Применение принципа проведения различия к информационным технологиям: опыт Китая

Чжисюн Хуан и Яохой Ин*

Чжисюн Хуан — обладатель звания «Выдающийся молодой ученый Янцзы», профессор Института международного права/Института киберуправления Уханьского университета и научный сотрудник Восточно-китайского университета политологии, входящий в Шанхайскую ключевую группу по инновациям и изучению правовых превентивных механизмов для реализации инициативы «Пояс и путь». Эл. почта: fxyhzx@whu.edu.cn.

Яохой Ин — аспирант факультета права Уханьского университета, Китай. Эл. почта: yingyaohui@whu.edu.cn

Аннотация

До настоящего времени правительство Китая делало лишь весьма общие заявления относительно применения норм международного гумани-

* Настоящее исследование проведено при поддержке отделения крупных проектов Национального китайского фонда социальных наук (грант № 20&ZD204). Авторы благодарят всех редакторов и анонимное жюри за полезные предложения и выражают признательность Эрику Йенсену, Кубо Мачаку, Игнасио де ла Расилье дель Моралю, Цзиньюань Су, Николь Хогг и Николасу Цагуриасу за ценные комментарии к более ранним редакциям настоящей статьи. Одна из ранних версий статьи была подана для включения в сборник статей семинара «Право в современных гибридных вооруженных конфликтах», проведенного Университетом Бригама Янга в феврале 2019 года. Мы также горячо благодарим всех участников этого семинара за все поступившие от них отзывы и комментарии.

тарного права к киберпространству. Китайские ученые, безусловно, уже опубликовали ряд работ, посвященных данному вопросу, однако в настоящее время дискуссии о принципе проведения различия недостает как хронологического масштаба, так и научной глубины. Исследования китайских ученых пока находятся на достаточно ранней стадии по сравнению с западной наукой. До сих пор никто из представителей научного сообщества Китая не пытался разобрать или разъяснить вопросы применения принципа проведения различия в киберпространстве.

В настоящей статье, которая является первой в Китае научной работой, посвященной именно этому отдельному вопросу, предлагается альтернативная точка зрения, подкрепляемая позициями различных должностных лиц КНР и мнениями китайских ученых. Цель авторов статьи — понять, могут ли действующие нормы полноценно применяться в отношении киберпространства, и при необходимости выяснить, как улучшить и уточнить их для такого применения. Приступая к рассмотрению этих вопросов, мы утверждаем, что, несмотря на потенциальные проблемы технического характера и факторы неопределенности, принцип проведения различия следует применять и к киберпространству. Необходимо также осуществить тщательную переоценку и уточнение аспектов такого применения для того, чтобы предотвратить чрезмерную милитаризацию и обеспечить максимальную защищенность интересов гражданских лиц. Элементы статуса комбатанта, установленные в обычном международном праве и соответствующих договорах, мало пригодны для применения на цифровом поле боя, когда целью является человек. Тем не менее киберкомбатанты обязаны демонстрировать свое отличие от гражданских лиц (то есть обеспечивать возможность проведения различия). В статье утверждается, что при применении принципа проведения различия стоит сосредоточиться на существенных, а не формальных элементах, то есть, например, на открытом ношении оружия или ношении определенного отличительного знака, явственно видимого издали. При трактовке понятия «непосредственное участие в военных действиях» порог вреда требует существования объективно оцененной вероятности, а не лишь субъективного намерения; должна быть подтверждена связь с воюющей стороной, а также должна иметься тесная причинно-следственная связь. Применение модели «поэтапной кибератаки» по аналогии помогает нам охватить и лучше понять весь процесс непосредственного участия в военных действиях в ходе кибервойны. Атака на военные объекты, не являющиеся людьми, должна в совокупности отвечать и критерию «эффективного вклада», и критерию «явного военного преимущества», которые в равной степени непреложны. Те же требования актуальны и для объектов двойного назначения. Кроме того, некоторые данные должны относиться к гражданским объектам.

Ключевые слова: Китай, принцип проведения различия, киберпространство, киберкомбатант, военный объект, данные.

: : : : : : : :

Введение

До настоящего времени правительство Китая не выработало четкой позиции относительно применения норм международного гуманитарного права (МГП)[1] к киберпространству. Среди китайских ученых ведутся отдельные предварительные обсуждения вопросов применения МГП в киберпространстве[2] — в особенности среди тех ученых, которые имеют опыт службы

1 Во избежание неточных трактовок стоит на данном этапе прояснить значение двух терминов, использованных в этой статье: «право вооруженных конфликтов» (ПВК) и «международное гуманитарное право». Неточное применение этих терминов вызывает некоторое беспокойство. Некоторые люди придерживаются мнения о том, что их значение полностью совпадает и они взаимозаменяемы, то есть в понятие «право вооруженных конфликтов», также известное как международное гуманитарное право, входят такие принципы, как принцип проведения различия между военными и гражданскими целями (International Committee of the Red Cross (ICRC), *The Law of Armed Conflict: Basic Knowledge*, Geneva, June 2002, p. 2, доступно по адресу: www.icrc.org/eng/assets/files/other/law1_final.pdf), в то время как другие считают «международное гуманитарное право» потенциально более узким термином, которым обозначаются исключительно правовые нормы, действующие в условиях вооруженных конфликтов относительно обращения с лицами — военными или гражданскими, ранеными или способными действовать полноценно (Mary O'Connell, "Historical Development and Legal Basis", in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 11). Высказываются также критические мнения по поводу объединения норм ведения боевых действий и гуманитарных целей, например, следующего содержания: «Потенциальный недостаток термина [МГП] состоит в том, что он может не учитывать некоторые правовые нормы ведения боевых действий (такие как нормы нейтралитета), первичное предназначение которых не имеет гуманитарного характера» (Jean Pictet, *Humanitarian Law and the Protection of War Victims*, A. W. Sijthoff, Leiden, 1975, p. 11). Комиссия международного права ООН разграничивает ПВК и МГП, определяя, что ПВК охватывает ход и последствия вооруженных конфликтов, а МГП входит в состав ПВК и представляет собой lex specialis, регулирующее ведение военных действий (Проект статей о последствиях вооруженных конфликтов для международных договоров. Принят Комиссией международного права на 63-й сессии, 26 апреля — 3 июня и 4 июля — 12 августа 2011 г. Док. ООН A/66/10, комментарий к проекту ст. 2, п. 4). Более развернутое обсуждение данной терминологической проблемы см.: Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, Cambridge and New York, 2010, pp. 22–26. Авторы руководств и работ, публикуемых в Китае, в целом придерживаются точки зрения, согласно которой понятие МГП возникло в результате развития права вооруженных конфликтов, или ПВК, и, соответственно, термины являются синонимичными; см., например: 朱文奇，何谓国际人道法，武大国际法评论, 2003, 1 (Wenqi Zhu, "What Is International Humanitarian Law?", *Wuhan University International Law Review*, Vol. 1, 2003, доступно только на китайском языке). Для целей настоящей работы будет использоваться в основном термин МГП, а термин «право вооруженных конфликтов» будет применяться в тех случаях, когда он фигурирует в цитируемых источниках.

2 См., например: Li Zhang, "A Chinese Perspective on Cyber War", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, p. 804, доступно по адресу: https://international-review.icrc.org/sites/default/files/irrc-886-zhang.pdf (все ссылки на интернет-ресурсы приводятся по состоянию на январь 2021 г.); Longdi Xu, "The Applicability of the Laws of War to Cyberspace: Exploration and Contention", 2014, p. 7, доступно по адресу: www.gov.uk/government/publications/the-applicability-of-the-laws-of-war-to-cyberspace-exploration-and-contention; Chris Wu, "An Overview of the Research and Development of Information Warfare in China", in Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright (eds), *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave Macmillan, London, 2006; 朱 欣, 信息网络战的国际法问题研究, 河北法学, 2009, 27(01) (Lixin Zhu, "Research on the International Law of Information Network Operations", *Hebei Law Science*, Vol. 27, No. 1, 2009, доступно только на китайском языке); 姜世波, 网络攻击与战争法的适用, 武大国际法评论, 2013, 16(02) (Shibo Jiang, "War by Internet Cyber Attack and the Application of the Law of War", *Wuhan University International Law Review*, Vol. 16, No. 2, 2013, доступно только на китайском языке); 李伯军, 论网络战及战争法的适用问题, 法学评论, 2013, 31(04) (Bojun Li, "On Cyber

или работы в вооруженных силах[3], — но на данный момент дискуссии о принципе проведения различия в киберпространстве недостает и хронологического масштаба, и научной глубины. Исследования китайских ученых пока находятся на достаточно ранней стадии по сравнению с западной наукой; в настоящее время готовится несколько докторских диссертаций, посвященных вопросам применения МГП в киберпространстве. До сих пор никто из представителей научного сообщества Китая не пытался разобрать или разъяснить вопросы применения принципа проведения различия в киберпространстве.

В настоящей статье, которая является первой в Китае научной работой, посвященной применению принципа проведения различия в ходе кибервойны, предлагается альтернативная точка зрения, подкрепляемая позициями различных должностных лиц КНР и мнениями китайских ученых. По мнению авторов, несмотря на то что позиции государств по поводу конкретных способов применения МГП в киберпространстве значительно разнятся, основной принцип проведения различия определенно может в нем применяться. Цель авторов настоящей статьи — понять, могут ли действующие нормы полноценно применяться в случае кибервойны, и при необходимости выяснить, как улучшить и уточнить их для такого применения. В связи с этим в первой части статьи представлено текущее положение дел с применением МГП в киберпространстве, а также приведены мнения должностных лиц КНР и членов китайского научного сообщества по данному вопросу. Далее, во второй части приводится анализ понятия принципа проведения различия и выявляются противоречивые проблемы, связанные с его применением в киберпространстве. В третьей и четвертой частях через призму дихотомии «люди — объекты» рассматриваются существенные правовые проблемы, возникающие в связи с таким применением, а также обсуждаются релевантные взгляды на эти проблемы в Китае. Третья часть посвящена анализу того, как применяются традиционные критерии определения допустимых человеческих целей для нападения в условиях военных действий в киберпространстве. Кроме того, в ней обозначаются актуальные

Warfare and the Application of the Law of War", *Law Review*, Vol. 31, No. 4, 2013, доступно только на китайском языке); 朱 欣, 平战结合与网络空间国际规则制定, 信息安全与通信保密, 2018(07) (Lixin Zhu, "Competition for International Rules in Cyberspace under the Combination of Peacetime and Wartime", *Information Security and Communications Privacy*, No. 7, 2018).

3 王海平, 武装冲突法研究进展及需要关注的问题, 当代法学, 2012, 26(05) (Haiping Wang, "The Research Progress of the Law of Armed Conflict and the Issues Needing Attention", *Contemporary Law Review*, Vol. 26, No. 5, 2012, доступно только на китайском языке); 李, 鲁笑英.浅析信息化战争条件下武装冲突法所面临的问题, 西安政治学院学报, 2012, 25(01) (Li Li and Xiaoying Lu, "A Brief Analysis of the Problems Faced by the Law of Armed Conflict under the Condition of Information-Based Warfare", *Journal of Xi'an Politics Institute of PLA*, Vol. 25, No. 1, 2012, доступно только на китайском языке); 朱雁新, 计算机网络攻击之国际法问题研究, 中国政法大学, 2011 (Yanxin Zhu, "The Research on the International Issues of Computer Network Attack", doctoral diss., China University of Political Science and Law, 2011, доступно только на китайском языке); 张天舒, 从"塔林手册" 看网络战争对国际法的挑战, 西安政治学院学报, 2014, 27(01) (Tianshu Zhang, "The Challenges of Cyber Warfare to International Law: From the Perspective of The Tallinn Manual on the International Law Applicable to Cyber Warfare", *Journal of Xi'an Politics Institute of PLA*, Vol. 27, No. 1, 2014, доступно только на китайском языке).

препятствия и вносятся соответствующие предложения о путях их преодоления. В четвертой части изложена проблематика, связанная с остальными (не человеческими) целями, а также приводится рассуждение на тему того, что может быть объектом нападения в кибервойне — то есть что в этом контексте следует считать военным объектом. В ней также рассматривается позиция китайской науки по вопросу о том, являются ли цифровые данные таким объектом сами по себе. В заключительной части вниманию читателя предлагается ряд предварительных заключений.

Без сомнения, вопросы мирного использования киберпространства имеют огромное значение для общего благополучия всего человечества. К счастью, до сего дня в мире не произошло ни одной катастрофической кибератаки с большим числом жертв, и не наблюдалось подобной «кибернетическому Пёрл-Харбору»[4] ситуации, которая бы имела аналогичную природу и стала бы поводом для развязывания войны. Тем не менее вызывающие все большее беспокойство враждебные действия в киберпространстве, такие как использование кибернетических средств и методов ведения войны в ходе вооруженных конфликтов, заставляют нас обратить пристальное внимание на применение норм МГП к киберпространству.

Несмотря на то что кибервойна[5] потенциально позволяет сохранять некоторый уровень анонимности на ситуативной основе и подразумевает

4 James J. Wirtz, "The Cyber Pearl Harbor", *Intelligence and National Security*, Vol. 32, No. 6, 2017; James J. Wirtz, "The Cyber Pearl Harbor Redux: Helpful Analogy or Cyber Hype?", *Intelligence and National Security*, Vol. 33, No. 5, 2018; US Department of Defense (DoD), "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City", 12 October 2012, доступно по адресу: https://content.govdelivery.com/accounts/USDOD/bulletins/571813.

