преступные группировки также берут на вооружение средства информационного воздействия.

Доктрина информационной безопасности России дает следующее определение: «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» . Специалисты выделяют «триаду» угроз международной информационной безопасности – террористическую, военную и преступную. Информационные технологии, в том числе информационное оружие, доступны, поэтому в информационном пространстве на равных действуют государства, террористические и преступные группировки.

Информационная безопасность включает в себя два аспекта: информационно-техническую и информационно-психологическую безопасность. Обеспечение информационно-технической безопасности представляет собой защиту, контроль и соблюдение законности и правопорядка в телекоммуникационной сфере (защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и пр.). Обеспечение же информационно-психологической безопасности предполагает защиту психологического состояния общества и государства от негативного информационного воздействия.

Особую опасность в рамках информационно-технологической компоненты информационного противоборства приобретает воздействие на критические информационные инфраструктуры государства. Нарушение информационной инфраструктуры АЭС или вывод из строя систем теплоснабжения на севере России, нарушение работы транспортных систем или систем вооружений может привести к более разрушительным последствиям, чем применение обычных вооружений. Воздействие на критические информационные инфраструктуры будет производиться именно через открытее сети, Интернет.

После террористических атак 11 сентября 2001 г. в США и странах Европейского Союза защита критических информационных инфраструктур стала одним их приоритетных направлений обеспечения безопасности. На международном уровне исследовательские программы, принятие модельных законов, а также другие действия по гармонизации законодательств начинают приниматься в рамках таких организаций как ОЭСР, «Группа восьми», НАТО, ООН, Всемирный банк. В настоящей статье мы сосредоточим внимание на информационно-технической стороне информационных войн и информационной безопасности, в рамках которой наибольшую опасность представляют атаки на критические информационные инфраструктуры.

Критические информационные инфраструктуры. Критически важная инфраструктура имеет ключевое значение для общественного порядка, экономической стабильности и национальной безопасности государств, особенно уязвимы развитые страны. Защита критической инфраструктуры затрагивает вопросы национальной безопасности, и потому входит в компетенцию государства. Тем не менее, большая часть инфраструктур находится в собственности частного бизнеса, поэтому государство и бизнес вынуждены совместно нести ответственность за безопасность и стабильное функционирование.

Значимость защиты критически важных информационных инфраструктур возрастает по ряду причин, среди которых:

— широкое распространение информационных технологий, в том числе, в целях обеспечения эффективной работы большинства инфраструктур и систем государства и бизнеса;
— возрастающая зависимость общества и государства от нормального функционирования критических инфраструктур;
— рост сложности, и, следовательно, уязвимости информационной составляющей критической инфраструктуры. Сложные информационные системы чувствительные не только в отношении информационных атак, они также подвержены сбоям в работе по причине ошибок в программном обеспечении, неточностей персонала и др. Выявить истинную причину неполадок зачастую бывает непросто.

В научном сообществе мира предпринимались попытки выработки общепринятого определения термина «критически важная инфраструктура», однако они не увенчались успехом. На сегодняшний день государства самостоятельно определяют, что относить к критически важным

инфраструктурам. Списки жизненно важных инфраструктур разнятся от страны к стране и определяются в соответствии с традициями, общественными и политическими причинами, а также географическими и историческими особенностями каждого государства[4]. «Акт Патриота» (Patriot Act) США дает следующее определение: «критические инфраструктуры - это системы и ресурсы, физические или виртуальные, настолько значимые для США, что их разрушение или нарушение нормальной работы способно подорвать военно-политическую безопасность государства, экономическую стабильность, здоровье граждан и общественный порядок, или повлечь за собой несколько вышеуказанных факторов в любой комбинации»[5].

В России нет официального документа, определяющего перечень критических инфраструктур или задающего направления обеспечения их безопасности. Однако в официальных документах можно найти ссылки на жизненную важность ряда систем для государственной безопасности, экономической стабильности и общественного порядка[6]. Отечественные исследователи, сотрудники Института проблем информационной безопасности МГУ дают следующее определение: «под инфраструктурой будем понимать набор отдельных взаимосвязанных структурных элементов системы, поддерживающих ее функциональность (работу по назначению). Под критической инфраструктурой будем понимать набор отдельных взаимосвязанных элементов, поддерживающих функциональность национально значимых для России сфер жизнедеятельности. Под критически важной информационной инфраструктурой будем понимать набор отдельных программно-аппаратных, сетевых и информационных компонентов, поддерживающих функциональной национально значимых для России сфер жизнедеятельности»[7].

