КОРОТКИЙ Т.Р.

директор Института национального и международного права Международного гуманитарного университета, доцент кафедры международного права и международных отношений Национального университета «Одесская юридическая академия», к.ю.н.

КОВАЛЬ Д.А.

аспирант кафедры международного права и международных отношений Национального университета «Одесская юридическая академия»

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ В МЕЖДУНАРОДНОМ ПРАВЕ

1. Во второй половине XX века на смену классическим видам вооруженных конфликтов приходят новые формы противостояния государств. Наиболее часто по отношению к ним используют дефиницию «война». Говорят об экономических, энергетических, дипломатических, психологических, информационных войнах. В большинстве случаев к собственно вооруженному конфликту эти «войны» прямого отношения не имеют, хотя и затрагивают соответствующие аспекты безопасности государств. Настоящее исследование посвящено только одному из этих явлений – информационным войнам.

Впервые термин «информационная война» был употреблен в отчете Томаса Рона «Системы оружия и информационная война», подготовленном в 1976 году для компании «Боинг»[1]. Тогда он вызвал повышенный интерес со стороны некоторых экспертов спецслужб США и с 1980-го года начал появляться в документах министерства обороны и других аналогичных институций.

Следует отметить, что информационная война – понятие неоднозначное. В широком смысле под информационной войной можно понимать любое негативное информационное воздействие на противника. Этим противником может быть и государство. Такое противостояние может быть между любыми субъектами – как частными, так и публичными. Поэтому стороны

[1] Thomas P. Rona. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976.

в такой войне – физические лица или группы лиц, действующие в индивидуальном порядке или организованно, спонтанно или по соглашению, юридические лица, государства. Ранее такое воздействие носило наименование пропаганды или идеологической войны, но с появлением Интернета и широкого применения электронных средств коммуникации круг участников такого воздействия, а также разнообразие его видов и форм резко увеличились. Такое воздействие может быть направленно и против системы обороноспособности, закрытой информации, банковско-финансовой системы, систем навигации – то есть против объектов, составляющих национальную безопасность государства. Несомненно, ограничение такого воздействия и введение ответственности за него является объектом правового регулирования, в том числе международно-правового, однако в настоящей статье в большей степени рассматривается проблематика регулирования информационных войн в узком смысле.

В узком смысле – это новый, не укладывающийся в международно-правовую квалификацию, вид или способ ведения вооруженных конфликтов[1]. С одной стороны, тем самым «смазывается» само понятие «вооруженный конфликт», однако реальные последствия информационной войны могут быть существенны, привести к значительным жертвам и разрушениям[2]. По мнению К.У. Уоткина, такого рода конфликты приведут «к проблеме определения статуса гражданских лиц, вооруженных процессором и клавиатурой и находящихся на другом континенте, и контроля за их действиями»[3]. Данный способ ведения вооруженного конфликта порождает те же проблемы, что и классический конфликт: разграничение по объектам и лицам; кого считать участниками такой войны и какими признаками должен обладать комбатант; являются ли такие комбатанты объектом нападения традиционными видами оружия; получают ли они статус военнопленных и т.п.[4] Отдельный вопрос – является ли информационная война вооруженным конфликтом, если она ведется вне «классической войны», или только это разновидность

---

[1] См. например, Черч, У. Информационная война // Междунар. журн. Красного Креста: сб. ст. – 2000. – С. 49–61.

[2] Как говорится в работе Greg Rattray, Strategic Warfare in Cyberspace 20 (The MIT Press, 2001): Цит по: Уоткин, К.У. Комбатанты, «непривилегированные воюющие» и конфликты XXI века. Материал для Неформальной встречи экспертов на высшем уровне, посвященной теме «Подтверждение и развитие международного гуманитарного права», Кембридж, 27-29 июня 2003 г. // http://www.sk-news.ru/mgp/doc/doc_07_05.doc

[3] Уоткин, К.У. Комбатанты, «непривилегированные воюющие» и конфликты XXI века. Материал для Неформальной встречи экспертов на высшем уровне, посвященной теме «Подтверждение и развитие международного гуманитарного права», Кембридж, 27-29 июня 2003 г. // http://www.sk-news.ru/mgp/doc/doc_07_05.doc

[4] Дискуссию по некоторым сложным вопросам применения норм международного гуманитарного права в современных вооруженных конфликтах см. Michael Schmitt, The Principle of Distinction in 21st Century Warfare, 2 Yale Human Rights and Dev. L.J. 143 (1999) и Michael Schmitt, Wired Warfare: Computer Network Attack and Jus in Bello 84 I.R.R.C. 365 (2002).