5 В настоящей статье термин «кибервойна» используется для обозначения «применяемых в условиях вооруженного конфликта средств и методов ведения войны, в основе которых лежат информационные технологии». См.: Jakob Kellenberger, "International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, Sanremo, Italy, 8–10 September 2011: Keynote Address by Dr Jakob Kellenberger", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, доступно по адресу: https://international-review.icrc.org/sites/default/files/irrc-886-kellenberger-spoerri.pdf. С точки зрения некоторых китайских ученых, кибервойна является особой формой информационной войны и представляет собой новое средство или метод ведения войны. Информационная война — это комплекс враждебных действий, к которым прибегают противные стороны для того, чтобы защитить свое право на получение, контроль и использование информации. Коннотация и охват этого понятия шире, чем у кибервойны. Так, оно может охватывать кибервойну, интеллектуальную войну, электронную войну, психологическую войну и др. «Кибервойной» называют процесс нарушения работы, уничтожения или угрозу таких действий в отношении информационных и сетевых систем других противных сторон при одновременном обеспечении защиты собственных информационных и сетевых систем посредством компьютерной сетевой инфраструктуры. См., например: B. Li (примечание 2 выше). Некоторые утверждают, что основной вопрос, выраженный в понятии «кибервойна», — это вопрос о том, могут ли субъекты кибернетического нападения, «вооруженные» клавиатурами, компьютерными вирусами и вредоносным программным обеспечением, стать (и не стали ли уже) новым средством или методом ведения войны. См.: 黄志雄主编, 网络空间国际规则新动向: "塔林手册 2.0 版" 研究文集, 社会科学文献出版社, 2019: 301 (Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, p. 301); 黄志雄, 国际法视角下的 "网络战" 及中国的对策——以诉诸武力权为中心, 现代法学, 2015, 37(05) (Zhixiong Huang, "International Legal Issues concerning 'Cyber Warfare' and Strategies for China: Focusing on the Field of *Jus ad Bellum*", *Modern Law Science*, Vol. 37, No. 5, 2015).

ощущение общей взаимосвязи, она остается одним из видов войны. Сами по себе многосторонние обсуждения по поводу того, применимо ли МГП как «комплекс норм, целью которых является смягчение последствий вооруженных конфликтов»[6] к киберпространству, ведутся уже не первое десятилетие. Прийти к консенсусу до сих пор не удалось. Определенную надежду на разрешение этой проблемы давал доклад Группы правительственных экспертов Организации Объединенных Наций (ГПЭ ООН) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2014–2015 годы, так как в нем упоминалась возможность применения принципов проведения различия и соразмерности в киберпространстве[7]: формулировка «международно-правовые принципы... в том числе... принцип индивидуализации»[8] рассматривается как компромиссная, поскольку ряд государств (предположительно включая Китай) выразили нежелание прибегать непосредственно к термину МГП[9]. Тем не менее в последующем докладе ГПЭ ООН за 2016–2017 годы консенсуса не наблюдается, а один из вопросов, по поводу которого возникли противоречия, был связан с применением МГП в киберпространстве[10]. После принятия в 2018[11] году Первым комитетом Генеральной Ассамблеи ООН двух отдельных (кто-то может даже сказать — противоречащих друг другу) резолюций перспективы достижения консенсуса государств в отношении применения МГП в киберпространстве кажутся все более неясными и неоднозначными.

Чисто теоретически можно утверждать, что, как только ситуация переходит границы определения вооруженного конфликта, применение норм права войны (jus in bello) в киберпространстве предполагает лишь распространение устоявшихся норм на новую сферу. Если считать кибервойну новым средством или методом войны, то к ней по умолчанию будут применяться нормы права войны (jus in bello), и такое применение не предполагает каких-либо неясностей. Однако реальность часто разительно отличается от теории. Ввиду огромного числа различий в природе кибернетического и обычного поля боя многие из существующих норм мало подходят для регулирования кибервойны и, следовательно, нуждаются в переосмыслении. Особенно справедливо это утверждение в случае принципа

6 См.: *МККК*. Война и право, доступно по адресу: https://www.icrc.org/ru/war-and-law.

7 См.: *ГПЭ ООН*. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, док. ООН A/70/174, 22 июля 2015 г., п. 28, доступно по адресу: www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

8 Там же.

9 Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", *Just Security*, 30 June 2017, доступно по адресу: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

10 См., например: ibid; Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?", *Lawfare*, 4 July 2017, доступно по адресу: https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

11 См.: "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased", *Council on Foreign Relations Blog*, 15 November 2018, доступно по адресу: www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased. Инициаторами двух упомянутых резолюций выступили Россия (док. ООН A/C.1/73/L.27/Rev.1) и Соединенные Штаты (док. ООН A/C.1/73/L.37) соответственно.

проведения различия. Например, существенным вопросом, возникающим в связи с этим принципом, является проведение различия между киберкомбатантами и гражданскими лицами. Комбатанты должны открыто носить оружие и иметь определенный и явственно видимый издали отличительный знак[12]. Эти требования практически неприменимы в киберпространстве, где анонимность часто является нормой, а возможность определить, кто непосредственно управляет компьютером, с которого осуществляется атака, отсутствует. Действующие нормы составлялись в эпоху, когда война была неразрывно связна с определенной физической близостью сторон в конфликте; в большинстве случаев комбатанты могли видеть друг друга, и потому было легко провести различие между комбатантом и некомбатантом, другом и неприятелем[13]. Если рассматривать ситуацию с точки зрения гражданских лиц, принимающих непосредственное участие в военных действиях[14], вопрос становится еще более запутанным. Неорганизованные отдельные лица с большой долей вероятности могут осуществлять кибератаки на того или иного противника; типичным примером такого явления можно назвать проведение группой хакеров-активистов распределенной атаки типа «отказ в обслуживании» (DDoS) в патриотических или идеологических целях. Например, анонимная кибератака на критически важную инфраструктуру, телекоммуникационные системы, DNS-серверы, вебсайты и серверы электронной почты в Эстонии, проведенная в 2007 году, по всей видимости, явилась политическим последствием переноса советского памятника освободителям Эстонии, знаменующего победу СССР над нацизмом, из центра Таллина на воинское кладбище на окраине города[15]. Кого из следующих лиц следует считать непосредственно принимающими участие в военных действиях: того, кто активирует вредоносный код, того,

12 Женевская конвенция (III) об обращении с военнопленными от 12 августа 1949 г. (вступила в действие 21 октября 1950 г.) (ЖК III), ст. 4(A)(2); Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I), от 8 июня 1977 г. (вступил в действие 7 декабря 1978 г.) (ДП I), ст. 44(3); *Хенкертс, Жан-Мари, и Досвальд-Бек*, Луиза. Обычное международное гуманитарное право. Том I: Нормы. МККК, 2006. С. 18–22 (Обычное МГП), доступно по адресу: https://ihl-databases.icrc.org/customary-ihl/rus/docs/v1.

13 Heather Harrison Dinniss, "Participants in Conflict — Cyber Warriors, Patriotic Hackers and the Laws of War", in Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff, Boston, MA, and Leiden, 2013, p. 256; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 145.

14 Норма 6 в исследовании «Обычное МГП» (примечание 12 выше) гласит, что гражданские лица пользуются защитой от нападений, за исключением случаев, когда и пока они принимают непосредственное участие в военных действиях. Обсуждение формулировки «непосредственное участие в военных действиях» по существу см.: *Мельцер, Нильс*. Непосредственное участие в военных действиях. Руководство по толкованию понятия в свете международного гуманитарного права. МККК, Женева, 2009 (Руководство по толкованию).

15 Подробное описание кибератак против Эстонии в 2007 г. см.: "Cyber Attacks against Estonia (2007)", *International Cyber Law in Practice: Interactive Toolkit*, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), доступно по адресу: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_ Estonia_(2007); Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE, Tallinn, 2010, pp. 15–16, 31.

кто пишет этот код (но не приводит его в действие), или того, кто изначально отдает приказ о написании кода?

Как страна с наибольшей численностью населения, пользующегося интернетом, которая при этом страдает от частых кибератак[16], Китай чрезвычайно активно ведет деятельность по пропаганде принципа верховенства права в киберпространстве. Тем не менее (даже при том, что Китай уже много лет является государством — участником Женевских конвенций[17] и Дополнительных протоколов I и II к ним (ДП I и ДП II))[18] государство не проявляет значительной инициативы в вопросах применения МГП в киберпространстве и систематически избегает участия в рассмотрении проблемы кибервойны и применимого к ней права[19].

Нежелание Китая подробно обсуждать вопрос МГП проявлялось явно и неоднократно. Так, в документе, недавно поданном в адрес Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Китай заявил, что «к применимости права вооруженных конфликтов и права объявлять войну (jus ad bellum) следует подходить с осмотрительностью»[20]. Это предполагает, что Китай по определенным (возможно, военным) причинам не желает обсуждать подробности применения МГП в киберпространстве и, следовательно, задерживает любое прояснение вопроса. Вместо того чтобы конкретизировать свою позицию и мотивы, Китай лишь неоднократно утверждал, что «кибервойну нельзя признавать правомерной ни при каких обстоятельствах»[21]. Подобное сопротивление было особенно явно выражено в речи одного из членов китайской делегации на Ежегодном заседании Афро-азиатской консультативно-правовой организации (ААКПО) в 2019 году:

> Китай придерживается принципа мирного использования киберпространства и твердо отвергает... кибервойну или гонку кибервооруже-

16 Chinese Academy of Cyberspace Studies (ed.), *China Internet Development Report 2017*, Springer, Berlin, 2019, p. 107; 国家互联网应急中心, 2020 年上半年我国互联网网络安全监测数据分析报告, 2020 (National Computer Network Emergency Response Technical Team/Coordination Centre of China, *Analysis Report of China's Internet Network Security Monitoring Data in the First Half of 2020*, 2020, доступно только на китайском языке), доступно по адресу: https://tinyurl.com/y2lpzdh4; Ministry of Foreign Affairs of the People' Republic of China, "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on September 29, 2020", доступно по адресу: https://tinyurl.com/y4xolw3g.

17 Китай присоединился к Женевским конвенциям (ратифицировал их) 28 декабря 1956 г. См.: ICRC Treaty Database, доступно по адресу: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=CN.

18 Китай присоединился к ДП I и ДП II (ратифицировал их) 14 сентября 1983 г. См.: ibid.

19 Binxin Zhang, "Cyberspace and International Humanitarian Law: The Chinese Approach", in Suzannah Linton, Tim McCormack and Sandesh Sivakumaran (eds), *Asia-Pacific Perspectives on International Humanitarian Law*, Cambridge University Press, Cambridge, 2019, p. 323.

20 См.: "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", p. 6, доступно по адресу: www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

21 Ibid.

ний. <...> В отсутствие государственной практики нам следует быть весьма осмотрительными при обсуждении применимости гуманитарного права в так называемых кибервойнах. Причина этого максимально проста, но в то же время фундаментальна: во-первых, в принципе не следует допускать каких-либо кибервойн, а во-вторых, кибервойна станет абсолютно новой формой высокотехнологичной войны. С учетом «цифрового разрыва» между развивающимися... и развитыми странами, развивающиеся страны в принципе будут находиться в невыгодной позиции при обсуждении и разработке подобных норм, обеспечить справедливость и честность которых будет сложно[22].

Китай придает огромное значение мирному использованию киберпространства и придерживается мнения, что чрезмерно активное обсуждение применения МГП может привести к отрицательным последствиям для мира и безопасности на международном уровне, усугубив гонку вооружений и милитаризацию киберпространства. К примеру, представители Китая выступили с критикой такого обсуждения, заявив, что «эта военная парадигма»[23] не учитывает принцип неприменения силы[24] и может пошатнуть стратегическое доверие, существующее между странами, и увеличить риск ошибочного восприятия действий одних государств другими, а также риск конфликтов между ними[25]. В подобной ситуации неудивительно, что правительство Китая не выражает четкой позиции по поводу применения принципа проведения различия в киберпространстве. Консервативное отношение Китая к этой проблеме в некоторой степени можно понять. Во-первых, на национальном уровне не существует широко признанного определения кибератаки; во-вторых, ввиду гистерезисного характера права в широком смысле применение МГП не следует регламентировать слишком поспешно[26]. Текущее отрицательное отношение правительства Китая к перспективе решения этого вопроса может быть также продиктовано тактикой затягивания, которой Китай пользуется, не имея четкого плана действий. С точки зрения авторов, для применения МГП, и особенно принципа проведения различия, в киберпространстве нет каких-либо правовых препятствий. Нельзя отрицать, что кибервойна уже реальна и будет оставаться таковой и в дальнейшем. Нравится это Китаю или нет, ему, вероятно, придется обозначить свою позицию относительно МГП в киберпространстве.

22 AALCO, *Verbatim Record of Discussions: Fifty-Eighth Annual Session*, AALCO/58/DAR ES SALAAM/2019/VR, Dar es Salaam, 21–25 October 2019, доступно по адресу: www.aalco.int/Final%20Verbatim%202019.pdf.

23 AALCO, *Verbatim Record of Discussions: Fifty-Fourth Annual Session*, AALCO/54/BEIJING/2015/VR, Beijing, 13–17 April 2015.

24 Xinmin Ma, "What Kind of Internet Order Do We Need?", *Chinese Journal of International Law*, Vol. 14, No. 2, 2015. Синьминь Ма (Xinmin Ma) занимал должность заместителя директора отдела по вопросам договоров и права Министерства иностранных дел КНР с 2014 по 2019 г.

25 AALCO, *Verbatim Record of Discussions: Fifty-Fifth Annual Session*, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, New Delhi, 17–20 May 2016.

26 Более подробное разъяснение по поводу отношения Китая к МГП см.: B. Zhang (примечание 19 выше).

