Электронная война: нападение на компьютерные сети и *jus in bello*

Михель Н. Шмитт

Несмотря на постоянные дискуссии о наличии или отсутствии «революции в военном деле», неоспоримо, что способы ведения войны в двадцать первом веке будут коренным образом отличаться от того, что видел век двадцатый. В начале нового века трагическим событием, к которому было приковано внимание мировой общественности, явились террористические акты 11 сентября 2001 г. и их последствия. Возможно, не менее значимым событием века будет формирование нового инструмента ведения военных действий – «информационной войны».[1] Это поставит под сомнение сегодняшнюю военную доктрину, потребует пересмотра концепции зоны боевых действий и расширит гамму имеющихся методов и средств ведения войны. Особого внимания заслуживает влияние информационных войн на принципы международного гуманитарного права и обратное влияние этих принципов на информационные войны.

Михель Н. Шмитт – профессор международного права и руководитель программы международных отношений и вопросов безопасности в Европейском центре исследования проблем безопасности им. Дж. Маршалла, Гармиш-Партенкирхен, Германия.

Обобщенно и коротко говоря, информационная война — это вид информационных операций, то есть «меры, предпринимаемые для оказания воздействия на информацию и информационные системы противника, для защиты собственной информации и собственных информационных систем»[2]. Такие операции включают, по существу, любые меры, направленные на обнаружение, видоизменение, уничтожение или передачу данных, хранящихся в компьютере, обрабатываемых компьютером или пересылаемых с помощью компьютера. Это может происходить в мирное время, во времена кризисов или при решении стратегических, оперативных или тактических задач в ходе вооруженных конфликтов.[3] Информа-

1 В документе «Национальная военная стратегия США» ключевым элементом стратегии на это столетие названо информационное превосходство. «Информационное превосходство – это способность собирать, обрабатывать и распространять непрерывный поток точной и надежной информации, одновременно используя в своих интересах деятельность неприятеля в этой области и препятствуя такой его деятельности». «Joint Chiefs of Staff, National Military Strategy (1997), http://www.dtic.mil/jcs/nms/strategy.htm. Превосходное собрание очерков о характере войн двадцать первого века см. Robert H. Scales (ed.). *Future War Anthology*, Carlisle Barracks, Pa., US Army College, 2000. По проблеме информации и конфликтов см. Stephan Metz, *Armed Conflict in the 2ist Century: The Information Revolution and Post-Modern Warfare*, Carlisle Barracks, Pa., US Army College, 2000; William A. Owens and Edward Offley, *Lifting the Fog of War*, John Hopkins University Press, Baltimore, 2000; Thomas E. Copeland (ed.). *The Information Revolution and National Security*, Carlisle Barracks, Pa., US Army College, 2000; David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging information Superiority*, 44ISR Cooperative Research Program, Washington D.C.. 1999; Dan Kuehl, *Strategic Information Warfare: A Concept*, Working Paper 322, Strategic & Defence Studies Centre, Australian National University, Canberra, 1999; Zaimay Khalilzad and John White (eds), *Strategic Appraisal: The Changing Role of information Warfare*. RAND, Santa Monica, 1999; Dorothy E. Denning, *Information Warfare and Security*, ACM Press, New York, 1999; James Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere*, Simon & Schuster, New York, 1998.

2 Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02, 12 April 2001 (далее – JP 1–02), p. 203. К операциям, которые могут рассматриваться в качестве информационных операций, относятся обеспечение оперативной безопасности, психологические операции, военные хитрости, электронная война, физическое нападение и компьютерное нападение на сети. См. Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3–13, 9 October 1998, pp. 1–9 (далее – JP 3–13).

3 В стратегическом плане информационные операции могут проводиться для «достижения национальных целей путем

ционные операции отличаются от других объектом нанесения ущерба или защиты. Этим объектом является информация.

Информационная война в более узком понимании — «информационные операции, проводимые во время кризиса или конфликта с целью достижения или содействия достижению конкретных целей в отношении конкретного противника или противников».[4] Таким образом, информационная война отличается от других операций тем, что она происходит в обстановке кризиса или конфликта. Например, обычный шпионаж мирного времени, в отличие от проводимого во время кризиса или военных действий, это информационная операция, не являющаяся информационной войной.

Нападения на компьютерные сети (НКС) которые могут означать как информационную войну так и просто информационные операции, — это «операции по нарушению, ухудшению или уничтожению информации, находящейся в компьютерах и компьютерных сетях, или предотвращению доступа к ней, а также операции по нарушению работы, ухудшению или уничтожению самих компьютеров и сетей».[5]

воздействия на все элементы (политический, военный, экономический, информационный) государственной власти противника или потенциального противника, при одновременной защите своих соответствующих элементов». В оперативном плане цель информационных операций заключается в «нанесении ущерба линиям связи, материально-техническому снабжению, командованию и управлению войсками и связанным с этим возможностям и действиям противника, при одновременной защите своих аналогичных возможностей и действий». И наконец, в тактическом плане цель заключается в нанесении ущерба «информации и информационным системам, относящимся к командованию и управлению, разведке и к другим информационно обусловленным процессам, непосредственно относящимся к проведению военных операций…». JP 3–13, *op. cit.* (примечание 2), p. 1–2–1–3.

4 JP 1–02, *op. cit.* (примечание 2), p. 203.

5 *Ibid.*, p. 88. В документе *USAF Intelligence Targeting Guide*, AF Pamphlet 14–210, 1 February 1998, (*Руководство ВВС США по разведке целей*, Инструкция 14–210 от 1 февраля 1998 г.), в п. 11.4.3 даны следующие понятия, относящиеся к информационной войне:

Искажение – изменение информационного содержания; манипуляции с данными, с тем чтобы они стали бессмысленными или ошибочными. Уничтожение существующих сведений.

Обман – особый тип искажения; изменение или добавление информации с тем, чтобы реальная ситуация была изображена в искаженном виде. Создание ложных сведений, включая маскировку.

Задержка – обратимое замедление проходящего через систему потока информации, а также замедление процесса приобретения и распространения новых сведений.

Предотвращение доступа – обратимая остановка потока информации на некоторое

Независимо от условий, в которых происходят НКС, суть их заключается в том, что в качестве средств нападения используют поток данных,[6] что отличает НКС от других видов информационных операций. Имеется широкий спектр таких средств. К ним, в частности, относятся: получение доступа к компьютерной системе с тем, чтобы иметь возможность управлять ею; пересылка вирусов, уничтожающих или изменяющих данные; установка в систему логических мин замедленного действия, рассчитанных на приведение в действие в определенных условиях или в назначенное время; введение «червей» в систему, которые начинают самотиражироваться и перегружают сеть; использование анализаторов для отслеживания и (или) перехвата данных.

В данной статье НКС рассматриваются в ситуации *международного* вооруженного конфликта и только в контексте *jus in bello* (права войны), то есть совокупности правовых норм, трактующих, что допустимо или недопустимо в ходе военных действий, независимо от законности или незаконности первоначального применения силы воюющими сторонами.[7] Рассмотрение поэтому концентрируется на НКС в контексте вооруженного конфликта «государство против государства». Следует также отметить, что статья рассматривает *позитив-*

время; в то время как на своей территории информация может передаваться и использоваться, противник не имеет к ней доступа. Предотвращение получения и распространения новых сведений.

Нарушение – снижение возможности поставлять и (или) обрабатывать информацию (обратимое). Это – сочетание задержки и искажения. Задержка получения и распространения новых сведений и уничтожение существующих сведений.

Ухудшение качества –постоянное снижение возможности поставлять и (или) обрабатывать информацию.

Разрушение – разрушение информации до ее передачи; долговременное уничтожение возможности поставлять и (или) обрабатывать информацию.

6 Следовательно, электронная атака (ЭА) не подпадает под эту категорию. Например, использование электромагнитного импульса для разрушения электронных схем компьютера будет ЭА, а передача кода или инструкции на центральный процессор, вызывающая электрическое замыкание, будет НКС. *Ibid*.

7 По проблеме НКС и *jus ad bellum* (права прибегать к силе), то есть совокупности международных правовых норм, определяющих законность применения государствами силы, см. Michael N. Schmitt, «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 885; Richard Aldrich, «How Do You Know You are at War in the Information Age?», *Houston Journal of International Law*, Vol. 22, 2000, p. 223.

ное право, а не *законодательство будущего*. Формулирование законодательства будущего совершенно необходимо по мере изменения характера войны,[8] но в данном случае мы просто анализируем применимость существующего гуманитарного права к нападениям на компьютерные сети и ищем возможные пробелы в этом праве.

Применимость существующего гуманитарного права к нападениям на компьютерные сети

Сначала следует выяснить, подпадает ли нападение на компьютерные сети вообще под действие гуманитарного права. Во-первых, ни в одном документе гуманитарного права нет ни одного положения, непосредственно рассматривающего НКС либо информационную войну или информационные операции, это может означать, что НКС во время вооруженных конфликтов пока не регулируется этим правом. Во-вторых, можно ссылаться на то, что НКС разрабатывались и применялись после принятия существующих договоров права, и, поскольку участники этих договоров не учитывали такие нападения, они не охватываются этим правом. В-третьих, возможным аргументом в пользу неприменимости является то, что гуманитарное право относится к методам и средствам силового характера, а так как в НКС мало «физического» воздействия, то оно выпадает из сферы действия гуманитарного права.[9] Другими словами, гуманитарное право относится к вооруженным конфликтам, а нападения на компьютерные сети осуществляется без «оружия».

Первые два аргумента легко опровергаются. Не суть важно, что в действующих конвенциях ничего не сказано об НКС. Во-первых, в оговорке Мартенса, являющейся общепризнанным

8 Анализ НКС в контексте права и этики, который приводит к выводу о необходимости новой конвенции, см. в работе William J. Bayles, «The Ethics of Computer Network Attack», *Parameters*, Spring 2001, p. 44.

9 По этому вопросу см. Emily Haslam, «Information Warfare: Technological Changes and International Law», *Journal of Conflict and Security Law*, Vol. 5, 2000, p. 157. В частности, следует обратить внимание на анализ автором доводов, приведенных в работах: Richard Aldrich, «The International Legal Implications of Information Warfare», *Airpower Journal*. Fall 1996, p. 99; and Mark Shulman, «Discrimination in the Laws of Information Warfare», *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 939.