ведения вооруженного конфликта, а во всех остальных случаях это «невоенные», вне рамок вооруженного конфликта, недружественные действия. Порождают ли такие действия международно-правовую ответственность или нет? Кто является стороной такого конфликта – традиционные стороны, или нет?

Весь перечень вопросов не может быть рассмотрен в одной статье. Поэтому, мы ограничили цель настоящего исследования только анализом дефиниции «информационная война», выявлением наиболее характерных признаков этого явления и особенностей международно-правового воздействия на информационные войны, прежде всего в контексте международного гуманитарного права.

Проблематика информационной войны, как в качестве самостоятельного объекта исследования, так и применительно к международному праву, достаточно широко освещена в научной юридической и военной литературе. Эти вопросы нашли свое отражение в трудах О.Н. Калиновского[1], И.Л. Морозова[2], С. Гриняева[3], У. Черча[4], К. Дормана[5], Томаса П. Рона[6], К.У. Уоткина[7], М. Н. Шмидта[8], Г. Ратрея[9], Л. Гринберга[10] и других ученых. В них исследованы вопросы определения понятия «информационная война», классификация её видов, понятия и видов информационного оружия, применения норм международного гуманитарного права применительно к информационным войнам.

---

[1] См. например: Калиновский О.Н. «Информационная война» – это война? // Военная мысль. 2000. – №1.

[2] См. например: Морозов И.Л. Глобальные кибернетические системы как фактор безопасности демократического транзита//http://morozov.vlz.ru/library.bezo.htm

[3] См. например: С. Гриняев С. Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – № 2. – 2002.

[4] См. например: Черч, У. Информационная война // Междунар. журн. Красного Креста: сб. ст. – 2000. – С. 49–61.

[5] См. например: Knut Dormann, Applicability of the Additional Protocols to Computer Network Attacks, International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19.11.2004// http://www.icrc.org/web/eng/siteeng0.nsf/html/68LG92

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

[7] См. например: Уоткин, К.У. Комбатанты, «непривилегированные воюющие» и конфликты XXI века. Материал для Неформальной встречи экспертов на высшем уровне, посвященной теме «Подтверждение и развитие международного гуманитарного права», Кембридж, 27-29 июня 2003 г. / http://www.sk-news.ru/mgp/doc/doc_07_05.doc

[8] См. например: Michael N. Schmitt, «The Impact of High and Low-Tech Warfare on the Principle of Distinction"/Briefing paper, Program on Humanitarian Policy and Conflict Research at Harvard University, 2003

[9] См. например: Rattray, Gregory J. Strategic warfare in cyberspace, Massachusetts Institute of Technology, 2001.

[10] См. например: Lawrence T. Greenberg, Seymur E. Goodman , Kevin J. Soo Hoo Information Warfare and International Law, National Defense University Press, 1998

2. Понятие «информационная война» анализируется военными, юристами, специалистами в области информационных технологий, о ней говорится в военных доктринах государств.

Наиболее широкое и демилитаризованное (т.е. находящееся вне понятия вооруженного конфликта – примечание наше, Т.К., Д.К.) понимание информационной войны связано с её трактовкой как явного либо скрытого целенаправленного информационного воздействия систем друг на друга с целью получения определенного выигрыша в политической, экономической, идеологической сфере[1].

В рамках такой трактовки информационной войны обычно выделяют два различных подхода. Согласно первому, взаимодействие систем имеет целью дезорганизацию системы управления, воздействие на системы вооружения, включая информационные технологии и информационные ресурсы враждебных государств, и защиту соответствующих элементов собственной информационной инфраструктуры от аналогичных воздействий[2].

Второй подход является более универсальным и предполагает воздействие посредством различных информационных технологий (информационного оружия) не только на военную инфраструктуру и кадры, но и на все население враждующего государства. Информационное оружие является ни чем иным, как алгоритмом или методикой воздействия (обучения) на информационную самообучающуюся систему, то есть систему, находящуюся под воздействием извне[3].

По нашему мнению, следовало бы выделить и третий подход – понимание информационной войны как исключительно информационно-идеологического воздействия на население.

