ГОСУДАРСТВО И ПРАВО, 2013, № 9, с. 82–88

ПРАВО И МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

МЕЖДУНАРОДНО-ПРАВОВЫЕ ПРОБЛЕМЫ ВРАЖДЕБНОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

© 2013 г. Галина Георгиевна Шинкарецкая[1]

***Краткая аннотация**: в статье анализируется проблема распространения международно-правового регулирования на новый вид военных действий – враждебного воздействия на информационные системы.*

***Annotation:** problems of application of international legal regulation to a new kind of warfare, that is, cyberattacks on information systems are discussed in the article.*

***Ключевые слова:** информационные системы, международное гуманитарное право, кибератаки, гражданское население, немеждународный конфликт.*

***Key words:** information systems, international humanitarian law, cyberattacks, civilian population, non-international conflict.*

Технологическое развитие мира привело к появлению в международных отношениях и, соответственно, в международном праве новой проблемы – необходимости регулирования так называемых информационных операций, т.е. использования информационных технологий, таких как атаки на компьютерные сети с целью внести изменения, разрушить, повредить или, напротив, защитить информационные системы и обслуживаемые ими системы инфраструктуры. Есть данные о том, что примерно более 30 стран обладают соответствующими возможностями. Однако примерно такие же технологии доступны и группам лиц, и различным неправительственным организациям, в том числе террористическим[2]. Эти технологии недороги, просты в использовании и могут быть пущены в ход с любого места.

В российской литературе пока нет не только специальных работ на эту тему, но чрезвычайно редки даже ее упоминания[3].

Проблема состоит в том, что в современном международном праве пока нет норм, специально регулирующих операции с информационными технологиями, включая военные и иные, враждебные по своему характеру. Применения международного права по аналогии недостаточно.

Современная история содержит уже несколько примеров враждебного воздействия на информационные системы: в 1991 г., во время операции "Буря в пустыне"; в Афганистане в 1999 г.; в 2010 г. – вмешательство Израиля во внутренние дела Ирана в рамках решения иранской ядерной программы. Современное международное право, как оно проявляет себя в науке и практике международной юриспруденции[4], ориентировано на пресечение международных преступных деяний в области компьютерных преступлений. Общей целью мирового сообщества, как это записано в Уставе ООН, является поддержание международной законности и правопорядка.

До сих пор правонарушения в компьютерной сфере подчинялись уголовному праву отдельных государств. Государства принимают собственные законы, криминализующие различные формы соответствующих деяний. Вполне в том же русле идет и принятая Советом Европы Конвенция о компьютерных преступлениях, по которой государства-участники обязуются криминализировать в своем уголовном праве атаки на компьютеры и совершенствовать сотрудничество в расследовании киберпреступлений[5].

---

[1] Ведущий научный сотрудник Института государства и права РАН, доктор юридических наук (E-mail:gshink@yandex.ru).

[2] См.: *Hollis D.B.* Why States need an International Law for Information Operations // LEWIS & CLARK LAW REVIEW. Vol. 11. 2007. № 4.

[3] См.: *Тузмухамедов Б.Р.* Новые сферы регулирования международного гуманитарного права (к 60-летию Женевских конвенций о защите жертв войны). Тезисы доклада // Росс. ежегодник международного права, 2009. СПб., 2010. С. 79–85.

[4] См. на этот счет: Международное уголовное право / Под общ. ред. В.Н. Кудрявцева. М., 1999; *Костенко Н.И.* Международное уголовное право. М., 2003; Международное право / Под ред. А.Н. Вылегжанина. М., 2009. С. 730 – 778; Международное право / Отв. ред. Г.В. Игнатенко, О.И. Тиунов. М., 2009. С. 559 – 599; Международное право / Отв. ред. А.А. Ковалев, С.В. Черниченко, А.А. Моисеев. М., 2008. С. 540–583.

[5] См.: Council of Europe. Convention on Cybercrime, C.E.T.S. No. 185 (Nov. 23, 2001), available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Однако в последние годы все шире распространяется идея о появлении нового вида оружия, основанного на новых видах коммуникации[6]. Поэтому встает вопрос: насколько применимы к данному виду оружия и по отношению к уже общеизвестным способам ведения военных действий нормы международного права, создававшиеся для "традиционных" международных отношений.