Принцип проведения различия и проблема его применимости к киберпространству

Обрисовав в рамках подготовительной части нашего анализа текущее положение дел в связи с применением МГП в киберпространстве и представив позиции должностных лиц КНР и взгляды некоторых китайских ученых по данному вопросу, мы переходим к обзору принципа проведения различия самого по себе и обобщению противоречивых проблем его применения в киберпространстве. Международный Суд ООН в своем консультативном заключении относительно законности угрозы ядерным оружием или его применения определяет принцип проведения различия как фундаментальный принцип права вооруженных конфликтов, который оформился в виде нормы обычного международного права[27]. Согласно статье 48 ДП I, стороны, находящиеся в конфликте, должны всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими и военными объектами, и, соответственно, направлять свои действия только против военных объектов[28].

В общих чертах принцип проведения различия предполагает двунаправленный подход к регулированию военных действий. Он запрещает неизбирательные средства и методы ведения войны, а также регламентирует использование тех средств и методов, которые являются правомерными. Это предполагает, что следует проводить различие между военными объектами и комбатантами с одной стороны и другими лицами и объектами, которых(-ые) необходимо уважать и защищать, — с другой. Нападения неизбирательного характера запрещены[29].

При «нападении» активируется широкий спектр механизмов правовой защиты в контексте проведения различия, особенно стоит отметить такие механизмы, установленные в статьях 49–58 ДП I. Таким образом, чтобы выяснить, как именно можно применять принцип проведения различия в киберпространстве, сначала необходимо выработать надлежащее определение кибератаки. Относительно того, что́ можно охарактеризовать как кибератаку, в научном сообществе ведутся глубокие и значимые дискуссии[30]. Наиболее широко признанное определение кибератаки основано

27 МС, Законность угрозы ядерным оружием или его применения. Консультативное заключение. 8 июля 1996 г., п. 78.

28 ДП I, ст. 48; Обычное МГП (примечание 12 выше), нормы 1, 7, с. 3 и 32.

29 ДП I, ст. 51(4); Обычное МГП (примечание 12 выше), норма 11, с. 48

30 См.: Marco Rossini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 178–182; William H. Boothby, "Where Do Cyber Hostilities Fit in the International Law Maze?", in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict*, Springer, Berlin, 2014, pp. 60–62; Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17–19 November 2004; *Дрёге, Кордула*. «Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц», *Международный журнал Красного Креста*, том 94, номер 886, 2012; Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law and Policy Review*, Vol. 25, No. 2, 2014.

на методе оценки последствий. Например, в Таллинском руководстве 2.0 по международному праву, применимому к кибероперациям (Таллинское руководство 2.0) содержится следующее определение кибератаки: «кибероперация, как наступательная, так и оборонительная, которая, как можно разумно ожидать, приведет к ранению или смерти людей либо нанесет ущерб объектам или станет причиной разрушения последних»[31]. Авторы настоящей статьи придерживаются в ней приведенного выше определения[32]. Ни одна из действующих правовых норм в явной форме не запрещает и не регламентирует кибервойну как форму ведения войны, отличную от других таких форм. МГП в настоящее время не устанавливает никаких норм по поводу вопросов проведения различия при кибервойне. В связи с этим некоторые ученые утверждают, что существующая рамочная система, основанная на праве международных договоров, мало приспособлена к условиям киберпространства; этот аспект виртуальной войны отрицательно влияет на перспективы применения принципа проведения различия[33]. Одной из причин такого положения, по заверениям некоторых ученых[34], является то, что гражданская и военная кибернетическая инфраструктура не только тесно взаимосвязана, но и, по сути, является единым целым. Такое утверждение может служить основанием для выводов, существенно затрудняющих применение принципа проведения различия. С учетом того, что бóльшая часть составляющих киберпространства, например, оптоволоконные кабели, спутники, маршрутизаторы и узлы, относится к объектам двойного назначения, которые одновременно служат для выполнения и военных, и гражданских задач, классифицировать такие объекты может быть затруднительно. Так возникают сложноразрешимые проблемы, свя-

31 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 92, p. 415.

32 Метод оценки последствий весьма полезен, так как он переключает внимание со средств и характера действия на его воздействие и последствия, тем самым обеспечивая наличие критерия «нарушения» и определяя динамичность и адаптивность соответствующего правового положения. Тем не менее относительно этого метода у авторов настоящей статьи все же остаются два опасения. Первое из них состоит в том, что с практической точки зрения оценка нанесенного урона (ущерба) оказывается чрезвычайно сложной, особенно когда последствия в основном носят косвенный характер. Второе опасение заключается в том, что метод оценки последствий ограничивает понятие нападения и исключает из него операции, приводящие к тяжкому и разрушительному нефизическому ущербу. Аналогичные опасения выражены в: *МККК*. Международное гуманитарное право и кибероперации во время вооруженных конфликтов, Женева, ноябрь 2019 г. (Документ МККК по кибероперациям). С. 9–10. МККК также отмечал, что чрезмерно ограниченное понимание нападения сложносовместимо с объектом и целью норм, регламентирующих ведение военных действий. Между тем их совмещение совершенно необходимо для защиты гражданского населения и гражданских объектов от последствий военных действий. См.: *МККК*. Доклад «Международное гуманитарное право и вызовы современных вооруженных конфликтов». Женева, 2015 г. (Доклад МККК 2015 г.), доступно по адресу: https://www.icrc.org/ru/download/file/40074/mezhdunarodnoe_gumanitarnoe_pravo_i_vyzovy_sovremennyh_konfliktov.pdf, с. 73–74.

33 См.: Jeffrey Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol. 106, No. 7, 2008, pp. 1429–1430.

34 Robin Geiss and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review*, Vol. 45, No. 3, 2012, pp. 381, 383.

занные с применением принципа соразмерности[35]. В то же время классифицировать отдельных людей как комбатантов или гражданских лиц не всегда можно с достаточной определенностью — это объясняется учащением такого явления, как активизация участия гражданских лиц в войне[36], которое характеризуется все более широким использованием сложных кибернетических технологий и приводит к размытию четких границ. Вооруженные подразделения и гражданские предприятия беспрецедентно активно коммуницируют, сотрудничают и объединяют усилия[37]. Например, Китай уже дважды включал стратегию гражданско-военной интеграции в свои аналитические доклады[38]. Кроме того, немало сложностей в таких условиях вызывает и установление ответственности[39]; отследить место запуска ракеты в большинстве случаев не трудно, а вот при осуществлении кибернетических операций дымового шлейфа не остается.

Ряд ученых тщательно прорабатывают вопрос применения принципа проведения различия к киберпространству[40], а несколько государств, в том числе Соединенные Штаты[41] и Дания[42], внесли информацию о применении принципа проведения различия в рамках кибервойны в соответствующие национальные военные уставы. Общепризнано, к примеру, что нападение не обязательно должно иметь кинетическое воздействие для того, чтобы подпадать под нормы МГП; что нападения неизбирательного характера[43] запрещены; и если нападение специально не направлено на конкретных комбатантов или на конкретные военные объекты, оно ни в коем случае не является допустимым. Подобной неизбирательностью

35 Согласно принципу проведения различия, непосредственными боевыми целями в ходе вооруженного конфликта могут быть только военные объекты. Тем не менее нападение на правомерные военные объекты порой может причинять случайный урон (ущерб) гражданским лицам или объектам. Подобное отрицательное сопутствующее воздействие регулирует принцип соразмерности, запрещающий нападения в случаях, когда при нападении можно ожидать нанесения ущерба гражданскими лицами или их собственности, объем которого избыточен в сравнении с ожидаемым военным преимуществом. Четкое объяснение принципа соразмерности приведено в ДП I, ст. 51(5)(b). См. также: Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law*, Edward Elgar, Cheltenham, 2013, pp. 55–57.

36 «Гражданские лица играют все более значительную и сложную роль в вооруженных конфликтах как в качестве жертв, так и в качестве исполнителей». Данная общая тенденция получила название активизации участия гражданских лиц ("civilianization"), см.: Andreas Wenger and Simon J. A. Mason, "The Civilianization of Armed Conflict: Trends and Implications", *International Review of Red Cross*, Vol. 90, No. 872, 2008.

37 L. Zhu, "Competition for International Rules in Cyberspace" (примечание 2 выше), p. 40.

38 State Council Information Office of the People's Republic of China (SCIO), *China's National Defense in the New Era*, Beijing, July 2019, доступно по адресу: www.scio.gov.cn/zfbps/32832/Document/1660325/1660325.htm; SCIO, *China's Military Strategy*, Beijing, May 2015, доступно по адресу: www.scio.gov.cn/zfbps/ndhf/2015/Document/1435159/1435159.htm.

39 См.: Документ МККК по кибероперациям (примечание 32 выше), с. 11.

40 См., например: J. Kelsey (примечание 33 выше), p. 1427; Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 261; Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*", *International Review of the Red Cross*, Vol. 84, No. 846, 2002, p. 365.

41 DoD, *Law of War Manual*, Washington, DC, 12 June 2015, pp. 985–999.

42 Danish Ministry of Defence, Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Copenhagen, September 2016.

43 ДП I, ст. 51(4).

может характеризоваться компьютерный вирус, если он способен бесконтрольно распространяться из подвергнутых нападению военных систем на связанные с ними гражданские системы. Несмотря на то что все признают необходимость проведения различия между военными объектами/комбатантами и гражданскими объектами/гражданскими лицами, когда дело касается более практического вопроса о том, что́ является военным объектом и кто является комбатантом в рамках вооруженного киберконфликта, ситуация становится чрезвычайно противоречивой. Кроме того, как отмечает один китайский ученый, основополагающая характеристика нелетальности кибернетических средств и методов в условиях кибервойны делает традиционно защищаемые объекты и соответствующих лиц более уязвимыми, чем в условиях обычной войны. Данное обстоятельство способно вызывать затруднения при оценке правомерности кибероперации и приводить к более частому нарушению принципа проведения различия при их проведении[44]. С учетом значимости принципа проведения различия для ведения военных действий в киберпространстве совершенно необходимо понять, могут ли действующие нормы полноценно применяться в отношении кибервойны, и выяснить, как улучшить и уточнить их для такого применения.

Принцип проведения различия в отношении человеческих целей в кибервойне

В рамках принципа проведения различия природа цели определяется в соответствии с дихотомией «люди — объекты». Независимо от степени развития кибертехнологий, исполнителем враждебного действия остается человек, и даже при внедрении вирусов или в случае нападения на системы сетевой защиты, осуществляемого лишь посредством нажатий на клавиши клавиатуры и кнопки мыши, дихотомия «люди — объекты», в соответствии с которой определяется «кто» и «что» может быть атакован(-о), остается применимой. В этой части статьи мы разберем вопрос о том, на кого можно правомерно нападать в киберпространстве. Основополагающий принцип здесь заключается в том, что гражданские лица не должны являться объектом нападений[45]. Принцип проведения различия подразумевает, что противные стороны способны четко отличать гражданских лиц от комбатантов; однако анонимность, характерная для киберпространства, это осложняет.

Любой комбатант ранее являлся гражданским лицом, и любое гражданское лицо может самостоятельно стать комбатантом[46], будучи призванным на военную службу, поступив в вооруженные силы одной из воюющих

44 陈鹏飞, 论当代武装冲突法面临的挑战, 西安政治学院学报, 2014, 27(05) (Pengfei Chen, "Analysis of the Challenges to Contemporary Armed Conflict Law", *Journal of Xi'an Politics Institute of PLA*, Vol. 27, No. 5, 2014, доступно только на китайском языке).

45 ДП I, ст. 51(2); Обычное МГП (примечание 12 выше), норма 6, с. 25–31.

46 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2016, p. 174.

сторон в качестве добровольца, приняв непосредственное участие в военных действиях (это ведет к утрате защищенного статуса)[47] или в спонтанных массовых выступлениях — явлении, которое создает возможность для правомерного перехода из статуса гражданского лица в статус комбатанта[48]. В настоящей статье мы не будем обращаться к понятию спонтанных массовых выступлений, так как оно подразумевает физическое вторжение на территорию какой-либо страны и участие большой доли населения[49], а обеспечить наличие этих факторов кибернетическими средствами практически невозможно[50].

Благодаря создающейся в таком случае возможности легко отрицать ответственность государства и низким затратам «большинство кибероперацій отдаются на внешний подряд гражданским специалистам по киберпространству»[51]. В связи с этой тенденцией возрастает вероятность того, что «значительная доля людей, непосредственно задействованных при проведении кибероперацій [за исключением кибернетических подразделений, входящих в структуру регулярных вооруженных сил], будет в действительности приходиться на гражданских лиц»[52]. Может ли в таком случае патриотично настроенный хакер или специалист быть объектом нападения? Ответ будет зависеть от того, как именно интерпретируется «непосредственное участие в военных действиях» в контексте кибероперацій.

Кто является киберкомбатантом?

Гражданские лица, принимающие непосредственное участие в военных действиях, теряют свой защищенный статус, и в их отношении не действует иммунитет, имеющийся у комбатантов; некоторые ученые даже утверждают, что такие лица являются «незаконными»[53] комбатантами. МГП проводит четкое и надежное различие между комбатантами и некомбатантами, и этот факт отражает то фундаментальное значение, которое имеет принцип проведения различия в рамках этого института права. Комбатанты имеют право принимать непосредственное участие в военных действиях[54] и, соот-

47 ДП I, ст. 51(3); Обычное МГП (примечание 12 выше), норма 6, с. 25–27; Руководство по толкованию (примечание 14 выше), с. 47–82.