принципом гуманитарного права, сказано, что в случаях, не предусмотренных международными соглашениями, «гражданские лица и комбатанты остаются под защитой и действием принципов международного права, проистекающих из установившихся обычаев, из принципов гуманности и из требований общественного сознания».[10] Согласно этой норме ко всем событиям, происходящим во время вооруженного конфликта, применимы принципы гуманитарного права, правового вакуума нет. Принятие «международного обычая» в качестве источника права в ст. 38 Статута Международного суда также показывает ошибочность утверждения о неприменимости, основанного на отсутствии конкретного lex scripta.[11]

10 Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I), (далее – Дополнительный протокол I), ст. 1(2). Женевские конвенции от 12 августа 1949 г. и дополнительные протоколы к ним. МККК. Москва. 2001 г. В первоначальной формулировке оговорки Мартенса, включенной в преамбулу Гаагской конвенции IV о законах и обычаях сухопутной войны от 18 октября 1907 г., говорится, что «население и воюющие стороны остаются под охраной и действием начал международного права, поскольку они вытекают из установившихся между образованными народами обычаев, из законов человечности и требований общественного сознания», Международное право. Ведение военных действий. Сборник Гаагских конвенций и иных соглашений. МККК. Москва. 1999 г., с. 19.

11 Статут Международного суда определяет обычай как всеобщую практику, признанную в качестве правовой нормы. Статут Международного суда, 26 июня 1977 г., ст. 38(1)(b). В Новой формулировке США отмечается, что обычай «проистекает из общей и последовательной практики государств, которой они придерживаются исходя из чувства правовой ответственности». Restatement (Third), Foreign Relations Law of the United States, sec. 102(2) (1987). См. также *North Sea Continental Shelf Cases*, 3 ICJ Reports 1969, p. 44 («Действия, о которых идет речь, должны не просто сводиться к установившейся практике, а должны быть такими или осуществляться таким образом, чтобы свидетельствовать об убеждении, что такая практика является обязательной в силу существования правовой нормы, требующей придерживаться такой практики»); *The Paquete Habana*, 175 US 677, 20 S.Ct. 290, 44 L.Ed 320 (1900); *The S.S. Lotus (France v. Turkey)*, PCIJ (ser. A) No. 10, 1927; *Asylum Case (Colombia v. Peru)*, 5 ICJ Reports, 1950, p. 266; *Case Concerning Right of Passage over Indian Territory (Portugal v. India)*, ICJ Reports, 1960, p. 6. Научные комментарии, касающиеся международного обычного права, см. в Jack L. Goldsmith and Eric A. Posner, «Understanding the Resemblance Between Modern and Traditional Customary International Law», *Virginia Journal of International Law*, Vol. 40, 2000, p. 639; Patrick Kelly. «The Twilight of Customary International Law», *Virginia Journal of International Law*, Vol. 40, 2000, p. 449; Anthony A. D'Amato, *The Concept of Custom in International Law*, Cornell University Press, Ithaca, 1971.

Аргументы, базирующиеся на том, что НКС появились после принятия сегодняшних нормативных документов, также несостоятельны. Точно такая аргументация была представлена Международному суду в документе *Законность угрозы ядерным оружием или его применения*. В своем консультативном заключении Суд сразу же отклонил утверждение, согласно которому гуманитарное право не применимо в отношении ядерных вооружений, так как его «принципы и нормы были разработаны до изобретения ядерного оружия». Как отметил Суд, «[п]о мнению подавляющего большинства государств, а также ученых, не может быть сомнений в применимости гуманитарного права к ядерному оружию».[12] Поскольку нет причин проводить различие между ядерным и компьютерным оружием, — во всяком случае, на основании времени их создания по отношению ко времени вступления в силу соответствующих норм гуманитарного права, — то тот же самый вывод можно отнести и к НКС. Более того, изучение нового оружия и систем вооружений с точки зрения их соответствия гуманитарному праву является правовым, а зачастую и политическим требованием.[13] Очевидно, что если по отношению ко вновь появляющимся методам и средствам ведения войны *изначально* не применимы существующие ранее законы, то это было бы не так.

12 Консультативное заключение Международного суда относительно законности угрозы ядерным оружием или его применения. ООН, A/51/218, 19 July 1996, ч. 85.

13 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 36: «При изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне». В США проверка вооружений предусмотрена параграфом 4.7.3.1.4. инструкции Министерства обороны № 5000.2 Operation of the Defense Acquisition System (Организация системы закупок для нужд обороны), где сказано, что «приобретение и закупка Министерством обороны вооружения и систем вооружений должны осуществляться согласно применимому внутреннему праву и всем применимым договорам, международному обычному праву и праву вооруженных конфликтов (известному также под названием «законы и обычаи войны»)… Кроме этого, поощряется правовая проверка новых, новейших и нарождающихся технологий, которые могут привести к разработке вооружений и систем вооружений».

Таким образом, остается третий аргумент в пользу неприменимости гуманитарного права к нападению на компьютерные сети, а именно, что это не *вооруженный* конфликт, во всяком случае, не является таковым при отсутствии обычных военных действий. В сущности, вооруженный конфликт является условием, приводящим в действие *право войны*. Статья 2, общая для четырех Женевских конвенций 1949 г., предусматривает, что, помимо постановлений, относящихся к мирному времени, эти конвенции будут «применяться в случае 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».[14] В Дополнительном протоколе I 1977 г., который, так же как и Конвенции, посвящен международным вооруженным конфликтам, принят тот же критерий вооруженного конфликта, ставшего в обычном праве общепринятым условием применения гуманитарного права.[15] В Дополнительном протоколе II 1977 г., — в контексте вооруженного конфликта немеждународного характера — также принят термин «вооруженный конфликт»[16], а это показывает, что вооруженный конфликт является условием, определяемым его характером, а не его участниками,[17] местом, где он происходит[18], или, как ранее в случае войны, объявлением таковой воюющими сторонами.[19]

14 Женевская конвенция от 12 августа 1949 г. об улучшении участи раненых и больных в действующих армиях, (далее – ЖК I), ст. 2; Женевская конвенция от 12 августа 1949 г. об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море, (далее – ЖК II), ст. 2; Женевская конвенция от 12 августа 1949 г. об обращении с военнопленными, (далее – ЖК III), ст. 2; Женевская конвенция от 12 августа 1949 г. о защите гражданского населения во время войны, (далее – ЖК IV), ст. 2, *op. cit.* (примечание 10), с. 3, 32, 57 и 137, соответственно.

15 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 1.

16 Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв вооруженных конфликтов немеждународного характера (Протокол II), принят 8 июня 1977 г., *op. cit.* (примечание 10).

17 Дополнительный протокол I рассматривает конфликты между государствами, а Дополнительный протокол II – конфликты между государством и группой (или группами) повстанцев.

18 Вооруженный конфликт немеждународного характера имеет место исключительно в пределах одного государства.

19 Гаагская конвенция III об открытии военных действий, 18 октября 1907 г., ст. 1, Международное право. Ведение военных

Итак, в общем и целом ясно, что гуманитарное право начинает действовать с началом вооруженного конфликта. Но что есть вооруженный конфликт? В комментариях Международного Комитета Красного Креста к Женевским конвенциям 1949 г. и в комментариях к Дополнительным протоколам 1977 г. этот термин понимается очень широко. В комментарии к Конвенциям вооруженный конфликт трактуется как «любой спор, возникший между двумя государствами и ведущий к *действиям вооруженных сил*, даже если одна из сторон конфликта отрицает наличие состояния войны. При этом не имеет значения, как долго длится конфликт и насколько велики жертвы».[20] Аналогичным образом в комментарии к Дополнительному протоколу I говорится, что «гуманитарное право распространяется на любой спор между двумя государствами *с применением их вооруженных сил*. При этом не имеет значение ни продолжительность, ни интенсивность конфликта...».[21] В комментарии к Дополнительному протоколу II вооруженный конфликт определяется как «наличие открытых *военных действий* между более или менее организованными *вооруженными силами*».[22] *Обязательным условием* во всех трех случаях является использование вооруженных сил.

Но спор или разногласие, ведущие к использованию вооруженных сил, не могут быть единственным критерием. Вооруженные силы постоянно используются против неприятеля, не при-

действий, *op. cit.* (примечание 10), с. 15. Согласно комментарию к Женевским конвенциям 1949 г. «… нет больше необходимости в формальном объявлении войны или в признании состояния войны в качестве предварительного условия применения Конвенции. Конвенция становится применимой с момента фактического начала военных действий». 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 (далее – GC I Commentary).

20 GC I Commentary, *op. cit.* (примечание 19), с. 32–33 (выделено нами).

21 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987, (далее – Additional Protocols: Commentry) ч. 62 (выделено нами). Комментарий к Дополнительному протоколу II отсылает к комментарию к ст. 3, общей для четырех Женевских конвенций 1949 г., и к Комментарию к Дополнительному протоколу I, Комментарий к Дополнительному протоколу II. МККК. Москва. 2000, ч. 4448.

22 Комментарий к Дополнительному протоколу II, *op. cit.* (примечание 21), ч. 4341 (выделено нами).

водя обязательно к состоянию вооруженного конфликта, например при авиационной рекогносцировке или наблюдении. Более того, сегодня общепризнано, что такие изолированные инциденты, как пограничные стычки или ограниченные по масштабу вылазки, не достигают уровня вооруженного конфликта в том смысле, как этот термин применяется в гуманитарном праве.[23] Отсюда следует, что практика государств, подтверждаемая трудами специалистов-международников, показывает, что содержащееся в Дополнительном протоколе I отрицание критериев интенсивности и продолжительности оказывается несколько преувеличенным.

Напротив, «вооруженные силы» более логично понимать как краткое нормативное обозначение деятельности определенного характера и интенсивности. Во времена создания соответствующих правовых актов *вооруженные* силы являлись субъектами, осуществлявшими рассматриваемые действия требуемого уровня интенсивности; цель достигалась именно тем, что внимание сосредоточивалось на вооруженных силах. Получившие подтверждение соответствующие положения Конвенций и комментарии к ним основывались на субъектах деяний, так как ссылка на субъекты нежелательных деяний, а именно на вооруженные силы, была в то время удобным и надежным способом регламентирования таких деяний.

О каких же деяниях идет речь? Логичный ответ нам дают цели, лежащие в основе гуманитарного права. Из изучения его документов, принципов становится ясно, что его суть заключается в предоставлении защиты лицам, не принимающим непосредственного участия в военных действиях, а также их имуществу.[24] Особенно следует отметить, что объектами защиты являются гражданское населе-

23 См., например, обсуждение этого вопроса в: Ingrid Detter De Lupis, *The Law of War*, 2nd ed., Cambridge University Press, Cambridge, 2000, pp. 20–21; Christopher Greenwood, «Historical Development and Legal Basis», in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflict*, Oxford University Press, Oxford, 1995, p. 42.

