МЕЖДУНАРОДНЫЙ ЖУРНАЛ Красного Креста

Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц

Кордула Дрёге*
Кордула Дрёге возглавляет секцию оперативного права Юридического отдела Международного Комитета Красного Креста (МККК)

Краткое содержание

Проблемам, связанным с кибернетической войной, уделяют немалое внимание политические и военные руководители во всем мире. Новые отделы по обеспечению кибернетической безопасности создаются на различных уровнях правительства, в том числе и в вооруженных силах. Но операции в киберпространстве в ситуациях вооруженных конфликтов могут иметь очень серьезные последствия, особенно когда их воздействие направлено не исключительно на конкретную компьютерную систему или компьютер, которые определены в качестве объекта нападения. Действительно, цель операций в киберпространстве обычно заключается в воздействии на «реальный мир». Например, вмешиваясь в работу компьютерных систем, можно манипулировать системой управления

* Мне хотелось бы выразить благодарность моим коллегам из МККК: Кнуту Дёрману, Бруно Демейеру, Реймонду Смиту, Тристану Ферраро, Елене Пеич и Гари Брауну за их важные замечания в отношении более ранних вариантов статьи, а также Неле Ферлинден за помощь в работе со ссылками. Если не указано иное, то посещение всех веб-сайтов, на которые имеется ссылка, происходило в октябре 2012 г. Настоящая статья написана в личном качестве и не обязательно отражает точку зрения МККК.

воздушным движением противника, системами регулирования нефтепроводов или управления ядерных установок. Воздействие на гражданское население некоторых операций в киберпространстве может быть огромным. Поэтому важно обсудить нормы международного гуманитарного права (МГП), которые регулируют такие операции, поскольку одной из задач этого корпуса права является защита гражданского населения от воздействия военных действий. В настоящей статье делается попытка рассмотреть отдельные вопросы, возникающие при применении МГП — свода норм, который был составлен с учетом реальности традиционной кинетической войны, — к кибернетической технологии. Первый вопрос: когда война в кибернетическом пространстве действительно является войной, то есть «вооруженным конфликтом»? После обсуждения этой проблемы в статье рассматриваются некоторые наиболее важные нормы МГП, регулирующие военные действия, и толкование этих норм применительно к кибернетической сфере, а именно принципы проведения различия, соразмерности и принятия мер предосторожности. В отношении всех этих норм информационная сфера ставит целый ряд вопросов, которые все еще остаются открытыми. В частности, взаимосвязанность кибернетического пространства бросает вызов самому основополагающему исходному положению права ведения военных действий — во всякое время может и должно проводиться различие между гражданскими и военными объектами. Таким образом, предстоит еще увидеть, предоставят ли традиционные нормы МГП гражданским лицам достаточную защиту от воздействия кибернетической войны. При их толковании необходимо будет, конечно, принять во внимание специфические черты кибернетического пространства. Поскольку нет отчетливого понимания того, какие последствия может иметь кибернетическая война, нельзя исключать, что могут потребоваться более строгие нормы и правила.

Ключевые слова: кибернетическая безопасность, кибернетическая война, кибернетическое нападение, международное гуманитарное право, операции в кибернетическом пространстве, кибернетическое оружие, вооруженный конфликт в кибернетическом пространстве, ведение военных действий, проведение различия, соразмерность, неизбирательное нападение, меры предосторожности.

: : : : : : :

Введение

Вопрос о кибернетической безопасности занимает важное место в повестке дня политических и военных руководителей всего мира. Недавно опубликованы результаты изысканий, проведенных Институтом по исследованию проблем разоружения Организации Объединенных Наций (ЮНИДИР). В этой публикации описаны меры, принимаемые 33 государствами, которые непосредственно включили понятие «кибернетическая война» в свое военное планирование и организацию, и подход 36 других государств к вопросу

кибернетической безопасности[1]. Это самые разные страны — от государств с очень хорошо разработанной доктриной и военными организациями, где работают сотни тысяч человек, до государств с менее сложными институтами, которые включают кибернетические нападения и кибернетические методы ведения военных действий в существующий потенциал для ведения электронной войны. Целый ряд государств создают в рамках своих вооруженных сил или за их пределами специализированные подразделения для изучения вопросов, касающихся операций в кибернетическом пространстве[2]. Сообщалось также, что 12 из 15 самых крупных военных держав в мире разрабатывают программы кибернетической войны[3].

Кибернетическая безопасность в целом и кибернетическая война в частности

В то время как интенсивно обсуждается вопрос о кибернетической безопасности в целом, широкая общественность мало осведомлена — пока — о военном планировании и политике государств относительно кибернетической войны.

Представляется, что стратегия правительств в основном заключается в сочетании оборонительной и наступательной стратегий. С одной стороны, государства прилагают все больше усилий к тому, чтобы защитить свою собственную инфраструктуру от кибернетических нападений. С другой стороны, они, как кажется, наращивают технологический потенциал, чтобы быть в состоянии начать операции в кибернетическом пространстве против своих противников во время вооруженного конфликта[4].

Политики и комментаторы обсуждают вопросы о том, все ли или только некоторые новые «кибернетические системы оружия» должны быть абсолютно запрещены, не следует ли обратить внимание на меры по укреплению доверия (сходные с теми, которые касаются ядерного разоружения)[5] и не нужно ли установить «правила дорожного движения» для поведения

1 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare — Preliminary Assessment of National Doctrine and Organization*, UNIDIR Resources Paper, 2011, доступно по адресу: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrineand-organization-380.pdf; см. также: Eneken Tikk, *Frameworks for International Cyber Security,* CCD COE Publications, Tallinn, 2011.

2 См., например: Ellen Nakashima, 'Pentagon to boost cybersecurity force', in *The Washington Post,* 27 January 2013; Gordon Corera, 'Anti-cyber threat centre launched', in *BBC News*, 27 March 2013.

3 Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials', in *The New York Times*, 26 September 2012, p. A10.

4 *Ibid.*

5 Ben Baseley-Walker, 'Transparency and confidence-building measures in cyberspace: towards norms of behaviour', in UNIDIR, *Disarmament Forum*, 'Confronting cyberconflict', Issue 4, 2011, pp. 31–40, доступно по адресу: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf; James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*, доступно по адресу: http://www.unidir.org/pdf/articles/pdf-art3168.pdf.

в кибернетическом пространстве[6]. Кроме того, более десяти лет ведется дискуссия о необходимости нового договора, касающегося кибернетической безопасности. Российская Федерация выступает за принятие такого договора с конца 1990-х гг., а Соединенные Штаты Америки (США) и западные государства считают, что в нем нет необходимости[7]. В письме, направленном Генеральному секретарю Организации Объединенных Наций (ООН), Китай, Российская Федерация, Таджикистан и Узбекистан предложили в сентябре 2011 г. Международный кодекс поведения, касающийся информационной безопасности, но в нем предусмотрена гораздо более широкая сфера действия, нежели только вооруженные конфликты[8]. Китай, Российская Федерация, Казахстан, Киргизия, Таджикистан и Узбекистан являются также сторонами соглашения, принятого в рамках Шанхайской организации сотрудничества в 2009 г.[9] В качестве наблюдателей принимают участие Индия, Исламская Республика Иран, Монголия и Пакистан. Официальный перевод данного соглашения на английский язык свидетельствует о том, что, как представляется, понятия «война» и «оружие» в нем расширены за пределы их традиционных значений в международном гуманитарном праве (МГП)[10].

6 См.: William Hague, 'Security and freedom in the cyber age — seeking the rules of the road', Speech to the Munich Security Conference, 4 February 2011, доступно по адресу: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road; и 'Foreign Secretary opens the London Conference on Cyberspace', 1 November 2011, доступно по адресу: https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.

7 См.: Проект резолюции, предложенный Российской Федерацией Первому комитету Генеральной Ассамблеи в 1998 г., письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций от 23 сентября 1998 г. на имя Генерального секретаря, Док. ООН A/C.1/53/3, 30 сентября 1998; John Markoff and Andrew E. Kramer, 'US and Russia differ on a treaty for cyberspace', in *The New York Times*, 28 June 2009, p. A1; John Markoff and Andrew E. Kramer, 'In shift, US talks to Russia on internet security', in *The New York Times*, 13 December 2009, p. A1; см. Adrian Croft, 'Russia says many states arming for cyber warfare', in Reuters, 25 April 2012, доступно по адресу: http://www.reuters.com/article/2012/04/25/germany-yberidUSL6E8FP40M20120425; Keir Giles, 'Russia's public stance on cyberspace issues', paper given at the 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis and K. Ziolkowski (eds), NATO CCD COE Publications, Tallinn, 2012, доступно по адресу: http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf.

8 Письмо от 12 сентября 2011 г. постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций на имя Генерального, Док. ООН A/66/359 от 14 сентября 2011 г.

9 Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.

10 Доступно по адресу: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf. Приложение 1 определяет информационную войну как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам и другим критически важным структурам, а также с целью подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны». Приложение 2 описывает угрозу разработки и применения информационного оружия, подготовки и ведения информационной войны, источником которой являются «создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений, будучи главной угрозой в международной информационной безопасности. Ее признаками являются применение информационного оружия в целях подготовки и ведения информационной войны, а также

Эта дискуссия, — в которой все стороны обвиняют друг друга в шпионаже и распространении вооружений, в открытой или несколько завуалированной манере[11], — по-прежнему ведется в очень общих понятиях с правовой точки зрения. В частности, не проводится никакого различия между ситуациями вооруженного конфликта и другими ситуациями, хотя применимость МГП зависит от такой дифференциации. Серьезное внимание, как представляется, концентрируется на шпионаже, направленном как против государств, так и против экономических интересов, но речь идет и о кибернетической войне, и о необходимости избежать распространения оружия в кибернетическом пространстве. Обычно не проводится никакого различия между ситуациями вооруженного конфликта и другими ситуациями, в которых операции в кибернетическом пространстве угрожают безопасности сторон, бизнеса и частных хозяйств. В большинстве случаев в дебатах по вопросу об информационной безопасности даже не упоминаются ситуации вооруженных конфликтов и неясно, подразумеваются ли они. Действительно, во многих отношениях, особенно в связи с защитой компьютерной инфраструктуры от проникновения, манипуляций и повреждения, не имеет значения, осуществляется ли информационное нападение в контексте вооруженного конфликте или вне его. Технические средства защиты инфраструктуры обычно являются одинаковыми. Однако если и справедливо утверждение, что большинство угроз в информационной сфере не имеют непосредственной связи с ситуациями вооруженного конфликта, но обусловлены скорее экономическим или иным шпионажем или организованной кибернетической преступностью, столь же очевидно, что применение кибернетического оружия и операций в кибернетическом пространстве играет все более значимую роль во время вооруженных конфликтов и что государства активно ведут подготовку к такому развитию событий.

Между тем нет ясности относительно применимости МГП к информационной войне, а это на самом деле может проистекать из различного понимания самой концепции информационной войны — от операций в кибернетическом пространстве, осуществляемых в контексте вооруженных конфликтов как они понимаются в МГП, до преступной информационной

воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные структуры» (на русском языке доступно по адресу: http://www.conventions.ru/view_base.php?id=1979).

11 Kenneth Lieberthal and Peter W. Singer, 'Cybersecurity and US–China relations', in *China US Focus,* 23 February 2012, доступно по адресу: http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/brookings-cybersecurity-and-u-s-china-relations-february-23-2012/; Mandiant Intelligence Centre Report, *APT1: Exposing one of China's Cyber Espionage Units,* доступно по адресу: http://intelreport.mandiant.com/?gclid=CKD6-7Oo3LUCFalxOgod8y8AJg; Ellen Nakashima, 'US said to be target of massive cyber-espionage campaign', in *The Washington Post*, 11 February 2013; 'North Korea says US "behind hack attack"', in *BBC News*, 15 March 2013.

деятельности любого рода. Некоторые государства, например США[12], Соединенное Королевство Великобритании и Северной Ирландии[13] и Австралия[14], заявили, что МГП применяется к информационной войне[15]. Однако в открытых формулировках позиций пока не рассматриваются подробно такие вопросы, как порог для определения вооруженного конфликта, определение «нападений» в МГП или последствия кибернетической войны в отношении так называемых объектов двойного использования. Упоминалось, что Китай не согласен с применимостью МГП к кибервойне[16]. Однако неясно, будет ли это официальной позицией Китая в ситуации вооруженного конфликта по смыслу МГП. Другая точка зрения:

> «Позиция Китая заключается в том, что государства мира должны сохранять ценность информационного пространства — первого социального пространства, созданного человечеством, — и должны твердо противостоять милитаризации интернета. <…> Действующий Устав ООН и право вооруженных конфликтов, а также основные принципы международного гуманитарного права, которые касаются войны и применения или угрозы применения силы, и далее применяются к информационному пространству — в частности такие императивы, как "неприменение силы" и "мирное урегулирование международных споров", а также принципы проведения различия и соразмерности в отношении средств и методов ведения войны»[17].

12 Harold Koh, 'International law in cyberspace', speech at the US Cyber Command Inter-Agency Legal Conference, 18 September 2012, доступно по адресу: http://opiniojuris.org/2012/09/19/harold-koh-oninternational-law-in-cyberspace/; Доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (далее — Доклад Генерального секретаря), 15 июля 2011 г., Док. ООН A/66/152, с. 21–23; См. также: US Department of Defense Strategy for Operating in Cyberspace: «Существующие издавна международные нормы, регулирующие поведение государств — в мирное время и во время конфликтов — применяются и к информационному пространству. Тем не менее уникальные свойства сетевой технологии требуют дополнительной работы по прояснению того, как эти нормы применяются и какие могут потребоваться новые соглашения для их дополнения». US Department of Defense Strategy for Operating in Cyberspace, July 2011, доступно по адресу: http://www.defense.gov/news/d20110714cyber.pdf.

13 Доклад Генерального секретаря, 23 июня 2004 г., Док. ООН A/59/116, с. 13; Доклад Генерального секретаря, 20 июля 2010 г., Док. ООН A/65/154, с. 16.

14 Доклад Генерального секретаря, примечание 12 выше, с. 8.

15 См. также предложение Верховного представителя Европейского союза по иностранным делам и политике безопасности: *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, JOIN (2013) 1 final.

16 См., например: Adam Segal, 'China, international law and cyber space', in *Council on Foreign Relations*, 2 October 2012, доступно по адресу: http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

17 Li Zhang, 'A Chinese perspective on cyber war' in *International Review of the Red Cross*, Volume 94, No. 886, pp. 801—807. В своей речи на заседании Первого комитета в сентябре 2011 г. посол Китая заявил, что Китай предлагает всем государствам «взять на себя обязательство не использовать информационные технологии и кибертехнологию для враждебной деятельности в ущерб международному миру и безопасности и не заниматься распространением информационного оружия, кибероружия и связанных с ними технологий. <…> Страны должны добиваться того, чтобы не допустить превращения информационного пространства и киберпространства в новое поле битвы». МГП не упоминается. См.: заявление о безопасности информационно-кибернетического пространства, сделанное г-ном послом Ван Цюнем на заседании Первого комитета во время

Насколько можно заметить, Российская Федерация не заняла официальной позиции по вопросу о применимости МГП к информационной войне[18].

С правовой точки зрения важно провести различие между кибернетической войной, то есть операциями в кибернетическом пространстве, осуществляемыми в контексте вооруженных конфликтов по смыслу МГП, и операциями в кибернетическом пространстве вне такого контекста. Нормы МГП применяются только в условиях вооруженных конфликтов, налагая особые ограничения на стороны в конфликте[19]. Таким образом, в настоящей статье термин «кибернетическая война» относится к средствам и методам ведения войны, являющимся операциями в информационном пространстве, которые могут считаться вооруженным конфликтом или вестись в контексте вооруженного конфликта только по смыслу МГП. Такие операции в информационном пространстве, часто называемые нападениями на компьютерные сети, направлены против компьютера или компьютерной системы или осуществляются через них посредством информационного потока[20]. У них могут быть различные цели, например проникнуть в компьютерную систему и собрать, экспортировать, уничтожить, изменить или зашифровать данные либо запустить или изменить процессы, контролируемые системой, в которую происходит проникновение, или иным образом манипулировать этими процессами. Другими словами, следующий анализ касается военных действий, которые заключаются в разработке и внедрении компьютерного кода от одного или нескольких компьютеров на компьютеры, подвергающиеся нападению.

66-й сессии Генеральной Ассамблеи. На русском языке доступно по адресу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/556/78/PDF/N1155678.pdf?OpenElement.

18 В военной доктрине Российской Федерации не упоминается МГП в отношении информационной войны; см.: Военная доктрина Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 февраля 2010 г., доступно по адресу: http://www.belvpo.com/ru/8746.html; не упоминает его и К. Джайлз (Keir Giles), примечание 7 выше; в работе Роланда Хейкерё (Roland Heikerö, 'Emerging threats and Russian Views on information warfare and information operations', FOI Swedish Defence Research Agency, March 2010, p. 49, доступно по адресу: http://www.highseclabs.com/Corporate/foir2970.pdf,) говорится, что Российская Федерация выступила с предложением о «применимости гуманитарных законов, запрещающих нападения на некомбатантов и налагающих запрет на дезинформацию в киберпространстве».

19 Для Международного Комитета Красного Креста (МККК) важно привлечь внимание к особой ситуации, когда операции в кибернетическом пространстве могут считаться вооруженным конфликтом или осуществляться в контексте вооруженного конфликта, — то есть к информационной войне в узком смысле слова. Это так, потому что в соответствии с Женевскими конвенциями (ЖК) 1949 г. МККК обладает конкретным мандатом по предоставлению помощи и защиты жертвам вооруженных конфликтов. Международное сообщество поручило ему также осуществлять деятельность по распространению знаний и информации о МГП. См., например: ЖК III, статья 126 (5), ЖК IV, статья 143 (5), и Устав Международного движения Красного Креста и Красного Полумесяца, статья 5 (2) (g).

20 US Department of Defense, *Dictionary of Military and Associated Terms*, 8 November 2010 (as amended on 31 January 2011), Washington, DC, 2010: «Нападения на компьютерные сети — это действия, предпринимаемые посредством использования компьютерных сетей для того, чтобы помешать доступу к информации, находящейся в компьютерах или компьютерных сетях, ухудшить или уничтожить ее или помешать работе самих компьютеров и компьютерных сетей».

Проблемы гуманитарного характера, вызывающие обеспокоенность

В гуманитарном плане обеспокоенность Международного Комитета Красного Креста, связанная с информационной войной, касается прежде всего ее возможного воздействия на гражданское население, в частности из-за того, что операции в кибернетическом пространстве могут серьезно затронуть гражданскую инфраструктуру[21], что обусловлено несколькими особыми характеристиками информационной сферы.