Объект регулирования

В науке современного международного права представлено следующее определение понятия "компьютерные войны": это такие операции, *в которых задействованы "электронные средства для получения доступа к информации или внесения изменений в информацию, содержащуюся в информационной системе, которая избрана целью воздействия, без разрушения ее физических компонентов*"[7]. Там же перечисляются примеры: электронная война; операции в компьютерной сети; психологические операции; военный обман; операционная безопасность. В целом все они представляют собой направленное использование энергии для того, чтобы сделать невозможным действие какой-то системы противника. Проявления их очень разнообразны. Характерно то, что лица, производящие все эти действия, остаются скрытыми и их почти невозможно обнаружить. Инструменты их также разнообразны: так называемые вирусы, червяки, троянцы, хотя в сущности это все фрагменты кодов, которые приклеиваются к другим компьютерным программам, и начинают действовать тогда, когда включается программа.

Некоторыми авторами делаются попытки предложить критерии для классификации названных выше операций[8], однако обнаружить существенные признаки для правового регулирования не удается.

Для таких операций характерно то обстоятельство, что они очень легко приобретают и международный, и внутренний характер, что запускаются они и государствами, и просто группами людей. В настоящее время уже в более чем в 30 странах есть возможности для военного использования информационных технологий.

Применение международного права по аналогии

Международное гуманитарное право, которое в научном плане обозначают через совокупность "законы и обычаи войны", с самого зарождения было направлено на гуманизацию военных действий, в частности стремясь ограничить вооруженные действия военными объектами. Однако информационные атаки нацелены на очень разные цели, а не только на армию. Хотя такие атаки могут повести к физическому разрушению материальных объектов, подобному тому, которое производится "обычными" снарядами, их действительной целью чаще является выведение из строя информационных систем. Впрочем, нельзя не признать, что нарушение информационных связей противника и в прежние века было целью военных действий.

Современные законы и обычаи войны не содержат специальных норм относительно компьютерных атак. Это не значит, что международное право здесь не действует. Еще более 100 лет назад замечательный российский ученый Ф.Ф. Мартенс доказал, что отсутствие договорного положения, ясно запрещающего какое-либо определенное поведение во время вооруженного конфликта, не означает, что международное право разрешает его. Названная в честь автора "оговорка Мартенса" впервые была включена в преамбулу II Гаагской конвенции 1899 г. о законах и обычаях сухопутной войны и затем фигурировала в последующих документах международного гуманитарного права, включая Женевские конвенции 1949 г.[9]

В Дополнительном протоколе I к Женевским конвенциям говорится: "В случаях, не предусмотренных настоящим Протоколом или другими международными соглашениями, гражданские лица и комбатанты остаются под защитой и действием принципов международного права, проистекающих из установившихся обычаев, из принципов гуманности и из требований общест-

[6] См.: *Schmitt M.N.* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework//37 COLUM. J. TRANSNAT'L. L., 1999. P. 890.

[7] Department of Defense, Office of General Counsel. An Assessment of International Legal Issues in Information Operations. (May 1999). P. 5 [Assessment of International Legal Issues]; War in the Fifth Domain, The Economist (1 July 2010). P. 25–27.

[8] См.: *Schmitt M.N.* Op. cit. P. 892.

[9] См.: Гаагская конвенция (IV) о законах и обычаях сухопутной войны от 18 октября 1907 г.; Женевская конвенция об облегчении участи раненых и больных в действующей армии (ст. 63); Женевская конвенция об облегчении участи раненых, больных и потерпевших кораблекрушение на море (ст. 62); Женевская конвенция об обращении с военнопленными (ст. 142); Женевская конвенция о защите гражданского населения во время войны (ст. 158).

венного сознания" (ст. 1.2)[10]. Другими словами, законы и обычаи войны регулируют информационные войны, не упоминая их конкретно.

Более того, согласно ст. 36 того же Протокола при изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны государства-участники должны определить, подпадает ли их применение (при некоторых или при всех обстоятельствах) под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых ими.

Таким образом, можно определенно сказать, на компьютерные атаки распространяется международное гуманитарное право, которое однозначно ориентировано на пресечение всей гаммы компьютерных преступлений в их совокупности.