В Соглашении ШОС по информационной безопасности 2009 г. критически важные инфраструктуры определяются как «объекты, системы и институты государства, воздействия на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества, государства»[8]. В этом же документе утверждается, что «информационные инфраструктуры – это совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации».

Подводя итог рассмотрению различных определений, отметим, что главной характеристикой критической инфраструктуры является ее ключевое значение для безопасности общества и государства. Критически важные инфраструктуры могут быть военными и гражданскими объектами, а также иметь двойное назначение. В информационной сфере гражданские и военные объекты тесно переплетены. В таблице 1 соотносятся российское и американское видение критических инфраструктур государства.

Таблица 1.

Критические информационные инфраструктуры России и США[11].

Российская Федерация[9]	**США[10]**	
Здравоохранение	Здоровье общества	Гражданские объекты
-	Службы экстренного реагирования	Гражданские объекты
-	Питание и сельское хозяйство	Объекты двойного назначения
Сельское хозяйство	Вода	Объекты двойного назначения
Водоснабжение	Государственное управление	Объекты двойного назначения
Государственное управление	-	Объекты двойного назначения
Очень большие информационные системы	Информационные и телекоммуникационные сети	Объекты двойного назначения
Информационные и телекоммуникационные сети	Энергетика	Объекты двойного назначения
Энергетика	-	Объекты двойного назначения
Теплоснабжение	Банковская и финансовая системы	Объекты двойного назначения
Банковская и финансовая системы	Наземный и водный транспорт	Объекты двойного назначения
-	-	Объекты двойного назначения
Транспортная система	Химическая промышленность и взрывоопасные материалы	Объекты двойного назначения
Индустрия	Критически важное производство	Объекты двойного назначения
-	Почтовая служба	Объекты двойного назначения
-	-	Объекты двойного назначения
Муниципальное управление		Объекты двойного назначения
Гражданская оборона		Объекты двойного назначения
-	Военно-промышленный комплекс	Военная цель
Оборона		Военная цель

Критические инфраструктуры

Отметим, что, помимо национальных, выделяют и международные критические информационные инфраструктуры, среди которых система доменных имен Интернета, коммуникационные спутники, межконтинентальные кабели и маршрутизаторы и др.

В настоящее время сосуществуют традиционные инфраструктуры, созданные до широкого распространения Интернета и информационных технологий и не опирающиеся на них в своем функционировании, и информационные инфраструктуры. Переход от традиционных к

информационным форматам организации – процесс постепенный. В развитых странах в условиях формирования «цифровой экономики» наблюдается все более широкое распространение сетевых, информационных инфраструктур, т.к. они более экономичны, эффективны, эргономичны.

В таблице 2 сопоставляются характеристики традиционных и информационных инфраструктур.

Таблица 2.

Традиционные и информационные критические инфраструктуры[12].

Традиционные критические инфраструктуры	Критические информационные инфраструктуры
Человеческий контроль над функционированием	Функционирование в режиме реального времени с опорой на ПО (напр. искусственный интеллект)
Человеческое регулирование межинфраструктурного взаимодействия	Сложный и взаимозависимый характер межинфраструктурного взаимодействия
Иерархическая структура использования и функционирования	Сетевая («снизу вверх») структура использования и функционирования
Примеры: госпитали, в которых ведутся бумажные записи и учет, система контроля полетов, основанная на радиосистемах и др.	Примеры: информационная финансовая система, автоматизированная система контроля полетов и др.

По ряду причин информационные инфраструктуры более уязвимы. Сложность и взаимозависимость информационных систем ведет к тому, что последствия нарушения их нормальной работы могут быть непредсказуемыми, в наихудшем варианте вызвать «эффект домино». Таким образом, именно воздействие на критические информационные инфраструктуры является наиболее опасным для общества и гражданского населения, может спровоцировать беспорядки, нестабильность, волнения.

Современные системы включают в себя элементы традиционной физической инфраструктуры, работа которых обеспечивается программным обеспечением и иными информационными системами и ресурсами. Маршрутизаторы, сетевые кабели уязвимы по отношению к традиционному оружию. Нормальную работу виртуальных элементов, таких, как программное обеспечение, стандарты, в большинстве случаев невозможно нарушить с помощью традиционных вооружений, однако их можно разрушить непрямым способом, с помощью информационного оружия, например, вирусов, вредоносного программного обеспечения, червей, закладок и др.