48 ЖК III, ст. 4A(6); Обычное МГП (примечание 12 выше), норма 106, с. 493, и в особенности норма 5, где объясняется, что участники спонтанных массовых выступлений являются исключением из определения гражданских лиц в том смысле, что они считаются комбатантами, хотя и не входят в личный состав вооруженных сил.

49 ЖК III, ст. 4A(6).

50 Tallinn Manual 2.0 (примечание 31 выше), Rule 88, p. 409.

51 Elizabeth Mavropoulou, "Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks", *Journal of Law and Cyber Warfare*, Vol. 4, No. 2, 2015, p. 78.

52 David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities", *Journal of Conflict and Security Law*, Vol. 17 No. 2, 2012, p. 292; см. также: Michael N. Schmitt, "'Direct Participation in Hostilities' and 21st Century Armed Conflict", in Horst Fischer and Dieter Fleck (eds), Crisis *Management and Humanitarian Protection: Festschrift for Dieter Fleck*, BWV, Berlin, 2004, p. 527.

53 Y. Dinstein (примечание 46 выше), p. 44.

54 ДП I, ст. 43(2).

ветственно, имеют иммунитет против преследования за действия, осуществляемые ими в соответствии с МГП[55]; таким образом, их можно рассматривать как цели. Данные закономерности актуальны и для кибервойны. Так как определение гражданских лиц основано исключительно на принципе исключения (гражданскими лицами считаются те, кто не является комбатантами[56]), вопрос о том, кого следует считать киберкомбатантом, обретает критическое значение[57].

Отмечается, что некоторые государства учреждают специальные подразделения в структуре своих вооруженных сил, которым поручается проведение кибероперации. Так, Соединенные Штаты учредили Кибернетическое командование США (КК США), присвоив одному из подразделений Стратегического командования США статус объединенного боевого командования[58], а Колумбия создала Объединенное кибернетическое командование вооруженных сил, исполняющее функции предупреждения и устранения угроз и нападений кибернетического характера, затрагивающих национальные ценности и интересы[59]. Определение киберкомбатанта — тема, заслуживающая тщательного обсуждения, так как от его результатов будет зависеть не только то, кто может являться правомерной целью, но и особенности присвоения статуса военнопленного в случае захвата.

В сущности, к комбатантам должен причисляться весь личный состав вооруженных сил противной стороны, будь то регулярных или нерегулярных, вне зависимости от принадлежности к действительным войскам или войскам запаса, в том числе члены военизированных формирований, де-факто относящиеся к вооруженным силам. Конкретная задача, выполняемая тем или иным лицом, которое является частью военного аппарата, значения в данном случае не имеет[60].

В Женевских конвенциях приводятся пять условий, соответствие которым является достаточным поводом для получения статуса правомерного комбатанта[61]. Первые четыре условия применимости статуса военнопленного и статуса правомерного комбатанта, выполняемые совместно, изложены в Гаагских и Женевских конвенциях. Отвечающие им лица: (i) имеют во главе лицо, ответственное за своих подчиненных (организо-

55 H. Harrison Dinniss, "Participants in Conflict" (примечание 13 выше), p. 254.

56 ДП I, ст. 50(1); Обычное МГП (примечание 12 выше), норма 5, с. 22–25.

57 Vijay M. Padmanabhan, "Cyber Warriors in the Jus in Bello", *International Law Studies*, Vol. 89, 2013; Maurizio D'Urso, "The Cyber Combatant: A New Status for a New Warrior", *Philosophy and Technology*, Vol. 28, No. 3, 2015; Jake B. Sher, "Anonymous Armies: Modern 'Cyber-Combatants' and Their Prospective Rights under International Humanitarian Law", *Pace International Law Review*, Vol. 28, No. 1, 2016; Sean Watts, "The Notion of Combatancy in Cyber Warfare" — работа, представленная на 4-й Международной конференции по киберконфликтам, проходившей в Таллине с 5 по 8 июня 2012 г.

58 Donald Trump, "Statement by President Donald J. Trump on the Elevation of Cyber Command", 18 August 2017, доступно по адресу: www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

59 *ООН*. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: доклад Генерального секретаря, док. ООН A/67/167, 23 июля 2012 г., с 6.

60 Y. Dinstein (примечание 46 выше), p. 41.

61 H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 144.

ванность); (ii) имеют определенный и явственно видимый издали отличительный знак; (iii) открыто носят оружие; (iv) соблюдают в своих действиях законы и обычаи войны (соблюдение)[62]. Данные четыре условия применяются к личному составу прочих ополчений и добровольческих отрядов, однако необходимость соответствия им подразумевается и для личного состава вооруженных сил сторон в конфликте. Еще одно, пятое, условие косвенно диктуется Женевскими конвенциями в следующей формулировке: (v) принадлежат к стороне, находящейся в конфликте[63].

По мнению авторов, элементы (i), (iv) и (v) являются существенными, а (ii) и (iii) — формальными. С учетом того, что в условиях кибервойны анонимность является нормальной характеристикой, более разумно будет сосредоточиться на существенных, а не на формальных элементах.

Первый элемент, то есть организованность, является ключевым в условиях кибервойны. Данный вопрос является скорее фактологическим, чем правовым, а это условие отражает наличие ответственного командования и иерархических связей[64]. Если же у киберформирования отсутствует достаточно четкая организационная структура — обычно структура «командующий — подчиненный», — нет четкого распределения обязанностей и механизма подотчетности, а также определенных элементов дисциплины и надзора, его члены не должны считаться правомерными комбатантами и определенно не должны иметь права на иммунитет комбатантов. Поскольку члены большинства киберформирований преследуют аналогичные цели, но при этом не имеют общей дисциплины, вероятность того, что существующее исключительно в онлайновой форме вооруженное формирование будет достаточно организованным, невелика[65]. Например, если внезапное прекращение участия, отказ от ведения военных кибернетических действий или нежелание подчиняться приказам командующего со стороны членов группы (члены кибергруппы могут быть вообще не знакомы между собой) не приводит к каким-либо последствиям для таких членов группы, то нет смысла утверждать, что столь слабо организованная группа отвечает критерию организованности. Это особенно справедливо в случае патриотических кибергрупп[66].

62 Женевская конвенция (I) об улучшении участи раненых и больных в действующих армиях от 12 августа 1949 г. (вступила в действие 21 октября 1950 г.), ст. 13(2); Женевская конвенция (II) об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море от 12 августа 1949 г. (вступила в действие 21 октября 1950 г.), ст. 13(2); ЖК III, ст. 4(A)(2); Женевская конвенция (IV) о защите гражданского населения во время войны от 12 августа 1949 г. (вступила в действие 21 октября 1950 г.), ст. 4(2); H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 145.

63 ЖК III, ст. 4(A)(6); H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 145.

64 Y. Dinstein (примечание 46 выше), p. 39; International Criminal Tribunal for Rwanda (ICTR), *The Prosecutor v. Jean-Paul Akayesu*, Case No. ICTR-96-4-T, Judgment (Trial Chamber), 2 September 1998, para. 626.

65 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 195.

66 Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law*, Oxford University Press, Oxford, 2018, pp. 104–108.

Четвертый элемент — то есть соблюдение МГП — остается неотъемлемым и не претерпел значительных изменений с приходом сетевых компьютерных технологий[67]. Если сами комбатанты не готовы соблюдать МГП, то они впоследствии не могут рассчитывать на этот правовой институт для получения предусматриваемых им преимуществ[68]. Последний элемент — это принадлежность к одной из сторон в конфликте. Он позволяет доказать наличие определенной связи между группой, осуществляющей кибератаку, и воюющим государством[69]. Компьютерные сети создают возможность использовать «кибероподчинение» и предлагают государствам привлекательные условия «отказа под благовидным предлогом», который становится невозможен только при обнаружении четкой связи между группой и государством. Участники таких формирований не считаются правомерными комбатантами[70]. Регулярным вооруженным силам государств не требуется доказывать наличие подобной связи, но когда речь идет об организованных онлайновых группах, не до конца ясно, какая степень контроля над ними со стороны государства будет достаточна для соответствия критерию[71].

Наиболее сложный вопрос связан со вторым и третьим элементами, которые требуют от комбатантов иметь определенный и явственно видимый издали отличительный знак и открыто носить оружие. Два данных условия тесно связаны с принципом проведения различия между комбатантами и гражданскими лицами. Ввиду того, что эти два условия призваны устранить риск ошибки при таком проведении различия и сделать любую попытку ввести противника в заблуждение невозможной[72], перенос этих условий в онлайновую среду будет заведомо осложнен, так как в такой среде нельзя выяснить, кто сидит за тем или иным компьютером, из-за анонимности киберпространства. Согласно предложениям некоторых ученых, в связи с невозможностью маркировки компьютерных пользователей отличительными знаками требование иметь отличительный знак должно применяться к компьютерам или системам, по аналогии с военными автомобилями, воздушными судами и кораблями, которые необходимо маркировать отличительными знаками. Подобные предложения в корне несостоятельны, так как маркировка компью-

67 H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 149.

68 Y. Dinstein (примечание 46 выше), p. 54.

69 См.: Denise Bindschedler-Robert, "A Reconsideration of the Law of Armed Conflicts", in *The Law of Armed Conflicts: Report of the Conference on Contemporary Problems of the Law of Armed Conflict*, 1971, p. 40; Katherine Del Mar, "The Requirement of 'Belonging' under International Humanitarian Law", *European Journal of International Law*, Vol. 21, No. 1, 2010.

70 H. Harrison Dinniss, "Participants in Conflict" (примечание 13 выше), p. 262.

71 Стандарт эффективного контроля, разработанный МС ООН в Никарагуа, представляется непригодным для определения того, что значит «принадлежать к стороне, находящейся в конфликте», так как эта формулировка предусматривает контроль над действием, а не над его исполнителем — в отличие от стандартов общего контроля и полной зависимости — и потому нацелена на конкретные действия. Marko Milanović, "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken", *Leiden Journal of International Law*, Vol. 22, No. 2, 2009, p. 317. О значении стандартов реального контроля, общего контроля и полной зависимости см.: Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, Vol. 18 No. 4, 2007.

72 Y. Dinstein (примечание 46 выше), p. 37.

тера как военной техники будет равносильна разрешению на правомерное нападение на любую систему, к которой такой компьютер будет подключен[73].

Кто-то возразит, что личный состав вооруженных сил мог бы в любом случае носить униформу, чтобы соответствовать требованию иметь определенный и явственно видимый издали отличительный знак[74]; например, можно было бы обязать личный состав КК США носить военную униформу при проведении кибероперациий. Такое мнение отражает благие намерения — было бы идеально, если бы регулярные войска могли носить униформу или другим образом обеспечивать проведение различия между ними и гражданскими лицами, но на практике такое требование не возымело бы большого воздействия, так как противные стороны все равно оставались бы в анонимном статусе. Объект и цель этого положения состоят в том, что предназначением униформы является устранение вероятности ошибки при проведении различия между гражданскими лицами и комбатантами. Во время обычных вооруженных конфликтов при ношении униформы в большинстве случаев ясно, кто является комбатантом, а кто — нет[75]. Но когда киберкомбатанты сидят у экранов своих компьютеров, порой на огромном расстоянии и вне пределов видимости для тех, на кого они нападают, другому воюющему государству безразлично, носят ли они униформу. В любом случае, даже если мы настаиваем на том, что весь личный состав официальных вооруженных сил должен носить униформу, когда речь идет о кибероополченцах, добровольческих киберформированиях или других организованных кибергруппах, это требование становится абсурдным. Кроме того, по-видимому, в киберпространстве не остается места для требования открыто носить оружие. Даже выработать определение кибероружия достаточно трудно, а обеспечить его открытое ношение — попросту невыполнимая задача[76]. Безусловно, нельзя

73 В интернете постоянно ведут поиск миллионы программ-ботов, предназначенных для обнаружения подключенных к сети компьютеров; бот, созданный для поиска компьютеров, выполняющих военные задачи, будет способен обнаружить их IP-адреса в течение нескольких минут. После обнаружения единственным эффективным способом вывести компьютер или систему из радиуса действия будет отключение их от сети, что приведет к нарушению их нормальной работы и сделает их бесполезными; следовательно, любая система, подключенная к сети тем или иным способом, будет полагаться исключительно на свои электронные средства обороны для предотвращения нарушения ее работы и для защиты против направленных на это действий. Таким образом, если изначально мысль об отличительных знаках для компьютеров и систем представляется полезным решением, на практике это создает дисбаланс между целью требования о ношении отличительных знаков и способностью проведения военных операций. См.: H. Harrison Dinniss, "Participants in Conflict" (примечание 13 выше), p. 257; H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), pp. 145–149.

74 Tallinn Manual 2.0 (примечание 31 выше), Rule 87, p. 405.

75 Это не всегда происходит именно так; например, гражданские лица, принимающие непосредственное участие в военных действиях, могут подвергнуться нападению, но они, скорее всего, не будут при этом носить военную униформу.

76 См.: Prashant Mali, "Defining Cyber Weapon in Context of Technology and Law", in Information Management Association, *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, PA, 2019; Jeffrey T. Biller and Michael N. Schmitt, "Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare", *International Law Studies*, Vol. 95, 2019; H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), pp. 250–278. H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 148.

исключать возможность кинетического нападения на киберкомбатантов. В заключение мы хотим заявить, что в условиях кибервойны второй и третий элемент не следует исключать полностью, но значительная потребность в продолжительном их обсуждении отсутствует.