Во-первых, из-за все более расширяющегося использования компьютерных систем гражданская инфраструктура крайне уязвима перед нападениями на компьютерные сети. В частности, целый ряд важнейших объектов, таких как электростанции, атомные станции, дамбы, системы очистки и распределения воды, нефтеперерабатывающие предприятия, газовые и нефтяные трубопроводы, банковские системы, системы больниц, железные дороги и авиадиспетчерская служба, полагаются на так называемые системы телеуправления и сбора данных (СКАДА) и распределенные системы управления (РСУ). Эти системы являются связующим звеном между цифровым и физическим мирами, и они крайне уязвимы перед внешним вмешательством, которое может быть осуществлено любым нападающим[22].

Во-вторых, целостность интернета представляет собой угрозу для гражданской инфраструктуры. Действительно, большинство военных сетей полагаются на гражданскую, главным образом коммерческую, инфраструктуру, например подводные оптоволоконные кабели, спутники, роутеры и узлы; и наоборот, гражданские транспортные средства, контроль над судоходством и авиадиспетчерская служба все чаще оборудованы навигационными системами, зависящими от глобальной навигационной спутниковой системы (GPS), которая используется и военными. Таким образом, в значительной степени невозможно провести различие между чисто гражданской и чисто военной компьютерной инфраструктурой. Как будет показано ниже, это бросает серьезный вызов одному из кардинальных принципов МГП, а именно принципу проведения различия между военными и гражданскими объектами. Более того, даже если военные и гражданские компьютеры или компьютерные системы не являются одними и теми же, межсетевое взаимодействие означает, что последствия нападения на военную цель не будут ею ограничены. Действительно,

21 В праве, касающемся ведения военных действий, «гражданские лица», «гражданское население» и «гражданские объекты» являются разными правовыми понятиями, к которым применяются разные нормы. Однако когда в настоящей статье говорится о воздействии информационной войны на гражданское население, имеется в виду и ущерб, наносимый гражданской инфраструктуре, а именно таким образом операции в киберпространстве, вероятнее всего, окажут воздействие на гражданское население.

22 Стефано Меле, анализируя вероятные сценарии вмешательства в работу военных и гражданских систем различных типов, утверждает, что манипулирование системами управления электрическими сетями является, возможно, самой большой опасностью в настоящее время. См.: Stefano Mele, 'Cyber warfare and its damaging effects on citizens', September 2010, доступно по адресу: http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

кибератака может затронуть различные другие системы, включая гражданские системы и сети, например путем распространения вредоносных программных средств, таких как вирусы и «черви», если они не поддаются контролю. Это означает, что нападение на военную компьютерную систему способно повредить гражданские компьютерные системы, что, в свою очередь, может оказаться крайне пагубным для некоторых гражданских служб, например водоснабжения, электроснабжения или передачи активов.

Пока у нас нет явных примеров информационных нападений во время вооруженных конфликтов или примеров, когда гражданское население серьезно пострадало в результате нападения на компьютерную сеть во время вооруженного конфликта. Однако, кажется, эксперты согласны в том, что технически вполне возможно, даже если и трудно, преднамеренно помешать работе систем аэропортов, других транспортных систем, дамб и электростанций, используя информационное пространство. Нельзя сбрасывать со счетов возможность катастрофических сценариев, например столкновение самолетов, утечку радиации с ядерных установок, высвобождение токсичных химикатов на химических предприятиях или нарушение работы важнейших инфраструктур и служб, таких как системы электро- и водоснабжения.

Такие сценарии могут и не быть самыми вероятными; операции в информационном пространстве, скорее всего, будут применяться для такого воздействия на гражданскую инфраструктуру, которое приведет к ее плохому функционированию или к нарушениям, не вызывая непосредственной гибели людей или повреждений. Эффект таких «бескровных» средств и методов войны может быть и не столь драматичным для гражданских лиц, как обстрел или бомбардировки. Тем не менее он может быть жестким — например, если нарушается снабжение электроэнергией и водой или если не работают системы связи или банковские системы. Поэтому надо прояснить, как такие последствия следует рассматривать в соответствии с нормами МГП.

Некоторые авторы заявляли, что угрозу нападений на компьютерные сети крупной гражданской инфраструктуры не следует переоценивать, в частности из-за того, что программы, используемые в качестве наступательного кибернетического оружия должны быть очень тщательно написаны для того, чтобы поразить конкретные компьютерные системы (как, например, вирус Stuxnet[23]), и не могут поэтому с легкостью быть перенаправлены

23 Так называемый вирус Stuxnet был направлен против предприятия по обогащению урана в Натанзе, что, как сообщалось, привело к разрушению тысячи центрифуг. По сообщениям прессы Соединенные Штаты и (или) Израиль стояли за этой операцией, но официально это не было подтверждено. David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? Preliminary assessment', ISIS Report, 22 December 2010, доступно по адресу: http://isis-online.org/isisreports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/; David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', in The New York Times, 1 June 2012, доступно по адресу: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacksagainst-iran.html?pagewanted=all&_moc.semityn.www

на другие цели[24]. Кроме того, в международной взаимосвязанной системе интернета и в глобализованной экономике государства могут не захотеть наносить друг другу ущерб, поскольку последствия, например для финансовых систем, могут повредить им так же сильно, как и противнику[25]. Может быть, это так, а может быть, и нет. Нападения на компьютерные сети способны повредить гражданские объекты, в некоторых случаях оказываются неизбирательными или используются неизбирательным образом либо могут иметь разрушительные побочные последствия для гражданской инфраструктуры и гражданского населения, — все это является достаточной причиной для того, чтобы было необходимо прояснить применимые нормы, касающиеся ведения военных действий, которые стороны в конфликте обязаны соблюдать.

Роль международного гуманитарного права

Каким же образом в подобных обстоятельствах МГП ищет решение вопроса о потенциальных последствиях кибернетической войны для гражданского населения?

Положения МГП не упоминают конкретно операции в киберпространстве. Это обстоятельство и сравнительная новизна кибернетической технологии иногда приводят к мнению, что теперь абсолютно качественно меняются средства и методы войны; приходится порой слышать, что МГП плохо приспособлено к информационной сфере и не может применяться к кибернетической войне[26]. Однако отсутствие в МГП конкретного упоминания операций в кибернетическом пространстве не означает, что такие операции не регулируются нормами МГП. Новые технологии любого рода разрабатываются постоянно, и масштаб МГП достаточно широк для того, чтобы учесть и такое развитие событий. МГП конкретно запрещает или ограничивает применение некоторых видов оружия (например, химического и биологического оружия или противопехотных мин). Но кроме того, оно регулирует своими общими нормами применение всех средств и методов ведения войны, включая способы применения всех видов оружия. В частности, статья 36 Дополнительного протокола I (ДП I) к Женевским конвенциям предусматривает, что:

> «при изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их

24 Thomas Rid, 'Think again: cyberwar', in *Foreign Policy*, March/April 2012, pp. 5 ff., доступно по адресу: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Thomas Rid and Peter McBurney, 'Cyber-weapons', in *The RUSI Journal*, February–March 2012, Vol. 157, No. 1, pp. 6–13; см. также: Maggie Shiels, 'Cyber war threat exaggerated claims security expert', in *BBC News*, 16 February 2011, доступно по адресу: http://www.bbc.co.uk/news/technology-12473809.

25 Стефано Меле (примечание 22 выше) считает, что по этой причине массивные электронные нападения на финансовые системы других стран маловероятны.

26 Charles J. Dunlap Jr., 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly,* Spring 2011, p. 81.

> применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне».

Кроме конкретного обязательства, которое эта норма налагает на государства — участники Дополнительного протокола I, она показывает, что нормы МГП применяются по отношению к новым технологиям.

И все-таки кибернетическая война бросает вызов отдельным основополагающим положениям МГП. Во-первых, МГП исходит из того, что стороны в конфликте известны и идентифицируемы. Это не всегда само собой разумеется даже в традиционных вооруженных конфликтах, особенно немеждународных. Однако в случае операций в кибернетическом пространстве, которые происходят ежедневно, анонимность является скорее правилом, нежели исключением. В некоторых случаях не представляется возможным узнать, кто именно их осуществляет, и даже когда это возможно, чаще всего на это требуется очень много времени. Поскольку любое право основывается на присвоении ответственности (в МГП — стороне в конфликте или отдельному лицу), возникают серьезные трудности. В частности, если лицо, осуществившее операцию, и, таким образом, связь операции с вооруженным конфликтом не могут быть установлены, крайне трудно определить, является ли МГП вообще применимым к данной операции. Так, например, если совершено нападение на правительственную инфраструктуру, но неясно, кто стоит за этим нападением, трудно определить, кто является сторонами в потенциальном вооруженном конфликте и, соответственно, имеет ли вообще место вооруженный конфликт. Аналогичным образом даже если стороны в конфликте известны, может оказаться очень трудным приписать деяние одной какой-то стороне. Во-вторых, МГП основывается на положении, что применение средств и методов ведения войны будет иметь сильное воздействие на физический мир. Многие операции в кибернетическом пространстве, скорее всего, будут иметь разрушительное воздействие, но воздействие, которое сразу же не будет восприниматься как разрушительное в физическом смысле. В-третьих, вся структура норм, касающихся ведения военных действий, в частности принцип проведения различия, основана на предположении, что гражданские объекты и военные объекты могут быть чаще всего различимы. На кибернетическом театре военных действий это, вероятнее всего, станет исключением, а не правилом, потому что большая часть кибернетической инфраструктуры по всему миру (подводные кабели, роутеры, серверы, спутники) используется как для гражданских, так и для военных целей.

Поэтому далее будет сделана попытка исследовать, как нормы МГП могут истолковываться, для того чтобы они обрели смысл в кибернетической сфере, и как кибернетическая технология может сказаться на их ограничениях. Как будет показано ниже, вероятно, слишком рано давать определенные ответы на многие возникающие вопросы, потому что еще

мало примеров и факты не отличаются абсолютной ясностью, а практике государств в отношении толкования и имплементации применимых норм еще только предстоит развиться. На сегодняшний день Таллиннское руководство по международному праву, применимому к кибернетической войне (далее — Таллиннское руководство), является наиболее обстоятельной попыткой истолковать нормы международного права (jus ad bellum и jus in bello) применительно к кибернетической войне[27]. Оно было составлено группой экспертов по поручению Совместного центра передовых технологий в области кибернетической обороны НАТО, в Руководстве содержится полезная подборка норм с комментариями, отражающими различные точки зрения по некоторым противоречивым вопросам, встающим в связи с этой новой технологией. МККК в качестве наблюдателя принимал участие в обсуждениях, проводимых группой экспертов, но разделяет не все мнения, нашедшие отражение в Руководстве.

Применимость международного гуманитарного права к кибернетическим операциям: что такое вооруженный конфликт в киберпространстве?

МГП может применяться только тогда, когда операции в кибернетическом пространстве ведутся в контексте вооруженного конфликта или в связи с ним. Таким образом, не должно вызывать возражений утверждение, что, если операции в киберпространстве проводятся в контексте вооруженного конфликта, они регулируются теми же нормами МГП, что и этот конфликт: например, если одновременно с бомбардировкой или ракетным ударом или в дополнение к ним сторона в конфликте осуществляет кибернетическое нападение на компьютерные системы своего противника.

Однако целый ряд операций, которые характеризуются как кибернетические военные действия, могут осуществляться и не в контексте вооруженных конфликтов. Такие термины, как «кибератаки» или «кибертерроризм», могут ассоциироваться с методами военных действий, но операции, которые они обозначают, не обязательно проводятся во время вооруженного конфликта. Операции в кибернетическом пространстве могут быть и на самом деле являются преступлениями, совершаемыми в повседневных ситуациях, которые не имеют ничего общего с войной.

Другие ситуации, которые находятся где-то между ситуациями существующих вооруженных конфликтов, ведущихся традиционными методами, и операциями в киберпространстве, и ситуации, которые никак не являются вооруженным конфликтом, классифицировать труднее. Так обстоят дела, в частности, когда нападения на компьютерные сети являются единственными совершаемыми враждебными действиями и тем более когда

27 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (forthcoming). Таллиннское руководство доступно по адресу: http://www.ccdcoe.org/249.html.

они остаются одиночными актами. Этот сценарий не является абсолютно футуристическим. Вирус Stuxnet, как представляется, предназначался для завода по обогащению урана в Натанзе в Исламской Республике Иран, и его распространение остается пока единичным нападением на компьютерную сеть (хотя оно и производилось в течение некоторого периода времени), и осуществлялось это нападение против Исламской Республики Иран, возможно, одним или несколькими государствами. Хотя вопрос о классификации события в качестве вооруженного конфликта не поднимался государствами, некоторые обозреватели высказывали предположение, что, если нападение осуществлялось государством, оно может считаться международным вооруженным конфликтом[28]. Другим возможным сценарием могут стать крупномасштабные и длительные операции в киберпространстве, осуществляемые негосударственной организованной вооруженной группой и направленные против правительственной инфраструктуры. Могут ли такие операции достигать уровня немеждународного вооруженного конфликта?

В соответствии с действующим МГП существуют два — и только два — типа вооруженного конфликта: международные вооруженные конфликты и немеждународные вооруженные конфликты. Мы не будем обсуждать здесь все критерии существования таких конфликтов. Рассмотрим только отдельные аспекты, которые, как представляется, ставят особенно трудные вопросы в связи с операциями в киберпространстве.

Международные вооруженные конфликты

В соответствии с общей статьей 2 четырех Женевских конвенций 1949 г. международным вооруженным конфликтом является любая ситуация «объявленной войны или всякого другого вооруженного конфликта, возникающего между двумя или несколькими Высокими Договаривающимися Сторонами, даже в том случае, если одна из них не признает состояния войны». Не существует никакого другого договорного определения международных вооруженных конфликтов, и к настоящему времени признано, что, согласно Международному уголовному трибуналу по бывшей Югославии (МТБЮ), международный вооруженный конфликт имеет место «всегда, когда в отношениях между государствами *применяется вооруженная сила*»[29]. Применимость МГП зависит от фактической ситуации, а не от признания состояния вооруженного конфликта сторонами в конфликте.

28 Michael N. Schmitt, 'Classification of cyber conflict', in *Journal of Conflict and Security Law*, Vol. 17, Issue 2, Summer 2012, p. 252; см. также: Gary Brown, 'Why Iran didn't admit Stuxnet was an attack', in *Joint Force Quarterly*, Issue 63, 4th Quarter 2011, p. 71, доступно по адресу: http://www.ndu.edu/press/why-iran-didntadmit-stuxnet.html. Г. Браун не рассматривает вопрос о классификации конфликта, но считает, что Stuxnet совершенно очевидно является нападением, возможно в нарушение запрета на применение силы и в нарушение права войны.

29 International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70 (курсив автора). Ситуации, предусмотренные статьей 1 (4) ДП I, также считаются международным вооруженным конфликтом для государств — участников ДП I.

Особый вопрос, который возникает в связи с кибернетической войной, заключается в том, может ли международный вооруженный конфликт начаться в результате нападения на компьютерную сеть при отсутствии какого-либо иного (кинетического) применения силы. Ответ зависит от следующих обстоятельств: 1) присваивается ли нападение на компьютерную сеть государству и 2) приравнивается ли оно к применению вооруженной силы — термин, который не имеет определения в МГП.

Присвоение поведения государству

Присвоение операции государству может вызвать особенно трудные вопросы, если речь идет о действиях в киберпространстве, где анонимность является скорее правилом, нежели исключением. И все же пока стороны не могут быть идентифицированы как два или более государств, невозможно классифицировать ситуацию в качестве международного вооруженного конфликта. Хотя эта проблема скорее фактическая, чем правовая, путь преодоления неопределенности лежит через правовые допущения. Например, если нападение на компьютерную сеть исходило из правительственной инфраструктуры конкретного государства, можно допустить, что операция приписывается государству — особенно в свете нормы международного права, которая устанавливает, что государства не должны сознательно разрешать использовать свою территорию для совершения актов, нарушающих права других государств[30]. Однако против такого подхода имеются два возражения.

Во-первых, существующие нормы международного права не поддерживают такого допущения. Например, Статьи об ответственности государств за международно-противоправные деяния Комиссии международного права не содержат норм, которые допускают присвоение поведения государству. Кроме того, Международный суд (МС) установил высокий порог для присвоения поведения государству в контексте права на самооборону. В деле о нефтяной платформе он постановил, что бремя доказывания лежит на государстве, ссылающемся на самооборону:

> «Суд должен просто определить, продемонстрировали ли Соединенные Штаты, что являлись жертвой "вооруженного нападения" со стороны Ирана, чтобы оправдать свое применение вооруженной силы для самообороны; и бремя доказывания фактов, свидетельствующих о существовании такого нападения, лежит на Соединенных Штатах»[31].

Хотя это постановление было вынесено в контексте права на самооборону в *jus ad bellum*, его можно обобщить по отношению ко всем фактическим вопросам присвоения поведения государству. Поскольку это допущение

30 International Court of Justice (ICJ), *Corfu Channel* case (*United Kingdom* v. *Albania*), Judgment of 9 April 1949, p. 22; см. также: норма 5 Таллиннского руководства, примечание 27 выше.

31 ICJ, *Oil Platforms* case (Islamic Republic of *Iran* v. *United States of America*), Judgment of 6 November 2003, para. 57.

о фактах, было бы бессмысленно делать подобное допущение для одной цели и не делать для другой.

Во-вторых, такое допущение будет и слишком далеко идущим в конкретном контексте кибернетической войны. Принимая во внимание трудности в обеспечении защиты компьютерной инфраструктуры от манипуляций и легкость, с которой можно дистанционно контролировать компьютер под чужим именем в кибернетическом пространстве, представляется, что бремя ответственности, возлагаемое на правительства за все операции, исходящие с их компьютеров, было бы слишком тяжелым без каких-либо дополнительных доказательств[32].

Другим, более часто обсуждаемым вопросом, является присвоение государству кибернетических нападений, совершаемых частными сторонами, такими как хакерские группы. Кроме фактических вопросов, обусловленных анонимностью операций в кибернетическом пространстве, правовые нормы, касающиеся присвоения действий частных сторон государству, излагаются в Статьях об ответственности государств за международно-противоправные деяния[33]. В частности, государство несет ответственность за поведение лица или группы лиц, «если это лицо или группа лиц фактически действует по указаниям либо под руководством или контролем этого государства при осуществлении такого поведения»[34]. Со временем придется прояснить, что точно означают слова «под руководством или контролем». Международный суд требует: для того чтобы действие частной стороны (будь то отдельное лицо или член организованной группы) вменялось в вину государству, руководство или эффективный контроль государства над операцией, в ходе которой были совершены предполагаемые преступления, должны быть продемонстрированы, и не только вообще в отношении всех действий, предпринимаемых лицами или группами лиц, совершившими нарушения[35]. Если такой контроль не осуществлялся над конкретной операцией, ее нельзя вменить в вину государству, даже если она проведена группой, степень зависимости которой от государственных властей была высокой[36]. В том же ключе комментарий к Статьям об ответственности государств требует, чтобы государство руководило конкретной операцией или контролировало ее и чтобы соответствующее поведение было

32 Таллиннское руководство придерживается такого же мнения с правовой точки зрения в норме 7: «Сам по себе факт, что операции в кибернетическом пространстве были запущены или иным образом исходили из правительственной инфраструктуры, не является достаточным свидетельством того, что операция должна быть присвоена государству, но указывает на связь государства с операцией».