Помимо категории информационная война говорят и об информационном оружии. Например, И.Л. Морозов указывает на существование информационного оружия и даже выделяет три его вида. Согласно его классификации, первый вид представляют собой системы дистанционного уничтожения или искажения информации в кибернетических системах (компьютерные вирусы, логические бомбы). Второй вид составляют системы хищения информации и несанкционированного доступа на удаленный компьютер (электронные шпионы). Третий вид оружия – системы комплексного воздействия на психику пользователя, работающего с глобальной кибернетической системой (мультимедийные сайты).[4]

---

[1] Расторгуев С.П. Информационная война как целенаправленное информационное воздействие информационных систем // Информационное общество. – № 1. – 1997. – С. 64-66.

[2] Расторгуев С.П. Информационная война как целенаправленное информационное воздействие информационных систем // Информационное общество. – № 1. – 1997. – С. 64-66.

[3] Там же

[1] Морозов И.Л. Глобальные кибернетические системы как фактор безопасности демократического транзита//http://morozov.vlz.ru/library/bezo.htm

3. В условиях вооруженного конфликта (и перед его началом) может вестись информационная война. По уровням она также может включать воздействия: на население; на системы управления и вооружения; комплексное воздействие. Именно третий уровень воздействия в сочетании с высокой интенсивностью позволяет говорить об особом виде вооруженного конфликта – информационной войне.

Примером третьего уровня воздействия является операция «Буря в пустыне», которая наглядно продемонстрировала, что комплексное и согласованное применение разноплановых методов информационного воздействия существенно влияет на ведение непосредственно военных операций. В данной операции применялись практически все методы и средства информационного влияния: логические бомбы (разрушение инфорсферы машинно-технических систем), дезинформирование (введение в заблуждение военного руководства иракской армии), пропаганда (психологическая подготовка войск объединенных сил), информационное влияние на формирование мнения мировой общественности (представление Ирака агрессором в глазах мировой общественности).

Возникает вопрос, как соотносится понятие информационная война с понятием вооруженный конфликт, и насколько собственно информационной войне присущи признаки вооруженного конфликта?

Например, О.Н. Калиновский утверждает, что употребление термина «информационная война» носит сугубо эмоциональный характер. Его употребление подчеркивает значимость информации для взаимодействия обществ и государств, ожесточенность противостояния в информационной сфере. Информационная война, по мнению данного автора, невозможна еще и потому, что ей не присущ целый ряд характерных для войны институтов, как то: объявление войны, заключение мира, военное положение, оружие и масса других. Более подходящим термином для характеристики этого явления автор называет «информационную борьбу»[1].

По нашему мнению подход, который ориентируется на характерные, но необязательные признаки вооруженного конфликта[2], ставя их во главу угла при сравнении информационной войны с войной (вооруженным конфликтом).

Кроме того, тезис О.Н. Калиновского об отсутствии у информационных войн характерных признаков спорен еще и потому, что он не учитывает современной трактовки некоторых таких признаков.

Китайская военная доктрина, признавая существование информационных войн, рассматривает их в широком и узком смысле. В узком смысле – это полевая информационная война, т.е. боевые действия в сфере управ-

---

[1] Калиновский О.Н. «Информационная война» – это война? // Военная мысль, 2000. – № 1.

[3] В международном гуманитарном праве отсутствует легальное закрепление определения «война», «вооруженный конфликт».

ления войсками. В широком смысле информационная война – это боевые крупномасштабные действия с преобладанием информационной составляющей, характеризующиеся применением специально предназначенных для ее ведения воинских формирований и высокоточного оружия[1]. Таким образом, информационная война трактуется как один из способов ведения боевых действий.

Китайская доктрина специфична, но не уникальна. Многие страны мира сегодня осознают важность и существенность информационной составляющей войны, а также нового вида оружия – информационного. США еще вначале 1980-х гг. начали формировать стратегию ведения информационной войны.

Франция, Германия, Великобритания и некоторые другие государства в настоящее время активно развивают у себя информационные стратегии нападения и обороны. Можно сказать, что существование информационной войны как вида или части вооруженного конфликта в этих странах не вызывает сомнения.

Интересен французский подход к данной проблеме. Французские эксперты придерживаются концепции информационной войны, состоящей из двух главных элементов: военного и экономического (гражданского). Военный элемент рассматривается в контексте вооруженных конфликтов и миротворческих операций, а экономический включает более широкий диапазон потенциального применения информационных операций.