24 Например, в Преамбуле к Дополнительному протоколу I говорится, что необходимо «… подтвердить и развить положения, предусматривающие защиту жертв вооруженных конфликтов, и дополнить меры, направленные на обеспечение более эффективного их применения…». Дополнительный протокол I, *op. cit.* (примечание 10).

ние и гражданские объекты, а также лица, вышедшие из строя (например, раненые и взятые в плен), или оказывающие гуманитарную помощь (например, медицинский персонал). Когда речь идет о целях защиты, на которую они имеют право, то обычно говорят о защите от ранения или смерти, а когда речь идет об имуществе, —от ущерба или разрушения. Эти цели Женевского права дополняются нормами Гаагского права, направленного на ограничение страданий путем, как правило, ограничений, налагаемых на определенные виды оружия и методы ведения военных действий.[25]

Это очень краткое изложение основных целей гуманитарного права помогает понять суть термина «вооруженный конфликт». Вооруженный конфликт имеет место, когда группа людей предпринимает действия, причиняющие ранения, смерть, ущерб или разрушение. Этот термин также обозначает действия, направленные на достижение таких результатов, или предвидимые последствия которых будут таковыми. Так как речь идет о jus in bello, а не о jus ad bellum, то мотивация, лежащая в основе этих действий, не имеет значения. Это же относится и к противоправности или законности таких действий. Поэтому, например, сторона, начинающая вооруженный конфликт такими действиями, возможно, руководствуется законными соображениями упреждающей (или препятствующей) самообороны; тем не менее, поскольку действия были направлены на причинение ранения, смерти, ущерба или разрушения, они регулируются гуманитарным правом. Следует отметить, что, согласно преобладающим сегодня взглядам, действия, носящие спорадический или изолированный характер, не удовлетворяют этим требованиям. Кроме этого, поскольку речь идет о праве, применимом к

25 Термин «Женевское право» относится к разделу права вооруженных конфликтов, предоставляющего покровительство следующим категориям лиц: гражданскому населению, военнопленным, больным, потерпевшим кораблекрушение, а также медицинскому персоналу. Оно отличается от Гаагского права, регулирующего применение методов и средств ведения военных действий, оккупацию и нейтралитет. О международных правовых документах, относящихся к каждому из этих разделов или включающих элементы обоих разделов, см.: Фредерик де Мулинен. Право войны. Руководство для вооруженных сил. МККК. Москва. 1999, с. 3–4.

международным вооруженным конфликтам, необходимо, чтобы ответственность за соответствующие действия можно было возложить на государство.[26]

Возвращаясь к рассматриваемой теме и не касаясь вопросов *ad bellum*, следует отметить, что принципы гуманитарного права применимы, когда нападение на компьютерные сети, которое может быть приписано государству, является отнюдь не спорадическим и изолированным инцидентом и либо имеет целью причинить ранение, смерть, ущерб или разрушение (или привести к аналогичным результатам), либо такие результаты предсказуемы. И не важно, что здесь не используются классические *вооруженные* силы. В соответствии с этим критерием нападение представителями какого-либо государства на компьютерную сеть системы управления воздушным движением большого аэропорта другого государства подпадает под действие гуманитарного права. Это же относится и к нападению с целью разрушения нефтепроводов путем резкого повышения давления нефти в них после взятия под контроль компьютеров, регулирующих расход нефти[27]; и к нападению, ведущему к расплавлению ядерного реактора путем нарушения работы его компьютерного центра управления; и к использованию компьютеров для выпуска токсичных химикатов из производственных помещений или хранилищ. С другой стороны, гуманитарное право не распространяется на нарушение работы университетской интрасети, на перекачку финансовой отчетности, на временную приостановку доступа к Интернету или на кибершпионаж, так как даже если такие нападения и являются частью широкой кампании аналогичных действий, их предсказуемые последствия не заключаются в причинении ранения, смерти, ущерба или разрушения.

26 О возложении ответственности за деяние на государство см. Проект статей «Ответственность государств за международно-противоправные деяния», принятый Комиссией международного права на ее пятьдесят третьей сессии (2001 г.). ООН, A/RES/56/83.

27 Возможность такого развития событий описана в *President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures*, October 1997, at A–46.

Должно быть ясно, что — с учетом прогресса в методах и средствах ведения войны, и особенно, информационной войны — критерий субъекта недостаточен для применения гуманитарного права; вместо него более подходит критерий последствий. Вряд ли это может считаться открытием в области права. Нельзя же отрицать, например, что биологическая или химическая война (без применения «силового» оружия) подпадают под гуманитарное право. Принятие возможных последствий в качестве критерия обосновано также тем, что с началом вооруженного конфликта законность или незаконность деяния никак не зависят от средства причинения ранения, смерти, ущерба или разрушения (за исключением запрещений, касающихся конкретных видов вооружений). Умышленный выбор гражданского лица или других пользующихся защитой лиц или объектов в качестве цели нападения является незаконным, независимо от применяемых для этого методов или средств. Использование голода, удушения, избиения, расстрела, бомбардировки и даже кибернападения — все это входит в сферу действия гуманитарного права, поскольку следствием является определенный результат. Этот факт опровергает любое утверждение о том, что кибернападения сами по себе не подпадают под действие гуманитарного права, поскольку они якобы не «вооруженная» сила. Нет, они могут либо подпадать, либо не подпадать — все зависит от характера и возможных последствий таких нападений.

Объекты нападения на компьютерные сети

Как указывалось выше, нападения на компьютерные сети подпадают под действие гуманитарного права, если они являются неотъемлемой частью либо классического конфликта, либо «кибернетической войны», целью или предвидимым последствием которых является причинение ранения, смерти, ущерба или разрушения. Если это так, то необходимо выяснить, на какие объекты могут быть направлены такие нападения.

Для начала полезно выяснить, на какое поведение распространяются нормы, основанные на обычае и регулирующие выбор целей. Поскольку в наиболее актуальных, в данном контексте,

положениях Дополнительного протокола I сформулированы нормы, применимые как к его участникам, так и к сторонам, не являющимся участниками (в качестве императивной нормы обычного права), то инструмент служит удобной отправной точкой для дальнейших рассуждений.[28] Статья 48, являющаяся основной нормой, обеспечивающей защиту гражданского населения, предусматривает, что «...стороны, находящиеся в конфликте, должны ... направлять свои действия только против военных объектов».[29] На первый

28 Не будучи участником Протокола I, США тем не менее считают, что многие его положения являются выражением обычного международного права. Неофициальное, но авторитетное, по общему мнению, описание таких положений см. в Michael J. Matheson, «Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions», *American University Journal of International Law and Policy*, Vol. 2, 1987, p. 419. См. также International & Operational Law Division, Office of the Judge Advocate General, Department of the Air Force, *Operations Law Deployment Deskbook*, tab 12, no date, and comments by the then State Department Legal Advisor Abraham D. Soafer in «Agora: The US Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims», *American Journal of International Law*, Vol. 82, 1988, p. 784.

29 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 48. Первостепенное значение этого принципа для гуманитарного права отмечено в комментарии МККК к этой статье:

«В этой статье подтверждена основная норма защиты и проведения различия. Это фундамент, на котором зиждется кодификация законов и обычаев войны: гражданское население и гражданские объекты пользуются уважением и защитой в период вооруженных конфликтов, и с этой целью необходимо проведение различия между ними и комбатантами и военными объектами. Вся правовая система, созданная в Гааге в 1899 и 1907 г. и в Женеве с 1864 по 1977 гг. основана на этой норме обычного права. Эта норма уже подразумевалась в Санкт-Петербургской декларации 1868 г. об отмене употребления взрывчатых и зажигательных пуль, в которой говорится, «что единственная законная цель, которую должны иметь государства во время войны, состоит в ослаблении военных сил неприятеля». Это было связано с желанием предотвратить чрезмерные повреждения и излишние страдания комбатантов путем запрещения использования взрывчатых снарядов весом менее 400 граммов и не было специально направлено на защиту гражданского населения. Тем не менее иммунитет гражданского населения в этом документе косвенно подтверждался… В Гаагских конвенциях 1899 и 1907 гг., так же как и в Женевских конвенциях 1929 и 1949 гг., норма защиты рассматривалась в качестве общепринятой нормы права, хотя в то время не считалось необходимым дословно формулировать эту норму в самих текстах. Эта норма включена в рассматриваемый Протокол с целью подтверждения необходимости проведения различия и установления ограничений на нападения на военные объекты». Additional Protocols: Commentry, *op. cit.* (примечание 21), ч. 1863–1864.

взгляд, ст. 48 исключает возможность *любой* военной операции, в том числе, НКС, направленной не против чисто военного объекта. Однако это не так. В последующих статьях запрещения постоянно формулируются с использованием термина «нападение»: «гражданское население как таковое, а также отдельные гражданские лица не должны являться объектом нападений»;[30] «гражданские объекты не должны являться объектом нападения»;[31] «нападения неизбирательного характера запрещаются»[32], «нападения должны строго ограничиваться военными объектами»[33] и так далее. Термин этот точно определен в ст. 49: «нападения» означают акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне». Следовательно, вообще говоря, запрещение касается не столько выбора невоенных объектов в качестве объектов нападения, сколько *нападения* на них, особенно с применением насилия. Подтверждением такой интерпретации служит ст. 51, в которой формулируется общий принцип, гласящий, что «гражданское население и отдельные гражданские лица пользуются общей защитой от *опасностей*, возникающих в связи с военными операциями», которая запрещает «акты *насилия* или угрозы *насилием*, имеющие основной целью терроризировать гражданское население».[34] Об этом же говорится в комментарии к ст. 48, где отмечается, что «слово «операция» следует понимать в контексте всего раздела; оно имеет в виду военные операции, в процессе которых используется *насилие*».[35]

В свете такой интерпретации — исключается ли нападение на компьютерные сети из категории «нападений» по той причине, что здесь отсутствует насилие? Нет, и по той простой причине, что вооруженные нападения могут включать и кибернападение. «Нападения» — это краткое нормативное обозначение, предназначенное для описания определенных последствий. Очевидно, что соответствующие положения направлены на защиту пользующихся покрови-

30 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 51(2).
31 *Ibid.*, ст. 52(1).
32 *Ibid.*, ст. 51(4).
33 *Ibid.*, ст. 52(2).
34 *Ibid.*, ст. 51(1) и 51(2) (выделено нами).
35 Additional Protocols: Commentry, *op.cit.* (примечание 21), ч. 1875 (выделено нами).