33 Комиссия международного права, Ответственность государств за международно-противоправные деяния (далее — Проект статей об ответственности государств), Документ ООН A/RES/56/83.

34 Проект статей об ответственности государств, статья 8.

35 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment of 27 June 1986, paras 115–116; ICJ, *Case concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina* v. *Serbia and Montenegro*), Judgment, 26 February 2007, paras 400–406.

36 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment of 27 June 1986, para. 115

неотъемлемой частью этой операции[37]. МТБЮ пошел дальше и заявил, что, если группа, такая как вооруженная оппозиционная группа, является организованной, достаточно, чтобы государственные власти осуществляли «общий контроль» над такой организованной и иерархически структурированной группой, и нет необходимости в том, чтобы осуществлялся конкретный контроль или руководство отдельной операцией[38]. Однако МТБЮ признал также, что, если осуществляющее контроль государство не является территориальным государством, «требуются более обширные и неоспоримые свидетельства для того, чтобы показать, что государство действительно осуществляет контроль над подразделениями и группами», — это означает, что участие государства в планировании военных операций или его роль координатора может быть трудно продемонстрировать[39]. В комментарии Комиссии международного права говорится: «Вопрос о том, была ли степень контроля государства над тем или иным поведением достаточной для того, чтобы присвоить ему это поведение, должен решаться с учетом обстоятельств каждого конкретного дела»[40]. Однако эта дискуссия не является относящейся конкретно к кибернетической сфере. Когда факты установлены, применяются те же самые правовые критерии, что и при любом другом присвоении поведения сторон, являющихся частными лицами, государству. Здесь снова трудность, вероятнее всего, будет заключаться в фактической оценке.

Применение вооруженной силы

Вторым критерием, который необходимо удовлетворить, является критерий «применения вооруженной силы» в отношениях между государствами.

Перед рассмотрением вопросов, поставленных кибернетической войной в этой связи, надо кратко разъяснить, что классификация конфликта в качестве международного вооруженного конфликта в соответствии с МГП (jus in bello) существует отдельно от вопроса jus ad bellum. Эти два вопроса часто объединяются, в том числе в кибернетической войне.

В соответствии с jus ad bellum вопрос заключается в том, являются ли применением силы — и если являются, то когда — операции в кибернетическом пространстве по смыслу статьи 2 (4) Устава ООН, и (или) являются ли они вооруженным нападением по смыслу статьи 51 Устава

37 Доклад Комиссии международного права о работе ее 53-й сессии (23 апреля — 1 июня и 2 июля — 10 августа 2001 г.), Док. ООН A/56/10, Комментарий к статье 8 Статей об ответственности государства, п. 3.

38 ICTY, *Prosecutor* v. *Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120. Иногда говорят, что вопрос, поставленный перед Трибуналом, касался квалификации конфликта в качестве немеждународного или международного; однако аргумент о том, что два вопроса являются абсолютно отдельными, неубедителен, поскольку он привел бы к выводу, что государство может быть стороной в конфликте в силу осуществления контроля над организованной вооруженной группой, но не нести ответственность за деяния, совершенные во время этого конфликта.

39 *Ibid*., paras 138—140.

40 Комментарий к статье 8 Проекта статей об ответственности государств, примечание 37 выше, п. 5.

ООН, и при каких обстоятельствах они вводят в действие право на самооборону[41]. Каковы бы ни были мнения, высказанные в этой дискуссии по jus ad bellum, следует вспомнить, что объекты регулирования jus ad bellum и jus in bello совершенно различны: в то время как jus ad bellum регулирует межгосударственные отношения и требования о законном применении силы в отношениях между государствами, jus in bello регулирует поведение сторон в конфликте, и его объектом и целью является предоставление защиты военным и гражданским жертвам войны. Таким образом, для целей квалификации международного вооруженного конфликта действие может представлять собой применение вооруженной силы без ущерба для вопроса о том, представляет ли оно собой применение силы по смыслу статьи 2 (4) Устава ООН (хотя это вероятно), уже не говоря о вооруженном нападении в соответствии со статьей 51. Эта дифференциация равным образом относится к операциям в кибернетическом пространстве.

Если говорить о jus in bello, то в МГП не существует договорного определения значения вооруженной силы, потому что это критерий, относящийся к судебной практике. Традиционно цель войны заключается в том, чтобы одержать победу над противником, и в классической войне конфликт связан с использованием военных средств, что ведет к военной конфронтации. Таким образом, когда используются традиционные средства и методы войны — бомбардировки, обстрел или развертывание войск, не вызывает никакого сомнения, что это вооруженная сила. Но нападения на компьютерные сети не связаны с применением такого оружия.

В отсутствие традиционных систем оружия и кинетической силы что может считаться вооруженной силой в кибернетической сфере?

В качестве первого шага надо сравнить последствия нападений на компьютерную сеть с последствиями применения кинетической силы. Большинство авторов придерживаются того мнения, что, если нападение на компьютерную сеть присваивается государству и имеет те же последствия, что и физическое применение силы, это будет международный вооруженный конфликт[42]. Действительно, если нападение на компьютерную

41 См.: Marco Roscini, 'World wide warfare — jus ad bellum and the use of cyber force', in *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 85; Michael N. Schmitt, 'Computer network attack and the use of force in international law: thoughts on a normative framework', in *Columbia Journal of Transnational Law*, Vol. 37, 1998–1999, p. 885; Herbert S. Lin, 'Offensive cyber operations and the use of force', in *Journal of National Security Law and Policy*, Vol. 4, 2010, p. 63; David P. Fidler, 'Recent developments and revelations concerning cybersecurity and cyberspace: implications for international law', in *ASIL Insights*, 20 June 2012, Vol. 16, no. 22; *Tallinn Manual*, Rules 10—17, см. примечание 27 выше.

42 M. N. Schmitt, 'Classification of cyber conflict', p. 251 (примечание 28 выше); Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', ICRC, 2004, p. 3, доступно по адресу: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 131; Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, p. 24, available at: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf. Нильс Мельцер утверждает, что, поскольку существование международного вооруженного конфликта зависит в основном от наличия вооруженных военных действий между государствами, операции в кибернетическом пространстве будут означать вооруженный конфликт не только по причинам гибели людей, ранений и разрушений, но также и в результате непосредственного отрицательного воздействия на военные операции или военный потенциал государства.

сеть служит причиной столкновений самолетов или поездов, приводящих к гибели людей и повреждениям, или крупного наводнения с широкомасштабными последствиями, нет серьезных причин рассматривать ситуацию иначе, чем аналогичные нападения, осуществляемые при помощи кинетических средств и методов ведения войны.

Такая параллель поэтому полезна для ситуаций, в которых нападения на компьютерную сеть приводят к гибели или ранениям людей, физическому ущербу или разрушению инфраструктуры. Однако может оказаться недостаточным зафиксировать весь диапазон возможных последствий операций в кибернетическом пространстве и ущерба, который они могут нанести, ведь они не обязательно будут напоминать физические последствия применения традиционного оружия. Операции в кибернетическом пространстве будут часто применяться для того, чтобы не физически уничтожить или повредить военную или гражданскую инфраструктуру, но скорее повлиять на ее функционирование, например манипулируя ею, и даже сделать это так, чтобы никто не заметил манипуляций. Например, энергетическая система может физически не быть повреждена, но тем не менее окажется выведена из строя в результате нападения на компьютерную сеть. Аналогичным образом, манипуляциям может подвергнуться банковская система страны, хотя инфраструктура не будет повреждена физически и сам факт манипуляции даже не будет заметен в течение какого-то времени. На первый взгляд даже в отсутствие традиционных военных средств или непосредственного физического разрушения потенциальное воздействие такого повреждения на население позволит считать его применением вооруженной силы, поскольку оно может быть гораздо обширнее и серьезнее, чем, например, разрушение какого-то здания или группы зданий. Однако государства — даже пострадавшие — могут попытаться избежать эскалации международной конфронтации или иметь другие причины, чтобы не рассматривать такие типы нападений как начало вооруженного конфликта. В настоящий момент трудно сформулировать какую-либо правовую позицию, поскольку государства, как представляется, сохраняют чаще всего молчание перед лицом кибернетических нападений[43]. В отсутствие четкой практики государств существует несколько возможных подходов к этому вопросу.

Один подход заключается в том, чтобы рассматривать любую враждебную операцию в кибернетическом пространстве, которая воздействует на функционирование объектов, как применение вооруженной силы. Объект и цели МГП в целом и, в частности, отсутствие порога насилия, при котором имеет место международный вооруженный конфликт, желание устранить пробел в защите, особенно защите гражданского населения от воздействия военных действий, говорят в пользу включения таких операций в кибернетическом пространстве в определение вооруженной силы для целей определения наличия вооруженного конфликта. Кроме того, с учетом значения, которое государства придают защите важнейшей инфраструктуры

43 См. также: G. Brown, примечание 28 выше.

в своей кибернетической стратегии, очень может быть, что они сочтут нападения другого государства на компьютерную сеть, направленные на выведение из ее строя, началом вооруженного конфликта[44]. Более того, в отсутствие вооруженного конфликта МГП не регулирует ситуацию и, значит, не предоставляет своей защиты. Другие отрасли права, такие как jus ad bellum, кибернетическое право, космическое право или телекоммуникационное право, могут, конечно, применяться и предоставлять свою собственную защиту. Анализ их действия не входит в задачи этой статьи, но все остальные своды права будут ставить свои собственные вопросы. Например, могло бы применяться международное право прав человека, но будет ли нападение на компьютерную сеть, направленное с другой стороны планеты против гражданской инфраструктуры, удовлетворять требованию эффективного контроля для целей применимости права прав человека? Кроме того, насколько достаточной будет защита, предоставляемая правом прав человека, от нарушения работы инфраструктуры, последствия которого для жизни гражданских лиц могут быть не установлены сразу же?

Другой подход может заключаться в том, чтобы не сосредоточивать внимание исключительно на аналогичных последствиях операции в киберпространстве, но рассмотреть сочетание факторов, которые будут указывать на вооруженную силу. К этим факторам будут относиться определенная серьезность последствий операции в киберпространстве, используемые средства, участие военных или других учреждений правительства во враждебной операции, характер цели (военная или нет) и продолжительность операции. Если взять пример вне кибернетической сферы, то убийство начальника штаба вооруженных сил государства во время воздушного нападения другого государства будет, конечно, считаться международным вооруженным конфликтом. Однако если он погиб в результате получения отравленного письма, будет ли это также приравниваться само по себе к международному вооруженному конфликту[45]? Что, если цель была

44 N. Melzer, примечание 42 выше, p. 14. Мельцер считает, что здесь возможна ссылка на концепцию критической инфраструктуры для того, чтобы учитывать «масштаб и воздействие» нападения на компьютерную сеть для целей определения вооруженного нападения по смыслу статьи 51 Устава ООН. О политике Франции см.: Agence Nationale de la Sécurité des Systèmes d'Information, *Défense et sécurité des systems d'informations,* доступно по адресу: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf; о политике Германии см.: Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen*, доступно по адресу: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html; о политике Канады см.: *National Strategy for Critical Infrastructure*, доступно по адресу: http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx; о политике Великобритании см.: *The UK Cyber Security Strategy*, доступно по адресу: http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy; о политике Австралии см.: CERT Australia, *Australia's National Computer Emergency Response Team*, доступно по адресу: https://www.cert.gov.au/.

45 В работе *How Does Law Protect in War*?, Vol. I, 3rd edn, ICRC, Geneva, 2011, p. 122, Марко Сассоли, Антуан Бувье и Анна Кинтен (Marco Sassòli, Antoine Bouvier, Anne Quintin) проводят различие между силой, применяемой военными или другими представителями государства: «Когда участвуют вооруженные силы двух государств, достаточно одного выстрела или одного захваченного в плен (в соответствии с указаниями правительства), для того чтобы стало применяться МГП, хотя в других случаях (например, суммарная казнь, осуществленная секретным агентом, направленным своим правительством за границу) требуется более высокий порог насилия».

гражданским объектом? Имеет ли значение, какие средства применялись для уничтожения инфраструктуры? Например, если части ядерной установки были выведены из строя в результате подрывных действий со стороны проникших на нее иностранных агентов, будет ли это также приравниваться к применению вооруженной силы? Имеет ли значение военный или гражданский характер цели?

В информационной сфере возможно, например, что государства будут относиться к нападениям на компьютерную сеть своей военной инфраструктуры не так, как к нападениям, направленным на гражданские системы. Возможно, это и не совсем логично с технической точки зрения, потому что применение силы — это применение силы в отношении как гражданских, так и военных объектов. Но уровень ущерба, который государства готовы понести, может быть ниже, если речь идет об операциях, направленных на снижение их военного потенциала.

Если нападение на компьютерную сеть носит точечный характер и является непродолжительным, то, следуя такому подходу, его могут счесть применением вооруженной силы, если его последствия особенно опасны. Пример с вирусом Stuxnet, как об этом писали в прессе, кажется, указывает на то, что нападения на компьютерную сеть могут — по крайней мере в течение какого-то времени — оставаться изолированными враждебными действиями одного государства против другого, без использования других кинетических операций, особенно если нападающий стремится быть анонимным, хочет, чтобы нападение не было обнаружено в течение какого-то времени, или пытается (по политическим или другим причинам) избежать эскалации применения силы и дальнейших военных действий и вооруженного конфликта. Если исходить исключительно из того, достигает ли кинетическое нападение с теми же результатами уровня вооруженного конфликта, можно прийти к выводу, что такое нападение является применением вооруженной силы, потому что вирус Stuxnet, как сообщалось, вызвал физическое разрушение приблизительно тысячи центрифуг IR-1, которые пришлось заменить на заводе по обогащению урана в Натанзе[46]. Действительно, если бы центрифуги на ядерной установке были разрушены в результате бомбардировки военно-воздушными силами другого государства, такое нападение считалось бы применением вооруженной силы и означало бы начало международного вооруженного конфликта. Но поскольку средство нападения не было кинетическим, не имелось информации ни о каких других нападениях в связи с этим и оно не причинило никакого иного, кроме разрушения центрифуг, ущерба, оно не может быть обозначено как применение вооруженной силы, что означало бы начало международного вооруженного конфликта.

Подводя итог, можно сказать, что предстоит еще только увидеть, будут ли государства и при каких условиях рассматривать нападения на компьютерную сеть как применение вооруженной силы. Просто вмешательство

46 Это мнение М. Н. Шмитта, примечание 28 выше, p. 252; о причиненном ущербе см.: D. Albright, P. Brannan and C. Walrond, примечание 23 выше; D. E. Sanger, примечание 23 выше.

в работу банковской системы или другие манипуляции, направленные против важнейшей инфраструктуры, даже если это приводит к серьезным экономическим потерям, возможно, все-таки выйдут за рамки понятия вооруженной силы, за пределы ее объекта и цели — воздействие нельзя приравнять к уничтожению, вызываемому физическими средствами. Но нарушение работы такой жизненно важной инфраструктуры, как системы электро- и водоснабжения, которое неизбежно приведет к серьезным трудностям для населения, если продлится в течение долгого времени, даже если и не вызовет гибели людей или повреждений, может тем не менее рассматриваться как применение вооруженной силы. Хотя воздействие не приравнивается к физическому воздействию, оно точно соответствует определению серьезных последствий, защитить от которых гражданское население должно МГП.

Государства, правда, не могут избежать выполнения своих обязательств в соответствии с МГП в силу своего собственного определения деяния. Применение права международных вооруженных конфликтов было отделено от необходимости официальных заявлений много десятилетий назад во избежание такого положения, когда государства могли бы отказываться от защиты этого свода норм. Это четко предусматривает общая статья 2, как поясняется Комментарием к ней МККК:

> «Государство, совершая враждебное действие, направленное против другого государства, может всегда сделать вид, что оно не ведет войну, но просто проводит полицейскую акцию или осуществляет законное право на самооборону. Выражение "вооруженный конфликт" делает выдвижение таких аргументов менее легким»[47].

Тем не менее, хотя и справедливо, что в конкретном инциденте классификация конфликта не зависит от позиции соответствующих государства, практика государств и opinio juris принимают толкование определения «международный вооруженный конфликт», предлагаемое международным правом. Классификация кибернетических конфликтов будет, возможно, точно определяться только будущей практикой государств.

Немеждународные вооруженные конфликты

Если говорить о немеждународных вооруженных конфликтах в кибернетической сфере, основной вопрос будет заключаться в том, как провести различие между преступным поведением и вооруженным конфликтом.

47 Jean Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32. Это вопрос, отличающийся от вопроса об *animus belligerendi*: отдельные действия иногда не считаются вооруженным конфликтом не потому, что они не достигают определенного уровня напряженности, но, скорее, потому что в них нет animus belligerendi, например в случайных вторжениях через границу; см.: *UK Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004, para. 3.3.1, доступно по адресу: http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

Нередко можно услышать или прочитать, что действия хакеров или других групп, включая такие группы, как Anonymous или Wikileaks, называют «войной»[48]. Конечно, в таких заявлениях не обязательно имеется в виду вооруженный конфликт или, точнее, немеждународный вооруженный конфликт в правовом смысле слова. Тем не менее стоит уточнить параметры для квалификации ситуации в качестве немеждународного вооруженного конфликта.

В отсутствие договорного определения практика государств и доктрина вывели определение немеждународного вооруженного конфликта, которое МТБЮ суммировал следующим образом: немеждународный вооруженный конфликт имеет место «всегда, когда… происходит длительное вооруженное насилие в отношениях между правительственными властями и организованными вооруженными группами или между такими группами в границах государства»[49]. Требование «длительное» со временем было включено в то требование, что насилие должно достичь определенной интенсивности. Таким образом, два критерия определяют наличие немеждународного вооруженного конфликта: вооруженное противостояние должно достичь определенного минимального уровня интенсивности и стороны в конфликте должны продемонстрировать минимальный уровень организации[50].

Организованные вооруженные группы

Для того чтобы группа считалась организованной вооруженной группой, которая может быть стороной в конфликте по смыслу МГП, необходимо, чтобы она обладала уровнем организации, который позволит ей осуществлять непрерывные военные действия и соблюдать МГП. К соответствующим признакам относятся наличие организационной схемы, определяющей структуру командования, полномочия для начала операций, в которых участвуют различные подразделения, способность вербовать новых комбатантов и проводить их подготовку и наличие правил внутреннего распорядка[51].