Информационная война: технологическое измерение. Государственное противоборство, перешедшее в информационное пространство, порождает информационные войны. В экспертном сообществе и среди политиков-практиков нет согласия относительно того, что являют собой информационные войны, насколько разрушительными могут быть их последствия и др. На международном уровне на сегодняшний день не было выработано общепринятого определения информационной войны и информационного оружия. Это связано с различием интересов и позиций государств в информационной сфере, а также нежеланием связывать себе руки в информационном пространстве.

Приведем определения, выработанные Шанхайской организацией сотрудничества: «Информационное оружие – это информационные технологии, средства и методы, применяемые в целях ведения информационной войны»[13], а «Информационная война – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам или ресурсам, критически важным и другим структурам, подрыва политической, экономической, социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[14].

Как правило, проблематику информационных способов ведения войны рассматривают в контексте революции в военном деле. Современное высокоточное, наукоемкое оружие (так называемое оружие шестого поколения войн) включает в себя и информационную компоненту. Научный сотрудник Российского института стратегических исследований А.В. Бедрицкий отмечает в этой связи: «сегодня основная роль информационных систем в военной сфере заключается не столько в повышении точности поражения цели, сколько в том, что с их помощью можно реорганизовать структуру вооруженных сил, сделать их более гибкими и эффективными, повысить скорость реагирования на поле боя, а также выработать новые тактические приемы»[15].

Описанные выше тенденции усиливают ассиметричный характер современных конфликтов. Китай в 2001 г. заявил о том, что в условиях существенного отрыва США в области развития науки и технологий, не представляется возможным достижение паритета, и в этих условиях КНР будет ориентироваться на информационные средства воздействия. Информационные технологии широко используются террористами не только как одна из новых форм оружия, но и в целях повышения эффективности организации между ячейками в рамках сетевой структуры, для широкого распространения информации о терактах.

Авторитетный российский ученый, доктор военных наук, профессор В.И. Слипченко, занимающийся анализом развития систем вооружений и революции в военном деле, полагает, что следующим поколением войн, седьмым по счету, будут информационные войны, которые будут вестись информационным оружием[16]. Вероятнее всего, полем боя в новых информационных войнах станет именно киберпространство.

Нужно отметить, что лидерство в области изучения проблем информационной безопасности принадлежит исследовательскому сообществу

США. Особенно следует выделить концепцию «информационных войн второго поколения», разработанную аналитиками RAND Corporation. В соответствии с данной концепцией, информационные атаки рассматриваются как атаки нового типа стратегического противоборства.

Использование информационных технологий в военно-политических целях лишь в ограниченной степени попадает в сферу действия норм международного права. Все более актуальной становится адаптация международного права к особенностям информационной сферы. Еще в 1998 г. Россия выступила с инициативой о постановке на международном уровне вопроса об обеспечении международной информационной безопасности. С 1998 г. резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» принималась Генеральной Ассамблеей ООН ежегодно. Россия ориентирует международное сообщество на исследование угроз в сфере информационной безопасности и возможных совместных мер по их устранению, в том числе на создание международно-правового режима, ограничивающего возможности создания и применения информационного оружия. Кроме того, Россия инициирует обсуждение проблемы информационной безопасности на региональном уровне, в рамках таких организаций как ШОС, ОБСЕ, ОДКБ, НАТО и др.

Средством ведения информационных войн является информационное оружие. Под информационным оружием понимают любые средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные инфраструктуры государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства. Вышеприведенное определение достаточно широко, чтобы включать в себя высокоточное оружие, радиоэлектронное оружие, вредоносное программное обеспечение, а также средства пропаганды и воздействия на психику человека.

По данным Конгресса США, в настоящее время более 120 стран занимаются разработками информационного оружия[17], что стало ответом на неспособность поддерживать баланс сил в области обычных вооружений и, в особенности, оружия массового поражения. В большинстве стран разрабатываются концепции ведения информационных войн и предпринимаются попытки их реализации. Развитие информационного оружия, ведение информационных войн способно расшатать сложившуюся систему международной безопасности и контроля над вооружениями. Как убедительно показал в своей работе М. Либики, один из признанных классиков теории информационной войны, традиционные меры сдерживания в информационном пространстве малоэффективны, вследствие дешевизны и доступности для террористических и преступных группировок информационного оружия, сложности выявления источника угрозы[18]. Возрастает актуальность уточнения международно-правовой базы, регулирующей глобальное информационное пространство.