Кто-то может сказать, что на цифровом поле боя нет реальной необходимости в отличительных знаках; кибератаку в отношении военных объектов осуществляет либо комбатант, либо гражданское лицо, принимающее непосредственное участие в военных действиях. В обоих случаях конкретное лицо, о котором идет речь, теряет свой защищенный статус. Тем не менее в этой ситуации некоторые вопросы все еще требуют решения — в особенности вопрос по поводу того, сможет ли такое лицо пользоваться статусом военнопленного в случае захвата[77]. Кроме того, гражданское лицо, осуществляющее нападение, может не соответствовать критериям «порога вреда» и «связи с воюющей стороной»[78] и, соответственно, в принципе не утратит защищенный статус.

Итак, определение того, кто является киберкомбатантом, не только связано с определенными затруднениями в области права, но и представляет собой чрезвычайно сложную техническую проблему для большинства государств. Действительность такова, что в настоящее время не существует способов четкого выявления киберкомбатантов, а имеющиеся нормы, таким образом, применимы в данном случае лишь частично. Если сравнивать вероятность участия гражданских лиц в кибернетических и обычных вооруженных конфликтах, то в первом случае она будет гораздо выше[79]. Как отмечает Майкл Шмитт, есть несколько причин активного участия гражданских лиц в конфликтах такого типа. С точки зрения соотношения затрат и получаемой пользы подготовка личного состава со специальными навыками проведения кибератак и обеспечения киберзащиты слишком дорогостояща и времязатратна для большинства стран, а кроме того, не гарантирует результат. Помимо этого, кибертехнологии в силу своей природы не поддаются стандартизации и количественному выражению. Технологии не только постоянно развиваются и обновляются, но и имеют слишком узконаправленный и специальный характер[80].

Описанные выше элементы (ii) и (iii) — требования иметь определенный и явственно видимый издали отличительный знак и открыто носить оружие — малопригодны для условий киберпространства и потому, вероятно, не должны учитываться при кибервойне. Однако, для того чтобы считаться правомерным комбатантом, лицо должно удовлетворять как минимум условиям элементов (i), (iv) и (v) — наличие ответственного командования и иерархических связей, соблюдение в своих действиях законов и обычаев войны и принадлежность к одной из сторон в конфликте. В иных случаях такое лицо либо остается защищенным от нападения, либо

77 H. Harrison Dinniss, *Cyber Warfare* (примечание 13 выше), p. 148.
78 Руководство по толкованию (примечание 14 выше), с. 53
79 M L. Zhu, "Competition for International Rules in Cyberspace" (примечание 2 выше), p. 40.
80 M. N. Schmitt (примечание 52 выше), p. 527.

считается принимающим непосредственное участие в военных действиях. С учетом этого приоритетной задачей следует сделать предотвращение чрезмерной милитаризации и минимизацию излишнего вреда, наносимого гражданским лицам. В то же время нельзя забывать, что, если имеются сомнения по поводу того, является ли тот или иной человек гражданским лицом, его следует считать таковым[81]. Таким образом, было бы неэтично и неправомерно толковать определение киберкомбатантов слишком широко.

Непосредственное участие гражданских лиц в кибернетических военных действиях

В отличие от комбатантов, гражданские лица не имеют права принимать непосредственное участие в военных действиях; а те из них, которые все же принимают такое участие, утрачивают право на общую защиту от угроз, связанных с военными операциями, и могут быть атакованы в период такого участия[82]. Кроме того, за подобное участие они могут быть подвергнуты судебному преследованию в судах национальной юрисдикции, даже если совершенные ими действия не являются противоправными с точки зрения МГП[83]. В условиях киберпространства понятие гражданских лиц, принимающих непосредственное участие в военных действиях, может быть даже более важным, если принимать во внимание существующую в современных вооруженных силах тенденцию к передаче специальных задач, требующих компетенций в киберпространстве, на внешний подряд гражданским лицам[84].

Как обсуждалось выше, термин «непосредственное участие в военных действиях» передает ту закономерность, согласно которой в общем случае гражданские лица не могут выбираться в качестве целей нападения, за исключением случаев, когда и пока они принимают непосредственное участие в военных действиях[85]. Эта закономерность также носит название иммунитета некомбатанта[86]. При обсуждении статьи 51 ДП I государства не пришли к соглашению о точном определении того, что означает фраза «непосредственное участие в военных действиях»[87]. Важный вклад в трактовку понятия непосредственного участия в военных действиях вносят два

81 ДП I, ст. 50(1); Обычное МГП (примечание 12 выше), норма 6, с. 31.
82 ДП I, ст. 51(3); Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв вооруженных конфликтов немеждународного характера (Протокол II), от 8 июня 1977 г. (вступил в силу 7 декабря 1978 г.); Обычное МГП (примечание 12 выше), норма 6, с. 25–31.
83 D H. Harrison Dinniss, "Participants in Conflict" (примечание 2 выше), p. 258.
84 D. Turns (примечание 52 выше), p. 279.
85 ДП I, ст. 51(3).
86 Judith G. Gardam, *Non-Combatant Immunity as a Norm of International Law*, Martinus Nijhoff, Dordrecht, 1993.
87 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Dordrecht, 1982, pp. 301–304.

следующих источника: дело «О целенаправленных убийствах»[88] и публикация МККК «Непосредственное участие в военных действиях. Руководство по толкованию понятия в свете международного гуманитарного права» (Руководство по толкованию)[89]. Публикация Руководства по толкованию вызвала активные дискуссии и некоторые противоречия[90]. С учетом того, что в этом вопросе остаются неясности и до конца не понятно, как именно можно применять это руководство на практике на физическом поле боя, названные факторы неопределенности еще более актуальны, когда речь идет о виртуальном поле боя[91].

Выработать определение непосредственного участия в военных действиях достаточно непросто, а определение непосредственного участия в кибернетических военных действиях — еще сложнее. Как отмечается в деле «О целенаправленных убийствах», для участия в военных действиях совершенно необязательно прибегать к использованию вооружений[92]. Следовательно, даже с учетом глубоких различий между современными средствами ведения войны и их предшественниками из прошлого века, воздействие таких средств ведения войны в сущности одинаково. Военные системы коммуникации будут одинаково неработоспособны как при нарушении их функционирования в результате воздействия компьютерного вируса, так и после их бомбардировки.

В целях дальнейшего членения этого вопроса на более конкретные аспекты и выработки указаний для специалистов-практиков автор Руководства по толкованию предлагает три совокупных критерия, при выполнении которых действие можно считать актом непосредственного участия в военных действиях. Во-первых, вероятным результатом действия должно быть негативное воздействие на военные операции или военный потенциал стороны в конфликте либо причинение смерти, ранение или разрушение соответственно людей или объектов, пользующихся защитой от непосредственного нападения (порог вреда). Во-вторых, должна существовать непосредственная причинная связь между действием и вредом, способным стать вероятным результатом действия или скоординированной военной операции, составной частью которой является указанное действие (непосредственное причинение). И в-третьих, действие должно быть специально направлено на достижение установленного порога вреда и быть совершено в поддержку одной стороны в конфликте и во вред другой (связь с воюющей стороной)[93]. В руководстве также рассматриваются сетевые компьютерные атаки и использование неприятельских компьютерных сетей в своих интересах, после чего приводится следующая оценка:

88 Israel High Court of Justice, *Public Committee against Torture in Israel v. Israel et al.*, Case No. HCJ 769/02, Judgment, 11 December 2005 (*Targeted Killings*).
89 Руководство по толкованию (примечание 14 выше), с. 53.
90 "Forum: Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010.
91 D. Turns (примечание 52 выше), p. 285.
92 Israel High Court of Justice, *Targeted Killings* (примечание 88 выше), para. 33.
93 Руководство по толкованию (примечание 14 выше), с. 53.

«Достаточными будут и электронное вмешательство в военные компьютерные сети противника, будь то посредством сетевых атак или использования неприятельских компьютерных сетей в своих интересах, перехват переговоров верховного командования или передача тактической информации о выборе цели для нападения»[94]. Такой трехкомпонентный аппарат критериев, в котором значение имеют порог вреда, непосредственное причинение и связь с воюющей стороной, является полезной отправной точкой для оценки того, должно ли гражданское лицо, проводящее враждебные кибернетические действия, утрачивать свой защищенный статус, и если да, то в какой мере[95]. Вопрос о том, следует ли трактовать эти критерии тем же образом применительно к киберпространству, остается открытым.

Первый критерий — порог вреда — отражает объективно оцененную вероятность причинения действием смерти или ранения людям или разрушения собственности. К примеру, если бы в ходе эстонского инцидента в 2007 году[96] или инцидента с компьютерным червем Stuxnet в 2010 году[97] действовали гражданские лица в международном вооруженном конфликте, можно было бы заключить, что кибератаки в Эстонии не достигли бы порога вреда, а вот в случае со Stuxnet такой порог был бы достигнут. Кибератаки, направленные на кибернетическую инфраструктуру Эстонии, привели к значительным неудобствам, так как эта страна является одним из мировых лидеров по «интернетизации», но не привели ни к одной смерти или причинению ранений, равно как и не вызвали разрушения или повреждения какой-либо собственности. Спровоцированные неудобства, сколь бы неприятными они ни были, не достигают порога вреда[98]. При этом определения «неудобства» не существует, и этот термин не используется в рамках МГП[99].

С другой стороны, кибератака на иранские центрифуги для обогащения ядерного топлива нанесла этим центрифугам физический ущерб[100]. В этом отношении Таллинское руководство 2.0 устанавливает, что «действие должно иметь предполагаемый или реальный эффект, выраженный в отрицательном воздействии на военные операции или военный потенциал противника, либо причинить смерть, физический вред или материальное разрушение соответственно людям или объектам, пользующимся

94 Руководство по толкованию (примечание 14 выше), с. 56.

95 Подобный трехкомпонентный тест был адаптирован к условиям кибервойны: Tallinn Manual 2.0 (примечание 31 выше), pp. 429–430.

96 "Cyber Attacks against Estonia (2007)" (примечание 15 выше); E. Tikk, K. Kaska and L. Vihul (примечание 15 выше), pp. 14–33.

97 "Stuxnet (2010)", *International Cyber Law in Practice: Interactive Toolkit*, CCD COE, доступно по адресу: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010); E. Tikk, K. Kaska and L. Vihul (примечание 15 выше), pp. 66–89.

98 D. Turns (примечание 52 выше), p. 286.

99 Доклад МККК 2015 г. (примечание 32 выше), с. 74.

100 По данным одного из отчетов, в период с конца 2009 г. по начало 2010 г. на заводе по обогащению ядерного топлива в Нетензе (Иран) пришлось заменить около 1000 центрифуг, что свидетельствовало об их поломке. David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Institute for Science and International Security, 22 December 2010; "Stuxnet (2010)" (примечание 97 выше).

защитой от непосредственного нападения»[101]. Таким образом, согласно Руководству, критерий порога вреда выполняется даже тогда, когда эффект действия является лишь предполагаемым. Подобная трактовка критерия порога вреда расширяет это понятие, представляя его не только как объективно оцененную вероятность, а скорее как либо субъективное намерение, либо объективно оцененную вероятность, и дает почву для дальнейших разночтений.

Второй элемент — непосредственную причинную связь — следует трактовать достаточно широко. Согласно Руководству по толкованию, соответствующий вред должен уместиться в «одном звене причинно-следственной цепи»[102]. Столь строгую трактовку причинно-следственной связи будет особенно проблематично применить к кибероперациям, где желаемым результатом атаки зачастую являются именно вторичный или опосредованный эффект определенного действия. Мы считаем, что формулировка «тесная причинно-следственная связь», подразумевающая как субъективную, так и объективную точку зрения, больше подходит для применения к киберпространству. В ней предусматривается объективность ущерба как нормального и естественного результата кибернетического действия, который можно субъективно предусмотреть[103].

Некоторые гипотетические сценарии помогут нам лучше понять механизм критерия тесной причинно-следственной связи в контексте киберпространства. Гражданские лица, нанятые для оказания общих компьютерных и ИТ-услуг, не будут считаться принимающими непосредственное участие в военных действиях, если они просто выполняют задачи, предусмотренные договором об оказании услуг, такие как обслуживание веб-сайтов и управление входными терминалами электронной почты[104], так как причинно-следственная связь не будет тесной (прямой), любой причиненный ущерб не будет являться нормальным и естественным результатом предусмотренных договором действий, а любые отрицательные последствия не могут быть предусмотрены теми, кто оказывает услуги. С другой стороны, любой сотрудник или подрядчик, нанимаемый специально для осуществления кибератаки против неприятеля, в теории будет удовлетворять критерию тесной причинно-следственной связи после того, как осуществит такую атаку.

Кроме того, чтобы проверить, имеется ли в той или иной ситуации тесная причинно-следственная связь, полезно будет попытаться применить к ней модель «поэтапной кибератаки»[105], разработанную корпорацией

101 Tallinn Manual 2.0 (примечание 31 выше), p. 429.
102 Руководство по толкованию (примечание 14 выше), с. 61.
103 Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge University Press, Cambridge, 1987, p. 181.
104 См.: Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare*, Sydney Law School Research Paper No. 12/10, 8 February 2012, доступно по адресу: https://ssrn.com/abstract=2001794.
105 См.: Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense", 2015, доступно по адресу: www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/ cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

Lockheed Martin. Модель поэтапной кибератаки — это упорядоченный перечень из следующих семи этапов кибератаки: разведка, создание вооружений, доставка, использование уязвимости, установка, командование и контроль, а также действие в отношении объектов[106]. Она позволяет взглянуть на общую структуру действий хакера по поражению той или иной цели, и несмотря на то, что не каждая кибератака включает в себя все семь этапов, данная модель тем не менее является хорошей отправной точкой. Первый этап — разведка — подразумевает изучение, выявление и отбор целей; за ним следует этап создания вооружений, в ходе которого подбирается комбинация вредоносных программ и создается готовая к доставке боевая нагрузка. Следующий этап — доставка — предусматривает транспортировку вооружений к цели (например, с помощью USB-приводов или приложений к электронным письмам); после доставки вооружения предпринимают попытку использовать уязвимость с целью получить доступ к жертве. До завершения четвертого этапа все еще сложно сказать, будут ли действия иметь прямую следственную связь с последствиями, так как дальнейшее развитие событий не всегда соответствует расчетам исполнителей атаки. Тем не менее на этапах установки, командования и контроля, а также действия в отношении объектов уже существует высокая вероятность того, что исполнителю удастся спрогнозировать развитие событий, и, соответственно, причиненный ущерб будет являться нормальным и естественным результатом соответствующих действий.