48 См., например: Mark Townsend et al., 'WikiLeaks backlash: The first global cyber war has begun, claim hackers', in *The Observer*, 11 September 2010, доступно по адресу: http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war; Timothy Karr, 'Anonymous declares cyberwar against "the system"', in *The Huffington Post*, 3 June 2011, доступно по адресу: http://www.huffingtonpost.com/timothy-karr/anonymousdeclares-cyberw_b_870757.html.

49 ICTY, *Prosecutor* v. *Tadic*, para. 70 (см. примечание 29 выше).

50 Существует два типа немеждународных вооруженных конфликтов. Все немеждународные вооруженные конфликты регулируются общей статьей 3 Женевских конвенций, кроме того, положения Дополнительного протокола II применяются к немеждународным вооруженным конфликтам, «происходящим на территории какой-либо Высокой Договаривающейся Стороны между ее вооруженными силами и антиправительственными вооруженными силами или другими организованными вооруженными группами, которые, находясь под ответственным командованием, осуществляют такой контроль над частью ее территории, который позволяет им осуществлять непрерывные и согласованные военные действия и применять настоящий Протокол» (ДП II, статья 1 (1).

51 Обзор факторов, принимаемых во внимание МТБЮ в его судебной практике, см.: ICTY, *Prosecutor* v. *Boskoski*, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, paras 199—203.См. также: ICTY, *Prosecutor* v. *Limaj*, IT-03-66-T, Trial Chamber Judgement of 30 November 2005, paras 94—134; ICTY, *Prosecutor* v. *Haradinaj*, IT-04-84-T, Trial Chamber Judgement of 3 April 2008, para. 60.

Хотя группе не обязательно иметь уровень организации, как у правительственных вооруженных сил, она должна обладать определенной иерархией и уровнем дисциплины и способностью выполнять основные обязательства в соответствии с МГП[52].

Что касается хакерских и других аналогичных групп, вопрос, который возникает, заключается в том, могут ли группы, которые организованы исключительно в интернете, представлять собой вооруженные группы по смыслу МГП. Как говорит Михель Шмитт:

> «члены виртуальных организаций, возможно, никогда не встречались и даже не знают настоящие имена друг друга. Тем не менее такие группы могут действовать скоординированным образом против правительства (или организованной вооруженной группы), получать приказы от виртуального руководства и быть высоко организованными. Например, один из состава группы может получить задание определить уязвимые места в системе наведения на цель, второй может разработать вредоносную программу для удара по этим слабым местам, третий может осуществить операции, а четвертый — обеспечить кибернетическую защиту от контрнападений»[53].

Однако требование, чтобы организованная вооруженная группа имела некоторое ответственное командование в какой-либо форме и обладала способностью соблюдать МГП, как представляется, должно воспрепятствовать квалификации виртуально организованных групп в качестве организованных вооруженных групп; было бы трудно, например, создать эффективную дисциплинарную систему в рамках такой группы для обеспечения соблюдения МГП[54]. Другими словами, маловероятно, что группы хакеров или группы, которые связаны просто виртуальными сообщениями, будут иметь организацию или командную (и дисциплинарную) структуру, требуемую для того, чтобы быть стороной в конфликте[55].

Интенсивность

Кибернетические операции, проведенные в контексте существующего немеждународного конфликта или в связи с ним, регулируются МГП. Встает вопрос, хотя он, возможно, покажется в настоящий момент несколько футуристическим: может ли быть достигнут требуемый для существования немеждународного вооруженного конфликта уровень интенсивности, если применяются только кибернетические средства? (Предполагается, что в конфликте есть две или более стороны.)

52 ICTY, *Prosecutor* v. *Boskoski*, *ibid*., para. 202.
53 M. N. Schmitt, p. 256, см. примечание 28 выше.
54 *Ibid.*, p. 257.
55 См. рассуждения в Таллиннском руководстве о различных типах групп, которые могут быть рассмотрены. Примечание 27 выше, Commentary on Rule 23, paras 13—15.

В отличие от вопроса о классификации международного вооруженного конфликта все согласны с тем, что немеждународный вооруженный конфликт существует только тогда, когда военные действия достигают определенного уровня интенсивности. МТБЮ указал на целый ряд факторов, которые должны быть приняты во внимание при оценке интенсивности конфликта, например коллективный характер военных действий, использование военной силы, а не просто сил полиции, серьезность нападений и увеличение числа вооруженных столкновений, их распространение по территории и во временном отношении, распределение оружия среди обеих сторон в конфликте, число гражданских лиц, вынужденных бежать из зон конфликта, типы используемого оружия, в частности применение тяжелого оружия, степень разрушений и число жертв, вызванных обстрелами и боями[56]. Будет ли необходимый порог интенсивности достигнут только в результате операций в кибернетическом пространстве?

И снова надо начать со сравнения тяжести последствий с последствиями кинетических операций. Нет причин, по которым операции в кибернетическом пространстве не могут иметь те же серьезные последствия, что и кинетические операции, например если они были использованы для открытия шлюзов дамб или для того, чтобы вызвать столкновение самолетов или поездов. В таких обстоятельствах и если это не случается спорадически, может быть достигнут порог для существования немеждународного вооруженного конфликта.

Однако операции в кибернетическом пространстве сами по себе не приведут ко многим из тех последствий, что перечислены в качестве показателей интенсивности насилия (вооруженные столкновения, использование военной силы, тяжелых орудий и т. д.). Это, скорее всего, будут только последствия операций в кибернетическом пространстве, которые достаточно серьезны для того, чтобы достичь необходимого уровня интенсивности, как, например, крупномасштабные разрушения или катастрофические последствия для значительной части населения из-за повторяющихся нападений.

Выводы

Вероятно, не вызовет возражений утверждение, что МГП будет применяться к операциям в кибернетическом пространстве, которые станут осуществляться в рамках протекающего международного или немеждународного вооруженного конфликта наряду с кинетическими операциями. В отсутствие кинетических операций «чисто» кибернетическая война не исключается в теории, но предстоит еще увидеть, насколько многочисленными окажутся случаи такой войны на практике в ближайшем будущем.

В частности, остается неясным, в каком направлении будет развиваться практика государств. Принимая во внимание нежелание государств

56 См., например: ICTY, *Prosecutor* v. *Limaj*, paras 135—170, примечание 51 выше; ICTY, *Prosecutor* v. *Haradinaj*, para. 49, примечание 51 выше; ICTY, *Prosecutor* v. *Boskoski*, paras 177—178, примечание 51 выше.

признавать ситуации вооруженного конфликта, особенно немеждународного вооруженного конфликта, можно предположить, что будут делаться попытки уклониться от обсуждения вопроса о наличии вооруженного конфликта. И это не только из-за вероятной анонимности многих нападений на компьютерные сети и практических проблем с присвоением действий, но и в силу того факта, что большая часть ситуаций может не представлять собой крайние случаи физического уничтожения, вызываемого нападениями на компьютерные сети, а быть скорее бескровными манипуляциями инфраструктурой на довольно низком уровне. Государства могут рассматривать такие ситуации с точки зрения правоприменительной практики и уголовного права, а не как ситуации, регулируемые правовой системой, применимой к вооруженным конфликтам.

Применение норм, касающихся ведения военных действий

Если операции в кибернетическом пространстве осуществляются в контексте вооруженного конфликта, они регулируются нормами МГП, в частности нормами, касающимися ведения военных действий. Тот факт, что кибернетическое оружие использует новые технологии, не ставит сам по себе под вопрос применимость к нему МГП.

Однако кибернетическая война порождает серьезные проблемы, касающиеся самих исходных предпосылок, на которых основывается МГП, в частности это проведение различия — и фактическая возможность проводить различие — между военными и гражданскими объектами. Таким образом, вопрос заключается не столько в том, применимы ли к кибернетической войне нормы ведения военных действий, сколько в том, как они применимы — как их следует толковать, чтобы они имели смысл в этой новой сфере.

Какие действия регулируются нормами ведения военных действий?

Прежде чем обратиться к нормам ведения военных действий, особенно к принципам проведения различия, соразмерности и принятия мер предосторожности, важно рассмотреть вопрос, который в свое время был предметом дебатов, а именно какой вид поведения, в частности какой вид операций в кибернетическом пространстве, приводит в действие нормы ведения военных действий.

Вопрос крайне важен. Только если определенная операция в кибернетическом пространстве попадает в сферу действия принципа проведения различия, запрещается делать объектом непосредственного нападения гражданскую инфраструктуру; а если она направлена против военной цели, побочное воздействие на гражданскую инфраструктуру должно приниматься во внимание, если операция попадает в сферу действия принципа соразмерности.

Причина, по которой эти дебаты начались, такова: кибернетическое пространство отличается от традиционных театров войны тем, что средства и методы нападения не связаны с традиционной кинетической силой, обычно понимаемой как насилие. Таким образом, целый ряд операций в кибернетическом пространстве может значительно воздействовать на объект нападения, нарушив его функционирование, но не причинив физического повреждения, что произошло бы в ходе традиционной войны.

Поэтому для гражданского населения крайне важно, чтобы этот вопрос был прояснен. В зависимости от того, узко или широко рассматривать типы операций в кибернетическом пространстве, которые попадают в сферу регулирования норм ведения военных действий, следующие из них могут быть запрещены или считаться законными в контексте вооруженных конфликтов:

- нарушение функционирования гражданской электроэнергетической системы или системы очистки воды (без их физического повреждения);
- нападение на банковскую интернет-систему, что лишит миллионы клиентов банков возможности доступа к банковским услугам[57];
- нарушение функционирования веб-сайта биржи государства-противника без воздействия на ее торговые функции[58];
- нападение на систему онлайн-резервирования частной авиакомпании, чтобы создать трудности для гражданского населения;
- блокирование веб-сайтов агентств «Аль-Джазира» или Би-би-си, потому что они содержат информацию, которая полезна для противника;
- блокирование доступа к Facebook для всего населения, потому что там содержатся пропагандистские материалы повстанцев;
- отключение интернета и мобильных телефонов в конкретном регионе, чтобы пресечь пропаганду, ведущуюся противником[59].

В связи с этим возникают два вопроса: во-первых, применяются ли основные нормы МГП, касающиеся ведения военных действий, то есть принципы проведения различия, соразмерности и мер предосторожности, только к операциям, которые являются нападениями по смыслу МГП, или они применяются к военным операциям в более общем плане?

57 Так случилось в Эстонии в мае 2007 г; см.: Larry Greenemeier, 'Estonian attacks raise concern over cyber "nuclear winter"', in *Information Week*, 24 May 2007, доступно по адресу: http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774.

58 См., например: Yolande Knell, 'New cyber attack hits Israeli stock exchange and airline', in *BBC News*, 16 January 2012, доступно по адресу: http://www.bbc.co.uk/news/world-16577184.

59 В Египте правительство заблокировало интернет и сеть мобильных телефонов на пять дней, чтобы пресечь протесты: 'Internet blackouts: reaching for the kill switch', in *The Economist*, 10 February 2011, доступно по адресу: http://www.economist.com/node/18112043. Аналогичные меры были приняты правительством Китая в ответ на волнения в Синьсяне и в Тибете: Tania Branigan, 'China cracks down on text messaging in Xinjiang', in *The Guardian*, 29 February 2010, доступно по адресуt: http://www.guardian.co.uk/world/2010/jan/29/xinjiangchina, и Tania Branigan, 'China cut off internet in area of Tibetan unrest', in *The Guardian*, 3 February 2012, доступно по адресу: http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

Во-вторых, какие операции в кибернетическом пространстве являются нападениями по смыслу МГП?

Когда начинают применять нормы, касающиеся ведения военных действий: во время «нападений», «военных операций», «военных действий»?

Что касается первого вопроса, разница во взглядах возникает из-за общей нормы ведения военных действий, как она сформулирована в статьях 48 и последующих Дополнительного протокола I и в значительной мере признана в качестве обычного права. Статья 48 Дополнительного протокола I требует:

> «Для обеспечения уважения и защиты гражданского населения и гражданских объектов стороны, находящиеся в конфликте, должны всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими объектами и военными объектами и соответственно *направлять свои действия* только против военных объектов» (курсив автора).

Последующие нормы, касающиеся ведения военных действий, сформулированы далее в основном как более конкретные ограничения на нападения. Например, статья 51 Дополнительного протокола I, постановив в своем первом пункте, что «гражданское население и отдельные гражданские лица пользуются общей защитой от опасностей, возникающих в связи с военными операциями», заявляет далее, что «гражданское население как таковое, а также отдельные гражданские лица не должны являться объектом нападений» и что «нападения неизбирательного характера запрещаются». Нападение в нарушение принципа соразмерности определено в статье 51 (5) (b) Дополнительного протокола I как «нападение, которое, как можно ожидать, попутно повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить». Статья 51 (6) запрещает «нападения на гражданское население или на отдельных гражданских лиц в порядке репрессалий». Статья 52 (2) устанавливает, что «нападения должны строго ограничиваться военными объектами». Принцип принятия мер предосторожности в статье 57 требует, чтобы в отношении нападений принимался целый ряд мер предосторожности. Есть много других статей, в которых употребляется термин «нападение», когда ограничиваются права воюющих[60].

Таким образом, первый аргумент сосредоточен на вопросе о том, ограничиваются ли нормы ведения военных действий теми враждебными

60 См., например: ДП I, статьи 12, 54—56.

актами, которые составляют нападения (как это определено в статье 49 Дополнительного протокола I), или же они применяются к более широкому диапазону военных действий. В общем, были выдвинуты три точки зрения.

Большинство авторов считают, что структура и формулировки Дополнительного протокола I демонстрируют, что, хотя статья 48 устанавливает общий принцип защиты гражданского населения, этот общий принцип «вводится в действие» в последующих статьях. Только те операции в кибернетическом пространстве, которые являются нападениями, подпадают под действие принципов проведения различия, соразмерности и предосторожности[61]. Аргумент, выдвигаемый Михелем Шмиттом в этом отношении, заключается в том, что некоторые военные действия могут быть преднамеренно направлены против гражданских лиц, например психологические операции, — и это, по его мнению, показывает, что не все военные операции находятся в сфере действия принципа проведения различия[62].

Нильс Мельцер считает, что дебаты о понятии «нападение» не предоставляют удовлетворительного ответа на вопрос, поскольку нормы ведения военных действий применяются не только к нападениям в строгом смысле слова, но и к другим операциям. По его мнению:

> «если точно понимать, то применимость ограничений, налагаемых МГП на ведение военных действий, к операциям в кибернетическом пространстве зависит не от того, квалифицируются ли данные операции как “нападения” (то есть основная форма ведения военных действий), но от того, являются ли они частью “военных действий” по смыслу МГП»[63].

По мнению Мельцера, операции в кибернетическом пространстве, направленные на то, чтобы причинить вред противнику, либо вызвав гибель людей, ранения и разрушения, либо непосредственным образом неблагоприятно повлияв на военные операции или военный потенциал, должны считаться военными действиями[64]. Например, операции в кибернетическом пространстве, цель которых заключается в том, чтобы нарушить функционирование или вывести из строя управляемые компьютерами радары или системы оружия, сети материально-технического снабжения или коммуникации противника, будут квалифицироваться как военные действия, даже если они не причиняют физического ущерба. Однако операции в кибернетическом пространстве, осуществляемые с общей целью сбора разведывательных данных, не подпадают под определение военных действий.

61 M. N. Schmitt, ‘Cyber operations and the jus in bello: key issues’, in *Naval War College International Law Studies*, Vol. 87, 2011, p. 91; Robin Geiss and Henning Lahmann, ‘Cyber warfare: applying the principle of distinction in an interconnected space’, in *Israeli Law Review*, Vol. 45, No. 3, November 2012, p. 2

62 M. N. Schmitt, *ibid*., p. 91.

63 Melzer, примечание 42 выше.

64 *Ibid*., p. 28.

Что же касается выведения из строя гражданских объектов, не сопровождаемого разрушениями, то Мельцер не приходит к определенному выводу, но указывает на дилемму между принятием слишком ограничительного и слишком разрешительного толкования права[65].

Аргумент Мельцера привлекателен тем, что вводит в действие сам объект и цель норм, касающихся ведения военных действий, а цель эта заключается в том, что «мирные гражданские лица должны оставаться за пределами военных действий, насколько это возможно, и пользоваться общей защитой от опасности, связанной с военными действиями»[66]. Однако это оставляет открытым наиболее критический вопрос, а именно входят ли операции, которые нарушают функционирование гражданской инфраструктуры, в понятие военных действий.

Хизер Хэррисон Диннис утверждает, что запрет на совершение нападений на гражданских лиц и гражданские объекты не ограничивается нападениями[67]. Она указывает на формулировки статьи 48 Дополнительного протокола I и первые предложения статей 51 и 57, чтобы показать, что гражданское население должно пользоваться защитой не только от нападений, но и, в более общем плане, от воздействия военных операций. Таким образом, она утверждает, что принципы проведения различия, соразмерности и принятия мер предосторожности применяются также и к нападениям на компьютерные сети, и такие нападения соответствуют определению военных операций. Для этого «нападение на компьютерные сети должно соотноситься с применением физической силы, но не должно само приводить к таким же разрушительным последствиям»[68].

Несмотря на эти аргументы в пользу расширения типов операций, к которым должны применяться нормы ведения военных действий, совершенно очевидно, что в Дополнительном протоколе I государства все-таки провели различие между общими принципами в соответствующих вводных положениях норм, касающихся проведения различия и мер предосторожности, и конкретными нормами, касающимися нападений, и что они сочли необходимым дать конкретное определение нападениям в статье 49 Протокола. Трудно отойти от этой дихотомии военных действий и нападений.

Тем не менее аргумент Диннис помогает осмыслить тот факт, что статьи 48, 51 и 57 содержат общие положения, которые налагают ограничения на военные действия, а не только на нападения, а иначе их содержание было бы трудно объяснить. Систематическое толкование этих положений означает, что их вводные части имеют значимое содержание и не являются излишними. Кроме того, аргумент, выдвигаемый Михелем Шмиттом, о том,

65 *Ibid*.
66 Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949,* ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, para. 1923 (далее — Комментарий к Дополнительным протоколам).
67 H. H. Dinniss, примечание 42 выше, p. 196—202.
68 *Ibid*., p. 201.