По нашему мнению, именно такое выделение составляющих понятия «информационная война» дает возможность разрешить споры относительно природы информационных воин и положительно разрешить вопрос о применимости норм международного гуманитарного права для регулирования средств и методов ведения информационной войны и защиты жертв конфликтов.

Примеры стран, занимающихся разработкой информационных военных стратегий, справедливо ставят вопрос о том, велись ли информационные войны раньше? Общепринято считать, что первой информационной войной была война 1991 г. в Персидском заливе между США и Ираком. Военные специалисты постсоветского пространства называли эту войну переломной вехой на пути развития военной стратегии и тактики из-за непропорционального использования военной авиации и ракет в соотношении с операциями наземными. Зарубежные же эксперты считали эту войну переломной именно из-за того, что она являлась первой информационной войной. В это понятие вкладывалось использование информационного оружия (например, компьютерных программ, поражающих связь, локационные воз-

[1] Гриняев С. Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – № 2. – 2002.

можности противника), применение самонаводящихся ракет, широчайшая дезинформация и т.д.[1]

4. Разновидностями информационных войн являются хакерские или Интернет-войны. Это воздействие представляют собой проникновение в информационные системы с целью их повреждения, неправильного функционирования и т.д., а также защиту от таких действий.

В отличие от других форм и способов противоборства информационное противоборство ведется постоянно в мирное время и влияет прямым и непосредственным образом практически на все стороны подготовки и ведения боевых действий в военное время. Доступность глобальной компьютерной сети позволяет передавать необходимую информацию в любой регион мира. Таким образом, можно выполнять задачи, связанные с информационным противоборством.

Уже сейчас такие конфликты могут регулироваться правом информационной безопасности. Центральное место здесь занимают «Руководящие принципы Организации по экономическому сотрудничеству по обеспечению безопасности информационных систем», которые были приняты в 2002 году. Кроме того, по вопросу обеспечения информационной безопасности было принято несколько резолюций Генеральной Ассамблеи ООН.

5. Рассмотрим международно-правовую характеристику «холодной» информационной войны, вне вооруженного конфликта и возможность ее квалификации по международному праву в качестве вооруженного конфликта.

В настоящее время такие действия запрещены на уровне норм общего международного права (принцип невмешательства во внутренние дела государств), однако конкретизирующие международные нормы, связанные с запретом информационного вмешательства, в международном праве отсутствуют.

В части идеологического вмешательства попытки закрепить его запрет существовали и на международном уровне. При разработке в ООН определения агрессии. СССР еще в 1953 г. предложил проект определения, которое охватывало и такие ее формы, как идеологическая агрессия. Согласно проекту, государство признается совершившим акт идеологической агрессии, в том случае, если оно «а) поощряет пропаганду войны; б) поощряет пропаганду применения атомного, бактериологического, химического и других видов оружия массового поражения; в) способствует пропаганде фашистско-нацистских взглядов, расовой и национальной исключительности, ненависти и пренебрежения к другим народам»[2]. По мнению И.И. Лукашука, это предложение об идеологической агрессии носило пропагандистский характер. Пропаганда определенных идей и взглядов запрещается

---

[1] Rattray, Gregory J. Strategic warfare in cyberspace, Massachusetts Institute of Technology, 2001.

[2] Известия.1953 г. – 26 августа.

специальными нормами международного права[1]. Однако информационное (идеологическое) воздействие может касаться не только запрещенных международным правовом идей и взглядов, и тем не менее порождать негативные социальные и экономические последствия. Такое информационное воздействие на население иностранного государства посредством различных средств воздействия является нарушением принципа невмешательства и может привести к негативным социальным последствиям. В отношении такого воздействия особое значение имеют средства такого воздействия. Они могут находиться как на территории государства, так и вне его. В отношении первой группы государство может принять меры воздействия путем контроля за СМИ, а во втором случае – нет. Ко второй группе относится Интернет, теле- и радиовещание. Тоталитарные государства, как правило, ограничивают такое воздействие извне – например, «глушение вражеских голосов» в СССР, запрет использования Интернета в КНДР. Возникновение Интернета перевело «информационно-идеологические» войны в иную плоскость, когда очень сложно проконтролировать источник воздействия.