Следует отметить, что попытка ввести регулирование была впервые сделана еще в 1998 г. Тогда Правительство РФ обратилось к мировому сообществу с призывом создать новые нормы международного права с целью запретить особенно опасные виды информационного оружия[11]. Из девяти государств, откликнувшихся на это письмо, только Куба и Белоруссия были согласны с необходимостью провести соответствующие переговоры. В конце концов Генеральная Ассамблея ООН приняла резолюцию с призывом к государствамчленам содействовать устранению существующих и потенциальных угроз информационной безопасности[12]. Показательно отрицательно к идее международно-правового запрета информационного оружия как такового выглядит позиция США.

Правительство США, в свою очередь, заявило о том, что для этой страны не было достаточных оснований поддерживать идею переговоров о формировании новых международно-правовых обязательств относительно информационных атак[13].

Комитет Красного Креста в 2003 г. выразил мнение о том, что существующие юридические рамки в целом соответствуют современным международным вооруженным конфликтам[14].

Такие мнения господствовали в то время и в литературе[15].

Таким образом, вплоть до начала 2000-х годов казалось достаточным применение международного гуманитарного права по аналогии.

Критерии применения международного гуманитарного права

Женевские конвенции 1949 г., воплощающие принципы гуманизации, содержат три основные требования: военные операции должны быть вызваны военной необходимостью; следует проводить различие между военными и гражданскими целями, и атаки должны быть пропорциональными[16].

Теперь рассмотрим эти требования подробнее.

1) *Необходимость*. Цель этого общепризнанного принципа состоит в обеспечении того, чтобы любая военная акция была продиктована условиями войны и нацелена на подавление противника в кратчайшие сроки и с наименьшими материальными и людскими потерями. В соответствии с данным принципом любое действие, не направленное на достижение непосредственной и исключительно военной цели, например неизбирательные бомбардировки, поражающие жилища или запасы продовольствия для гражданского населения, запрещено.

Статья 52 (2) Дополнительного протокола о защите жертв международного вооруженного конфликта 1977 г. (Протокол I) говорит о том, что атака должна быть ограничена исключительно военными целями. В том, что касается объектов атаки, военные цели ограничены теми объектами, которые по своей природе, расположению, назначению, использованию могут в значительной

[10] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г.

[11] См. Письмо Постоянного представителя Российской Федерации при ООН Генеральному секретарю ООН // GAOR, 53d Sess., U.N. Doc. A/C.1/53/3(1998), available at // http://daccessdds.un.org/doc/UNDOC/GEN/N98/284/58/PDF/N9828458.pdf; The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/54/213 (Aug. 10, 1999).

[12] См.: U.N. GAOR, 53d Sess., 79th plen. mtg. at 1, U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

[13] См.: Office of Gen. Counsel, Dep't of Def., An Assessment of International Legal Issues in Information Operations (Nov. 1999), available at // http://www.nwc.navy.mil/cnws/ild/studiesseries.aspx

[14] См.: INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 4 (2003), available at // http://www.icrc.org/web/eng/sisteeng).nsf/htmlall/5XRDCC/$File/ IHLContemparmedconflictsFINALANG.pdf; Sean Watts, Civilian Participation in Computer Network Attacks 32 .

[15] См.: *Jensen E.T.* Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?//18 AM. U. INT'L L. REv. 2003. P. 1149.

[16] См.: Статьи 48, 51, 52(2) и 57 Дополнительного протокола I от 12 декабря 1977 г. к Женевским конвенциям от 12 августа 1949 г. о защите жертв международных вооруженных конфликтов.

степени способствовать военному успеху и полное или частичное уничтожение, нейтрализация или захват которых в конкретных обстоятельствах могут дать определенные военные преимущества.

Это значит, что правомерной военной целью может быть такая цель, достижение которой вносит эффективный вклад в военные действия и разрушение которой дает определенные военные преимущества. Если избранный объект атаки – часть военной инфраструктуры противника, как, например, склады оружия или военные центры связи, атака соответствует требованиям необходимости.

2) *Избирательность атаки*. Содержание данного требования состоит в следующем: в военных атаках должны использоваться такое оружие и такие методы ведения действий, которые позволяли бы делать различия между военными и гражданскими целями и объектами. В Протоколе I установлено, что для обеспечения уважения и защиты гражданского населения и гражданских объектов стороны в конфликте обязаны в каждом случае применения силы делать различия между гражданским населением и комбатантами, а также между гражданскими объектами и военными и направлять свои атаки только против военных объектов.