тельством лиц от ранения и смерти, а пользующихся покровительством объектов — от ущерба и разрушения. В терминологическом смысле «насилие» следует рассматривать здесь в качестве *последствий* насилия, а не *актов* насилия. Большие физические или душевные страдания[36] людей естественным образом подпадают под концепцию ранения; аналогичным образом полная потеря средств (например, денег, акций и др.), которые могут быть превращены в реальную собственность, представляет собой ущерб или разрушение. Дело в том, что причинение неудобства или беспокойства или лишь ухудшение качества жизни не удовлетворяют этому требованию; достаточным критерием являются страдания людей. Например, подрыв фондового рынка или банковской системы могут, по существу, привести к краху экономики и, как результат, — к тяжелой безработице, голоду, душевным страданиям и т. д., что подтверждается трагическими событиями депрессии 1930-х гг. Если НКС приведет к таким же тяжелым страданиям, то оно явится «нападением» в том смысле, в котором этот термин применяется в гуманитарном праве.

Другие статьи этого раздела подтверждают такое толкование. Например, в правилах соразмерности говорится о нападении, которое может повлечь «потери жизни среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам или то и другое вместе»[37]; в правилах, относящихся к охране окружающий среды, говорится о методах и средствах, которые причинят «обширный, долговременный и серьезный ущерб»[38]; защита плотин, дамб и атомных электростанций формулируется с использованием терминов «тяжелые потери среди гражданского населения»[39], «которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить». Кроме этого, во время переговоров по Дополнительному протоколу I был поднят вопрос о том, является ли установка наземных

36 Учет человеческих страданий вполне логичен, так как Дополнительный протокол запрещает терроризировать, то есть психологически воздействовать. Дополнительный протокол I, *op. cit.* (примечание 10), ст. 51(2).

37 *Ibid.*, ст. 51(5)(b); 57(2)(a)(iii); 57(2)(b).

38 *Ibid.*, ст. 35(3) and 55(1).

39 *Ibid.*, ст. 56(1).

мин нападением. Большинство посчитало, что является, так как «всякий раз, когда человек подвергается опасности в результате установки мины, это нападение»[40]. Аналогичным образом нападение на компьютерную сеть, представляющее предсказуемую угрозу для покровительствуемых лиц или имущества, является нападением.

Вернемся снова к ст. 48. В качестве общего правила (различные другие запрещения рассмотрены ниже) эта статья запрещает такие направленные против невоенных целей НКС, целью или предсказуемым результатом которых являются ранение, смерть, ущерб или разрушение. При отсутствии иных специальных запрещающих положений гуманитарного права операции НКС, которые едва ли могут привести к вышеуказанным последствиям, допустимы против невоенных объектов, например против гражданского населения.[41] В результате такого разграничения важность тщательной оценки того, является или не является операция информационной войны «нападением», явно возрастает. В прошлом подход к этой проблеме сводился к формулировке *res ipsa loquitor (лат.* — вещь говорит сама за себя). Однако НКС гораздо менее однозначны по сравнению с традиционными военными операциями и поэтому требуют более глубокого рассмотрения с точки зрения их последствий.

НКС резко расширяют возможности для выбора целей (но не нападения) среди невоенных объектов, но неверно было бы рассматривать это как ослабление всей правовой структуры. Напротив, это просто отражает расширение диапазона допустимых методов и средств в результате технологического прогресса, а существующие нормы не меняются. Вспомним, например, что психологические операции против гражданского населения, не причиняющие физического вреда, совершенно допустимы, если их целью не является терроризирование.[42] И не важно, носит ли операция воен-

40 Additional Protocols: Commentry, *op. cit.* (примечание 21), ч. 1881.

41 См.: Haslam, *op. cit.* (примечание 9), p. 173.

42 США даже разработали доктрину ведения психологических операций. Joint Chiefs of Staff, Joint Doctrine for Psychological Operations, Joint Publication 3–53, 10 July 1996. Акты, имеющие целью терроризировать гражданское население, запрещены Дополнительным протоколом I, *op. cit.* (примечание 10), ст. 51(2).

ный или невоенный характер. Однако, несмотря на то что объективный режим остается неизменным, появление НКС обнаруживает правовой пробел, который, оставаясь незаполненным, неминуемо усилит воздействие войны на гражданское население.

Если операция НКС есть «нападение», то на что оно нацелено? Теоретически возможные цели подразделяются на три обширные категории: 1) комбатанты и военные объекты; 2) гражданское население и гражданские объекты; 3) объекты двойного назначения. Кроме этого, отдельные виды потенциальных целей пользуются специальной защитой. Полезно рассмотреть каждую из этих категорий в отдельности.

Комбатанты и военные объекты

Комбатанты и военные объекты являются по определению законными целями и могут подвергаться нападению, если используемые для этого методы и средства, как об этом будет говориться в следующем разделе, соответствуют ограничениям, налагаемым гуманитарным правом. Лица, планирующие нападения или принимающие решение о нападении, обязаны сделать «все практически возможное», чтобы удостовериться в том, что объекты нападения являются законными, то есть не пользуются иммунитетом от нападения согласно гуманитарному праву.[43]

43 Additional Protocol I, *op. cit.* (примечание 10), ст. 57(2)(a)(i). В комментарии к этому положению более подробно объясняется эта обязанность:

«Конечно, лица, планирующие такое нападение или принимающие решение о нем, будут исходить из информации, которую они получают, и нельзя ожидать, что они лично будут знать объект нападения или его точные характеристики. Это, однако, не снимает с них ответственности, и в сомнительных случаях, даже при малейшем сомнении, они должны затребовать дополнительную информацию и, при необходимости, дать указание тем из своих подчиненных и тем лицам, отвечающим за огневую поддержку (особенно за артиллерию и авиацию), в компетенцию которых это входит и которые несут перед ними ответственность, о проведении дополнительной разведки. В случае дальнего огневого воздействия информацию получают, в частности, при помощи воздушной разведки и служб разведки, которые, естественно, пытаются собрать данные о вражеских военных целях, используя различные средства. При оценке информации следует тщательно проверять ее надежность, не забывая при этом, что ничто не мешает противнику устраивать ложные военные объекты и маскировать реальные. На самом деле ясно, что никакой ответственный военачальник не заинтересован нападать на объекты, не пред-

Комбатантами называются лица, входящие в состав вооруженных сил, кроме медицинского и духовного персонала; вооруженные силы «состоят из всех организованных вооруженных сил, групп и подразделений, находящихся под командованием лица, ответственного перед этой стороной [находящейся в конфликте] за поведение своих подчиненных... Такие вооруженные силы подчиняются внутренней дисциплинарной системе, которая, среди прочего, обеспечивает соблюдение норм международного права, применяемых в период вооруженных конфликтов»[44]. Нападение на компьютерные сети, заставляющее, например, военную систему управления воздушным движением выдавать ложную навигационную информацию, в результате чего разбивается самолет военно-транспортной авиации, перевозящий комбатантов, безусловно, допустимо.

К военным объектам, согласно ст. 52 Дополнительного протокола I, относятся те 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».[45] Военное оборудование и установки, кроме предметов медицинского и религиозного назначения, безусловно, являются военными объектами и, следовательно, могут быть подвергнуты нападению на компьютерные сети. Это, однако, очевидные примеры. В других случаях зачастую бывает трудно определить, какие объекты являются военными.[46] Проблема заключается в установлении требуемой связи между объектом нападения и военными операциями.

Суть дилеммы — в толковании терминов «эффективный» и «явный». Некоторые структуры, например Международ-

ставляющие интерес с военной точки зрения. В этом отношении интересы гуманитарного права и военные интересы совпадают». Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 2195.

44 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 43(1)–(2).

45 *Ibid.*, ст. 52(2).

46 В Комментарии констатируется: «Текст данного параграфа, безусловно, может послужить хорошим руководством, но его не всегда легко толковать, особенно тем, кто принимает решение о нападении, и о том, какие использовать для этого средства и методы». Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 2016.

ный Комитет Красного Креста (МККК), дают очень узкое толкование этим терминам. Согласно Комментарию МККК к Протоколу, эффективный вклад вносят объекты «непосредственно используемые вооруженными силами» (например, оружие и оборудование), объекты, «особо значимые для военных операций» (например, мосты), а также объекты, которые предполагается использовать, или уже использующиеся для военных целей.[47] Что касается «явного военного преимущества», то Комментарий исключает нападения, которые предполагают лишь «возможное или неопределенное» преимущество.[48] В отличие от этого, США, не ставя под сомнение формулировку определения термина, включают сюда экономические объекты, которые «косвенно, но эффективно поддерживают способность противника вести военные действия», то есть очень широко интерпретируют его.[49]

Это различие наводит на интересные мысли в отношении нападений на компьютерные сети. Допустимо ли нападать на банковскую систему, если богатство является основой военной мощи? А как быть с министерством по налогам? А фондовый рынок? А допустимы ли нападения на брокерские фирмы, если это подорвет заинтересованность инвестирования в экономику? А если экспортная выручка страны слишком зависит от какой-либо одной отрасли промышленности (например, нефтедобывающей), то можно ли использовать нападение на компьютерные сети для подрыва производства и распределения? Проблема удара по экономическим целям особенно актуальна, поскольку функционирование большинства из них глубоко компьютеризировано и поэтому очень привлекательно для тех, кто выбирает цели для информационной войны.

47 *Ibid*. ч. 2020–2023.

48 *Ibid*.ч. 2024.

49 US Navy/Marine Corps/Coast Guard, *The Commander's Handbook on the Law of Naval Operations* (NWP 1–14M, MCWP 5–2.1, COMDTPUB P5800.7), para 8.1.1 (1995), reprinted as an annotated version in *US Naval War College's International Law Studies series*, Vol. 73 (далее – Handbook [Наставление]). Это утверждение названо «формулировкой обычного международного права». В подтверждение ее в Наставлении цитируется General Counsel, Department of Defense, Letter of 22 September 1972, reprinted in *American Journal of International Law*, Vol. 67, 1973, p. 123.