Другой аспект проблемы, когда такое воздействие осуществляется не в отношении населения иностранного государства, а на третьи государства и международное сообщество в целом с целью дискредитировать иностранное государство, проводимую им политику. Прямой запрет на такие действия отсутствует в международном праве, хотя они в полной мере могут считаться информационной войной.

Сводить информационную в войну исключительно к информационно-идеологическому воздействию, на наш взгляд, нецелесообразно – появление новых средств – Интернета, сущности такого воздействия не изменило, в отличие от более глобального и массового воздействия на информационные системы.

Определенная аналогия прослеживается с попыткой введения международно-правового запрета экономической агрессии. Еще при принятии Устава ООН Бразилия высказывала предложение дополнить ст. 2 Устава ООН положением о запрете экономических угроз. Это предложение не было положительно проголосовано. Таким образом, государства мира показали, что пока что они не готовы признать экономическую, да и какую-нибудь другую (в том числе информационную) угрозу так же серьезно, как и военную[2].

Предложения о дополнении ст. 2 Устава ООН, а также доктринальные попытки расширения понятия «вооруженный конфликт» схожи с процессом международного согласования термина «агрессия». В 1953 году СССР обратился к мировому сообществу с предложением сформулировать четы-

[1] Лукашук И.И. Право международной ответственности. – М.: Волтерс Клувер, 2004. – С. 316.

[2] Lawrence T. Greenberg, Seymur E. Goodman , Kevin J. Soo Hoo Information Warfare and International Law, National Defense University Press, 1998

ре вида агрессии государств, три из которых не являлись агрессией в ранее признаваемой военной форме. Как уже отмечалось, речь шла и об идеологической, и об экономической агрессии.[1] Мировое сообщество не признало такую формулировку. При этом в отношении экономического принуждения была выражена негативная позиция Генеральной Ассамблеи ООН, как одной из форм вмешательства во внутренние дела, в том числе в п. 2 Декларации о недопустимости вмешательства во внутренние дела 1965 г., согласно которой «Ни одно государство не вправе применять или поощрять применение экономических, политических или любых других мер в целях принуждения другого государства для того, чтобы добиться от него подчинения при осуществлении им своих суверенных прав или получить от него преимущества другого рода». Следует отметить, что если цель правомерна, например, добиться от государства выполнения принятых им на себя обязательств по защите прав человека, на наш взгляд, такое воздействие допустимо и возможно (вне зависимости от того, кто его осуществляет), и не является нарушением принципа невмешательства. Является ли информационное воздействие вмешательством извне, если отсутствуют нарушение международных обязательств, с одной стороны, и нарушение внутреннего права государства, как это может иметь место в случае ведения массированной информационной компании международными экологическим организациями по защите фауны и флоры, когда формально отсутствует нарушение со стороны государства (например, компания по запрету убийства детенышей тюленей в РФ)[2]? Является ли такое воздействие информационной войной с точки зрения субъектного состава и целей? С нашей точки зрения, нет.

По нашему мнению, об информационной войне может идти речь только в том случае, если целью информационного воздействия является принуждения другого государства для того, чтобы добиться от него подчинения при осуществлении им своих суверенных прав или получить от него преимущества другого рода. Особенности международно-правой регламентации экономической и других форм принуждения дают нам возможность полагать, что информационные войны описанного формата не будут в ближайшее время непосредственно регулироваться международным правом в качестве самостоятельно вида вооруженного конфликта. Причина состоит в том, что международное правовое сознание не готово признать расширение термина «война» и «вооруженный конфликт» выделив новые их виды.

6. В случае ведения «горячих» информационных войн, войн с высокой степенью воздействия на информационные системы противника, возникает вопрос о применении международного гуманитарного права. Другие по-

---

[1] Лукашук И.И. Право международной ответственности. – М.: Волтерс Клувер, 2004. – С. 316.

[2] http://www.regnum.ru/news/1130522.html

зиции не столь категоричны в отрицании информационной войны как вида войны и вооруженного конфликта.

По нашему мнению, вне зависимости от понимания, информационная война всегда должна оставаться в рамках международного гуманитарного права, а это означает, что и право Женевы, и право Гааги должно применяться при ведении информационной войны.