Элемент связи с воюющей стороной имеет в большей степени фактологическую, нежели правовую природу. То есть определенно требует того, чтобы «действие [было] специально предназначено для достижения установленного порога вреда и [было] совершено в поддержку одной стороны в конфликте и во вред другой (связь с воюющей стороной)»[107]. Этот элемент не имеет ничего общего с критерием субъективной стороны преступления. Значение имеет лишь цель действия, которая должна объективно предусматривать нанесение вреда. Это приводит нас к выводу о том, что враждебные действия, совершенные под давлением или непреднамеренно, не будут отвечать критерию связи с воюющей стороной. В свете того, что сетевые бот-атаки — явление не редкое, следует отметить, что необходимо предусмотреть исключение из положения о потере иммунитета для тех случаев, когда гражданский компьютер взломан сетью ботов и соответствующий пользователь не знает о вирусе и нападении. В таких случаях соответствующего пользователя нельзя рассматривать как исполнителя действия; соответственно — поскольку он не проявляет какой-либо активности, — критерий связи с воюющей стороной выполнен не будет.

Если роль гражданского лица заключается лишь в написании вредоносной программы, действие которой приведет к отключению крити-

106 См.: Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense", 2015, доступно по адресу: www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/ cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

107 Руководство по толкованию (примечание 14 выше), с. 53.

чески важной инфраструктуры, его действия не должны рассматриваться как непосредственное участие в кибернетических военных действиях, так как обыкновенно они не будут соответствовать всем трем критериям, и в любом случае причинно-следственная связь будет слишком отдаленной. Схожим образом гражданские ученые и эксперты по вооружениям обычно рассматриваются как обладающие защитой от прямого нападения[108]. Даже если это гражданское лицо отправляет самостоятельно написанную им вредоносную программу представителям вооруженных сил, которые он поддерживает, такое действие все равно не будет считаться непосредственным участием в военных действиях — по аналогии с транспортировкой вооружения. Однако если эта вредоносная программа предназначена для совершения конкретного враждебного действия, такое действие становится неотъемлемой частью кибернетической военной операции, и тем самым выполняется критерий тесной причинно-следственной связи. Когда гражданское лицо запускает такую вредоносную программу, — независимо от того, действует ли оно в рамках договора с вооруженными силами или по собственной инициативе, — оно, вероятно, будет соответствовать критериям и потому потеряет свой защищенный статус и станет правомерной целью — как минимум на период работы программы.

Статьей 51 ДП I также определяются временны́е рамки конкретных действий, считающихся непосредственным участием в военных действиях, а именно в ней говорится, что гражданские лица теряют защиту от прямого нападения «на такой период», пока они принимают непосредственное участие в военных действиях[109]. Если «такой период» завершился, то защищенный статус гражданского лица восстанавливается. Данные нормы следует отличать от тех, что установлены для участников вооруженных подразделений организованных вооруженных групп, принадлежащих стороне в вооруженном конфликте; данные лица прекращают быть гражданскими лицами и, следовательно, утрачивают защиту от непосредственного нападения на время выполнения ими постоянных боевых функций. Гражданские же лица утрачивают защиту от непосредственного нападения на время совершения каждого конкретного акта, составляющего непосредственное участие в военных действиях[110].

Особенно важным вопросом в контексте киберпространства является способ расчета временны́х рамок потери гражданским лицом защиты при рассмотрении повторяющихся кибероперацій в относительно сжатый период времени. Если гражданское лицо неоднократно проводит кибер-

108 ICRC, *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report*, Geneva, 27–28 November 2006, p. 48. Авторы настоящей статьи отмечают, что выражались некоторые сомнения по поводу того, можно ли придерживаться данной процедуры оценки в исключительных ситуациях, а именно в тех, когда специальные знания конкретного гражданского лица имеют чрезвычайное значение и потенциально могут решить исход вооруженного конфликта. Примером в данном случае могут служить эксперты по ядерному оружию во время Второй мировой войны.

109 ДП I, ст. 51(3); Обычное МГП (примечание 12 выше), норма 6, с. 25–31.

110 Руководство по толкованию (примечание 14 выше), с. 89.

операции, которые могут подпадать под определение непосредственного участия в военных действиях, каковы будут временны́е рамки или период утраты защиты от нападения?

В условиях обычных военных действий Руководство по толкованию предписывает рассматривать каждое из таких действий отдельно друг от друга[111], но в материалах дела «О целенаправленных убийствах» выражена обеспокоенность таким явлением, как «вращающаяся дверь»[112]. Согласно Руководству по толкованию, «вращающаяся дверь» защиты гражданских лиц предотвращает нападения на гражданских лиц, не представляющих в данный момент военной угрозы[113]. Поскольку понятие непосредственного участия в военных действиях относится к конкретным враждебным актам, МГП восстанавливает защиту гражданского лица от непосредственного нападения каждый раз, когда оно прекращает быть вовлеченным во враждебные акты[114]. С учетом того, что большое число кибероперациий, таких как DDoS-атаки, проводится неоднократно в течение одного временно́го периода, столь строгая демаркация времени является малопрактичной. Тем не менее авторы настоящей статьи также скептически относятся к перспективе подсчета продолжительности такого периода со времени первой операции и на всем протяжении прерывающегося действия. Эта точка зрения обусловлена тем, что гражданские лица, принимающие непосредственное участие в военных действиях, по статусу не равны участникам организованных вооруженных групп: несмотря на то что и те, и другие соответствуют критериям объектов для нападения, они представляют собой разные типы человеческих целей. Как упоминалось ранее, участники организованных вооруженных групп могут быть целями непосредственного нападения в течение всего периода выполнения ими постоянных боевых функций, а гражданские лица, принимающие непосредственное участие в военных действиях, утрачивают защиту от непосредственного нападения на время совершения каждого конкретного акта. «Гражданское лицо, однократно или эпизодически принимающее непосредственное участие в военных действиях, которое затем прекращает совершать это действие, с момента прекращения действия вновь подлежит защите от нападения»[115]. Итак, предположим, что гражданское лицо участвует в неоднократных кибератаках. Если весь временной промежуток (с начала первой кибератаки до конца последней) без перерывов будет засчитываться как период, в течение которого гражданское лицо может быть объектом нападения, в некотором смысле мы распространим на гражданское лицо, непосредственно участвующее в военных действиях, стандарты комбатантов (выполнение посто-

111 Руководство по толкованию (примечание 14 выше), с. 85, 86.
112 Israel High Court of Justice, *Targeted Killings* (примечание 88 выше), para. 40.
113 Руководство по толкованию (примечание 14 выше), с. 85–87.
114 См. характеристику непосредственного участия в военных действиях как потенциально «кратковременного и непостоянного»: ICTR, *The Prosecutor v. Strugar*, Case No. IT-01-42-A, Judgment (Appeals Chamber), 17 July 2008, para. 178.
115 Supreme Court of Israel, *Public Committee against Torture in Israel v. Government of Israel*, Case No. HCJ 769/02, 13 December 2006, para. 39.

янных боевых функций), так как промежутки между актами будут рассматриваться как часть периода, в течение которого лицо может являться объектом нападения. Строго говоря, гражданские лица, принимающие непосредственное участие в военных действиях, теряют защиту вследствие совершения конкретных актов, и при этом не подразумевается, что они совершают какие-то враждебные действия в период между такими актами. С одной стороны, гражданское лицо, которое присоединилось к военной организации и совершило ряд враждебных актов, перемежающихся короткими промежутками бездействия, теряет свой иммунитет против нападения на всем протяжении своих действий. Для такого лица промежутки бездействия являются не чем иным, как временем подготовки к совершению следующего враждебного акта[116].

В заключение можно утверждать, что при трактовке понятия «непосредственное участие в военных действиях» порог вреда требует существования объективно оцененной вероятности, а не лишь субъективного намерения; кроме того, должна быть подтверждена связь с воюющей стороной и должна иметься тесная причинно-следственная связь. Временны́е рамки потери защиты очень важны, но их весьма сложно установить. В настоящий момент правоприменительная практика по данному вопросу отсутствует, и задачу прояснения данного понятия еще предстоит решить членам научного сообщества, будущим государственным руководителям и судьям, выносящим соответствующие решения.

Принцип проведения различия в отношении не человеческих целей в кибервойне

Все не человеческие цели[117] можно подразделить на две категории: военные объекты и гражданские объекты. Гражданскими объектами являются все те объекты, которые не являются военными объектами[118]. Нападения должны ограничиваться военными объектами[119]. В этой части статьи мы обсудим, на какие объекты можно правомерно совершить нападение с учетом принципа проведения различия в киберпространстве, а точнее — что является военным объектом в киберпространстве. Беспокойство вызывает то обстоятельство, что почти у всех компонентов киберпространства есть огромный военный потенциал. В связи с этим проблема объектов двойного назначения обретает беспрецедентно большое значение при выборе цели. На фоне растущей важности данных в кибернетических вооруженных

116 Supreme Court of Israel, *Public Committee against Torture in Israel v. Government of Israel*, Case No. HCJ 769/02, 13 December 2006, para. 39; Daniel Statman, "Targeted Killing", *Theoretical Inquiries in Law*, Vol. 5, No. 1, 2004, pp. 179, 195.

117 Авторы настоящей статьи будут стараться не использовать в этом разделе термин «объекты», так как вопрос о том, существуют ли не человеческие цели, не являющиеся «объектами», будет рассмотрен в следующих разделах.

118 ДП I, ст. 52(1); Обычное МГП (примечание 12 выше), норма 9, с. 42.

119 ДП I, ст. 52(2); Обычное МГП (примечание 12 выше), норма 7, с. 32–37.

конфликтах будет также рассмотрен вопрос о том, можно ли рассматривать сами данные как военный объект.

Понятие «военного объекта»: два эквивалентных элемента

Широко принято следующее определение всех не человеческих боевых целей: что касается объектов, то военные объекты ограничиваются теми объектами, 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[120].

Понятие «военного объекта» является критически важным, так как именно от него напрямую зависит, на что можно совершать нападение в соответствии с принципом проведения различия. В действительности термин «военный объект» трактуется порой противоположными способами. Некоторые придерживаются мнения о том, что он подразумевает способность боевого функционирования или поддержания боя в целях ведения военных действий в формулировке статьи 52(2) ДП I и охватывает цели, которые «косвенно, но эффективно поддерживают и обеспечивают способность неприятеля к боевому функционированию»[121]. На практике соответствие первому критерию «эффективного вклада» обычно приводит к возникновению благоприятных условий, соответствующих второму критерию «явного военного преимущества»[122]. Другие заявляют, что только одновременное выполнение этих двух критериев может свидетельствовать о военном характере объекта в трактовке, приведенной в Протоколе[123]. Другими словами, проверка военного статуса того или иного объекта имеет два измерения, а два критерия эквивалентны друг другу[124].

Авторы настоящей статьи не согласны с тем, что «эффективный вклад» включает цели, которые «косвенно, но эффективно поддерживают и обеспечивают способность неприятеля к боевому функционированию», особенно в киберпространстве. Подобная трактовка слишком широка и обесценивает предназначение ограничения военных целей — и действи-

120 ДП I, ст. 52(2); Обычное МГП (примечание 12 выше), норма 8, с. 38–41; Jacob Kellenberger, "International Humanitarian Law at the Beginning of the 21st Century", statement given at the 26th Round Table on Current Problems in International Humanitarian Law, Sanremo, 5–7 September 2002.

121 DoD (примечание 41 выше), p. 210; Charles J. Dunlap, "The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era", *Strategic Review*, Vol. 9, 2000, p. 17; US Department of the Navy and Department of Homeland Security, *The Commander's Handbook on the Law of Naval Operations*, July 2007, para. 8.2. Существуют также и противоположные взгляды, отраженные, например: Laurent Gisel, "The Relevance of Revenue-Generating Objects in Relation to The Notion of Military Objective", in ICRC, *The Additional Protocols at 40: Achievements and Challenges*, 18th Bruges Colloquium, 19–20 October 2017.

122 Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, MA, 2010, p. 49.

123 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on APs), para. 2018.

124 E. Mavropoulou (примечание 51), p. 44.

тельно, охарактеризовав вклад как «эффективный», а преимущество как «явное», составители ДП I пытались избежать подобной широкой трактовки того, что является военным объектом[125]. В контексте киберпространства широкая трактовка также сделала бы проведение различия еще более затрудненным[126]; с учетом того, что почти у всех компонентов киберпространства есть огромный военный потенциал, если косвенная поддержка будет засчитываться как эффективный вклад, свобода трактовки станет практически неограниченной, так как это позволит «квалифицировать любую из информационных функций противника, которые имеют значение для его боеспособности, в качестве правомерной цели»[127]. Поэтому такое понимание противоречит предмету и цели статьи 52(2) ДП I.