Вопрос критерия, о котором говорилось выше, заключается в следующем: повлечет ли за собой нападение ранения, смерть, ущерб и разрушение? Как только это определено, начинаются различные толкования понятия «военный объект», результатом чего, вероятнее всего, будут различия в оценке легитимности нанесения удара по цели. С другой стороны, если бы операция была нацелена на причинение, например, лишь неудобства, то она не достигла бы уровня нападения и поэтому была бы допустимой, независимо от наличия или отсутствия связи объекта с военной операцией. Например, если бы во время ударов войск НАТО по Белграду в апреле 1999 г. вместо «силового» оружия против сербской государственной телестанции было использовано НКС, то вероятнее всего не было бы ни ранений, ни смертей, ни ущерба или разрушений. В этом случае критика в отношении того, что был-де атакован гражданский объект, скорее всего, не была бы услышана и не было бы той негативной общественной реакции, так же как и рассмотрения в Европейском суде по правам человека.[50]

Гражданское население и гражданские объекты

Гражданские лица — это лица, не рассматриваемые в качестве комбатантов,[51] а гражданский объект — это объект, не являющийся военным.[52] Запрет на нападение на гражданских лиц и гражданские объекты является почти абсолютным. В частности, Дополнительный протокол I предусматривает:

> Статья 51(2): «Гражданское население как таковое, а также отдельные гражданские лица не должны являться объектом нападений. Запрещаются акты насилия или угрозы насили-

50 *Bankovic & Others v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom*, ECHR, App. No. 52207/99 (2001). 12 декабря 2001 г. Суд принял решение, что это заявление неприемлемо.

51 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 50(1).

52 *Ibid.*, ст. 52(2).

ем, имеющие основной целью терроризировать гражданское население».

Статья 52: «Гражданские объекты не должны являться объектом нападения или репрессалий».[53]

При сомнении относительно статуса объекта или лица статус следует считать гражданским.[54] И опять же, в случае нападения на компьютерные сети вопрос критерия заключается в следующем: является ли целью или предсказуемым результатом нападения причинение ранения, смерти, ущерба или разрушения? Если да, то применяется установленное ранее запрещение, которое, безусловно, подтверждает существующее обычное право.

К сожалению, имеются трудности в толковании ясных, на первый взгляд, норм. Ранее было показано, что критерии отличия гражданских объектов от военных могут быть разными. Подобные же различия существуют в отношении того, в каких случаях можно нападать на гражданское лицо. Такая возможность допускается Дополнительным протоколом I только в случае, если гражданское лицо принимает «непосредственное участие в военных действиях», о чем в Комментарии говорится как о «враждебных действиях, которые по своей природе или намерению могут нанести фактический ущерб персоналу или оборудованию вооруженных сил противника».[55] Это – проблема незаконных комбатантов. Некоторые предлагают даже более строго ограничить иммунитет гражданских лиц, например, считать, что гражданские лица, не участвующие непосредственно во враждебных действиях, но выполняющие на военной базе во время военных действий существенные с точки зрения

53 *Ibid.*, ст. 51(2) и 52. Статут Международного уголовного суда также запрещает умышленные нападения на гражданское население или на гражданские объекты. Римский статут Международного уголовного суда (в дальнейшем – Римский статут). Статьи 8(2)(b)(i) и (ii). См. также M. Cherif Bassiouni, *The Statute of the International Criminal Court: A Documentary History*, Transnational Publishers, New York, 1999. p. 39.

54 *Ibid.*, ст. 50(1) (в отношении гражданского населения) и ст. 52(3) (в отношении гражданских объектов).

55 *Ibid.*, ст. 51(3); Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 1944.

поставленных задач функции, являются законными целями для нападения.[56]

В контексте информационных операций вопрос определения гражданских лиц и объектов приобретает большое значение. В некоторых странах предпочитают передавать функции информационной войны, будь то обслуживание оборудования или ведение операций, сторонним лицам. Более того, нападение на компьютерные сети может быть поручено невоенным государственным службам. В случае если гражданский подрядчик или невоенный персонал выполняют вспомогательные функции, необходимые для проведения операций, например обслуживают оборудование для НКС, то, с точки зрения последней интерпретации, на них можно сразу же нападать. Поскольку они являются важными целями, то любой причиненный им вред не будет учитываться при оценке соразмерности нападения (см. выше). С другой стороны, если критерий «непосредственное участие в военных действиях» понимать в узком смысле, то это означает, что сохраняется покровительство, которым они пользуются в качестве гражданских лиц, а в случае пленения они в качестве лиц, «следующих за вооруженными силами», имеют право не статус военнопленных.[57]

Если гражданские лица сами участвуют в нападении на компьютерные сети, то проблема становится более сложной. Если результатом НКС явилось причинение ранения, смерти, ущерба или разрушения или если была предсказуемая угроза такого результата, то «преступники» являются незаконными комбатантами. Этот статус применим, поскольку они принимали непосредственное участие в военных действиях, не выполняя требований, предъявляемых к комбатантам. В качестве незаконных комбатантов они могут подвергаться непосредственным нападениям, а причиненный им вред не будет учитываться при оценке соразмерности, в случае же пленения они не будут иметь права на статус военнопленных.

56 Письмо от начальника управления военной юстиции Министерства армии США советнику посольства ФРГ по вопросам исследований в области обороны и технологии (экономика) от 22 января 1988 г., цитируется по W.H. Parks, «Air War and the Law of War». *Air Force Law Review*, Vol. 32, 1992. p. 1.

57 ЖК III, *op. cit.* (примечание 14), ст. 4(4).

И наоборот, если гражданские лица осуществляли операции, связанные с компьютерными сетями, которые не достигли уровня «нападений», то такие лица не будут считаться незаконными комбатантами, так как они не совершили «враждебных действий, которые по своей природе или намерению могут нанести фактический ущерб персоналу или оборудованию вооруженных сил противника». Их гражданский статус и соответствующее право на покровительство остаются неизменными. Тем нем менее, так же как и вспомогательный персонал, если они приписаны к военной части и следуют за ней, то в случае пленения они получают статус военнопленных.[58] Конечно, сооружения и оборудование, используемые для осуществления операций, безусловно, могут стать военными целями и в результате быть подвергнуты нападению; но непосредственно на операторов нападать нельзя.

Понятно, что использование гражданских лиц, будь то подрядчики или государственные служащие, чревато юридическими ловушками. Очевидно, что разумный подход заключается в использовании военного персонала для целей информационной войны.

Объекты двойного назначения

Объект двойного назначения — это объект, используемый как для гражданских, так и для военных целей. Примерами общеизвестных объектов двойного назначения являются аэропорты, железные дороги, энергосистемы, коммуникационные системы, заводы, производящие предметы военного и гражданского назначения и спутники, как, например, INTELSAT, EUROSAT и ARABSAT, и др. Если объект используется для военных целей, то он является военным объектом и может подвергнуться нападению, включая нападение на компьютерные сети, даже если военное назначение объекта вторично по сравнению с гражданским.

Здесь следует сделать несколько оговорок. Во-первых, является ли объект военным объектом, зависит от того, какое толкование термина — узкое или широкое — принимается. Во-вторых, являет-

58 *Ibid*.

ся ли объект объектом двойного назначения и, следовательно, военным объектом, зависит от характера конкретного конфликта. Например, летное поле в одном случае может использоваться для снабжения войск, а в другом — не использоваться в военных целях. В-третьих, объект, который можно использовать для военных целей, но который в настоящее время используется исключительно для гражданских целей, является военным объектом в том случае, если вероятность его военного использования обоснована и не отдалена по времени от момента конфликта. И наконец, объекты двойного назначения следует тщательно оценить с точки зрения требований проведения различия и соразмерности, о чем говорилось выше, так как нападение на такие объекты связано с риском причинения побочного вреда и случайного ущерба гражданскому населению и гражданским объектам.

Объекты, пользующиеся особой защитой

Кроме общих норм, относящихся к защите гражданского населения, некоторые объекты пользуются особой защитой. Противоречивой категорией объектов, подлежащих особой защите, являются плотины, дамбы и атомные электростанции. Поскольку функционирование этих объектов зависит от компьютеров и компьютерных сетей, то они особенно уязвимы для НКС. Статья 56 Дополнительного протокола I, с которой не согласны США, запрещает нападать на подобные сооружения, «если такое нападение может вызвать высвобождение опасных сил [например, воду или радиоактивность] и последующие тяжелые потери среди гражданского населения».[59]

59 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 56(1). Это запрещение распространяется и на нападения на другие военные объекты, находящиеся поблизости от них, если нападение может вызвать высвобождение опасных сил. Имеются исключения к общему запрещению, предусмотренному этой статьей:

«2. Общая защита от нападения, предусмотренная в пункте 1, прекращается:

a) в отношении плотин и дамб только в том случае, если они используются каким-либо образом, отличающимся от их нормального функционирования, и для регулярной существенной и непосредственной поддержки военных операций и если такое нападение является единственным практически возможным способом прекратить такую поддержку;

b) в отношении атомных электростанций только в том случае, если они вырабатывают электроэнергию для регулярной существенной и непосредственной поддержки военных операций и если такое

Данное запрещение действует, даже если это военные объекты. Между прочим, НКС — это достаточно надежное средство нейтрализации таких сооружений без высвобождения опасных сил, что трудно выполнимо при использовании «силового» оружия.

Запрещаются нападения с целью вызвать голод среди гражданского населения или иным способом лишить его объектов, необходимых для выживания,[60] даже если «жертвой» таких нападений, как предполагалось, должны были стать вооруженные силы противника.[61] В число необходимых для выживания объектов входят запасы продуктов питания, посевы, скот, питьевая вода. Согласно этому ограничению нападение на компьютерные сети, скажем, системы хранения и распределения продуктов питания или водоочистных сооружений, обслуживающих гражданское население, недопустимо, даже если ими пользуются также и вооруженные силы.

Кроме этого, Дополнительный протокол I запрещает проведение военных операций, которые могут причинить обширный, долговременный и серьезный ущерб природной среде,[62] хотя США не

нападение является единственным практически возможным способом прекратить такую поддержку;

c) в отношении других военных объектов, размещенных в этих установках или сооружениях или поблизости от них только в том случае, если они используются для регулярной существенной и непосредственной поддержки военных операций и если такое нападение является единственным практически возможным способом прекратить такую поддержку».

Ibid., ст. 56(2).

60 *Ibid.*, ст. 54(2). См. также Римский статут, *op. cit.* (примечание 53), ст. 8(2)(b)(xxv).

61 Additional Protocols: Commetnary, *op. cit.* (примечание 21), ч. 2110. Запрещение, однако, не применяется в отношении объектов, используемых противником для жизнеобеспечения исключительно его вооруженных сил или «для прямой поддержки военных действий». Дополнительный протокол I, *op. cit.* (примечание 10), ст. 54(3). Примером последнего может служить использование сельскохозяйственных угодий в качестве укрытия для вооруженных сил.