что некоторые операции, например психологические, могут быть направлены против гражданских лиц, а это значит, что некоторые военные действия могут быть направлены против гражданских лиц, основан на неправильном понимании концепции военных операций. Действительно, хотя и справедливо то, что некоторые операции в кибернетическом пространстве, такие как психологические операции, могут быть направлены против гражданского населения, они не являются военными операциями или военными действиями по смыслу, который имелся в виду составителями Протокола. В соответствии с Комментарием МККК термин «действия» (в английском тексте статьи 48 «operations») означает военные действия и относится ко «всем передвижениям и актам, связанным с военными действиями, которые осуществляются вооруженными силами»[69]. Термин «военные операции» в статье 51 описывается как «все передвижения и деятельность, осуществляемые вооруженными силами и связанные с военными действиями»[70]. И в статье 57 это «следует понимать как любые передвижения, маневры и любая другая деятельность, осуществляемая вооруженными силами с боевой целью»[71]. Другими словами, такие операции, как пропаганда, шпионаж или психологические операции, не входят в понятие военных действий или военных операций и поэтому не регулируются принципами проведения различия, соразмерности и предосторожности, даже если они осуществляются вооруженными силами.

Таким образом, в то время как часть содержания статей 51 и 57 Дополнительного протокола I, касающаяся наиболее конкретных вещей, может относиться к специфическим характеристикам нападения, существует весомый аргумент в пользу того, что другие военные действия не могут быть полностью исключены из сферы действия обязательства проводить различие, соблюдать принцип соразмерности и принимать меры предосторожности, поскольку статья 48 и первые предложения статей 51 и 57 были бы тогда излишними. Однако хотя не существует согласия относительно этого вопроса, будет разумным тем не менее внимательнее взглянуть на определение нападения и на то, какие типы операций в кибернетическом пространстве ему соответствуют. Действительно, большинство операций в кибернетическом пространстве в вышеупомянутых примерах соответствуют понятию нападения и оказались бы запрещены, будь они направлены против гражданской инфраструктуры. Таким образом, становится ясно, что в большинстве вышеупомянутых примеров операции являются нападениями, и поэтому вопрос о том, регулируются ли только «нападения» или также «военные действия» и «военные операции» нормами ведения военных действий, имеет чисто академический характер.

69 *Commentary on the Additional Protocols*, para. 1875, см. примечание 68 выше.
70 *Ibid*., para. 1936.
71 *Ibid*., para. 2191.

Что такое нападение?

Как уже было сказано, операции в кибернетическом пространстве отличаются от традиционной войны тем, что средства и методы нападения не связаны с применением традиционной кинетической силы — или того, что обычно называется насилием. И все же нападения определены в статье 49 (1) Дополнительного протокола I (которая отражает обычное МГП) как «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне». По мнению составителей это означало физическое насилие.

Прежде всего следует помнить следующее: основываясь на том, что нападение должно быть актом насилия, все сегодня согласны с тем, что насилие не указывает на средства нападения — обычно имеются в виду только кинетические средства[72]. Военные действия, которые приводят к серьезным последствиям, являются нападениями. Например, не вызывает разногласий тот факт, что применение биологических, химических или радиоактивных веществ является нападением, даже несмотря на то, что нападение не связано с физической силой[73]. Поэтому в течение долгого времени считалось общепринятым, что определяет нападение все же не насильственный характер средств, но серьезность последствий[74]. Таким образом, даже поток данных, передаваемых по кабелям или через спутники, может входить в понятие нападения.

Разногласия касаются последствий операций в кибернетическом пространстве. Речь идет о тех операциях, которые не становятся причиной гибели и ранений людей или физического уничтожения либо повреждения объектов, как это было бы в случае кинетических операций, но, скорее, нарушают функционирование объектов, не причиняя им физического ущерба — как это показано в вышеприведенных примерах. Как они демонстрируют, последствия операций в кибернетическом пространстве не обязательно имеют сильное воздействие — в том смысле, что они не причиняют физического ущерба и не вызывают разрушений. В вышеприведенных примерах последствия в физической сфере будут, самое большее, опосредованными: например, если линия электропередачи не действует, это может привести к прекращению подачи энергии на такие жизненно важные объекты, как, например, больницы. В некоторых случаях последствия ограничены невозможностью установить связь или заниматься коммерческой

72 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 84; M. N. Schmitt, p. 5, см. примечание 61 выше.

73 ICTY, *Prosecutor* v. *Dusko Tadić*, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, paras 120 and 124 (в отношении химического оружия); *Tallinn Manual*, Commentary on Rule 30, para. 3, см. примечание 27 выше; Emily Haslam, 'Information warfare: technological changes and international law', in *Journal of Conflict and Security Law*, Vol. 5, No. 2, 2000, p. 170.

74 *Шмитт, Михель Н.* Электронная война: нападение на компьютерные сети и jus in bello // Международный журнал Красного Креста. Сборник статей. 2002. С. 133; *Tallinn Manual*, Commentary on Rule 30, para. 3, см. примечание 27 выше.

деятельностью, когда, например, нарушено функционирование банковской системы. Могут ли такие операции считаться нападениями по смыслу статьи 49 Дополнительного протокола I?

По отношению к этому вопросу существуют две позиции. Согласно более ранним работам Михеля Шмитта:

> «операция в кибернетическом пространстве, как и любая другая операция, является нападением, если приводит к гибели или ранениям людей, независимо от того, являются они военнослужащими или гражданскими лицами, или к повреждениям и уничтожению объектов, как военных целей, так и гражданских объектов»[75].

Повреждения, согласно этому мнению, означают только физические повреждения. Нападения на компьютерные сети, которые причиняют лишь неудобства или просто временно нарушают работу объектов, не являются нападениями, если они не вызывают страдания людей. Простое нарушение работы объекта, если это не приводит к человеческим страданиям и физическим повреждениям или полной и окончательной утрате возможности использовать данный объект, не является нападением[76].

По мнению Кнута Дёрмана, операции в кибернетическом пространстве также могут быть нападениями, даже если они не приводят к уничтожению объектов. Эта точка зрения основывается на определении военного объекта в статье 52 (2) Дополнительного протокола I, которая устанавливает, что военные объекты, это такие объекты, «полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество». Термин «нейтрализация» позволяет понять, что «не имеет значения, выведен ли объект из строя путем уничтожения или любым другим способом»[77]. Критики отвечают, что определение военных объектов не совсем имеет отношение к делу, поскольку оно прежде всего предполагает нападение и не определяет само нападение[78]. Такие критики не признают, что «нейтрализация» включает «нападение с целью не дать противнику возможность использовать объект, не обязательно уничтожив его»[79]. Это свидетельствует о том, что составители имели в виду не только нападения, которые направлены на

75 M. N. Schmitt, p. 6, см. примечание 61 выше.

76 Сейчас Михель Шмитт придерживается несколько иного мнения и считает, что «уничтожение включает операции, которые, не причиняя физического ущерба, тем не менее "ломают" объект, выводят его из строя, как в случае операций в кибернетическом пространстве, которые делают невозможным работу системы, зависящей от компьютера, если ее не отремонтировать». "'Attack' as a term of art in international law: the cyber operations context', in 2012 *4th International Conference on Cyber Conflict*, C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012, NATO CCD COE Publications, Tallinn, p. 291; см. также: M. N. Schmitt, p. 252, примечание 28 выше

77 K. Dörmann, p. 4, примечание 42 выше.

78 M. N. Schmitt, p. 8, примечание 61 выше.

79 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Dordrecht, 1982, p. 325.

уничтожение или повреждение объектов, но и нападения с целью помешать противнику использовать объект, не уничтожая его. Так, например, система противовоздушной обороны противника может быть нейтрализована на какое-то время посредством операции в кибернетическом пространстве путем вмешательства в работу ее компьютерной системы, не уничтожая и не повреждая ее физическую инфраструктуру[80].

Позднее Таллиннское руководство так определяет кибернетическое нападение: это «операция в кибернетическом пространстве, как наступательного, так и оборонительного характера, которая, как обоснованно ожидается, вызовет ранения и гибель людей или повреждения и уничтожение объектов»[81]. Однако, как показывает комментарий, эксперты не придерживаются единого мнения относительно того, что же точно понимается под «повреждением» объектов и будут ли охватываться этим определением нарушения функционирования объекта и какого типа нарушения[82].

Слабая сторона первой точки зрения заключается в том, что она является слишком ограничительной. Во-первых, абсурдно считать неповрежденным гражданский объект, который выведен из строя, независимо от того, каким это сделано способом. Была ли энергосистема выведена из строя посредством физического повреждения или в результате вмешательства в работу компьютеров, которыми она управляется, — это не может быть разумным критерием. Иное мнение способно привести к выводу, что уничтожение одного дома в результате бомбардировки будет нападением, но выведение из строя энергосети, снабжающей тысячи или миллионы людей, — не будет.

Во-вторых, ссылка на принцип соразмерности указывает на побочный ущерб, от которого нормы ведения военных действий должны защитить гражданских лиц, а именно случайные потери жизни среди гражданского населения, ранения гражданских лиц, ущерб гражданским объектам. Ущерб отличается от уничтожения. Он означает «вред… снижающий ценность или полезность чего-либо»[83]. Таким образом, нарушение функционирования определенных систем путем вмешательства в их компьютерные системы может быть приравнено к ущербу, поскольку уменьшает их полезность. В-третьих, та точка зрения, что критерием служит полная и постоянная утрата функционирования без физического ущерба, не имеет смысла в информационной технологии. Поскольку данные могут всегда быть восстановлены или изменены, не может быть постоянной и полной утраты функциональности объекта, если не будет физического ущерба. Таким образом,

80 По имеющимся сообщениям именно это произошло в сентябре 2007 г., когда Израиль совершил нападение на сирийскую структуру, в которой, как считалось, находилась программа разработки ядерного оружия. Израиль проник в систему противовоздушной обороны Сирии и контролировал ее во время нападения; см.: 'Arab & Israeli cyber-war', in *Day Press News*, 22 September 2009, доступно по адресу: http://www.dp-news.com/en/detail.aspx?articleid=55075.

81 *Tallinn Manual*, Rule 30, см. примечание 27 выше.

82 *Ibid.*, Commentary on Rule 30, paras 10—12

83 *Concise Oxford Dictionary.*

нападение должно также пониматься как включающее такие операции, которые нарушают функционирование объекта без нанесения ему физического ущерба и без его уничтожения, даже если выведение из строя является временным.

И все же слишком широкое толкование термина «нападение» означало бы, что все вмешательства в работу гражданских компьютерных систем можно приравнять к нападениям: нарушение работы электронной почты или социальных сетей, систем резервирования или покупок онлайн и т. д. Приравнивание к нападениям таких нарушений, когда, по сути, нарушается функционирование систем коммуникации, возможно, выходит за границы предполагаемой сферы действия норм ведения военных действий. Эти нормы традиционно имели целью предотвратить ущерб гражданской инфраструктуре, которая существует в физическом мире, а не вмешательство в пропаганду, коммуникацию или экономическую жизнь. В сегодняшнем мире зависимость гражданской жизни от систем коммуникации размывает эти линии и нелегко провести различие между тем, что является «просто» передачей информации, а что выходит за ее пределы.

Существующие нормы МГП, их объект и цель дают целый ряд указаний для проведения различия между операциями, которые можно приравнять к нападениям, и операциями, которые не являются таковыми. Во-первых, как уже сказано, понятие нападения не включает распространение пропаганды, эмбарго или другие нефизические средства психологической или экономической войны[84]. Операции в кибернетическом пространстве, которые эквивалентны шпионажу, распространению пропаганды, эмбарго или другим нефизическим средствам психологической или экономической войны, не включаются в определение нападений.

Во-вторых, МГП не запрещает блокаду или экономические санкции, которые преднамеренно направлены не только против военных, но и против гражданского населения и экономики. Таким образом, термин «нападение» не может включать операции в кибернетическом пространстве, которые были бы равнозначны экономическим санкциям. Это не означает, что такие операции не будут подвергаться ограничениям в соответствии с МГП (таким, как запрет на уничтожение, вывоз или приведение в негодность объектов, необходимых для выживания гражданского населения, или обязательство в отношении пропуска гуманитарной помощи). Однако поскольку они не являются нападениями, в соответствии с МГП не существует запрета осуществлять их против гражданского населения.

В-третьих, нормы, касающиеся ведения военных действий, не имеют целью запретить все операции, которые вмешиваются в работу гражданских систем коммуникации. Например, не все операции типа «отказ в обслуживании»[85], такие как блокирование телевизионного вещания или веб-сайта

84 M. Bothe et al., p. 289, примечание 79 выше.

85 То есть операции в кибернетическом пространстве, которые делают обслуживание компьютерной системой, являвшейся объектом нападения, недоступным для обычных пользователей и клиентов.

университета, будут считаться нападением. Просто создание помех для ведения пропаганды, например, также, наверное, не будет являться нападением. Аналоги подобных операций в физическом мире — глушение радио- и телевизионного вещания — также не считаются нападением по смыслу МГП.

Для того чтобы провести различие между теми операциями, которые можно считать нападениями, и теми, которые ими не являются, иногда выдвигается критерий неудобства[86]. Аргумент — неудобство, такое как нормированное распределение продовольствия, не следует принимать во внимание как побочный ущерб для гражданского населения. Поэтому то, что просто причиняет неудобства, не может приравниваться к нападению. Хотя критерий неудобства и имеет некоторые достоинства, не все могут одинаково понимать, что такое неудобство, если говорить о вмешательстве в кибернетическую технологию и коммуникацию. Например, хотя и возможно согласиться с тем, что нарушение системы резервирования онлайн причиняет просто неудобства, трудно добиться консенсуса относительно таких вопросов, как вмешательство в систему банковских услуг. Еще неизвестно, как такие действия будут рассматриваться в будущем, в частности в практике государств.

Резюме

Подводя итог вышесказанному, сделаем вывод, что операция в кибернетическом пространстве может являться нападением по смыслу МГП, если она приводит к гибели или ранениям людей или физическим разрушениям или повреждениям, но также если она нарушает функционирование объекта, в результате взлома его компьютерной системы. Таким образом, если система противовоздушной обороны выводится из строя посредством операции в кибернетическом пространстве, если операция в кибернетическом пространстве нарушает функционирование сетей электроснабжения или выводит из строя банковскую систему, это эквивалентно нападению. Однако не все операции в кибернетическом пространстве, цель которых заключается в нарушении функционирования инфраструктуры, можно приравнять к нападениям. Если операция направлена не против физической инфраструктуры, зависящей от компьютерной системы, но, по сути, на блокирование коммуникации, это скорее похоже на глушение радиосигналов и телевещания — если, конечно, не является частью нападения, такого, например, как блокирование системы противовоздушной обороны. Разница заключается в том, что в некоторых случаях только коммуникативная функция киберпространства является целью;

86 Михель Н. Шмитт, p. 121–163, см. примечание 74 выше; Program on Humanitarian Policy and Conflict Research at Harvard University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, 2010, Commentary on Article 1(d), para. 7, доступно по адресу: http://www.ihlresearch.org/amw/aboutmanual.php; Michael N. Schmitt, 'Cyber operations in international law: the use of force, collective security, self-defense and armed conflict', in *National Research Council, Proceedings of a Workshop on Deterring Cyber Attacks*, Washington, DC, The National Academies Press, 2010, p. 155.

в других случаях это функционирование объекта вне киберпространства, в физическом мире. В то время как вмешательство в кибернетические системы, которое ведет к нарушению в физическом мире, является нападением, вопрос о вмешательстве в системы коммуникации, такие как системы электронной почты или информационные средства, окончательно не решен.

Принцип проведения различия

Принцип проведения различия требует того, чтобы стороны в конфликте проводили во всякое время различие между гражданскими лицами и комбатантами и между гражданскими объектами и военными объектами[87]. Это, по мнению Международного суда ООН, является кардинальным принципом МГП[88]. Нападения могут быть направлены только против комбатантов или военных объектов. Это означает, что при планировании и осуществлении операций в кибернетическом пространстве единственно разрешенными объектами нападения в соответствии с МГП являются военные объекты, такие как компьютеры или компьютерные системы, которые вносят эффективный вклад в конкретные военные операции. Нападения в кибернетическом пространстве не могут быть направлены против компьютерных систем, используемых на объектах исключительно гражданского характера.

Некоторые дискуссии относительно военных объектов в кибернетическом пространстве вызывают озабоченность с точки зрения защиты гражданского населения. Действительно, представляется, что операции в кибернетическом пространстве могут быть особенно эффективны для поражения определенных гражданских объектов, потому что они дают возможность воюющим получить доступ к отдельным целям, которые были не столь доступны ранее, например к финансовым сетям или сетям, где хранятся медицинские данные[89]. Некоторые авторы заявляли, что кибернетическая война может привести к некоему «расширению перечня объектов нападения»[90] по сравнению с традиционной войной. Кроме того, поскольку операции в кибернетическом пространстве могут вывести из строя объект, не нанося ему физических повреждений, некоторые авторы говорят, что использование операций в кибернетическом пространстве расширяет диапазон законных целей, так как дает возможность осуществить нападение

87 ДП I, статьи 48, 51 и 52; Хенкертс Ж.-М., Досвальд-Бек, Л. Обычное международное гуманитарное право. Т. I: Нормы. М.: МККК, 2006. [Далее — Обычное международное гуманитарное право.] Нормы 1—10.

88 Консультативное заключение Международного суда относительно угрозы ядерным оружием или его применения, 8 июля 1996 г., п. 78.

89 Michael N. Schmitt, 'Ethics and military force: the jus in bello', Carnegie Council for Ethics in International Affairs, 7 January 2002, доступно по адресу: http://www.carnegiecouncil.org/studio/multimedia/20020107/index.html.

90 Это выражение, которое использовал Эрик Тальбот Йенсен: Eric Talbot Jensen, 'Unexpected consequences from knock-on effects: a different standard for computer network operations?', in *American University International Law Review*, Vol. 18, 2002—2003, p. 1149.

с обратимым эффектом на объекты, которые в противном случае были бы запрещенными целями[91]. Высказывалось также мнение, что:

> «потенциально несмертельный характер кибернетического оружия может сделать более неопределенной оценку законности нападения, приводя к более частым нарушениям принципа проведения различия в этой новой форме войны по сравнению с обычной войной»[92].

На этом фоне важно вспомнить нормы МГП, регулирующие нападения на объекты, и рассмотреть целый ряд конкретных правовых проблем, которые могут возникнуть из-за нападений на компьютерные сети.

В соответствии с МГП гражданскими объектами называются все объекты, которые не являются военными объектами[93]. Военные объекты определены в статье 52 (2) Дополнительного протокола I как объекты:

> «которые в силу своего характера, расположения, 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».

В соответствии со статьей 52 (3) Дополнительного протокола I предполагается, что объекты, которые обычно предназначены для гражданских целей, не используются для эффективного вклада в военные действия. Поэтому, например, если какая-то особенно сложная гражданская инфраструктура, такая как большинство химических предприятий, зависит от закрытой компьютерной сети, эта сеть должна считаться гражданской.