Наибольшую опасность представляет возможный ассиметричный ответ на использование агрессивного информационного потенциала, в том числе с использованием обычных вооружений, а в наихудшем случае – ОМУ. Традиционные вооружения в современном мире сосуществуют с информационными. Переход к новым, информационным методам ведения войны не происходит в одночасье.

В Таблице 3 приведены черты традиционных и информационных форм оружия.

Таблица 3.

Характеристики традиционных и информационных видов оружия[19].

Традиционное оружие	Информационное оружие
основано на использовании силы (кинетической, электромагнитной и ядерной), биологических и химических реакций	основано на использование логики
непосредственная цель – физические объекты	цель – информация или контроль
ресурсы специально разработаны для вооруженного конфликта	ресурсы, как правило, имеют гражданское назначение
доступ к наиболее опасным строго ограничен	низкий порог доступности, который продолжает понижаться
базовые виды вооружений недорогие, наиболее продвинутые – крайне дорогие	большинство информационных видов оружия недорогие
Примеры: традиционное оружие, улучшенное за счет возможностей ИКТ (ГПС, сетевые подразделения, средства удаленного контроля и др.)	Примеры: черви, вирусы, удаленный контроль, кражу паролей и др.

Конвенции, лежащие в основе международного гуманитарного права, составлялись в то время, когда войны велись исключительно традиционными вооружениями. Информационные же виды оружия предполагают широкое использование информационных технологий. Как уже было отмечено выше, информационные формы оружия привнесли много нового в формы и методы ведения войны. Нужно сказать, что процесс перехода от первых к последним носит постепенный характер. Несмотря на то, что в настоящее время в конфликтах могут использоваться оба типа вооружений, есть определенные стимулы к созданию более продвинутых систем вооружений, которые представляют собой либо улучшенную версию традиционных, либо принципиально новые, информационные виды оружия.

Опираясь на определения информационного оружия и критических инфраструктур, можно выделить четыре принципиально различных направления информационного противоборства:

— использование традиционных вооружений против традиционной критической инфраструктуры (ситуация, аналогичная войнам XX века, подпадает под действие международного гуманитарного права);
— использование традиционных вооружений против сетевой критической инфраструктуры (критической информационной инфраструктуры) маловероятно;
— использование информационного вооружений против традиционной критической инфраструктуры – атака с использованием глобальной системы позиционирования (GPS, ГЛОНАСС и др.) на транспортные и иные инфраструктурные сети, сетевые войска атака с видео-поддержкой, атака дистанционно-управляемого воздушного аппарата на объекты критической инфраструктуры;
— использование информационного вооружений против сетевой критической инфраструктуры (критической информационной инфраструктуры). – собственно, войны будущего. Атака с помощью ПО на правительственные информационные системы, закладки и др.

Очевидно, что изучение вопроса применимости и достаточности международного гуманитарного права для правового регулирования действий с применением информационного оружия осуществимо только при понимании того, что признается существование и возможность использования информационных систем как оружия, а организованное противоборство с его использованием признается как война. В настоящее время международное сообщество приходит к такому пониманию. Страны склонны признавать свою уязвимость в информационной сфере и проявляют готовность принимать международно-правовые документы, регулирующие и ограничивающие возможность агрессивных действий в информационной сфере.

Применимость международного гуманитарного права в информационной сфере. Информационные войны в меньшей степени подпадают под регламентацию международного публичного права, чем войны, ведущиеся в «реальном» мире. Тем не менее, это не отменяет необходимости нормативно-правовой регламентации. Многие из положений международного гуманитарного права были выработаны применительно к обычным условиям ведения войны и в современных условиях требуют доработки.

Право вооруженных конфликтов, несмотря на свою оторванность от политической практики, определяет правила цивилизованного ведения вооруженных действий. Международное гуманитарное право обладает лишь ограниченной применимостью по отношению к информационным конфликтам. Между тем существует насущная потребность в выработке правил регулирования конфликтов в информационной сфере. Это связано с тем, что информационные атаки по своим последствиям становятся все более масштабными, создавая реальную угрозу безопасности государству. Более того, участниками информационных конфликтов могут быть не только государства, но и неправительственные участники, в том числе террористические группировки.