62 *Ibid.*, ст. 35(3) и 55. См. также Римский статут, *op. cit.* (примечание 53), ст. 8(2)(b)(iv). По проблеме ущерба, причиняемого природной среде во время вооруженных конфликтов см.: Jay E. Austin and Carl E. Bruch (eds), *The Environmental Consequences of War: Legal, Economic, and Scientific Perspectives*, Cambridge University Press, Cambridge, 2000; Michael N. Schmitt, «Green War: An Assessment of the Environmental Law of International Armed Conflict», *Yale Journal of International Law*, Vol. 22.1997, pp. 1–109; Richard J. Grunawalt, John E. King and Ronald S. McClains (eds). *Protection of the Environment during Armed Conflict and other Military Operations*, US Naval War College International Law Studies. Vol. 69, 1996.

считают, что это положение является формулировкой обычного права. Нападение на компьютерные сети вполне может привести к таким опустошительным последствиям. Удар по ядерному реактору может вызвать расплавление его активной зоны и последующее высвобождение радиоактивности. Аналогичным образом НКС может быть использовано для того, чтобы вызвать утечку химикатов из производственных или складских емкостей или для разрушения крупного нефтепровода. Существует много других возможностей причинения ущерба природной среде при помощи НКС. Необходимо отметить, что запрещение применимо и в том случае, если нападение было направлено на законную военную цель и даже если это нападение отвечает требованию соразмерности. Если ожидаемый ущерб превышает допустимый уровень, то операция запрещается.

И наконец, необходимо отметить, что существует ряд других объектов, лиц и видов деятельности, пользующихся особой защитой, которые уязвимы для нападений на компьютерные сети, но которые не представляют в отношении НКС каких-либо особенных преимуществ или проблем. При выборе целей нападения с этими объектами следует обращаться так же, как и при планировании «силовых» нападений.[63] Кроме того, имеются ограничения на нанесение

63 Например, военные и гражданские медицинские формирования и предметы медицинского снабжения не подлежат нападению, если они не используются для военных целей. Дополнительный протокол I, *op. cit.* (примечание 10), ст. 12. Имеются специальные критерии для распространения этой защиты на гражданские учреждения. *Ibid.*, ст. 12(2). См. также Римский статут, *op. cit.* (примечание 53), ст. 8(2)(b)(ix) и (xxv). Медицинский транспорт пользуется аналогичным покровительством. Дополнительный протокол I, *op. cit.*, ст. 21–31. Степень защиты зависит от типа санитарных перевозок и их местоположения. Другими объектами, пользующимися покровительством, являются культурные ценности, места отправления культа, а также убежища, оборудование и материалы организаций гражданской обороны. *Ibid.*, ст. 53 и 62(3). Кроме этого, запрещается затруднять проведение операций по оказанию гуманитарной помощи. *Ibid.*, ст. 70. Применяются специальные положения в отношении того, когда такие операции имеют право на защиту. Римский статут, *op. cit.* (примечание 53), ст. 8(2)(b)(iii). Согласно этим запрещениям нападение на компьютерные сети с целью, например, изменения информации о группах крови в базе данных больницы, или отключения электроэнергии в бомбоубежище, или преднамеренной переадресации грузов гуманитарной помощи будет незаконным. Конечно, использование покровительствуемых объектов или зон не по назначению, для военных целей, превращает их в законные военные объекты, которые можно подвергать нападению.

ударов, в том числе, на нападения на компьютерные сети, по некоторым объектам и лицам — в качестве репрессалий.[64]

Ограничения, налагаемые на нанесение ударов по законным целям

Основные предписания относительно нанесения ударов по законным целям базируются на принципе проведения различия.[65] Этом принцип наиболее наглядно показывает, как в гуманитарном праве соблюдается баланс интересов государства, прибегающего к насилию, и более широких человеческих интересов, заключающихся

64 Репрессалии – это незаконные в других случаях действия, применяемые в ответ на незаконное поведение противника. Они должны применяться с единственной целью – заставить противника действовать законно. Противник при этом должен быть предварительно предупрежден (если это возможно); репрессалии должны быть соразмерны нарушениям, допускаемым противником, и должны прекращаться, как только он начнет соблюдать существующие ограничения на свое поведение. Право на репрессалии было сильно ограничено договорным правом, которое в большой степени отражает обычное право. Существуют специальные запрещения на репрессалии против гражданского населения; военнопленных, раненых, больных и лиц, потерпевших кораблекрушение; медицинского и духовного персонала и их оборудования; покровительствуемых зданий, оборудования и судов; гражданских объектов; культурных ценностей; объектов, необходимых для выживания гражданского населения; установок, содержащих опасные силы; а также против природной среды. ЖК I *op. cit.* (примечание 14), ст. 46; ЖК II *op. cit.* (примечание 14), ст. 47; ЖК III *op. cit.* (примечание 14), ст. 13; ЖК IV *op. cit.* (примечание 14), ст. 33; Дополнительный протокол I, *op. cit.* (примечание 10), ст. 20, 51–56. Следует признать, что некоторые страны считают, что ограничения, налагаемые Дополнительным протоколом I на репрессалии, не отражают обычного права. США, признавая, что в большинстве случаев репрессалии против гражданского населения нецелесообразны (и незаконны), утверждают, что их абсолютное запрещение «устраняет важное сдерживающее средство, которое в настоящее время защищает гражданское население и другие жертвы войны всех участвующих в конфликте сторон». Soafer, *op. cit.* (примечание 28), p. 470. Официальную точку зрения США по вопросу репрессалий против гражданского населения см. в Handbook, *op. cit.* (примечание 49), части 6.2.3 и 6.2.3.1–3. При присоединении к Протоколу Соединенное Королевство заявило оговорку точно такого же содержания. Перепечатано в Red Cross Treaty Database (договорная база данных МККК) на сайте http://www.icrc.org/ihl. По мнению этих и других стран, принявших данную точку зрения, нападения в качестве репрессалий на компьютерные сети являются вопросом не права, а политики.

65 Подробный анализ этого принципа см. в Esbjörn Rosenblad, *International Humanitarian Law of Armed Conflict: Some Aspects of the Principle of Distinction and Related Problems*, Henry Dunant Institute, Geneva, 1979.

в защите не принимающих в нем участия людей от последствий, — того, что, в лучшем случае, является печальной необходимостью.

Требование проведения различия двояко. В отношении оружия оно запрещает использование таких его видов, которые не способны действовать, проводя различие между комбатантами и военными объектами, с одной стороны, и гражданским населением, гражданскими объектами и другими находящимися под покровительством объектами — с другой. В отношении тактики и использования оружия оно требует, чтобы при осуществлении военных операций принимались меры для проведения различия между указанными двумя категориями — военной и гражданской. В Дополнительном протоколе I это сформулировано в ст. 51(4):

«К нападениям неизбирательного характера относятся: (a) нападения, которые не направлены на конкретные военные объекты; (b) нападения, при которых применяются методы или средства ведения военных действий, которые не могут быть направлены на конкретные военные объекты; или (c) нападения, при которых применяются методы или средства ведения военных действий, последствия которых не могут быть ограничены, как это требуется в соответствии с настоящим Протоколом, и которые, таким образом, в каждом таком случае поражают военные объекты и гражданские лица или гражданские объекты без различия».

Подпункт (a) относится к неизбирательному использованию, а подпункты (b) и (c) — к неизбирательным оружию и тактике. Проблема неизбирательного использования включает три взаимосвязанных компонента: проведение различия, соразмерность и сведение к минимуму побочного вреда и случайного ущерба.[66]

66 Эта классификация заимствована из работы: Christopher Greenwood, «The Law of Weaponry at the Start of the New Millennium», in Michael N. Schmitt and Leslie C. Green (eds), *The Law of Armed Conflict: Into the Next Millenium*, Naval War College, Newport, RI, 1998, p. 185; работа опубликована также в *US Naval War College International Law Studies*, Vol. 71, 1998. В ВВС США используют категории военной необходимости, гуманности и рыцарства, а принцип соразмерности является частью категории необходимости, а ВМС США используют категории военной необходимости, гуманности и рыцарства. Ср.: Department of the Air Force, I*nternational Law: The Conduct of Armed Conflict and Air Operations*, AF Pamphlet 110–31, 1976, at 1–5–1–6 with Handbook, *op. cit.* (примечание 49), para. 5–1.

Оружие неизбирательного действия

Нападения на компьютерные сети осуществляются системой оружия, состоящей из компьютера, программы и средств, при помощи которых эта программа передается. Очевидно, что сам компьютер — машина избирательного действия, так как он может очень точно пересылать программу на те или иные компьютеры или сети. Так, например, работает электронная почта. Можно написать программу, которая — возможно умышленно — окажется абсолютно неизбирательной. Известным примером является компьютерный вирус, который без всякого участия его создателя распространяется от компьютера к компьютеру. Так как программу, даже если это неуправляемый вирус, можно нацеливать на конкретные военные объекты, то ее нельзя относить к оружию неизбирательного действия на том основании, что ею нельзя управлять. Впрочем, такая программа может оказаться неизбирательной в том случае, если ее *последствия* нельзя ограничить. Во многих случаях после запуска программы-вируса для поражения компьютера или сети оператор, осуществивший нападение, не имеет никаких возможностей ограничить ее последующую ретрансляцию. Это вполне возможно и в отношении закрытых сетей, так как вирус можно передавать при помощи дискет. Короче говоря, злонамеренная программа, которая может бесконтрольно распространяться по гражданским сетям, является оружием неизбирательного действия и потому подлежит запрету.

Но следует, однако, осторожно относиться к этому ограничению. Заметим, что в ст. 51(4) говорится о «методах и средствах ведения военных действий». Средство ведения военных действий определено в комментарии к Дополнительному протоколу I как «оружие», а методы ведения военных действий — это способ использования оружия.[67] В обычном значении «оружие» — это то, что может использоваться для *нападения* на противника. Из вышеизло-

67 Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 1957.

женной трактовки термина «нападения» в гуманитарном праве следует, что компьютерная программа явится частью системы оружия только в том случае, если она может оказать воздействие, охватываемое этим термином, а именно, причинять ранение, смерть, ущерб и разрушение (в том числе и такие сопутствующие виды воздействия, как причинение тяжелых душевных страданий, запугивание и т. д.). Если же она не может оказать такого воздействия, то программа не является частью системы оружия и, следовательно, не подлежит запрету — во всяком случае, на основании ее неизбирательного характера.

Проведение различия

Принцип проведения различия, который, безусловно, является частью обычного гуманитарного права, сформулирован в ст. 48 Дополнительного протокола I: «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». Если запрещение нападать на гражданское население превращает определенную категорию потенциальных объектов нападения в незаконные цели, то требование проведения различия распространяет защиту на случаи, когда нападение, возможно, и не направленно непосредственно на гражданское население и гражданские объекты, но возможность удара по ним, тем не менее, высока. Так происходит, например, когда производится выстрел вслепую, хотя оружие позволяет осуществить прицеливание.