Следовательно, определение военного объекта должно содержать два в равной степени важных критерия: эффективный вклад и явное преимущество. Выполнение первого критерия по умолчанию не обеспечивает выполнение последнего, так как они не зависят друг от друга. Критерий явного военного преимущества подробно обсуждался при составлении ДП I. В рамках этого обсуждения были рассмотрены и отвергнуты следующие определения [в скобках приведены варианты на английском и французском языке]: «выраженное» (distinct/distinct), «прямое» (direct/direct), «чистое» (clear/net), «непосредственное» (immediate/immediat), «очевидное» (obvious/evident), «конкретное» (specific/specifique) и «существенное» (substantial/substantiel)[128]. Очевидно, что у определения «явное» есть свои сильные стороны и им нельзя пренебрегать — преимущество должно быть явным и определенным[129]. Потенциальные или неопределенные формы преимущества неприемлемы для установки критерия, равно как и политические[130]. Иными словами, нападение запрещено осуществлять в случаях, когда оно дает только потенциальное или неопределенное преимущество[131].

Данные два элемента — эффективный вклад и явное военное преимущество — также являются эквивалентными. Зачастую определить ожидаемое в результате той или иной атаки преимущество бывает весьма затруднительно, особенно в контексте киберпространства, где оценка эффекта кибероперациий может быть связана с рядом проблем[132]. В области кибертехнологий, где военные, осуществляя свою деятельность, пользуются той же киберинфраструктурой, что и гражданское население, второй критерий определения становится еще более обширным. В этой связи следует делать соответствующий вывод с еще большей осторожностью, так как

125 Marco Sassòli, "Military Objectives", in *Max Planck Encyclopedia of Public International Law*, 2015, para. 7.
126 J. Kelsey (примечание 33 выше), p. 1440.
127 M. Roscini (примечание 65 выше), p. 186.
128 ICRC Commentary on APS (примечание 123 выше), para. 2019.
129 Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts*, Hart Publishing, Oxford, 2008, pp. 60, 131.
130 ICRC Commentary on APS (примечание 123 выше), para. 2024.
131 Ibid, paras 2024–2025.
132 M. Roscini (примечание 65 выше), p. 188.

поспешное принятие решения может серьезно подорвать ценность второго критерия[133]. По сравнению с другими целями киберпространство отличается относительной устойчивостью. При атаке на киберинфраструктуру, например сети коммуникаций, поток данных отличается такой гибкостью, что даже при разрушении некоторых каналов коммуникации в результате атаки пакеты данных все равно могут достигать конечного адресата по ряду других каналов[134]. В такой ситуации частичное разрушение сети может вносить эффективный вклад в военные действия, но вряд ли в итоге приведет к получению явного преимущества. Таким образом, суждение о явном военном преимуществе зависит от множества факторов, и этот критерий не может считаться выполненным по умолчанию сразу после того, как оказывается выполнен критерий эффективного вклада.

Явное военное преимущество в киберпространстве всегда сложно (если вообще возможно) измерить и представить количественно. После инцидента с червем Stuxnet Международное агентство по атомной энергии сообщило, что Иран прекратил подачу урана в тысячи центрифуг на заводе в Нетензе (хотя власти страны отрицали, что инцидент привел к серьезному ущербу). Никто не может точно сказать, какие последствия повлекла за собой атака Stuxnet для иранской ядерной программы, и до сих пор не ясно, было ли решение отказаться от использования центрифуг в Нетензе вызвано воздействием Stuxnet или технической неисправностью оборудования[135].

В контексте киберпространства отдельно стоит упомянуть тот факт, что требование определить явное военное преимущество, связанное с нападением на конкретные цели, чаще всего проявляется тогда, когда рассматривается перспектива нападения на объекты потенциально двойного назначения. Тот или иной объект может служить для выполнения исключительно гражданских или военных задач, но также может сочетать оба типа задач, и в таком случае будет являться объектом двойного назначения[136]. Базовая инфраструктура, такая как мосты, объекты электрогенерации и нефтеперерабатывающие заводы, также обладает потенциалом использования одновременно и для гражданских, и для военных целей[137].

Фундаментальное отличие условий кибервойны от условий обычной войны лежит в уникальной характерной черте киберпространства — а именно в «систематической взаимной связанности гражданской

133 R. Geiss and H. Lahmann (примечание 34 выше), p. 388.
134 Ibid.
135 Marco Roscini, "Military Objectives in Cyber Warfare", in Mariarosaria Taddeo and Luciano Floridi (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence of Excellence Initiative*, Springer, Cham, 2017, p. 108; Katharina Ziolkowski, *Stuxnet — Legal Considerations*, CCD COE, Tallinn, 2012, p. 5, доступно по адресу: https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.
136 Dominik Steiger, "Civilian Objects", in *Max Planck Encyclopedia of Public International Law*, 2011, para. 12.
137 Ibid.

и военной инфраструктуры»[138]. Так, по некоторым оценкам, около 98% коммуникаций правительства США[139] осуществляются посредством сетей, находящихся в гражданской собственности и обслуживаемых гражданскими лицами[140]. Гражданские спутники, маршрутизаторы, кабели, серверы и даже компьютеры — все это является инфраструктурой потенциально двойного назначения. Реальность такова, что «каждый компонент киберинфраструктуры, каждый бит объема памяти устройств обладает военным потенциалом», в связи с чем граница между гражданскими и военными объектами размывается[141]. Профессор Инженерного университета Военно-воздушных сил Китая Чжу Лисинь подчеркивает, что вооруженные силы США придают огромное значение построению устойчивых к внешним воздействиям систем разведки, рекогносцировки и наблюдения (РРН), использующих искусственный интеллект и квантовые вычислительные технологии, а также активно закупают вооружения, такие как бомбы малого радиуса действия, беспилотные системы группового действия, гиперзвуковое оружие и оружие направленной передачи энергии, чтобы обеспечить летальность. Для организации так называемых систем РРН требуется дорогостоящая техника, такая как квантовые компьютеры, спутники и системы искусственного интеллекта, многие образцы которой могут использоваться как в военных, так и в гражданских целях[142]. Несмотря на все сложности, с точки зрения права объекты двойного назначения не являются отдельной категорией; они в равной степени должны отвечать двунаправленному критерию статьи 52(2) ДП I. Предположение о том, что интернет сам по себе может быть военным объектом (целью), вероятно, необоснованно, так как при том, что использование военного кода в интернете может вносить определенный вклад в военные действия, такой вклад едва ли будет эффективен. Соответственно, нападение не будет оправданным, ведь сами по себе сбои в работе интернета вряд ли дадут необходимое «явное военное преимущество»[143]. В любом случае нападение на интернет в целом будет нарушать принцип соразмерности[144] и, следовательно, никак не может быть правомерным.

Более того, поскольку концепция двойного назначения не является инновацией, характерной только для кибервойны, ДП I содержит примечательное допущение для писанного закона (lex scripta): в случае сомнения

138 R. Geiss and H. Lahmann (примечание 34 выше), p. 385.

139 Во избежание неясности относительно приведенных цифр мы бы хотели напомнить читателям, что не все правительственные коммуникации приравниваются к военным коммуникациям или военным объектам.

140 Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks", *Texas Law Review*, Vol. 88, No. 7, 2010, pp. 1522, 1542.

141 R. Geiss and H. Lahmann (примечание 34 выше), p. 388.

142 L. Zhu, "Competition for International Rules in Cyberspace" (примечание 2 выше), p. 40.

143 International Criminal Tribunal for the former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, 13 June 2000, para. 75.

144 ДП I, ст. 51(5)(b), 57(2)(iii).

по поводу использования какого-либо объекта в военных целях предполагается, что такой объект используется в гражданских целях[145]. Норма 102 Таллинского руководства 2.0 также гласит, что «при возникновении сомнений по поводу того, используется ли в данное время объект и связанная с ним киберинфраструктура, в нормальной ситуации предназначенные для выполнения гражданских задач, для достижения эффективного вклада в военные действия, соответствующее решение может приниматься только после проведения тщательной оценки»[146].

Вопрос принадлежности данных к категории военных объектов

Данные становятся основой жизнедеятельности общества во многих странах. Во время вооруженного конфликта манипуляции с данными, направленные на причинение физического вреда, безусловно должны ограничиваться МГП, однако вопрос о том, могут ли данные сами по себе являться военным объектом, по-прежнему остается противоречивым. Целью кибератак могут быть данные, при этом какое-либо физическое воздействие может отсутствовать, например в случае кибератак на гражданские финансовые системы. Согласно позиции некоторых ученых, военным объектом, удовлетворяющим критериям цели, на которую можно совершить нападение, могут быть только материальные, осязаемые вещи[147]. Лишь меньшая часть экспертов, участвовавших в подготовке Таллинского руководства 2.0, сочла, что определенные данные следует рассматривать как объекты, и, соответственно, как военные цели[148]. Здесь важно проиллюстрировать характер связей между терминами «военный объект (цель)» и «объект». В сущности, из формулировки статьи 52(2) ДП I «что касается объектов, то военные объекты ограничиваются теми объектами, которые...» следует, что военный объект — это объект, отвечающий определенным критериям. Спорным вопросом здесь является то, могут ли данные сами по себе считаться объектом. Сомнения по поводу того, что данные могут являться военными объектами, в основном вызваны двумя причинами, и обе они связаны с определением понятия «объект». Первая — это неосязаемая природа данных, которая не соответствует обычному значению «объекта». Вторая причина отражена в одном из наблюдений, приведенных в Комментарии к Дополнительным протоколам МККК: «Объект характеризуется... как нечто видимое и осязаемое»[149]. Соответственно, данные явно не соответствуют определению объекта. Тем не менее некоторые уче-

145 ДП I, ст. 52(3).
146 Tallinn Manual 2.0 (примечание 31 выше), p. 448.
147 Yoram Dinstein, "Legitimate Military Objectives under the Current *Jus in Bello*", *International Law Studies*, Vol. 78, 2002, p. 142.
148 Tallinn Manual 2.0 (примечание 31 выше), Rule 100, p. 437; M. N. Schmitt (примечание 30 выше), p. 269; Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross*, Vol. 96, No. 893, 2015, p. 200.
149 ICRC Commentary on APS (примечание 123 выше), paras 2007, 2008.

ные утверждают, что данные следует считать объектами[150]. Они обосновывают такое утверждение тем, что кибероперации против гражданских данных на фактическом уровне являются неправомерными нападениями на гражданские цели. С точки зрения этих ученых, важно подчеркнуть, что любое воздействие, прямое или косвенное, на гражданские данные в рамках действий, направленных против правомерных кибернетических целей, должно измеряться в рамках анализа соответствия принципу соразмерности и подпадает под требования о сведении к минимуму случайного ущерба гражданским лицам и объектам[151]. Преимущество такого прочтения в том, что оно защищает гражданское население от потенциального отрицательного воздействия кибероперациий. В то же время оно слишком широко, имеет слишком большой охват и будет распространяться даже, например, на психологические кибероперации, которые уже осуществляются в некоторых странах на регулярной практической основе[152]. Вкратце, эта критика и сомнения относительно позиции, которую занимают большинство экспертов — авторов Таллинского руководства 2.0, сосредоточены вокруг исключения данных из области защиты, обеспечиваемой правом прицеливания (выбора цели) в ДП I. Согласно данной позиции, даже кибероперации, не влекущие за собой физических последствий, должны проверяться как минимум на соответствие принципу соразмерности и предосторожности[153], если они связаны с повреждением или уничтожением данных, пусть даже их воздействие на гражданское население является лишь потенциальным[154]. Другие ученые с этим не согласны и отмечают, что данные следует

150 См., например: Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, Vol. 48, No. 1, 2015; Документ МККК по кибероперациям (примечание 32 выше), с. 10–11; Доклад МККК 2015 г. (примечание 32 выше), с. 73–74; ICRC. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions,* Geneva, 2019 (ICRC Challenges Report 2019), p. 28.

151 Michael N. Schmitt, "International Cyber Norms: Reflections on the Path Ahead", *Netherlands Military Law Review*, 17 September 2018, доступно по адресу: http://puc.overheid.nl/doc/PUC_248171_11.

152 Ibid; Michael N. Schmitt, "Notion of Objects during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review*, Vol. 48, No. 1, 2015.

153 Как отмечается в работе Y. Dinstein (примечание 46 выше), pp. 164–174, принцип принятия мер предосторожности предусматривает как активные меры предосторожности при нападении (ДП I, ст. 57), так и пассивные меры предосторожности (ДП I, ст. 58). Активные меры предосторожности при нападении требуют «(a) делать все практически возможное, чтобы удостовериться в том, что объекты нападения [позволяют совершить его правомерно]; и (b) принимать все практически возможные меры предосторожности при выборе средств и методов нападения, с тем чтобы избежать случайных потерь жизни среди гражданского населения, ранения гражданских лиц и случайного ущерба гражданским объектам и, во всяком случае, свести их к минимуму». Пассивные меры предосторожности требуют от сторон «в максимальной практически возможной степени: (i) стремиться... удалить гражданское население... и гражданские объекты, находящиеся под их контролем, из районов, расположенных вблизи от военных объектов; (ii) избегать размещения военных объектов в густонаселенных районах или вблизи от них; и (iii) принимать другие необходимые меры предосторожности для защиты гражданского населения... и гражданских объектов... от опасностей, возникающих в результате военных операций».

154 Paul Ducheine and Terry Gill, "From Cyber Operations to Effects: Some Targeting Issues", *Netherlands Military Law Review*, 17 September 2018, доступно по адресу: https://puc.overheid.nl/doc/PUC_248377_11/1.