К настоящему времени существует множество международно-правовых актов, регулирующих отношения государств в период вооруженного конфликта. К рассмотренным в работе группы экспертов источникам международного гуманитарного права отнесены:
— Женевская конвенция 1964 г. об улучшении состояния раненых на поле боя;
— Гаагские конвенции 1899 г. и 1907 г. о законах и обычаях сухопутной войны;
— Женевский протокол 1928 г. о запрещении использования на войне удушающих газов и бактериологического оружия;
— Женевская конвенция 1949 г. об улучшении состояния раненых и больных и членов экипажа судов на море;
— Женевская конвенция 1949 г. об обращении с военнопленными;
— Женевская конвенция 1949 г. об улучшении положения гражданского населения во время войны;
— Женевская конвенция 1975 г. о запрещении разработки создания и хранения бактериологических и токсических вооружений и их уничтожении;
— Дополнительные протоколы к Женевским конвенциям 1977 г. о защите жертв международных вооруженных конфликтов, о защите жертв немеждународных вооруженных конфликтов, о принятии дополнительных отличительных знаков.

Некоторые из этих конвенций были отобраны, так как они определяют механизмы защиты и запрещенные вооружения, которые могут нанести ущерб персоналу, обслуживающему критические инфраструктуры. Термин «критическая инфраструктура» не используется в Женевских конвенциях о правах, обычаях и защите жертв войны. Однако сама идея ресурсов и персонала, жизненно важных для гражданских и гуманитарных целей, хорошо проработана в ряде статей. Конвенции исторически обеспечивают строгие требования к ресурсам и персоналу, находящимся под строгой защитой:
— «занимающие незначительную часть территории …»;
— «малонаселенные в сравнении с возможностью размещения …»;
— «далеко отстоящие от военных объектов или крупных промышленных мощностей …»;
— «не расположенные на территории, значимой для ведения военных действий …»;

— «средства коммуникации и транспорта не должны использоваться для военного персонала или материалов …»;
— «не защищаемые военными средствами …»;
— «отмеченные красными крестами (красными полумесяцами, красными львами и солнцами …»;
— «все необходимые шаги должны быть предприняты, чтобы освободить … здания, используемые в целях религии, искусства, науки или благотворительности, исторические здания, госпитали и здания, где размещены больные и раненые ... в том случае, если они не используются в военных целях»
— «подводные кабели, соединяющие оккупированную территорию с нейтральными территориями»[20].

В самом широком смысле критические инфраструктуры – это системы, имеющие важнейшее значение в защите человеческой жизни, обеспечении экономической стабильности и национальной безопасности, причем, в центральное значение придается человеческой безопасности. Несмотря на то, что термин «защита критических инфраструктур» не используется в Конвенциях, безопасность человека, в особенности гражданского населения, имеет прямое отношение к их содержанию. Большое значение в праве вооруженных конфликтов придается защите гражданских объектов – «гражданские объекты не должны являться объектом нападения или репрессалий»[21]. Конвенции предписывают исключение такого рода объектов из возможных объектов атаки, а также постоянную защиту и осторожное обращение. В случае прекращения действия защищаемого статуса гражданских объектов, атакующая сторона обязуется сделать должное предупреждение.

Таким образом, международное гуманитарное право применимо к защите объектов критической информационной инфраструктуры, используемой в гражданских целях, как например, информационные ресурсы и системы, обеспечивающие работу госпиталей и больниц. Вполне эффективно могут применяться положения Дополнительного протокола 1 Гаагской конвенции 1907 г., запрещающие подвергать нападению или уничтожению объекты, необходимые для выживания гражданского населения (запасы пресной воды, запасы продуктов питания и др.). Отметим, что среди критических информационных инфраструктур можно выделить лишь незначительное количество систем, используемых исключительно в гражданских целях, что сужает применимость норм гуманитарного права. Большая часть может использоваться как в гражданской, так и в военной сферах, вследствие чего нормы права нуждаются в доработке. Гражданские информационные ресурсы и системы не обладают отличительными знаками, что потенциально повышает их уязвимость и снижает степень защиты.

Особое внимание в Дополнительном протоколе к Женевским конвенциям 1949 г. уделяется установкам и сооружениям, сдерживающим опасные силы, таким, как плотины, дамбы и др. Такие установки и сооружения не должны подвергаться нападению даже если относятся к военным объектам, «если такое нападение может вызвать высвобождение опасных сил, и последующие тяжелые потери среди гражданского населения»[22].