В ст. 51(4) Протокола I после установления о запрещении неизбирательной атаки приводится ее определение. Это такая атака, которая не направлена против специфически военного объекта; которая производится методами или средствами, не направленными на специфически военный объект; которая производится методами или средствами, которые не могут быть ограничены согласно настоящему Протоколу, и атака, таким образом, направляется и против военного, и против гражданского объектов. В случае затруднений в определении принадлежности объекта атаки к военным или гражданским или использования гражданского объекта в военных целях. Женевская конвенция требует от атакующей стороны презюмировать, что объект не принесет значительного военного успеха. Однако это слишком слабый и неотчетливый критерий, чтобы быть надежным подспорьем при принятии решений.

М. Шмитт, иллюстрируя трудность различения военных и гражданских объектов и целей, проводит аналогию между информационными атаками и использованием ракет СКАД во время первой иракской войны в Персидском заливе[17]. По его мнению, ракеты СКАД не являются однозначно неизбирательным оружием. Они могут весьма точно нацеливаться, например, на военные формирования в пустыне. Однако их применение в населенных пунктах не было избирательным, даже если иракское командование намеревалось ударить по военным объектам, расположенным в этих пунктах. Поэтому вероятность поражения защищаемых лиц и объектов больше, чем поражение правомерных целей, что делает применение СКАД неприемлемым.

Гораздо сложнее разбираться в операциях против гражданских коммуникационных систем. Есть данные о том, что 98% всей правительственной связи и 95% военной связи Соединенных Штатов Америки идет через гражданские системы коммуникаций, а не через специальные военные каналы[18]. Поэтому логично, что в случае войны именно гражданские каналы в первую очередь станут объектами нападения. Нужно еще учесть, что в силу единого характера и структурной однородности систем связи практически невозможно выделить ту часть, которая используется военными, и вся система будет уничтожаться или выводиться из строя целиком, что для гражданского населения может оказаться катастрофой.

Такое уничтожение стало бы чрезвычайно эффективным с военной точки зрения, так что военным властям было бы очень соблазнительно произвести такую атаку.

3) *Пропорциональность*. Данный критерий дает возможность оценить уникальность компьютерных операций, а также необходимость гибкого определения допустимости таких операций. В этом критерии отражено общепризнанное мнение о том, что во время войны право сторон в конфликте на выбор методов и средств ведения военных действий не является неограниченным; запрещено применение такого оружия и таких методов, которые причиняют неоправданные страдания[19].

Это ограничение направлено на защиту и комбатантов, и гражданских лиц. Женевские конвен-

[17] См.: *Schmitt M.N.* Wire Warfare: Computer Network Attack and Jus in Bello//84 International Review of the Red Cross (2002). P. 390.

[18] См.: *Jensen E.T.* Cyber Warfare and Precautions Against the Effects of Attacks//88 Texas Law Review (2010) 7. P. 1534.

[19] См.: ст. 35(1)-(2) Дополнительного протокола I; ст. 22 IV Гаагской конвенции о законах и обычаях сухопутной войны. 18 октября 1907 г. // http://www.unhcr.org/refworld/docid/4374cae64.html (посещение 28 апреля 2011 г.).

ции 1949 г. о законах и обычаях войны содержат дополнительные гарантии для гражданского населения: атака должна быть отложена или отменена, если очевидно, что объектом нападения является не военный объект, а объект, имеющий право на специальную защиту, или если атака может причинить гибель, раны и увечья гражданскому населению, разрушение гражданских сооружений, и все эти последствия будут несоразмерно велики по сравнению с ожидаемыми военными результатами[20].

Таким образом, даже если выбор цели диктуется военной необходимостью и по мере возможности произведено различие между военными и гражданскими компонентами цели, планируемая операция может квалифицироваться как нарушение гуманитарного права, если атака поведет или может повести к причинению излишних страданий комбатантам или гражданскому населению. В сущности, оценка пропорциональности – это установление практических рамок операции. Именно этот аспект практической оценки позволяет вводить в употребление новые виды вооружения, в том числе и информационные операции.

Таким образом, по всем трем критериям нельзя обнаружить существенных отличий информационных атак от атак, производимых с помощью иных видов оружия.