Это запрещение особенно актуально в контексте нападения на компьютерные сети. Например, оно относится к случаю, когда, используя определенные средства НКС, имеется возможность выбрать в качестве объекта нападения военную цель, а вместо этого предпринимается широкомасштабное нападение, способное причинить ущерб гражданским системам. Аналогия этому — обстрелы Ираком ракетами СКАД населенных пунктов Саудовской Аравии и Израиля во время войны в Персидском зали-

ве в 1990–1991 гг.[68] Ракеты СКАД не являются по своей природе оружием неизбирательного действия. Наоборот, их можно нацеливать с достаточной точностью, например на военные соединения в пустыне. Однако использование ракет СКАД против населенных пунктов было действием неизбирательного характера, даже если в намерение Ирака входило нанесение удара по военным объектам, находящимся в этих пунктах. Вероятность поражения лиц и объектов, находящихся под защитой, была настолько выше, чем поражение законных целей, что использование этих ракет было недопустимым. Учитывая сегодняшнюю взаимосвязь компьютерных систем, нападение на компьютерные сети вполне может быть таким же.

Соразмерность

Умысел – это то, что отличает принцип соразмерности от принципа проведения различия. Проведение различия ограничивает непосредственные нападения на находящиеся под покровительством лица и объекты, а также нападения, при которых преступно пренебрегают возможными последствиями для таких лиц и объектов. В противоположность этому принцип соразмерности относится к ситуациям, в которых ущерб находящимся под покровительством лицам или объектам является предсказуемым, но не намеренным. Этот принцип чаще всего нарушается (иногда не преднамеренно, а по преступной небрежности) в результате: 1) отсутствия достаточного знания или понимания того, против чего совершается нападение; 2) неспособности точно рассчитать силу удара по цели; и 3) невозможности обеспечить поражение выбранной цели с абсолютной точностью.[69] Все три юридические ловушки нужно иметь в виду, говоря о нападениях на компьютерные сети.

68 Об этих ракетных обстрелах см. US Department of Defense, «Conduct of the Persian Gulf War», Title V Report to Congress, 1992, p. 63, reprinted in 31 *International Legal Materials*. 1992, p. 612.

69 Подробно по этому вопросу см. в Michael N. Schmitt, «Bellum Americanum: The US View of Twenty-First Century War and its Possible Implications for the Law of Armed Conflict», *Michigan Journal of International Law*, Vol. 19, 1998, p. 1051, pp. 1080–1081.

Как сказано в Дополнительном протоколе I, нападение является неизбирательным, 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».[70] Конкретное и непосредственное военное преимущество — это преимущество «существенное и относительно близкое по времени [;] ... малозаметные и отдаленные преимущества не принимаются во внимание».[71] Более того, принимается во внимание преимущество, получаемое от всей операции, а не только от данного единичного нападения.[72]

По существу, принцип соразмерности требует нахождения баланса, то есть решения очень сложной задачи, так как различные составляющие (страдания и ущерб в сравнении с военным преимуществом) взвешиваются без учета общей шкалы ценностей.[73] Осложняет дело то, что ответы на эти и подобные вопросы — даже если предположить, что существуют «правильные» ответы на них, — очень контекстуальны, так как военное преимущество, полу-

70 Дополнительный протокол I, *op. cit.* (примечание 10), ст. 51(5)(a) и 57(2)(a)(iii) и (b). По проблеме соразмерности см.: William J. Fenrick. «The Rule of Proportionality and Protocol Additional I in Conventional Warfare», *Military Law Review*, Vol. 98, 1982, p. 91; Judith G. Gardam, «Proportionality and Force in International Law», *American journal of International Law*, Vol. 87, 1993, p. 391.

71 Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 2209.

72 По этому вопросу было сделано много заявлений о понимании, деклараций и оговорок странами – участницами Протокола. Например, Соединенное Королевство сделало следующую оговорку при ратификации Дополнительного протокола I в 1998 г.: «По мнению Соединенного Королевства, военное преимущество, которое предполагается получить в результате нападения, следует понимать как военное преимущество, которое предполагается получить от нападения в целом, а не только от отдельных или конкретных частей нападения». Сайт МККК, *op. cit.* (примечание 64).

73 Например, как сравнить жизни пассажиров с ценностью военного самолета при организации нападения на компьютерные сети системы управления воздушным движением? Каков допустимый предел человеческих страданий в результате отключения электрических сетей, удовлетворяющих как военные, так и гражданские нужды? Можно ли нападать на телекоммуникационные системы, если это приведет к ухудшению работы служб спасения населения в чрезвычайных ситуациях?

чаемое в результате нападения, всегда зависит от военной обстановки в данный момент.[74] Признавая сложность реального осуществления этого принципа, авторы комментария к Дополнительному протоколу I говорят, что «осуществление этих положений на практике потребует высокой степени доброй воли воюющих сторон, а также желания действовать согласно общим принципам уважения гражданского населения».[75]

Дополнительно усложняет дело «эффект домино», то есть не прямой результат нападения, но его последствия. Иными словами, речь идет о последствиях последствий нападения. Наиболее часто упоминаемым примером этого является нападение на электрические сети Ирака во время войны в Персидском заливе в 1990–1991 гг. Это нападение полностью вывело из строя оперативную систему управления войсками Ирака, но одновременно оно лишило электроэнергии и гражданское население («первичный» результат), что нанесло ущерб больницам, холодильным установкам, службам чрезвычайной помощи и так далее. Аналогичным образом, когда во время операции Allied Force («Союзная сила») войска НАТО нанесли удар по югославским сетям электроснабжения, одним из результатов этого явилось отключение станций снабжения питьевой водой.[76] Эти нападения инициировали «эффект домино» и «вторичным» результатом стали страдания населения. Очевидно, что будь это НКС, результат был бы точно такой же. Более того, «эффект домино» при нападениях на компьютерные сети выглядит более угрожающим, чем при «силовом» нападении, так как компьютеры, в частности компьютеры военных и гражданских сетей, соединены между собой.

74 Проблема заключается также в том, что сам процесс оценки сложен. Например, ценностные критерии диктуются культурой, эти ценностные критерии меняются во времени. О воззрениях на систему ценностей в связи с причинением ущерба природной среде во время вооруженного конфликта более подробно см. в Michael N. Schmitt, «War and the Environment: Fault Lines in the Prescriptive Landscape», *Archiv des Völkerrechts*, Vol. 37, 1999, p. 25.

75 Additional Protocols: Commentary, *op. cit.* (примечание 21), ч. 1978.

76 «NATO Denies Targeting Water Supplies». BBC World Online Network, 24 May 1999, http://www.news.bbc.co.uk/hi/english/world /europe/newsid_351000/351780.stm.

«Эффект домино» оказывает влияние на анализ соразмерности, так как его нужно учитывать при сопоставлении риска причинения побочного ущерба и случайного ранения с военными преимуществами. К сожалению, при нападении на компьютерные сети такие ущерб и ранения, будь то прямые или косвенные, трудно прогнозировать, не зная, как работают эти компьютерные сети и к каким другим системам они подсоединены. Несмотря на эту трудность, лица, планирующие нападение или принимающие решение о нем, обязаны всегда, когда это практически возможно, попытаться избежать причинения побочного ущерба и случайного ранения. Эта обязанность подразумевает принятие некоторых мер для того, чтобы спрогнозировать ущерб или ранения, которые могут быть причинены в результате нападения.[77] Учитывая сложность нападения на компьютерные сети, высокую вероятность повреждения гражданских систем, а также относительно слабое понимание существа и последствий этого лицами, отдающими приказ о нападении, на всех стадиях планирования при выполнении боевой задачи должны иметься специалисты-компьютерщики для оценки возможных побочных и случайных последствий.[78] Кроме этого, неоценимую помощь в оценке возможного «эффекта домино» могут оказать моделирование и имитация, подобные тем, которые уже были проведены в отношении ядерного оружия. Очень хорошо было бы сделать это до начала военных действий, в спокойной обстановке, вне дыма и пыла сражений.

Минимизация побочного ущерба и случайных ранений

Определяя соразмерность, устанавливают, можно ли вообще нападать на военный объект. Впрочем, даже если выбранная цель является законной и планируемое нападение соразмерно, нападающий обязан избрать метод и средства ведения военных дей-

77 См. Дополнительный протокол, *op. cit.* (примечание 10), ст. 57.

78 Объединенный центр военного анализа, размещаемый в центре ВМФ в Дальгрене, штат Виргиния, в настоящее время занимается моделированием инфраструктур иностранных государств и непредвиденных последствий.

ствий, которые, как ожидается, при прочих равных условиях (например, риск для осуществляющих нападение сил, вероятность успеха, запасы оружия и т. д.) причинят наименьшие побочный ущерб и случайные ранения.[79] Более того, если для достижения цели можно атаковать различные объекты, то выбор следует остановить на объекте, нападение на который связан с наименьшим риском причинения побочного ущерба и случайных ранений.[80]

Наличие такого средства, как нападение на компьютерные сети, фактически увеличивает выбор способов сведения к минимуму побочного ущерба и случайного ранения. Если в прошлом для нейтрализации объекта, поддерживающего усилия противника, возможно, требовалось его физическое уничтожение, то сегодня такой объект можно будет просто «выключить». Например, вместо того чтобы бомбить аэродром, можно нарушить систему управления воздушным движением. Это же относится к системам производства и распределения энергии, коммуникационным системам, промышленным предприятиям, и т. д. Те, кто планируют такие нападения или принимают решение об их осуществлении, должны, как и ранее, думать о побочном ущербе, случайном ранении и об «эффекте домино» (как в вышеприведенном примере с электрическими сетями в Ираке). Однако риски, связанные с классическими «силовыми» военными действиями, существенно снижаются при использовании НКС. В каких-то случаях желаемый результат может быть достигнут простым прерыванием работы объекта-цели. Такая тактика особенно привлекательна в случае объекта двойного назначения. Рассмотрим системы электроснабжения. Военная необходимость, возможно, потребует выключить систему только на короткое время, например непосредственно перед штурмом и во время его. Как только настоятельная необходимость ее приостановки отпадет, система может быть вновь запущена, чем будут уменьшены негативные последствия для гражданского населения. Поскольку объекты физически не разрушаются и, следовательно, не потребуют ремонта или восстановления, ускоряется процесс возврата населения к нормальной жизни по прекращении конфликта.

79 *Ibid.*, ст. 57(2)(a). **80** *Ibid.*, ст. 57(3).