В большинстве случаев в информационной сфере сложнее определить гражданские объекты, так как в наступательных и оборонительных операциях могут быть задействованы гражданские объекты. К военным относятся объекты, «которые в силу своего характера, размещения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество»[23].

Международное гуманитарное право разрабатывалось государствами, которые не только являются субъектами права, но и легитимными участниками военных действий. Государства подписывают и ратифицируют Конвенции, соглашаясь, таким образом, с их положениями. Исторически войны велись государствами или этническими группами, которые ставили своей главной целью получение контроля над территорией. В информационной сфере стираются такие понятия, как «территория», «котроль», «театр военных действий». Информационные технологии создают новую «территорию», в которой на равных действуют государства и негосударственные акторы, а провести разделительную черту между комбатантами и некомбатантами крайне сложно.

Отметим, что несмотря на пробелы в международном праве, информационная безопасность в большинстве стран регулируется внутренними законодательными нормами. Пионерами в данном контексте являются США, в которых после событий 11 сентября 2001 г. безопасность критических информационных инфраструктур начинает рассматриваться в контексте антитеррористической стратегии.

Почти все государства рассматривают информационную безопасность объектов критической инфраструктуры как проблему национальной безопасности. В настоящее время многие элементы национальной инфраструктуры находятся в сфере владения частного сектора и не являются собственностью государства. Поэтому важным в организации системы ее эффективной защиты является создание органов координирования, которые бы состояли из представителей как правительственных, так и общественных организаций, с привлечением коммерческих структур, осуществляющих деятельность в ключевых секторах национальной критической инфраструктуры. Очевидно, что опыт внутригосударственного регулирования

должен быть использован при выработке международно-правовых норм.

Подводя итог рассмотрению применимости международного гуманитарного права к информационным войнам, отметим: несмотря на то, что большая часть его положений разрабатывалась в отношении обычных вооружений, все эти положения нацеливались на гуманизацию войн, предотвращение страданий мирного населения, поэтому можно считать, что они устарели лишь формально, но не по сути.

Можно выделить несколько ключевых особенностей информационной сферы в целом, и конфликтов, в частности, оказывающих существенное влияние на применимость международно-правовых норм к данной области:

— защищенные и незащищенные объекты критической инфраструктуры в информационном пространстве тесно переплетены между собой;
— гуманитарные объекты критической информационной инфраструктуры не обладают отличительными знаками, отмечающими их особый правовой статус;
— в информационной войне сложно провести разделение между гражданскими и военными целями;
— влияние негосударственных участников и неправительственных акторов в информационной сфере сопоставимо с государственной мощью;
— информационное оружие обладает характеристиками, отличающими его от традиционных вооружений, вследствие чего его действие частично выпадает из сферы действия международного гуманитарного права;
— информационная война может вестись без предупреждения, сложно определить инициаторов информационной атаки, однозначно оценить масштаб ущерба, а также меру ответного удара; применять традиционные механизмы сдерживания.
— международно-правовое регулирование информационной войны необходимо для сохранения сложившейся системы международной безопасности.

Группа российских и американских ученых выработала следующие рекомендации по международно-правовой регламентации информационной сферы:

— привлечение частного сектора и НПО к совету по разделению защищенных и незащищенных инфраструктур;
— использование отличительных знаков для защищенных объектов в информационной сфере;
— признание роста влияния негосударственных акторов и пользователей Интернета;
— исследование и анализ «международной ситуации, отличной от войны»[24].

Критические инфраструктуры уязвимы по отношению к информационным атакам. Нормы международного информационного права могут быть использованы с целью обеспечить необходимую защиту объектам гражданской информационной инфраструктуры. Однако, конвенции применимы только в условиях войны. В информационной же сфере сложно определить начало военных действий, нет даже определения информационной войны. В этих условиях эксперты рекомендуют осмыслить международно-правовой статус операций «иных, чем война», информационных операций, сопровождающих конкурентные отношения между государствами без объявления войны.

К обсуждению проблем международно-правовой защиты критических информационных инфраструктур необходимо привлекать представителей бизнеса, экспертного сообщества и гражданского общества. Подобные модели сотрудничества постепенно получают все большее распространение в мировой политике и международных отношений и получили название многосторонних партнерств и многоуровневой дипломатии.