Несколько других параметров оценки информационного оружия

а) контроль за распространением

Некоторые специалисты отмечают такую характеристику воздействия компьютерных операций вообще и информационных технологий, в частности, как возможность довольно быстрого восстановления, в отличие от разрушений, производимых традиционными военными операциями. Так, в докладе Министерства обороны США об оценке первой войны в Персидском заливе против Ирака указывается, что физическое разрушение электростанций в Ираке привело к десятилетиям нехватки энергии для нужд гражданского населения[21]. Не восстановленная после бомбежки в 1999 г., электростанция в 2003 г. подверглась нападению боевиков, что поставило страну на грань катастрофы[22].

Однако нельзя не признать, что информационные атаки могут привести к долговременным непредвиденным последствиям, например вирус или вредоносная программа, внедренные в ту систему, которая является непосредственной целью, могут распространиться в другие системы, в том числе в важные системы жизнеобеспечения гражданского населения. При этом лицо, внедрившее вирус или программу, может быть не в состоянии контролировать их распространение, в том числе в закрытые системы, например через съемный диск.

Подобные "вторичные" эффекты возможны и в случае применения обычного оружия. Например, в приведенном выше примере с электростанцией в Ираке в 1999 г. Разрушение ее вывело из строя командный пункт иракской армии, однако гражданское население также осталось без электричества, и были парализованы системы охлаждения воздуха, службы чрезвычайной помощи, медицинские учреждения.

В таком случае вирус или вредоносная программа должны быть квалифицированы как неизбирательное оружие.

б) характер наносимых повреждений

По сравнению с "традиционными" видами оружия информационное оружие не наносит непосредственных ранений, так что его даже называют "бескровным оружием" и предсказывают ему большое будущее[23]. Действительно, вместо причинения ран и увечий на много лет информационные атаки как будто вполне соответствуют требованиям Женевских конвенций о минимизации причиняемых страданий. Дж. Келси утверждает, что международное гуманитарное право должно признать правомерным применение информационного оружия на том основании, что с его помощью можно наносить удары противнику с меньшими затратами человеческих жизней и меньшими разрушениями гражданских сооружений[24]. Р. Ханземан замечает: "Это оружие не связано с крупномасштабными взрывами. Меньше

[20] См.: ст. 57(2)(b) Протокола I. Статья 51(5) Протокол I.

[21] См.: Department of Defense, Office of General Counsel, An Assessment of International Legal Issues in Information Operations. (May 1999). P. 5, available at // http://www.msnbc.msn.com/id/32726457/ (Дата обращения: 28 апреля 2011 г.).

[22] См.: Associated Press, Iraq suffers hot summer amid power problems (7 Sept. 2009).

[23] См.: *Dervan L.* Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown // Goettingen Journal of International Law. V. 3. 2011. #1. P. 373–396.

[24] *Kelsey J.T.G.* Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare // 106 Michigan Law Review 2008. № 7. P. 1445.

взрывов – значит, меньше разрушенной собственности и меньше незапланированных человеческих жертв"[25].

в) ликвидация последствий

Во многих случаях повреждения, нанесенные компьютерными атаками, могут быть ликвидированы. Например, если произведенная атака против определенного объекта нанесла больший ущерб гражданскому населению, чем предполагалось, скажем, вывела из строя электростанцию, может быть произведено еще одно компьютерное проникновение с целью снова ввести эту электростанцию в действие. Такое возвращение в первоначальное состояние невозможно представить в случае применения кинетического оружия, повреждения от которого будут невосстановимы. Поэтому некоторые авторы считают компьютерное оружие с этой точки зрения более соответствующим международному гуманитарному праву, в частности п. 2 ст. 57 Дополнительного протокола I[26].

Страна, действующая добросовестно, должна подготовить такую восстанавливающую операцию заранее, до нанесения повреждения[27]. С нашей точки зрения, все же нереально ожидать, что сторона (а это может быть не только государство), планирующая произвести компьютерную атаку, заранее разработает специальную программу обнаружения вируса или даже иммунизации компьютерной системы, как предлагает Дж. Терри.

Необходимость специального регулирования

Более пристальный анализ показывает недостаточность регулирования по аналогии.

Во-первых, к действиям, составляющим атаку на информационные системы, должно быть применимо определение применения силы или угрозы силой[28]. Запрещено применение силы против территориальной целостности или политической независимости государств, однако в практике государств объект угрозы квалифицируется шире. Комиссия международного права характеризовала данное запрещение как *jus cogens*[29]. В понятие угрозы или применения силы обычно не включаются экономические и политические формы давления, и в целом среди специалистов не складывается общего согласия относительно кибернетической войны как угрозы силой[30].