Как четко указывает формулировка статьи 52 (2), должна быть тесная связь между потенциальной целью нападения и военными действиями. Термин «военные действия» означает здесь военный потенциал противника. Эта связь устанавливается посредством четырех критериев: характер, расположение, назначение и использование. Характер — это присущее объекту свойство, такое как оружие. Объекты, которые не являются военными по своему характеру, также могут вносить эффективный вклад в военный потенциал в силу их расположения, назначения или использования в данный момент.

В этом отношении необходимо осветить четыре вопроса, которые могут иметь серьезные последствия для гражданской инфраструктуры: самый важный касается того, что большинство международных кибернетических структур являются на практике так называемыми структурами двойного использования; становятся ли военными объектами предприятия,

91 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, 1999, pp. 963 ff.

92 Jeffrey T. G. Kelsey, 'Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare', *in Michigan Law Review*, Vol. 106, 2007—2008, p. 1439.

93 ДП I, статья 52 (1), отражающая обычное международное право; Обычное международное право, примечание 87 выше, норма 9.

производящие аппаратное оборудование и программное обеспечение, используемое военными; определение таких объектов для нападения, которые имеют потенциал для поддержания военных усилий; и правовые последствия использования социальных сетей в военных целях, например для получения информации о целях.

Объекты двойного использования в кибернетическом пространстве

Так называемые объекты двойного использования — термин как таковой не употребляется в положениях МГП — это те объекты, которые используются как для гражданских, так и для военных целей. Поскольку они используются для военных целей, они становятся военными объектами согласно статье 52 (2) Дополнительного протокола I и законными целями для нападения. В качестве примеров нередко приводят элементы гражданской инфраструктуры, которая осуществляет снабжение военных для проведения операций, например электростанции или линии электропередачи.

Согласно мнению, преобладающему в настоящее время, объект не может быть гражданским и военным одновременно. Как только он начинает использоваться для военных действий, он становится полностью военным объектом (за исключением случаев, когда отдельные части остаются гражданскими — например, различные здания больницы)[94]. В отличие от предложения МККК, выдвинутого в 1956 г., которое, кроме чисто военного оборудования и установок, называет гражданские системы связи, транспорт и промышленные предприятия, «имеющие важное военное значение» или «важное значение для ведения войны»[95], сейчас обычно считается, что объект становится военным объектом, даже если его военное использова-

94 *The Commander's Handbook on the Law* of Naval Operations, Department of the Navy/Department of Homeland Security, USA, July 2007, para. 8.3; Tallinn Manual, Commentary on Rule 39, para 1, см. примечание 27 выше.

95 В проекте Правил МККК, касающихся ограничения опасности, грозящей гражданскому населению во время войны (Draft Rules for the Limitation of Danger incurred by the Civilian Population in Time of War), перечень, составленный организацией с помощью военных экспертов и представленный в качестве модели для внесения поправок, таков: «1. Объекты следующих категорий считаются по общему признанию представляющими большое значения для военных целей: … (6) Те линии и средства связи (железнодорожные линии, дороги, мосты, туннели и каналы), которые являются *крайне важными с военной точки зрения*; (7) Установки для радиовещания и телевещательные станции; телефонные и телеграфные станции, имеющие большое военное значение; (8) Отрасли промышленности, имеющие большое значение для ведения войны: а) заводы по производству вооружений… б) предприятия для производства припасов и материалов военного характера… в) фабрики и заводы, составляющие другие производственные центры, имеющие большое значение для ведения войны, такие как металлургические, машиностроительные и химические предприятия, *чей характер и назначение являются по сути своей военными*; г) складские и транспортные помещения, чья основная функция заключается в обслуживании предприятий, перечисленных в п. а–в; д) установки, снабжающие энергией в основном объекты национальной обороны, например тепловые станции, станции, использующие другие виды топлива, атомные станции и предприятия, производящие газ или электричество для военного использования» (курсив автора). См.: *Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War*, ICRC, 1956, доступно по адресу: http://www.icrc.org/ihl/INTRO/420?OpenDocument.

ние является маргинальным по сравнению с его гражданским применением, например если предприятие предоставляет небольшой процент топлива, которое используется в военных действиях, даже если это не является его основным назначением, оно становится военным объектом.

Опасности в кибернетическом пространстве очевидны: практически вся международная киберинфраструктура — компьютеры, роутеры, кабели и спутники — используется для передачи информации как гражданского, так и военного характера[96]. Подводный кабель, по которому передается военная информация, становится военным объектом — из чего следует, что (при условии соблюдения других норм МГП, а именно соразмерности) он может не только оказаться объектом операции в киберпространстве для нарушения военной связи, но и быть уничтоженным. Аналогичным образом сервер, содержащий 5 % военных данных, станет законной целью для нападения. Об этом особенно важно помнить в эру облачных технологий, когда пользователи обычно не знают, на каком сервере хранятся их данные и какие другие данные хранятся на этом сервере. Есть сведения, что приблизительно 98 % правительственной связи США осуществляется через сети, владельцами и операторами которых являются гражданские лица и организации[97].

Опасность того, что любая часть кибернетической инфраструктуры может стать объектом нападения, весьма реальна. Действительно, хотя при определенных обстоятельствах государства могут попытаться вывести из строя очень специфические функции военной инфраструктуры противника, тот факт, что все кибернетическое пространство используется для военных операций, означает, что в любом вооруженном конфликте важно будет в стратегических целях разрушить коммуникационные сети противника и помешать его доступу в киберпространство. Это будет означать недопущение противника к важнейшим маршрутам в киберпространстве, разрушение его роутеров и недоступность главных коммуникационных узлов, а не просто нападение на конкретные компьютерные системы военной инфраструктуры[98]. В отличие от естественных театров войны, таких как суша или воздушное пространство, созданное человеком кибернетическое поле боя означает, что воюющие сосредоточат внимание не только на передвижении оружия, но и на самих маршрутах[99]. Например, в воздушном пространстве только летательный аппарат считается военным объектом; однако в кибернетической войне физическая инфраструктура, через которую проходит кибернетическое оружие (враждебный программный код), квалифицируется как военных объект.

Последствия такой ситуации в гуманитарном плане оказывают сильное влияние на возможность обеспечить защиту гражданскому населению.

96 См. также: R. Geiss and H. Lahmann, p. 3, примечание 61 выше

97 Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks', in *Texas Law Review,* Vol. 88, 2010, p. 1534.

98 US Department of Defense, *Quadrennial Defence Review Report,* February 2010, pp. 37—38, доступно по адресу: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

99 R. Geiss and H. Lahmann, p. 9, см. примечание 61 выше.

В мире, в котором большая часть гражданской инфраструктуры, гражданские линии связи, финансовые операции, экономика и торговля зависят от международной кибернетической структуры, становится слишком легко для сторон в конфликте разрушить эту инфраструктуру. Нет необходимости говорить, что банковская сеть используется для военных целей или что линии электропередачи имеют двойное назначение. Выведение из строя основных кабелей, узлов, роутеров или спутников, от которых зависят эти системы, почти всегда можно будет оправдать тем фактом, что эти маршруты используются для передачи военной информации и поэтому являются военными объектами.

В Таллиннском руководстве говорится:

> «Обстоятельства, при которых интернет в полном объеме может стать объектом нападения, столь маловероятны, что в настоящее время это делает такую возможность чисто теоретической. Поэтому Международная группа экспертов пришла к выводу, что и с юридической точки зрения, и практически почти любое нападение на интернет должно быть ограничено его определенными дискретными сегментами»[100].

В Руководстве также упоминаются принципы соразмерности и принятия мер предосторожности, которые необходимо соблюдать, если нападение совершается на интернет или его значительные части. Однако если это и может показаться на первый взгляд утешительным, остается проблема, заключающаяся в том, что независимо от того, допустимо ли превращать в объект нападения интернет в полном объеме, любой из его сегментов может стать объектом нападения, если он используется для военных целей и его уничтожение или нейтрализация дают определенное военное преимущество (опять же при соблюдении принципов соразмерности и принятия мер предосторожности).

Более того, кибернетическое пространство устойчиво к внешнему воздействию в том смысле, что, если для передачи информации заблокирован какой-то один канал, существует множество маршрутов и альтернатив, и информация обычно может быть передана иным способом. В Таллиннском руководстве сказано:

> «Операции в кибернетическом пространстве ставят в этом отношении совершенно уникальную проблему. Давайте рассмотрим сеть, которая используется как для военных, так и для гражданских целей. Возможность определить, по какой части сети передаются военные сообщения, а по какой — сообщения гражданские, весьма маловероятна. В таких случаях вся сеть (или по крайней мере те ее части, которые, как можно с достаточными основаниями предположить, используются для передачи) является военным объектом»[101].

100 *Tallinn Manual*, Commentary on Rule 39, para 5, примечание 27 выше.
101 *Ibid*., Commentary on Rule 39, para 3.

Последствием этого может быть то, что при некоторых обстоятельствах почти все части интернета могут считаться военными объектами, потому что являются возможными маршрутами для передачи военной информации.

Уже и в физическом мире преобладающее широкое понимание объектов двойного использования как военных объектов создает проблемы[102]. В кибернетическом пространстве последствия могут усугубляться до крайности, если не остается ничего гражданского, и основная норма, в силу которой гражданское население пользуется общей защитой от опасностей, возникающих в результате военных операций, оказывается практически лишенной содержания, и соблюдаются только принципы соразмерности и предосторожности.

И последнее: если бóльшая часть кибернетической инфраструктуры в мире имеет характер двойного использования и может считаться военным объектом, это ставит важнейший вопрос о географических границах вооруженного конфликта. В кибернетическом пространстве действительно нет границ, и на компьютерные системы можно совершить нападение (дистанционно) из любого места, в их работу можно вмешаться, трансформировать их в средства ведения войны и военные объекты. Следует помнить, что последствием будет не только то, что такие компьютеры могут стать объектом ответного нападения со стороны компьютерных систем, которые уже оказались объектом нападения. Теоретически, будучи военными объектами, они могут быть уничтожены и кинетическими средствами. Например, сеть ботнет может быть использована для осуществления нападения, уничтожающего кибернетическую инфраструктуру противника. Для проведения такой операции сторона в конфликте, осуществляющая нападение, будет дистанционно управлять тысячами или миллионами компьютеров по всему миру, которые будут передавать вредоносные программы на компьютеры, которые являются объектом нападения. Если такая зомби-сеть будет связана со всеми миллионами компьютеров, которые она использует по всему миру и которые определены в качестве военных объектов, и если, следовательно, нападение на них допустимо, результатом может быть что-то вреде тотальной кибернетической войны. Логический вывод о том, что все эти компьютеры по всему миру становятся военными целями, будет противоречить самим основам права нейтралитета в международных вооруженных конфликтах (и в большей степени лежащей в его основе посылке, что необходимо щадить третьи стороны и их жителей, ограждая их от воздействия военных действий) или географическим пределам поля боя во время

102 См. также: Marco Sassòli, 'Legitimate targets of attacks under international humanitarian law', Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, 27—29 January 2003, HPCR, 2003, pp. 3—6, доступно по адресу : http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf; William M. Arkin, 'Cyber warfare and the environment', in *Vermont Law Review*, Vol. 25, 2001, p. 780, в работе описываются последствия воздушного нападения в 1991 г. на сети электроснабжения в Ираке, что повлияло не только на электроснабжение гражданского населения, но и на систему водоснабжения, очистки и канализации, а также на инфраструктуру здравоохранения; R. Geiss and H. Lahmann, p. 16, примечание 61 выше.

немеждународных вооруженных конфликтов[103]. Во время международных вооруженных конфликтов право нейтралитета налагает определенные ограничения на право пострадавшего от нападения государства вести оборону, нападая на инфраструктуру нейтральной территории[104]. Во-первых, государство, на которое совершено нападение, должно уведомить нейтральное государство и предоставить ему разумное время для прекращения нарушений; во-вторых, государство, на которое совершено нападение, может принять меры для прекращения нарушения нейтралитета, только если это нарушение представляет собой серьезную и прямую угрозу его безопасности и только если не существует никаких других практически возможных и своевременных альтернатив для ответа на угрозу. Эти ограничения достаточно широки, и для того, чтобы иметь действительно защитную силу для гражданского населения нейтрального государства, они должны, по-видимому, толковаться довольно узко. Во время немеждународных вооруженных конфликтов право нейтралитета не применяется. Однако географические границы поля сражения в немеждународных вооруженных конфликтах будут абсолютно уничтожены, если считать, что вооруженный конфликт имеет место везде, где компьютер, кабель или узел используются в военных целях (и поэтому представляют собой военные объекты).

Одним словом, становится очевидно, что в кибернетическом пространстве принцип проведения различия, как представляется, мало что обещает в плане защиты гражданской кибернетической инфраструктуры и всей гражданской инфраструктуры, которая от нее зависит. В таких ситуациях основной защитой для гражданской инфраструктуры будет принцип соразмерности — о нем речь пойдет ниже[105].

Проблема, заключающаяся в том, что в кибернетическом пространстве бóльшая часть инфраструктуры имеет двойное использование, вызывает, конечно, сильнейшую озабоченность, и другие вопросы представляются менее неотложными. Некоторые из них будут тем не менее рассматриваться в следующих разделах.

103 Границы поля боя во время немеждународных вооруженных конфликтов являются спорным вопросом, который выходит за рамки настоящей статьи, но трудности, обусловленные кибернетической войной, кажутся в связи с этим почти непреодолимыми. О точке зрения МККК см.: *Report on International Humanitarian Law and the challenges of contemporary armed conflicts*, 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November — 1 December 2011, Report prepared by the ICRC, October 2011, pp. 21—22; о географических пределах в кибернетической войне см.: *Tallinn Manual*, Commentary on Rule 21, см. примечание 27 выше.

104 Они вытекают из статьи 22 Руководства Сан-Ремо по международному праву, применимому к вооруженным конфликтам на море, от 12 июня 1994 г., на русском языке см.: Международное право: Ведение военных действий: Сборник Гаагских конвенций и иных соглашений. М.: МККК. На английском языке доступно по адресу: http://www.icrc.org/IHL.nsf/52d68d14de6160e0c12563da005fdb1b/7694fe2016f347e1c125641f002d49ce!OpenDocument.

105 *Commentary on HPCR Manual on Air and Missile Warfare*, примечание 86 выше, Commentary on Rule 22 (d), para. 7; *Tallinn Manual*, Commentary on Rule 39, para. 2, см. примечание 27 выше; E. T. Jensen, p. 1157, см. примечание 90 выше.

IT-корпорации, продукция которых используется для военных действий

Поскольку аппаратное оборудование и программное обеспечение используются для значительной части военного оборудования, IT-корпорации могут рассматриваться как «военные объекты, оказывающие поддержку военному усилию»[106] наравне с предприятиями, производящими боевую технику. Это, вероятно, будет означать, что целый ряд IT-корпораций во всем мире станут законными военными объектами нападения, поскольку многие из них, скорее всего, производят какую-то часть информационной инфраструктуры для военных[107]. Эрик Тальбот Йенсен, например, задает вопрос: будет ли корпорация Microsoft законной целью «на основании той поддержки, которую она оказывает военным усилиям США, облегчая им военные операции»? По его мнению, «тот факт, что корпорация и ее штаб-квартира предлагают продукт, который военные считают важнейшим для своего функционирования, а также услуги для потребителей этого продукта, может являться достаточным для вывода, что она является объектом двойного использования», но он сомневается в том, что определенное военное преимущество будет достигнуто таким нападением[108].

Приведенный пример демонстрирует, что сравнение с предприятием, производящим военное оборудование, не следует слишком расширять. Соответствующий критерий, согласно статье 52 (2) Дополнительного протокола I, таков: объект должен по своему использованию вносить эффективный вклад в военные действия.

Во-первых, корпорации как таковые являются не физическими объектами, а юридическими лицами, и поэтому вопрос будет заключаться в том, станут ли какие-либо места их расположения (то есть здания) военными объектами. Во-вторых, существует разница между оружием и информационными инструментами. Системы оружия являются по своей природе военными объектами, а базовые информационные системы — нет. Таким образом, придется проводить различие между предприятиями, которые фактически разрабатывают то, что можно назвать кибернетическим оружием, то есть конкретные коды/протоколы, которые будут использоваться для конкретного нападения на компьютерную сеть (так, например, объект, где создается конкретный вирус, подобный Stuxnet), и теми, которые

106 M. N. Schmitt, p. 8ff, см. примечание 61 выше.

107 Сообщается, что Министерство обороны США будет с готовностью сотрудничать с организациями, которые хотят предложить новые технологии для ведения кибернетической войны: S. Shane, примечание 3 выше.

108 E. T. Jensen, pp. 1160, 1168, см. примечание 90 выше; см. также: E. T. Jensen, p. 1544, примечание 97 выше: «…если гражданская компьютерная компания производит и обслуживает правительственные кибернетические системы или оказывает им поддержку, представляется очевидным, что противник может считать, что эта компания удовлетворяет условиям статьи 52 и может стать объектом нападения».

просто предоставляют военным базовые информационные материалы, не сильно отличающиеся от, скажем, продовольственных припасов[109].

Способность вести войну и поддержание военного потенциала

В кибернетической войне, где соблазн превратить гражданскую инфраструктуру в объект нападения, вероятно, больше, нежели во время традиционной войны, важно помнить: для того чтобы гражданский объект стал военным объектом, его вклад в военные действия должен быть направлен на фактические возможности стороны в конфликте вести войну. Если объект просто вносит вклад в поддержание военного потенциала стороны в конфликте (ее общего военного потенциала), его нельзя квалифицировать как военный объект.

В Наставлении США по праву военно-морских операций для командиров выражение «вносят эффективный вклад в военные действия» из статьи 52 (2) Дополнительного протокола I было расширено и заменено на формулировку «эффективный вклад в способность противника вести военные действия и поддерживать свой военный потенциал»[110]. Такая установка направлена в основном против экономических объектов, которые могут косвенно поддерживать или укреплять военный потенциал противника[111]. В проведенной в 1999 г. оценке права Юридическим советом Министерства обороны США касательно операций в кибернетическом пространстве, имеется следующая формулировка:

> «Чисто гражданские инфраструктуры не должны подвергаться нападению, если силы нападающей стороны не могут продемонстрировать, что определенное военное преимущество ожидается от этого нападения. …В ходе длительного вооруженного конфликта ущерб экономике противника и его способности вести научно-исследовательские и опытно-конструкторские работы может значительно подорвать его военные усилия, но в кратковременном и ограниченном конфликте может быть

109 Составители Таллиннского руководства также не пришли к определенному выводу по этому вопросу: «К трудному случаю относится предприятие, производящее предметы, которые не имеют конкретного военного назначения, но которые тем не менее часто используются в военных целях. Хотя все эксперты согласны с тем, что ответ на вопрос о том, можно ли квалифицировать такое предприятие в качестве военного объекта, зависит от масштаба и значимости военных закупок, Группа не смогла прийти к определенному выводу относительно точного порога».