В многосторонних партнерствах государства привносят политическую легитимность и способ применять санкции для проведения решений, экспертное сообщество и неправительственные организации – экспертизу и информационные ресурсы, а также легитимность, бизнес-сообщество – коммерческий ресурс и потенциал проведения в жизнь принятых решений.

Korotkov A.V., Zinovieva E.S. Critical Information Infrastructure Protection in International Humanitarian Law.

Summary: *Information security is on the top of the international security agenda as a result of growing dependence of state, society and personal life on information infrastructures. Information infrastructures are vulnerable to both logical and physical weapons. The article analyses the question of application of international humanitarian law to the information sphere.*

Ключевые слова

общество, защита критических инфраструктур, международные конвенции, кибернетические войны, кибернетические конфликты.

Keywords

information society, critical infrastructure protection, international conventions, cyber warfare, cyber conflicts.

Примечания

1. K.Rauscher, A.Korotkov. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace. East-West institute, 2011. URL: http://www.ewi.info/working-towards-rules-governing-cyber-conflict
2. Федоров А.В. Информационная безопасность в мировом политическом процессе. М.: МГИМО (У), 2008. С. 73.
3. Доктрина информационной безопасности РФ. Утверждена Президентом РФ 9.09.2000. Пр-1895.
4. International critical information infrastructure protection handbook 2008 / 2009. / Ed. by A. Wenger, V. Mauer and M. Cavelty. Center for Security Studies, ETH Zurich., 2009.
5. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.
6. Закон РФ «О безопасности» (с изменениями 02.03.2007) . Утв. Президентом 05.03.1992. N 2446-I; Стратегия национальной безопасности России до 2020 г. Утверждена указом Президента № 357 от 12.05.2009.
7. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. / О.О. Андреев и др. Под ред. В.А. Васенина. М.: МЦНМО, 2008. С. 37.
8. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира. Сборник материалов. / Под ред. С.А. Комова. М., 2009. С. 242.
9. Закон РФ «О безопасности» (с изменениями 02.03.2007) . Утв. Президентом 05.03.1992. N 2446-I; Стратегия национальной безопасности России до 2020 г. Утверждена указом Президента № 357 от 12.05.2009.
10. Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138; White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No.63; Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Federal Register, Vol. 66, No. 196, (October 8, 2001); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 H.R. 3162; U.S. Department of Homeland Security, The National Strategy for Homeland Security, July 16, 2002; White House, Executive Office of the President, The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, (February, 2003); Homeland Security Presidential Directive 7, HSPD-7, December, 2003.
11. K.Rauscher, A.Korotkov. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace. East-West institute, 2011. URL: http://www.ewi.info/working-towards-rules-governing-cyber-conflict
12. Там же.
13. Соглашение между правительствами государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009 г. // Международная информационная безопасность: дипломатия мира. Сборник материалов. / Под ред. С.А. Комова. М., 2009. С. 242.
14. Там же.
15. Бедрицкий Александр Владимирович. Реализация концепции информационной войны военно-политическим руководством США на современном этапе. Автореферат диссертации… кандидата политических наук : 23.00.04 Москва, 2007. С. 7.
16. Слипченко В.И. Война будущего (прогностический анализ). [Электронный ресурс]. URL: http://lib.rus.ec/b/161078/read
17. Крутских А.В., Сафронова И.Л. Международное сотрудничество в области информационной безопасности. [Электронный ресурс].URL: http://www.cryptography.ru/db/msg.html?mid=1169389
18. См. Libicki M. Cyberdeterrence and Cyberwar. RAND Corporation, 2009. 238 p. URL: http://www.rand.org/pubs/monographs/MG877.html
19. K.Rauscher, A.Korotkov. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace. East-West institute, 2011. URL: http://www.ewi.info/working-towards-rules-governing-cyber-conflict
20. Цит. по: K.Rauscher, A.Korotkov. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace. East-West institute, 2011. URL: http://www.ewi.info/working-towards-rules-governing-cyber-conflict
21. Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов. (Протокол I). Женева, 8 июня 1977 г. (ст. 52).
22. Там же. (ст. 56).
23. Второй протокол к Гаагской конвенции о защите культурных ценностей в случае вооруженного конфликта 1954 года. Гаага, 26 марта 1999 г. (ст. 1).
24. K.Rauscher, A.Korotkov. Working towards rules for governing cyber conflict. Rendering Geneva and Hague conventions in cyberspace. East-West institute, 2011. URL: http://www.ewi.info/working-towards-rules-governing-cyber-conflict