Не вызывает сомнения тот факт, что международное гуманитарное право применялось в Американо-Иракской войне, а жертвы войны находились под защитой Женевских конвенций 1949 г. Так как обсуждаемая война была первой в своем роде, то и её информационная составляющая только начинала играть важную роль во всем вооруженном конфликте. Мы считаем, что именно из-за этого не вызывало особых споров применение международного гуманитарного права во время войны. Кроме того, одним из главных элементов «информационности» той войны были самонаводящиеся ракеты, а их применение, как бы парадоксально это не звучало, способствуют реализации основных положений международного гуманитарного права. Так, Михаэль Н. Шмидт, считает, что оружие информационной эры (то есть то, которое может распознавать объекты поражения), как раз способствует соблюдению принципа различия гражданских и военных объектов. Избирательность действия оружия – вот что достигается с помощью нового типа оружия. Таким образом, только злой умысел человека может привести к поражению гражданского объекта с помощью самонаводящегося оружия[1].

Больше вопросов возникнет в случае применения оружия, которое является собственно информационным (компьютерные вредоносные программы, логические бомбы и т.д.). Что, если такое информационное оружие будет направленно не на военные объекты, а на те, которые традиционно находятся под защитой международного гуманитарного права? Будет ли это нарушением именно гуманитарного права и возможно ли защитить такие объекты с его помощью?

По сравнению с применением других видов оружия, организация нападения на информационные сети не требует значительных материальных ресурсов. Химическое или биологическое оружие называют оружием массового поражения не из-за объема разрушительной энергии, выделяемой при их применении, а из-за количества вызываемых ими потерь и неизбирательности действия. Широкомасштабное применение обычных вооружений также вызывает серьезный ущерб. Несмотря на природу информационной атаки, не требующую приложения значительных сил, разрушение систем цифрового контроля атомной электростанции может иметь столь же мас-

[1] Michael N. Schmitt, «The Impact of High and Low-Tech Warfare on the Principle of Distinction"/ Briefing paper, Program on Humanitarian Policy and Conflict Research at Harvard University, 2003

штабные последствия[1]. Важность предотвращения информационных атак такого рода осязаема и бесспорна.

К сожалению, Международный Комитет Красного Креста пока еще не выработал единой доктрины, которая бы однозначно отвечала на все вопросы, связанные с международно-правовым регулированием информационных войн.

Большинство юристов-международников не оспаривают обязательное применение международного гуманитарного права в вооруженных конфликтах нового поколения, к которым относят войну в Персидском заливе. Но когда речь идет о собственно информационных войнах, без непосредственного применения традиционных вооружений, мнения расходятся. Приведенный пример нападения на атомную электростанцию большинством разрешается в пользу применимости международного гуманитарного права в случае наличие реального вооруженного конфликта между странами (то есть конфликта длящегося во времени) и значительных физических потерь, как в материальном, так и в человеческом измерение[2].

В случае же, когда информационное оружие будет использоваться отдельно, являясь единственным видом оружия войны, настоять на применение норм международного гуманитарного права будет крайне сложно, как МККК, так и государствам-участникам конфликта. По мнению К.У. Уоткина, такого рода конфликты приведут «к проблеме в определение статуса гражданских лиц, вооруженных процессором и клавиатурой и, возможно, находящихся на другом континенте, и контроль за их действиями»[3].

К глубочайшему сожалению, серьезные изменения в международном гуманитарном праве наступают лишь после огромных жертв и поэтому восприятие нового вида войн и применимость международного гуманитарного права к ним вероятно будет иметь место только после широкомасштабных информационных войн.

Однако уже сейчас необходимо сконцентрировать внимание на использование информационного оружия в конфликтах, которые имеют и более традиционные формы активности сторон. Такие конфликты, как уже упоминалось выше, многими учеными также называются информационны-

---

[1] Уоткин К.У. Комбатанты, «непривилегированные воюющие» и конфликты XXI века : материал для Неформальной встречи экспертов на высшем уровне, посвященной теме «Подтверждение и развитие международного гуманитарного права» / К.У. Уоткин. – Кембридж, 27-29 июня 2003 г. – http://www.sk-news.ru/mgp/doc/doc_07_05.doc

[2] См. напр.: Knut Dormann, Applicability of the Additional Protocols to Computer Network Attacks, International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19.11.2004// http://www.icrc.org/web/eng/siteeng0.nsf/html/68LG92

[3] Уоткин К.У. Комбатанты, «непривилегированные воюющие» и конфликты XXI века : материал для Неформальной встречи экспертов на высшем уровне, посвященной теме «Подтверждение и развитие международного гуманитарного права» / К.У. Уоткин. – Кембридж, 27-29 июня 2003 г. / http://www.sk-news.ru/mgp/doc/doc_07_05.doc

ми, но они уже предполагают применение различных видов оружия и различных стратегий.