110 *The Commander's Handbook on the Law of Naval Operations*, para. 8.2, примечание 94 выше.

111 M. N. Schmitt, 'Fault lines in the law of attack', in S. Breau and A. Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law*, British Institute of International and Comparative Law, London, 2006, pp. 277–307. Логическое обоснование такого подхода см., например: Charles J. Dunlap, 'The end of innocence, rethinking noncombatancy in the post-Kosovo era', in *Strategic Review*, Vol. 28, Summer 2000, p. 9; Jeanne M. Meyer, 'Tearing down the façade: a critical look at current law on targeting the will of the enemy and Air Force doctrine', in *Air Force Law Review*, Vol. 51, 2001, p. 143; см. J. T. G. Kelsey, примечание 92 выше, p. 1447, Дж. Т. Кесли выступает за новое определение военного объекта, которое должно включить конкретные гражданские инфраструктуры и службы.

трудно определить любое ожидаемое военное преимущество, получаемое от нападения на экономические объекты»[112].

Такие подходы игнорируют правовые ограничения, налагаемые МГП. Причинять ущерб гражданскому хозяйству противника, его способности вести научно-исследовательские и опытно-конструкторские работы гражданского характера само по себе никогда не разрешается МГП, независимо от предполагаемого военного преимущества и независимо от продолжительности конфликта. В противном случае у войны не будет практически никаких ограничений, поскольку вся экономика страны может рассматриваться как поддерживающая военный потенциал[113]. Особенно важно помнить об этом в контексте кибернетической войны и указать на возможные ужасающие последствия широкого определения военных объектов для гражданского населения.

Средства массовой информации и социальные сети

Таллиннское руководство затрагивает трудный вопрос о социальных сетях, которые используются в военных целях[114]:

> «Недавние конфликты высветили проблему использования социальных сетей в военных целях. Например, Facebook использовалась для организации операций вооруженного сопротивления, а Twitter — для передачи информации военного характера. Здесь необходимы три предупредительных сигнала. Во-первых, следует помнить, что эта норма [устанавливающая, что объект, используемый как для гражданских, так и военных целей, является военным объектом] применяется без ущерба для нормы соразмерности и требования о принятии мер предосторожности при нападении… Во-вторых, вопрос о законности операций в кибернетическом пространстве, направленных против социальных сетей, зависит от того, достигают ли такие операции уровня нападения. Если нет,

112 Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 7, доступно по адресу: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/ dod-io-legal.pdf. Позиция США, отраженная в последнем Докладе Генерального секретаря, является по крайней мере неоднозначной: в ней утверждается, что принципы jus in bello «запрещают нападения на чисто гражданскую инфраструктуру, сбой работы или разрушение которой не приведет к достижению значимых военных преимуществ». Если имеется в виду, что нападения на чисто гражданскую инфраструктуру будет разрешено в том случае, когда ее разрушение или выведение из строя принесет значительно военное преимущество, это будет противоречить МГП, которое никогда не разрешает нападения на исключительно гражданские объекты (Доклад Генерального секретаря, 15 июля 2011 г. Док. ООН A/66/152, с. 23).

113 M. Sassòli, примечание 102 выше; Stephan Oeter, 'Means and methods of combat', in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, para. 442.5.

114 Сообщалось, например, что НАТО признало, что социальные сети, такие как Twitter, Facebook и YouTube, помогали им в определении целей в Ливии после того, как данные проверялись через другие источники: Graeme Smith, 'How social media users are helping NATO fight Gadhafi in Libya', in *The Globe and Mail*, 14 June 2011; Tim Bradshaw and James Blitz, 'NATO draws on Twitter for Libya strikes', in *The Washington Post*, 16 June 2011.

> то вопрос о квалификации объекта в качестве военного является чисто теоретическим… В-третьих, это не означает, что Facebook или Twitter как таковые могут становиться объектами нападения; нападать можно только на те их компоненты, которые используются для военных целей [если при нападении выполняются другие требования права вооруженных конфликтов]»[115].

Квалификация социальных сетей, таких как Facebook или Twitter, в качестве военных объектов, создала бы целый ряд проблем. Действительно, такие сети содержат огромный объем данных, большинство из которых абсолютно не связаны с конкретной информацией, способной стать объектом нападения, поэтому представляется трудным квалифицировать такую сеть в качестве военного объекта. Другой вопрос заключается в том, возможно ли технически нанести удар только по тем компонентам, которые используются для военных целей, принимая во внимание неструктурированный характер данных в таких сетях.

Такой же трудный вопрос возникает в отношении средств массовой информации. В Таллиннском руководстве говорится:

> «Интересный случай связан с репортажами в средствах массовой информации. Если такие репортажи вносят эффективный вклад в понимание противником оперативной обстановки, то лишение его доступа к подобным репортажам может дать определенное военное преимущество. Некоторые члены Международной группы экспертов придерживаются мнения, что кибернетическая инфраструктура, способствующая их передаче, может квалифицироваться как военный объект, хотя они предупреждают, что нападения на инфраструктуру допустимы только при соблюдении норм, касающихся нападений, особенно соразмерности… и мер предосторожности при нападении. …В частности, они отмечают, что последнее требование, как правило, приведет к требованию осуществлять операции в кибернетическом пространстве только для блокирования каких-то определенных передач. Другие эксперты утверждают, что связь между кибернетической инфраструктурой и ее вкладом в военные действия слишком трудно определяема, чтобы инфраструктура могла считаться военным объектом. Все члены Международной группы экспертов согласны с тем, что оценки такого типа обязательно будут сильно зависеть от контекста»[116].

Даже если конкретный репортаж способен внести эффективный вклад в военные действия, это не дает возможности прийти к выводу, что либо соответствующая корпорация СМИ, либо передающая кибернетическая инфраструктура могут стать объектом нападения. Что касается корпораций, то потенциальные последствия признания их разрешенными объектами

115 *Tallinn Manual*, p. 114, см. примечание 27 выше.
116 *Ibid*., p. 113.

нападения были бы очень серьезными. В качестве примера рассмотрим такую вещательную компанию, как Би-би-си. Во-первых, выражение «эффективный вклад в понимание противником оперативной обстановки» можно толковать очень широко — шире, чем внесение непосредственного вклада в военные действия противника, как того требует статья 52 (2) Дополнительного протокола I. Во-вторых, даже если бы репортажи в СМИ содержали тактическую информацию, например касательно конкретных целей, крайне проблематичным остается предположение, что медийная компания может стать объектом нападения. Если вся кибернетическая инфраструктура, посредством которой передаются репортажи, а не только сама корпорация, должна считаться военным объектом, это будет означать, что большая часть кибернетической инфраструктуры планеты может быть разрушена или уничтожена — так же, как и в случае с объектами двойного использования, когда последствие квалификации объекта в качестве военного означает, что на него можно совершать нападения и кинетическими средствами, то есть нападать на то физическое место, из которого и посредством которого передаются репортажи. И последнее, как уже было сказано, пример с медийными корпорациями резко выделяет проблему географических границ поля боя. Кроме того, во время международного вооруженного конфликта право нейтралитета наложило бы целый ряд ограничений на право государства превращать в объект нападения инфраструктуру в нейтральном государстве[117].

Запрет на неизбирательные нападения и неизбирательные средства и методы ведения войны

Нападения неизбирательного характера запрещены[118]. К неизбирательным относятся нападения:

- которые не направлены на конкретный военный объект;
- в ходе которых используются методы и средства боя, которые не могут быть направлены на конкретный военный объект;
- или в ходе которых используются методы и средства боя, воздействие которых не может быть ограничено, как этого требует МГП;

и, следовательно, которые в каждом таком случае поражают без какого-либо различия как военные объекты, так и гражданских лиц и гражданские объекты. Стороны в конфликте «никогда не должны применять оружие, которое не дает возможности проводить различие между гражданскими и военными целями»[119].

Как уже было сказано, тот факт, что значительную часть кибернетического пространства можно считать объектом двойного использования,

117 См. раздел «Объекты двойного использования в кибернетическом пространстве» выше.
118 Обычное международное гуманитарное право, норма 12; ДП I, статья 51 (4).
119 МС, п. 78, см. примечание 88 выше.

затрудняет разграничение военной инфраструктуры и гражданской. Однако даже если такое разграничение можно сделать, проведя различие между военной и гражданской инфраструктурами, существует опасность того, что нападения будут иметь неизбирательный характер из-за взаимосвязанности кибернетического пространства[120]. Кибернетическое пространство состоит из бесчисленного числа переплетающихся между собой компьютерных систем по всему миру. Даже если военные компьютерные системы существуют отдельно от гражданских, они часто связаны с коммерческими гражданскими системами и зависят от них полностью или частично. Таким образом, скорее всего, невозможно осуществить кибернетическое нападение на военную инфраструктуру и ограничить это нападение или его последствия лишь этим военным объектом. Вирусы и «черви» являются примерами методов нападений на компьютерные сети, которые могут попадать в эту категорию, если их воздействие не ограничили их создатели. Использование «червей», которые воспроизводят себя и не могут быть управляемыми и поэтому способны причинять значительный ущерб гражданской инфраструктуре, было бы нарушением МГП[121].

Некоторые авторы считают такую обеспокоенность преувеличенной, особенно на основании того факта, что большинство операций в киберпространстве будут эффективными, только если их мишенью станет очень конкретная, высокоспециализированная система, их воздействие на другие компьютеры не будет вызывать повреждений. В качестве примера приводится вирус Stuxnet, который был очень четко прописан и использовался против ядерных установок в Исламской Республике Иран[122].

Действительно, если вирус внедряется в закрытую военную систему или создан таким образом, что не допускается его распространение на другие системы, может быть, и не будет опасности для внешней гражданской инфраструктуры. Но вполне вероятно, что сторона в конфликте не принимает надлежащих мер предосторожности или разрабатывает кибернетическое оружие, которое воздействуют на сети таким образом, который создатели не предвидели. Тот факт, что возможно создать кибернетическое оружие, которое не является неизбирательным, не означает, что не существует серьезных возможностей для неизбирательных нападений. Даже случай с вирусом Stuxnet, как об этом сообщалось в средствах массовой информации, свидетельствует о том, насколько трудно контролировать воздействие вирусов; сообщалось, что этот вирус не предназначался для заражения компьютеров за пределами систем ядерных установок, на которые совершалось нападение, но каким-то образом он воспроизвел себя за пределами Ирана[123]. Допустим, что распространение вируса далеко за границы,

120 K. Dörmann, p. 5, см. примечание 42 выше.

121 «Червь» нельзя ни направить на конкретный военный объект (см. Обычное международное гуманитарное право, норма 12 (b), ДП I, статья 51 (4) (b)), ни ограничить его воздействие, как это требуется в соответствии с МГП (см. Обычное международное гуманитарное право, норма 12 (c), ДП I, статья 51 (4) (c)).

122 T. Rid, примечание 24 выше.

123 D. E. Sanger, примечание 23 выше.

предполагаемые его создателями, возможно, и не причинило какого-либо ущерба, сам этот факт свидетельствует о том, как трудно контролировать такое распространение.

Поэтому на воюющих сторонах лежит двойное бремя. Во-первых, они не могут использовать кибернетическое оружие, которое является неизбирательным по своей природе, такое как вирусы или «черви», которые воспроизводятся, и этот процесс нельзя контролировать (что, например, можно сравнить с бактериологическим оружием). Использование такого оружия должно быть запрещено при его обсуждении, когда оно только разрабатывается или приобретается, — если его нельзя применять, не поражая военные и гражданские объекты без проведения различия, оно несовместимо с требованиями МГП[124]. Во-вторых, при каждом нападении воюющая сторона должна удостовериться в том, что в конкретных обстоятельствах используемое кибернетическое оружие может быть направлено, причем направлено на военный объект, и что последствия его применения могут контролироваться по смыслу МГП.

Принцип соразмерности

Принимая во внимание двойное использование большей части инфраструктуры, с одной стороны, и, с другой — опасность того, что из-за целостности кибернетического пространства будет затронута и гражданская инфраструктура, когда исключительно военные компьютеры или компьютерные системы окажутся объектом нападения, существует серьезная обеспокоенность в связи с тем, что гражданская инфраструктура сильно пострадает в результате операций в кибернетическом пространстве во время вооруженных конфликтов. Таким образом, принцип соразмерности становится важнейшим правилом для защиты гражданского населения.

Принцип соразмерности сформулирован в статье 51 (5) (b) Дополнительного протокола I, которая отражает обычное международное право[125]. Нападение запрещено, если оно, «как можно ожидать, попутно повлечет за собой потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам, или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить».

Как уже было сказано, ущерб, причиняемый объектам, означает «вред… снижающий ценность или полезность чего-либо»[126]. Таким образом, совершенно очевидно, что ущерб, который следует принимать во внимание, состоит не только в физическом ущербе, но и в утрате функциональности гражданской инфраструктуры даже при отсутствии физического повреждения. Высказывалось суждение, что «кибернетические нападения могут изменить

124 Это вытекает не только из обязательства государств — участников ДП I (статья 36), но и из общего обязательства воюющих сторон не использовать оружие неизбирательного действия.
125 Обычное международное гуманитарное право, примечание 87 выше, норма 14.
126 *Concise Oxford Dictionary.*

значение, придаваемое временным последствиям» при оценке соразмерности[127], но для этого нет никаких правовых оснований в МГП. Как пишут об этом Гайс и Ламан, любое другое прочтение привело бы к тому, что:

> «уничтожение одного гражданского автомобиля будет иметь значение с правовой точки зрения, хотя и считаться незначительным "побочным ущербом", отключение же тысяч или миллионов домов, компаний и общественных служб от интернета или других средств связи или прекращение финансовых операций в режиме онлайн для всей экономики страны и соответствующие экономические и социальные последствия как таковые не будут считаться имеющими отношение к делу элементами, которые должны приниматься во внимание при расчете соразмерности»[128].

Однако следует признать, что, если и когда нападения на компьютерные сети все-таки причиняют ущерб гражданской инфраструктуре, в том числе временно нарушая ее функционирование, принцип соразмерности страдает целым рядом недостатков (как и в ходе традиционной войны).

Во-первых, как и при всяком применении принципа соразмерности, остается некоторая неопределенность относительно того, что считать чрезмерным побочным ущербом для гражданских объектов по сравнению с конкретным и непосредственным военным преимуществом. Тот факт, что побочный ущерб гражданской инфраструктуре является чрезмерным по сравнению с военным преимуществом, устанавливался крайне редко[129]. Это не означает, что принцип соразмерности не налагает ограничений на все нападения. Но еще предстоит увидеть, как он будет толковаться в отношении кибернетических нападений.

С одной стороны, можно сказать, что операции в киберпространстве пока находятся на ранней стадии развития, поэтому мало известно об их воздействии и от командиров нельзя ожидать точного представления об их последствиях. Трудно предсказать, что является «ожидаемым» побочным ущербом для гражданского населения и гражданских объектов

127 Oona Hathaway et al., 'The law of cyber-attack', in *California Law Review*, Vol. 100, No. 4, 2012, p. 817.

128 R. Geiss and H. Lahmann, p. 17, примечание 61 выше.

129 См.: Louise Doswald-Beck, 'Some thoughts on computer network attack and the international law of armed conflict', in Michael N. Schmitt and Brian T. O'Donnell (eds), *Computer Network Attack and International Law*, International Law Studies, Vol. 76, 2002, p. 169: '…примеры… обычно касались случаев, когда либо возможная цель была чем-то, что являлось военным по своему характеру, но в данных обстоятельствах не использовалось, либо ценность объекта в качестве военного объекта не могла быть точно установлена». См. также: ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* (далее — Final Report to the Prosecutor), 13 June 2000, para. 19. В ответ на бомбардировку силами НАТО индустриального комплекса Панчево и нефтеперерабатывающего завода в г. Нови Сад во время войны в Косово в 1999 г., которая привела к утечке около 80 тысяч тонн сырой нефти в почву и высвобождению многих тонн других токсичных веществ, Комитет заявил, что «трудно оценить относительную ценность получаемого военного преимущества и вреда природной среде и что о необходимости выполнения принципа соразмерности легче заявить, чем применить его на практике».

в кибернетической войне. С другой стороны, эта неопределенность является скорее количественной, а не качественной; именно в силу переплетения сетей последствия для гражданской инфраструктуры очевидны. Другими словами, побочного ущерба следует ожидать в большинстве случаев, даже если его точные масштабы трудно оценить.

Во-вторых, хотя к настоящему времени в основном не вызывает споров тот факт, что эффект, подобный эффекту цепной реакции, то есть косвенное воздействие второго или третьего порядка, следует учитывать, все еще ведутся дискуссии относительно того, каков объем этого обязательства[130]. В соответствии с формулировкой статьи 51 (5) (b) Дополнительного протокола I («как можно ожидать») разумно считать, что предвидимый ущерб должен быть принят во внимание, даже если это ущерб, который становится очевиден не сразу — ущерб второй или даже третьей очереди[131]. В кибернетическом пространстве благодаря взаимосвязанности сетей может быть труднее предвидеть последствия, чем в случае применения классического кинетического оружия, но тем более важно сделать все практически возможное для оценки этих последствий. В практической плоскости это приводит, главным образом, к вопросу о мерах предосторожности при нападении. Учитывая взаимосвязанность информационных сетей и систем, которые от них зависят, чего можно ожидать от командира в плане установления точных данных для того, чтобы оценить, каков будет отдаленный эффект нападения на компьютерную сеть?[132]

Принцип принятия мер предосторожности

Принцип предосторожности в МГП имеет два аспекта: меры предосторожности при нападении и меры предосторожности в отношении последствий нападений[133].

Меры предосторожности при нападении

При ведении военных действий следует постоянно заботиться о том, чтобы пощадить гражданское население и гражданские объекты[134]. К особым мерам предосторожности, которых требует МГП, относится принятие всех практически возможных мер для проверки того, является ли объект нападения

130 См., например: *Commentary on HPCR Manual on Air and Missile Warfare*, примечание 86 выше, Commentary on Rule 14, para. 4; Michael N. Schmitt, 'Computer network attack: the normative software', in *Yearbook of International Humanitarian Law*, The Hague, TMC Asser Press, 2001, p. 82.

131 *Tallinn Manual*, Commentary on Rule 51, para. 6, см. примечание 27 выше; R. Geiss and H. Lahmann, p. 16, см. примечание 61 выше.

132 Это следует отличать от неизбирательного нападения, при котором последствия не поддаются контролю.

133 См.: ДП I, статьи 57 и 58; Обычное международное гуманитарное право, примечание 87 выше, нормы 15—24.

134 ДП I, статья 57 (1); Обычное международное гуманитарное право, примечание 87 выше, норма 15.