Этот вид вражеского воздействия не может расцениваться как военные меры, что косвенно подтверждается Уставом ООН. В ст. 41 "меры, не связанные с использованием вооруженных сил" – это, в частности, "полный или частичный перерыв… почтовых, телеграфных, радио- или других средств сообщения". Но означает ли это, что, например, проникновение в систему управления воздушным движением не является актом применения силы? Или это означает, что на компьютерные атаки вообще не распространяется Устав ООН, что, конечно, не соответствует действительности?

Во-вторых, еще более очевидной недостаточность регулирования по аналогии становится в случае конфликтов немеждународного характера,

---

[25] *Hanseman R.G.* The Realities and Legalities of Information Warfare // 42 Air Force Law Review (1997). P. 198.

[26] 2. В отношении нападений принимаются следующие меры предосторожности:

a) те, кто планирует нападение или принимает решение о его осуществлении:

i) делают все практически возможное, чтобы удостовериться в том, что объекты нападения не являются ни гражданскими лицами, ни гражданскими объектами и не подлежат особой защите, а являются военными объектами в значении п. 2 ст. 52 и что в соответствии с положениями настоящего Протокола не запрещается нападение на них;

ii) принимают все практически возможные меры предосторожности при выборе средств и методов нападения, с тем чтобы избежать случайных потерь среди гражданского населения, ранения гражданских лиц и случайного ущерба гражданским объектам, во всяком случае свести их к минимуму;

iii) воздерживаются от принятия решений об осуществлении любого нападения, которое, как можно ожидать, вызовет случайные потери среди гражданского населения, ранение гражданских лиц и нанесет случайный ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерными по отношению к конкретному и прямому военному преимуществу, которое предполагается получить;

b) Нападение отменяется или приостанавливается, если становится очевидным, что объект не является военным, что он подлежит особой защите или что нападение, как можно ожидать, вызовет случайные потери среди гражданского населения, ранение гражданских лиц и нанесет случайный ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерными по отношению к конкретному и прямому военному преимуществу, которое предполагается получить.

[27] См.: *Terry J.P.* The Lawfulness of Attacking Computer Networks in Armed Conflicts and in Self-Defense in Periods Short of Armed Conflict: What are the Targeting Constraints? // 169 Military Law Review (2001). P. 86, 87.

[28] Статья 2 (4) и ст. 42 и 51 Устава ООН.

[29] Доклад Комиссии международного права о работе ее 18-й сессии. U.N. Doc. A/CN.4/191 (July 19, 1966) // http://www.un.org/law/ilc/index.htm

[30] *Robertson H. B.* Jr. Self-Defense Against Computer Network Attack Under International Law // 76 INT'L. L. STUD. 2002. P. 134.

на которые также распространяется международное гуманитарное право. Чаще всего речь в этом случае будет идти о деятельности террористических групп, для которых характерно "расползание" по территориям нескольких соседних (и даже далеко отстоящих) государств. Компьютерные атаки, производимые от имени террористической группы, могут сами по себе повести к возникновению вооруженного конфликта. Более того, если враждебные действия в основном состоят из атак на информационные системы, границы конфликта размываются и становятся трудно определимыми, что, в свою очередь, затрудняет определение положения гражданского населения[31].

Правда, трудно определимым становится и характер конфликта как международного или немеждународного: в том случае, например, если атака производится с территории другого государства. Международный уголовный трибунал по бывшей Югославии определил, что немеждународный конфликт существует в том случае, если внутри государства имеет место обширное насилие между организованными вооруженными группами[32]. Это определение завоевало популярность, поскольку в нем даются два критерия такого конфликта – его интенсивность и участие организованных вооруженных групп. Последующие решения Трибунала по Югославии закрепили его. Однако нормативного закрепления этого понятия пока нет.

Таким образом, специальные нормы, применимые к регулированию правоотношений, возникающих в ходе компьютерной войны или нападения на информационные системы, пока не сформированы. Но можно с уверенностью утверждать, что они будут формироваться на основе общепризнанных принципов и норм общего международного права, а также на основе принципов международного гуманитарного права.

---

[31] См.: Tallinn Manual on the International Law Applicable to Cyber Warfare. M. Schmitt. Geneva, 2013. P. 37.

[32] См.: ICTY. *Tadić.* Decision on the Defence Motion for Interlocutary Appeal, Edited by para.70.