В первую очередь следует уяснить, что применение к таким конфликтам международного гуманитарного права обязательно. Вопросы могут возникнуть при применение собственно информационного оружия. При этом применимость международного гуманитарного права будет носить особо важное значение в случае применения информационного оружия к объектам, содержащим опасные силы природы и обеспечивающим жизнедеятельность регионов (атомные электростанции, плотины, системы водоснабжения), к медицинским объектам (больницы, госпитали, эпидемиологические центры) и т.д. Нормы международного гуманитарного права содержат прямой запрет на нападение на такие объекты, вне зависимости от характера используемых средств нападения – в них указывается на последствия нападения – высвобождение опасных сил природы. Такой запрет содержится как в Дополнительных протоколах к Женевским конвенциям, так и в Гаагских конвенциях.

Интересный прецедент создает решение окружного суда Токио по делу Шимоды и Ко против Японии, которое рассматривалось с 1955 по 1963 гг. В этом деле истцы добивались признания атомной бомбардировки Хиросимы и Нагасаки такой, которая не соответствует международному праву. Суд своим решением постановил, что использование нового вида оружия разрешено, пока не будет принят международный договор, запрещающий его применение. Вместе с тем, Суд определил исключение из этого правила. Оно состоит в том, что когда применение такого оружия неизбежно, предполагается запрет на его использование исходя из аналогии существующих норм и правил в международном праве, оно не должно применяться. Также в решении было указано, что применение приносящих излишние страдания видов оружия противоречит принципам международного права и поэтому запрещается.

Исходя из этого решения можно сделать вывод, что информационное оружие ограничивается в применении именно в случае его использования против объектов, разрушение которых может вызвать неоправданные потери среди гражданских лиц и/или значительные и масштабные последствия, которые негативно скажутся на здоровье людей, на состоянии окружающей среды и т.д.

Такой же запрет касательно новых видов оружия закреплен и в ст. 36 Дополнительного Протокола I к Женевским конвенциям: «При исследовании, разработке, покупке или принятие на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона обязана определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запреты, которые содержатся в этом Протоколе либо в любых других нормах международного права, применимых к

Высокой Договаривающейся Стороне». Эта норма хоть и не прямо, но налагает на государства обязаность не применять новые виды оружия способом, который может противоречить существующим международно-правовым нормам.

Исходя из двух вышеуказанных правовых позиций, можно сделать вывод, что информационные войны должны регулироваться международным гуманитарным правом как в отношении методов и способов ведения войны, так и в отношении защиты жертв вооруженных конфликтов.

Исходя из вышеизложенного, можно сделать следующие выводы:

1. Можно выделить два вида информационных войн: вне вооруженных конфликтов, назовем их «холодные информационные войны»; в условиях вооруженных конфликтов, или предшествующие вооруженному конфликту (следующие за его окончанием). Несомненно, в крайних формах эти виды переходят один в другой, и здесь напрашивается аналогия с степенью насилия, характеризующего последовательно преступность, состояние внутренней напряженности, массовые беспорядки, вооруженный конфликт.

По степени интенсивности информационная война может включать: идеологическое воздействие; воздействие на системы управления и вооружения; комплексное воздействие.

2. Информационные войны в экономическом (гражданском) понимание, не подпадают под действие международного гуманитарного права. К ним должно применяться право информационной безопасности, которое на данный момент существует, но развивалось несколько в ином («невоенном») ключе.

3. Вооруженные конфликты с применением информационной составляющей уже происходили. Международное гуманитарное право к ним применялось и должно применяться впредь.

4. Конфликты с преобладанием информационного оружия, стратегии и тактики пока не проводились (по крайней мере, мы затрудняемся отнести к таким конфликтам хотя бы один из завершенных или длящихся конфликтов на сегодня). Международное гуманитарное право к таким конфликтам должно применяться, особенно, что касается предотвращения неизбирательного поражения гражданских лиц, окружающей среды. В любом случае к таким конфликтам применима оговорка Мартенса.