Вероломство

Важнейшие нормативные ограничения на нападения на компьютерные сети проистекают из принципа проведения различия, тем не менее несколько других связанных с этим аспектов гуманитарного права необходимо учитывать при использовании этого нового средства войны. Один из них — запрещение вероломства. Вероломство — это симулирование права на защиту с целью злоупотребления доверием противника. Примерами этого служат симулирование ранения, болезни, или обладания статусом некомбатанта, или сдачи в плен, неправомерное использованием эмблем, предоставляющих защиту, например красного креста или красного полумесяца. Вероломство отличается от военных хитростей, которые направлены на то, чтобы ввести противника в заблуждение или побудить его действовать опрометчиво, но которые не связаны с ложным притязанием на право на защиту. Военные хитрости не запрещаются.

Информационная война, включая нападения на компьютерные сети, предоставляет множество возможностей для военных хитростей и вероломства. Объясняется это тем, что оба способа предназначены для передачи... ложной информации. Например, законная военная хитрость может заключаться в передаче ложных данных о развертывании или переброске войск, которые предназначены для того, чтобы их перехватил противник. Или она может состоять во внесении изменений в базы данных разведки противника, или в пересылке сообщений в штабы противника, якобы из нижестоящих подразделений, или в направлении указаний в нижестоящие подразделения, якобы из их штабов.[81] Все такие действия являются совершенно законными.

С другой стороны, любое действие, направленное на то, чтобы заставить противника поверить, что обладаешь статусом, предо-

81 Статья 39 запрещает использовать военные эмблемы, воинские знаки различия или форменную одежду противника. Это запрещение, с которым США не согласны, за исключением случаев такого использования во время боя (см. Handbook, *op. cit.*, [примечание 49], para 12.1.1, fn 2), не распространяется на использование кодов, паролей и т.п. Micheal Bothe, Karl J. Partsch and Waldermar A. Solf, *New Rules for Victims of Armed Conflicts*, M. Nijhoff, The Hague, 1982. Впрочем, ст. 38 запрещает неправомерное использование защитных сигналов.

ставляющим защиту, и тем самым получить возможность убивать, причинять ранения или брать в плен противника, будет незаконным.[82] Например, медицинские формирования и санитарно-транспортные средства могут использовать для своего опознавания коды и сигналы, установленные Международным союзом электросвязи, Международной организацией гражданской авиации и Межправительственной морской консультативной организацией.[83] Передача обманным образом этих кодов/сигналов или — что более вероятно в контексте нападения на компьютерные сети — перевод системы противника в режим отображения приема таких сигналов было бы явным примером вероломства. Министерство обороны США также высказало мнение, что использование «компьютерной трансформации для создания изображения руководителя государства-противника, извещающего свои войска о подписании соглашения о перемирии или прекращении огня, явилось бы военным преступлением, если такое извещение ложно».

Заключение

В общем и целом, существующие гуманитарные нормы достаточны для обеспечения защиты, которой пользуются гражданское население, гражданские объекты и другие находящиеся под защитой лица и объекты. Тем не менее некоторые ранее не существовавшие аспекты НКС действительно создают новые, и иногда тревожные, ситуации. Некоторые трудности в оценке происходящего в связи с методами компьютерной войны во время операции НАТО против Югославии в 1999 г. являются неопровержимым свидетельством того, что вопрос о том, как рассматривать НКС в свете положений гуманитарного права, пока еще остается открытым.[84]

82 Дополнительный Протокол I, *op. cit.* (примечание 10), ст. 37, Римский статут, (примечание 53), ст. 8(2)(b)(vii) и (xi). Конвенция (IV) о законах и обычаях сухопутной войны, 18 октября 1907 г., прилагаемое Положение, ст. 23(b)7, в сборнике «Международное право. Ведение военных действий», (примечание 10), с. 27, запрещают вероломное убийство.

83 Дополнительный протокол I, *op. cit.* (примечание 10), Приложение, ст. 11.

84 О сомнениях в отношении применения НКС во время операции «Союзная сила» см. Bradley Graham, «Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia», *Washington Post*, 8 November 1999, p. A1.

Во-первых, для того чтобы применить существующие нормы к НКС, необходимо принять ряд принципов в плане толкования терминов. Наиболее важным из них является толкование терминов «вооруженный конфликт» и «нападение» на основе критерия последствий. При отсутствии такого понимания этих терминов применимость, и следовательно, адекватность существующих принципов гуманитарного права ставится под вопрос. Между прочим, рассмотрение нападения на компьютерные сети в контексте *jus ad bellum* (права прибегать к силе) также приводит к толкованию, основанному на критерии последствий.[85]

Во-вторых, даже если принять параметры, проистекающие из предлагаемых толкований, пробелы в праве остаются. Наиболее существенным является то, что нападения на гражданское население и гражданские объекты, не причиняющие ранений, смертей, ущерба или разрушений (или иным образом не ведущие к недопустимым страданиям) в целом разрешаются. Учитывая, что «силовые» нападения обычно вызывают такие последствия, гражданское население и гражданские объекты пользуются широкой защитой во время традиционных военных операций. Тем не менее нападение на компьютерные сети, поскольку оно может и не являться *нападением*, открывает широкие возможности для избрания в качестве целей нападения находящиеся под защитой лица и объекты. Стимулы для проведения таких операций тем сильнее, чем более принудительный характер носят «цели войны» стороны, которая осуществляет НКС. Например, желание «выключить свет» гражданскому населению, чтобы побудить его оказать давление на свое руководство с тем, чтобы оно придерживалось определенной линии поведения или воздерживалось от нее (именно это предлагал сделать командующий ВВС НАТО во время операции «Союзная сила») будет расти по мере увеличения возможностей достижения

85 См. Schmitt, «Computer Network Attack», *op. cit.* (примечание 7).

этой цели.[86] Отсутствие «силовых» результатов, по существу, провоцирует НКС.

С гуманитарной точки зрения, это весьма удручающее обстоятельство. Часть нападений на компьютерные сети, возможно, и не достигнут уровня нападения, но другие, безусловно, достигнут. То, что нападение на цель можно совершить не только «силовым» способом, вовсе не означает, что нормы гуманитарного права становятся неприменимыми. Гражданское население и гражданские объекты продолжают пользоваться статусом, предоставляющим защиту, в отношении тех воздействий НКС, которые причиняют человеческие страдания и физические разрушения. Более того, даже при нападениях на компьютерные сети военных объектов принцип соразмерности продолжает защищать гражданское население и гражданские объекты от ранений и ущерба, чрезмерных по отношению к военному преимуществу. Например, отключение подачи электроэнергии в город с целью вывода из строя оперативной системы управления войсками и связи противника может допускаться в том случае, если это не причинит чрезмерных страданий населению. Впрочем, если операция направлена не на военный объект, то вопрос ставится так: достигает ли причиненный ущерб уровня ущерба от «нападения»? Если достигает, то НКС запрещается.

В-третьих, и это вселяет надежду, НКС, возможно, позволят достигать желанных военных целей, причиняя меньше сопутствующих разрушений и случайных ранений, чем это происходит при обычных «силовых» нападениях. Безусловно, военачальники будут обязаны, в некоторых случаях, задействовать свои кибернетические средства вместо «силового» оружия, если этим можно умень-

86 Вот что вспоминает генерал-лейтенант ВВС США, который руководил действиями авиации во время операции «Союзная сила»:

«Я считал, что в первую же ночь следует отключить электроэнергию, уничтожить основные мосты через Дунай и прекратить подачу воды, с тем чтобы на следующее утро именитые граждане Белграда, проснувшись, спросили себя: «Зачем мы это делаем?» А затем обратились бы с этим вопросом к Милошевичу».

Craig R. Whitney. «The Commander: Air Wars Won't Stay Risk-Free, General Says», *The New York Times,* 18 June 1999, p. A1.

шить сопутствующие и случайные последствия.[87] Кроме того, при оценке соответствия нападения принципу соразмерности совершенно необходимо тщательно анализировать последствия таких операций, и особенно «эффект домино». Это потребует участия стратегов, юристов и специалистов-компьютерщиков на всех стадиях определения объектов нападения.[88]

И наконец, использование сугубо гражданских технологий и ноу-хау для проведения военных операций при помощи компьютеров испытывает на прочность не только существующее понятие «нападение», но и традиционный статус комбатанта. Несоблюдение строгих ограничений на участие гражданских лиц в военных действиях неминуемо увеличит опасности, поджидающие гражданское население, и ослабит действие норм гуманитарного права.

Таким образом, решение еще предстоит найти. Несмотря на то что гуманитарное право в своем сегодняшнем виде обычно является достаточным для того, чтобы защитить от последствий нападений на компьютерные сети покровительствуемые лица, и хотя оно даже обещает периодически усиливать такую защиту, тем не

87 В комментарии к Дополнительным протоколам, *op. cit.* (примечание 21), ч. 1871, говорится, что «обязанностью участвующих в конфликте сторон является иметь средства, позволяющие уважать положения Протокола. В любом случае недопустимо, чтобы сторона, обладающая такими средствами, не применяла их и тем самым сознательно не проводила требуемого различия».

88 Стандартное подразделение информационных операций показано в JP 3–13, *op. cit.* (примечание2), на рис. IV–4 и в сопровождающем тексте. Оно включает: офицера по информационным операциям из J–3 (Joint Staff Operations Directorate – Управление операциями Объединенного штаба); представителей J–2 (Joint Staff Intelligence Directorate – Управления разведки Объединенного штаба), J–4 (Joint Staff Logistics Directorate – Управления материально-технического снабжения Объединенного штаба), J–5 (Strategic Plans and policy Directorate – Управления стратегического планирования Объединенного штаба), J–6 (Joint Staff Command, Control & Communications Systems Directorate – Управления системами оперативного руководства и связи Объединенного штаба), J–7 (Operational Plans and Joint Force Development Directorate – Управления оперативных планов и развития объединенных сил), органов управления боевых частей и подразделений, служебные и функциональные подразделения; начальника военно-юридической службы, а также специалистов по связи с общественностью, контрразведке, связи с гражданскими властями, определению целей, специальным операциям, электронной войне, психологическим операциям, дезинформации и обеспечению безопасности действий войск.

менее существенные нормативные провалы налицо. Поэтому, по мере расширения возможностей для нападений на компьютерные сети, – как в смысле их изощренности, так и доступности таких возможностей, – постоянный правовой мониторинг совершенно необходим. Нельзя терять из виду гуманитарные принципы, иначе допустимое в ходе ведения войны будет вытеснено возможным.

●