военным объектом[135], а при выборе средств и методов ведения войны принятие всех практически возможных мер, с тем чтобы избежать или в любом случае свести к минимуму случайные жертвы среди гражданского населения и ущерб гражданским объектам[136]. Также МГП требует, чтобы стороны в конфликте отменили или отложили нападение, если становится ясно, что оно причинит чрезмерный «случайный ущерб»[137].

Таким образом, этот принцип может повлечь за собой такие обязательства, как принятие мер по сбору всей имеющейся информации для точного установления характера цели и возможных случайных последствий нападения[138]. Во время кибернетической войны меры предосторожности могут включать составление карты сети противника[139], что часто будет являться частью разработки нападений на компьютерную сеть, если они направлены конкретно против определенной компьютерной системы. Если имеющейся информации недостаточно, — что очень вероятно в кибернетическом пространстве в результате его взаимосвязанности, — масштаб нападения, возможно, придется ограничить только теми целями, о которых имеется достаточно информации[140].

Принцип предосторожности может потребовать специальных технических знаний. Таллиннское руководство устанавливает, что «с учетом сложности операций в кибернетическом пространстве, большой вероятности поражения гражданских систем и порой ограниченного понимания их характера и воздействия со стороны лиц, которым поручено дать разрешение на осуществление операций в кибернетическом пространстве, те, кто планирует выполнение боевой задачи, должны, если это практически выполнимо, иметь возможность обратиться за помощью к техническим экспертам при определении того, были ли приняты соответствующие меры предосторожности»[141]. Если нет соответствующих знаний и опыта и поэтому возможности оценить характер цели или случайные потери среди гражданского населения и случайный ущерб гражданским объектам, нападающей стороне, возможно, придется отказаться от нападения.

135 ДП I, статья 57 (2) (a) (i); Обычное международное гуманитарное право, примечание 87 выше, норма 16.

136 ДП I, статья 57 (2) (a) (ii); Обычное международное гуманитарное право, примечание 87 выше, норма 17.

137 ДП I, статьи 57 (2) (b); Обычное международное гуманитарное право, примечание 87 выше, норма 19.

138 ICTY, *Final Report to the Prosecutor*, para. 29. В своем Заключительном докладе Комитет, созданный для рассмотрения вопроса о бомбардировках силами НАТО Федеративной Республики Югославия, описал обязательство таким образом: «Военный командир обязан создать эффективную систему сбора разведывательных данных, чтобы собрать и оценить информацию, касающуюся возможных объектов нападения. Кроме того, командир должен дать указания своим силам использовать имеющиеся технические средства надлежащим образом, чтобы идентифицировать цели во время операций. Как командир, так и экипаж летательного аппарата, фактически участвующего в операциях, должны обладать некоторой свободой для определения того, какие имеющиеся в распоряжении ресурсы будут использованы и каким образом».

139 E. T. Jensen, p. 1185, см. примечание 90 выше.

140 *Tallinn Manua*l, Rule 53, para. 6, см. примечание 27 выше.

141 *Ibid*., Rule 52, para. 6.

Однако вполне вероятно, что многие кибернетические нападения в ситуации обороны будут автоматическими, заранее запрограммированными операциями в кибернетическом пространстве против внешнего вторжения[142]. Такие ответные удары являются автоматическими и просто направляются на компьютеры, с которых было осуществлено вторжение; поскольку решается техническая проблема, неважен характер компьютеров — гражданские они или военные. В таких условиях и с учетом того, что такие кибернетические нападения будут осуществляться с тысяч или даже миллионов компьютеров, государствам придется внимательно оценивать законность подобных автоматических ответных ударов в свете принципа принятия мер предосторожности.

Если взглянуть с другой точки зрения, то принцип принятия мер предосторожности может в некоторых случаях повлечь за собой обязанность использовать кибернетическую технологию, когда она имеется. Действительно, операции в кибернетическом пространстве могли бы причинить и меньше случайного ущерба гражданским лицам и гражданской инфраструктуре, чем кинетические операции. Например, нарушение функционирования некоторых служб, используемых для военных и гражданских целей, может быть менее разрушительным, чем полное уничтожение инфраструктуры. Однако вопрос об объеме обязательства прибегать к использованию более сложной технологии — в нашем случае кибернетической — не решен окончательно. Действительно, на международном уровне все еще не существует консенсуса относительно того, что воюющие стороны обязаны во всякое время использовать наиболее точное и наиболее совершенное в технологическом плане оружие (этот вопрос обсуждается в основном в отношении высокоточных управляемых боеприпасов)[143]. Тем не менее принцип предосторожности предусматривает обязанность не только соблюдать принципы проведения различия и соразмерности, но и делать все практически возможное для того, чтобы избежать или в любом случае свести к минимуму случайные потери среди гражданского населения и случайный ущерб гражданским объектам. В таких случаях принцип предосторожности, по мнению многих, означает, что командиры должны выбирать для достижения своей военной цели имеющиеся на конкретный момент средства, наносящие наименьший вред[144].

142 В соответствии с ДП I, статья 49, такие оборонительные операции также являются нападениями, при которых должны применяться принципы проведения различия, соразмерности и предосторожности.

143 См.: Jean-François Quéguiner, 'Precautions under the law governing the conduct of hostilities', in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, p. 801; *Commentary on HPCR Manual on Air and Missile Warfare*, Commentary on Rule 8, para. 2, см. примечание 86 выше.

144 K. Dörmann, примечание 42 выше; Michael N. Schmitt, 'The principle of discrimination in 21st century warfare', in *Yale Human Rights and Development Law Journal*, Vol. 2, 1999, p. 170; *Commentary on HPCR Manual on Air and Missile Warfare*, Commentary on Rule 32 (b), para. 3 (примечание 86 выше), об оружии, обладающем большей точностью или меньшей разрушительной способностью.

Меры предосторожности в отношении последствий нападений

Принцип предосторожности в отношении последствий нападений требует, чтобы стороны в конфликтах «в максимальной практически возможной степени… [стремились] удалить гражданское население, отдельных гражданских лиц и гражданские объекты, находящиеся под их контролем, из районов, расположенных вблизи от военных объектов» и принять «другие необходимые меры предосторожности для защиты гражданского населения, отдельных гражданских лиц и гражданских объектов, находящихся под их контролем, от опасностей, возникающих в результате военных операций»[145]. Это означает, что государства обязаны либо размещать военные объекты вдали от мест, где находятся гражданские лица и гражданские объекты, либо (и особенно если это невозможно) принимать другие меры для защиты гражданских лиц и гражданской инфраструктуры от опасностей, связанных с военными действиями.

Как говорится в Таллиннском руководстве, это может включать «разграничение военной кибернетической инфраструктуры и гражданской; отделение компьютерных систем, от которых зависит важнейшая гражданская инфраструктура, от интернета; сохранение важных данных гражданского характера в отдельном месте; заблаговременное принятие мер для обеспечения своевременного ремонта важных компьютерных систем на случай кибернетических нападений, которые можно предвидеть; хранение в оцифрованном виде важных культурных и духовных объектов для облегчения их реконструкции в случае их разрушения во время вооруженного конфликта; применение антивирусных мер для защиты гражданских систем, которые могут быть разрушены или уничтожены во время нападения на военную кибернетическую инфраструктуру»[146].

И действительно, часто слышатся голоса в пользу разграничения военных и гражданских сетей[147]. Как рекомендуется в оценке правовых вопросов Министерства обороны США, «если есть такая возможность, военные системы должны быть отдельными от инфраструктур, используемых для важнейших гражданских целей»[148]. Однако это вряд ли выполнимо. В первые дни существования интернета все создавалось, вероятно, без учета таких проблем. Имеются, конечно, закрытые военные сети, и, разумеется, очень уязвимая гражданская инфраструктура также отделена от внешних сетей. Но принимая во внимание слабость, присущую норме об отделении гражданских объектов от военных (статья 58 (a) Дополнительного протокола I), которая обязывает государства только стараться отделить военные объекты от гражданских и только в максимально практически возможной степени, маловероятно, что она будет толковаться в практике государств

145 ДП I, статья 58; Обычное международное гуманитарное право, примечание 89 выше, нормы 22 и 24.
146 *Tallinn Manual*, Commentary on Rule 59, para. 3, см. примечание 27 выше.
147 E. T. Jensen, p. 1533—1569, см. примечание 97 выше; Adam Segal, 'Cyber space governance: the next step', Council on Foreign Relations, *Policy Innovation Memorandum No.* 2, 14 November 2011, p. 3, доступно по адресу: http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.
148 Department of Defense Office of General Counsel, p. 7, см. примечание 112 выше.

как обязанность отделить гражданские сети от военных. Хотя теоретически это, быть может, и выполнимо, но будет так практически нецелесообразно и дорого, что это сочтут практически невозможным по смыслу статьи 58 Дополнительного протокола I. Государствам пришлось бы создавать свои собственные аппаратные средства и программное обеспечение для использования военными и свои собственные линии связи для военных нужд по всему миру, включая кабели, роутеры и спутники[149].

Кроме того, разграничение военной и гражданской кибернетических инфраструктур опирается на предположение, что между ними есть различие и это различие должно сохраняться. Строго говоря, статья 58 не запрещает двойного использования: она исходит из положения, что есть различие между гражданскими и военными объектами, даже если некоторые гражданские объекты используются в качестве военных. Уже в физическом мире значительные части важнейшей инфраструктуры имеют двойное использование, например сети электропередачи и часто нефтепроводы, электростанции и дорожные сети. В кибернетическом пространстве принцип становится относительно бессмысленным, если проблема заключается не в расположении гражданских и военных инфраструктур в одном месте, а в том, что они являются одной и той же инфраструктурой[150].

Вопрос тогда возникает относительно того, будет ли статья 58 (c) Дополнительного протокола I требовать, чтобы по крайней мере часть гражданской инфраструктуры (например, атомные станции, химические предприятия и больницы) находилась под защитой от повреждений в случае кибернетического нападения, а также требовать, чтобы государства принимали меры для обеспечения ее функционирования. Эрик Тальбот Йенсен, например, рекомендует США принять целый ряд мер, для того чтобы выполнить свое обязательство в соответствии со статьей 58. Эти меры должны включать составление карты гражданских систем, сетей и промышленных предприятий, которые станут военными объектами, и обеспечить достаточную защиту частному сектору, а также подготовить решения, касающиеся ответных ударов, или создать стратегические резервные каналы интернета[151]. Многие страны мира уже идут в этом направлении с целью обеспечить защиту своей важнейшей инфраструктуре — хотя маловероятно, что правительства задумываются о такой защите в плане пассивных мер предосторожности по смыслу статьи 58 (c).

Заключение

Как уже отмечалось во введении, операции в кибернетическом пространстве вызовут появление новых средств и методов боя, воздействие которых все еще не проверено или плохо понято. Представляется, однако, что военное

149 E. T. Jensen, pp. 1551—1552, см. примечание 97 выше.
150 См. также: R. Geiss and H. Lahmann, p. 14, см. примечание 61 выше.
151 E. T. Jensen, p. 1563 ff, см. примечание 97 выше.

использование информационной технологии создает серьезные проблемы для применения МГП, особенно в отношении самого исходного положения, что между гражданскими и военными объектами должно проводиться различие во время вооруженных конфликтов. Для того чтобы получить четкие заявления о том, как государства собираются соблюдать принципы проведения различия, соразмерности и предосторожности, необходимо этот вопрос обсуждать более открыто и откровенно, чем это делалось до сих пор.

С учетом тех опасностей, которым кибернетическая война подвергает гражданскую инфраструктуру, предлагается целый ряд решений *de lege lata* и *de lege ferenda*. Одно из предложений заключается в том, чтобы государства заявили о создании своих цифровых «безопасных районах», то есть о гражданских объектах, которые они будут считать запретными при ведении кибернетических операций[152]. Если стороны достигнут соглашения, такие районы будут аналогичны демилитаризованным зонам, предусматриваемым в статье 60 Дополнительного протокола I. Для этого потребуется диалог и меры по установлению доверия, о которых сейчас говорится и которые остаются за пределами темы данной статьи. Адам Сигал утверждает, что «в отношении некоторых вещей консенсуса достигнуть сравнительно легко — это больницы и медицинские данные, — но гораздо труднее в отношении других, таких как финансовые системы, линии электропередачи и инфраструктура интернета»[153]. Хотя и интересно исследовать этот путь, — и, возможно, он будет рассмотрен в ходе международного диалога о мерах по установлению доверия, — скептицизм в отношении быстрого осуществления такого метода, вероятно, не будет казаться излишне пессимистичным. Учитывая скрытый характер большой части того, что представляется сегодня манипуляциями в кибернетическом пространстве и проникновением в него, неясно, насколько можно будет доверять соглашениям и заявлениям об информационных зонах, запретных для военного использования.

Другое предложение, сделанное Гайсом и Ламаном, заключается в том, чтобы расширить по аналогии перечень «установок и сооружений, содержащих опасные силы», представленный в статье 56 Дополнительного протокола I[154]. Он может включать конкретные компоненты кибернетической инфраструктуры, такие как ключевые узлы интернета или центральные серверы, от которых зависят миллионы важных гражданских инфраструктур. Подобно дамбам, плотинам и ядерным электростанциям, они не могли бы становиться объектами нападения, даже если и являются военными объектами, потому что опасность для гражданского населения всегда будет считаться несоразмерно больше военного преимущества, получаемого от нападения на такие объекты. Однако Гайс и Ламан также признают, что невелика вероятность того, что такое предложение будет благосклонно

152 A. Segal, примечание 147 выше.
153 *Ibid*.
154 R. Geiss and H. Lahmann, p. 11, см. примечание 61 выше.

принято государствами. В частности, хотя эффект цепной реакции в случае нейтрализации или уничтожения кибернетической инфраструктуры может быть очень серьезным, трудно его сравнивать с высвобождением радиоактивных материалов или прорывом плотины. Если тем не менее он и будет иметь такие катастрофические последствия, логическое обоснование статьи 56 Дополнительного протокола I может в равной степени предоставить убедительный аргумент для защиты и кибернетической инфраструктуры.

И далее, проблемы, возникающие в компьютерной сфере, поставили и вопрос о том, не должны ли (некоторые) средства и методы кибернетической войны быть запрещены совсем или регулироваться международным договором. Как уже говорилось во введении, некоторые государства выступали за заключение нового договора, хотя очертания того, что должно и что не должно быть разрешено, еще не всегда четко обозначались. Одновременно дебаты проводятся среди специалистов по кибернетической безопасности и ученых. Некоторые предлагают принять новые договоры, касающиеся кибернетической войны[155], другие утверждают, что должен быть какой-то вид договора о разоружении, содержащий запрет на все или по крайней мере некоторые виды кибернетического оружия[156]. Третьи возражают, что невозможно будет обеспечить соблюдение такого договора из-за трудностей присвоения действий, что технически невозможно провести различие между инструментами кибернетической войны и кибернетического шпионажа, что запрещенное оружие может быть менее разрушительным, чем традиционное, и что проверка выполнения окажется неосуществимой[157].

Некоторые авторы предлагают другие решения, такие как «неформальные многосторонние отношения»[158] или создание международной организации кибернетической безопасности, аналогичной Международному агентству

155 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 964; Davis Brown, 'A proposal for an international convention to regulate the use of information systems in armed conflict', in *Harvard International Law Journal*, Vol. 47, No. 1, Winter 2006, p. 179; Duncan B. Hollis, 'Why states need an international law for information operations', in *Lewis and Clark Law Review*, Vol. 11, 2007, p. 1023.

156 См.: Mary Ellen O'Connell, 'Cyber mania', in *Cyber Security and International Law*, Meeting Summary, Chatham House, 29 May 2012, доступно по адресу: http://www.chathamhouse.org/sites/default/files/public/ Research/International%20Law/290512summary.pdf; Misha Glenny, 'We will rue Stuxnet's cavalier deployment', in *The Financial Times*, 6 June 2012, где цитируется Евгений Касперский, российский специалист в сфере информационной безопасности; Scott Kemp, 'Cyberweapons: bold steps in a digital darkness?', in *Bulletin of the Atomic Scientists*, 7 June 2012, доступно по адресу: http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness; Bruce Schneier, 'An international cyberwar treaty is the only way to stem the threat', in US News, 8 June 2012, доступно по адресу: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat; Duncan Holis, 'An e-SOS for cyberspace', in *Harvard International Law Journal*, Vol. 52, No. 2, Summer 2011, где приводятся аргументы в пользу введения электронного сигнала бедствия (e-SOS).

157 Herb Lin and Thomas Rid, 'Think again: cyberwar', in *Foreign Policy*, March/April 2012, p. 7, доступно по адресу: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Jack Goldsmith, 'Cybersecurity treaties: a skeptical view', in Peter Berkowitz (ed.), Future Challenges in *National Security and Law* (forthcoming), доступно по адресу: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

158 A. Segal, примечание 108 выше.

по атомной энергии, в качестве независимой платформы для международного сотрудничества в целях разработки договоров по контролю над кибернетическим оружием[159].

Сейчас трудно предсказать, куда приведут эти дискуссии и — особенно — готовы ли государства открыто обсуждать реальные опасности кибернетической войны и принимать меры для предотвращения самых худших сценариев. Но если стороны в конфликтах выбирают кибернетическое оружие во время вооруженных конфликтов, они должны понимать, что существует правовая основа в качестве минимального свода норм, которые необходимо соблюдать несмотря на их несовершенство. Они должны соответствующим образом инструктировать свои силы и предоставлять им соответствующую подготовку. Важно содействовать обсуждению этих вопросов, привлекать внимание к необходимости оценить воздействие развивающихся технологий в гуманитарном плане и проследить за тем, чтобы они не были преждевременно использованы в условиях, когда соблюдение права не может быть гарантировано.

В заключение надо сказать, что не возникает вопросов относительно применимости МГП к кибернетической войне. Однако вопрос о том, предоставит ли оно достаточную защиту гражданскому населению, в частности не допустив ущерба гражданской инфраструктуре, будет зависеть от того, как МГП — составители которого не предвидели таких операций — толкуется в связи с такими операциями. И только добросовестное и крайне внимательное его толкование сделает возможным предоставление защиты гражданской инфраструктуре от превращения ее в непосредственный объект нападения или от ущерба, который может стать катастрофичным для гражданского населения. Даже и в этом случае, учитывая потенциальные слабые стороны принципов проведения различия, соразмерности и принятия мер предосторожности, — и в отсутствие более глубоких знаний о наступательном потенциале и последствиях применения кибернетического оружия, — нельзя исключать, что могут стать необходимыми более строгие нормы.

159 Eugene Kaspersky, 'Der Cyber-Krieg kann jeden treffen', in *Süddeutsche*, 13 September 2012, доступно по адресу: http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.1466845.