рассматривать как военный объект лишь в тех случаях, когда они соответствуют критериям. С их точки зрения, восприятие данных как объекта «привело бы к значительному расширению категории допустимых в рамках ведения войны целей»[155] и противоречит объекту и цели укрепления защиты гражданских лиц при вооруженных конфликтах. Более того, обычное значение термина «объект» может трактоваться по-разному. В текстах ДП I на шести аутентичных языках наблюдаются обусловленные процессом перевода разночтения[156]. Так, например, в испанском и французском языке термин «un bien» может переводиться на английский язык и как «a good» («благо» — *прим. пер.*), и как «a property» («имущество» — *прим. пер.*), а во французском языке данный правовой термин включает в себя как осязаемое, так и неосязаемое имущество[157]. В сущности, в китайском языке термином «объект»[158] обозначаются предметы, состоящие из материалов, которые занимают определенный объем пространства[159], и, следовательно, неосязаемые данные не будут считаться объектом.

По мнению некоторых ученых данные следует подразделять на две категории: данные «операционного уровня» и данные «содержательного уровня»[160]. В таком случае подразумевается, что данные содержательного уровня, например текст настоящей статьи или записи медицинских баз данных, сведения из библиотечных каталогов и аналогичных источников, в основном исключаются из охвата понятием военного объекта[161]. А вот данные операционного уровня — те, которые обеспечивают функционирование аппаратного обеспечения и его способность выполнять требуемые задачи, — должны считаться военным объектом[162].

К сожалению, китайские ученые уделяют мало внимания вопросу о том, следует ли считать гражданские данные гражданскими объектами и, следовательно, распространяется ли на такие данные защита, предусмотренная МГП. Чжу Яньсинь — доцент Института политологии Университета национальной обороны НОАК — считает, что данные можно определить как военную цель, не рассматривая при этом их как «объект»[163].

155 K. Mačák (примечание 150 выше).

156 ДП I, ст. 102: «Подлинник настоящего Протокола, английский, арабский, испанский, китайский, русский и французский тексты которого являются равно аутентичными...».

157 K. Mačák (примечание 150 выше).

158 В тексте ДП I на китайском языке используется термин “物体”. См.: www.icrc.org/zh/doc/assets/files/other/mt_070116_prot1_c.pdf.

159 由物质构成的, 占有一定空间的个体”. См.: 当代汉语词典, 上海辞书出版社, 2001 (*Contemporary Chinese Dictionary*, Shanghai Dictionary Publishing House, 2001); 现代汉语大词典, 下册, 上海辞书出版社, 2009 (*Modern Chinese Dictionary*, Vol. 2, Shanghai Dictionary Publishing House, 2009);新华汉语词典, 崇文书局, 2006 (*Xinhua Chinese Dictionary*, Chongwen Publishing House, 2006); 近现代词源, 上海辞书出版社, 2010 (*Etymology of Modern Times*, Shanghai Dictionary Publishing House, 2010).

160 Heather Harrison Dinniss, “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives”, *Israel Law Review*, Vol. 48, No. 1, 2015, p. 41.

161 Ibid.

162 Ibid.

163 朱雁新, 数据的性质: 对军事目标法律含义的重新解读, 载黄志雄主编, 网络空间国际规则新动向: “塔林手册2.0版” 研究文集, 社会科学文献出版社, 2019: 410–413 (Yanxin Zhu, “The Nature

По его словам, данные — это «не-объектный» военный объект (цель)[164]. Этот аргумент основывается на формулировке в начале второго предложения статьи 52 ДП I:

> Нападения должны строго ограничиваться военными объектами. Что касается объектов, то военные объекты ограничиваются теми объектами, 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[165].

Дословная формулировка статьи явно допускает существование военных объектов, которые являются объектами и не-объектами.

Мнение авторов настоящей статьи в основном совпадает с позицией, выраженной в программном документе МККК от 2019 года[166]. Данные определенных типов, как минимум гражданские данные[167], должны считаться гражданскими объектами, так как обычное значение термина «объект» развивается, и такое восприятие будет соответствовать предмету и цели Женевских конвенций и Дополнительных протоколов к ним. Термин «объект» не обязательно исключает данные из категории военных объектов; следует помнить, что обычное значение этого термина не следует ограничивать восприятием, существовавшим на момент принятия договора, так как оно развивается с течением времени[168]. Толкуя любые договоры на основании лишь текстуального подхода, мы будем игнорировать другие методы толкования, закрепленные в Венской конвенции о праве международных договоров[169]. Так, например, в контексте предмета и цели ДП I «утверждение о том, что в нашем мире, зависимом от данных, удаление или искажение таких важнейших данных гражданского назначения не запрещается МГП, с трудом согласуется с объектом и целью МГП»[170]. Утверждение о том, что замена досье и документов на бумажных носителях на цифровые файлы в форме данных не должна снизить степень защиты, которую им обеспечивает МГП, является убедительным аргументом[171]. Если не считать данные объектом, кибероперации против гражданских данных не будут регулиро-

of Data: A Reinterpretation of the Legal Meaning of Military Objective", in Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, pp. 410–413, доступно только на китайском языке).

164 Ibid, p. 410.

165 ДП I, ст. 52(2).

166 Документ МККК по кибероперациям (примечание 32 выше), с. 11.

167 Там же, с. 11.

168 K. Mačák (примечание 150 выше).

169 См.: Венская конвенция о праве международных договоров, 23 мая 1969 г. (вступила в действие 27 января 1980 г.), ст. 31(3)(a).

170 Документ МККК по кибероперациям (примечание 32 выше), с. 11.

171 ICRC Challenges Report 2019 (примечание 150 выше), p. 28.

ваться МГП, а кибероперации, причиняющие существенный ущерб жизни гражданских лиц, не будут запрещены правом (законом)[172].

В Таллинском руководстве 2.0 военные объекты (цели) приравниваются к объектам. Продемонстрируем это наглядно, приведя определение военных объектов из нормы 100, которое не предусматривает существования не-объектов: «Военные объекты — это те объекты, которые…»[173]. Мнение, согласно которому данные могут являться военными целями, не будучи при этом объектами, является спорным в силу двух основных причин. Во-первых, такое утверждение разрушило бы традиционную дихотомию «люди — объекты», которая (в контексте построения этих положений) представляется оптимальной; государства даже отвергли выделение третьей категории, такой как «места»[174]. Во-вторых, это привело бы к невозможности выделения критерия, пригодного для оценки того, являются ли конкретные данные военным объектом[175]. Дихотомия «люди — объекты» обеспечивает критерии эффективного вклада и явного преимущества для неодушевленных объектов, в то время как для одушевленных целей действуют другие требования[176]. Если не считать данные объектом, это создаст основания для необоснованного допущения о том, что данные следует оценивать на тех же основаниях, что и живые цели. Именно поэтому идея о возможности определить данные как военный объект, который при этом не является объектом, неубедительна.

Заключение

Афоризм Цицерона — «пусть молчат законы среди оружия» — совершенно не отражает современную действительность. Несмотря на все сопутствующие проблемы, принцип проведения различия в рамках права войны является применимым и к кибервойне. Ввиду отсутствия соответствующих договорных положений и судебных решений, учитывающих особенности киберпространства, толкование существующих правовых норм приходится основывать на доступных материалах научной дискуссии по данному вопросу и ограниченной практике государств. Существует потребность в общем прояснении и дальнейшей проработке принципа проведения различия в контексте киберпространства; например, следовало бы выработать единые четкие определения «кибернетического военного объекта» и «киберкомбатанта», так как в настоящее время трактовка этих понятий сильно варьируется. Как отметил Генеральный секретарь ООН, выступая на Всемирном экономическом форуме, «нам необходимо прийти к минимальному общемировому консенсусу по поводу того, как следует интегри-

172 См.: M. N. Schmitt (примечание 151 выше).
173 Tallinn Manual 2.0 (примечание 31 выше), p. 435.
174 M. Bothe, K. J. Partsch and W. A. Solf (примечание 87 выше), pp. 301–304.
175 K. Mačák (примечание 150 выше).
176 ДП I, ст. 52(2).

ровать новые технологии в законы войны, созданные много десятилетий назад в совершенно иных условиях»[177].

До настоящего времени правительство Китая не выработало четкой позиции относительно применения МГП в киберпространстве. Безусловно, китайские ученые уже опубликовали ряд работ, посвященных применению МГП в киберпространстве, однако в настоящее время дискуссии о принципе проведения различия недостает как хронологического масштаба, так и научной глубины. Исследования китайских ученых по данному вопросу пока находятся на достаточно ранней стадии по сравнению с западной наукой. До настоящего момента никто из представителей научного сообщества Китая не пытался разобрать или разъяснить вопросы применения принципа проведения различия в киберпространстве. Несмотря на потенциальные проблемы технического характера и факторы неопределенности, принцип проведения различия следует применять и к киберпространству. Необходимо также провести тщательную переоценку и уточнение аспектов такого применения для того чтобы предотвратить чрезмерную милитаризацию и обеспечить максимальную защищенность интересов гражданских лиц. Элементы статуса комбатанта, установленные в общем международном праве и соответствующих договорах, мало пригодны для применения на цифровом поле боя в контексте человеческих целей. Тем не менее киберкомбатанты обязаны демонстрировать свое отличие от гражданских лиц (то есть обеспечивать возможность проведения различия). Авторы статьи утверждают, что при применении принципа проведения различия стоит сосредоточится на существенных, а не формальных элементах, то есть, например, на открытом ношении оружия или ношении определенного отличительного знака, явственно видимого издали. При трактовке понятия «непосредственное участие в военных действиях» порог вреда требует существования объективной вероятности, а не лишь субъективного намерения; должна быть подтверждена связь с воюющей стороной, а также должна иметься как минимум тесная причинно-следственная связь. Применение модели «поэтапной кибератаки» по аналогии помогает нам охватить и лучше понять весь процесс непосредственного участия в военных действиях в ходе кибервойны. Нападение на все остальные (не человеческие) военные объекты должно в совокупности отвечать и критерию «эффективного вклада», и критерию «явного военного преимущества», которые являются в равной степени непреложными. Те же требования актуальны и для объектов двойного назначения. Что касается статуса данных, то обычное значение термина «объект» может трактоваться по-разному. В текстах ДП I на шести аутентичных языках наблюдаются обусловленные процессом перевода разночтения; во французском языке данный правовой термин включает в себя как осязаемое, так и неосязаемое имуще-

177 World Economic Forum, "António Guterres: Read the UN Secretary-General's Davos Speech in Full", 24 January 2019, доступно по адресу: https://www.weforum.org/agenda/2019/01/these-are-the-global-priorities-and-risks-for-the-future-according-to-antonio-guterres/.

ство, а в китайском языке этим термином обозначаются предметы, состоящие из материалов, которые занимают определенный объем пространства, и, следовательно, неосязаемые данные не будут считаться объектом. Кроме того, один из китайских ученых утверждает, что определенные данные относятся к категории «не-объектных» военных объектов.

С распространением интернет-технологий среди широких слоев населения в XXI веке в этой области произошли беспрецедентные изменения. Будущее применения МГП к киберпространству все так же находится в руках государств, особенно в том смысле, что они вырабатывают собственную трактовку действующих положений и норм. Война, технологии и право войны обрели значительную взаимосвязь и взаимопроникают друг в друга с самого начала организованных межчеловеческих конфликтов, но праву приходится приспосабливаться к меняющейся действительности и оно всегда «на одну войну отстает»[178] от нее. Таким образом, столкнувшись с изменениями в технологиях и науке, человечество должно использовать методы динамичной и развивающейся трактовки международных договоров и принципов международного права, чтобы обеспечить их полноценное действие. Следует признать, что все большее совершенствование вооружений и быстрое развитие науки и техники окажут огромное воздействие на жизнь человеческого общества, и право войны будет корректироваться и адаптироваться соответствующим образом. Тем не менее было бы наивно полагать, что изменения в МГП будут производиться своевременно и эффективно.

Пожалуй, еще не время призывать к принятию нового международного договора, регулирующего эту область. В любом случае перспективы того, что государствам удастся достичь согласия по поводу содержания всеобъемлющей конвенции о кибервойне в ближайшем будущем, крайне туманны. Вместо этого стоит воспользоваться базовыми нормами регулирования вопросов прицеливания (выбора целей) в киберпространстве, которые предоставляет существующее позитивное право (lex lata). Государственная практика, судебные решения и взгляды и теории ученых должны стать ведущими факторами толкования действующей системы права и оценки того, способна ли она разрешать соответствующие гуманитарные вопросы во многоаспектной области киберпространства. Стоит ожидать, что в процессе такого развития права государства могут рассуждать по аналогии, инициировать или творчески заполнять существующие в МГП пробелы или использовать позитивное право в контексте принципа проведения различия вне его нормативных границ при осуществлении новых стратегий в эпоху кибервойн. Подобную тенденцию следует строго ограничить; тем не менее исключать возможность установления норм было бы слишком самоуверенно. Для того чтобы предотвратить чрезмер-

178 Jimena M. Conde Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law", *Tilburg Law Review*, Vol. 15, No. 1, 2010. См. также: *Сассоли, Марко и Бувье, Антуан*. Правовая защита во время войны. Т. I. МККК, 2008. С. 135.

ную милитаризацию и обеспечить максимальную защищенность интересов гражданских лиц, следует предельно осмотрительно переосмыслить принцип проведения различия. До сих пор в мире не произошло ни одной катастрофической кибератаки с большим числом жертв. Данное обстоятельство, однако, не отменяет того, что, когда трактовки и прояснения действующих норм недостаточно, следует разрабатывать новые нормы — во избежание потенциального «кибернетического Пёрл-Харбора»[179].

179 DoD (примечание 4 выше); J. J. Wirtz, "The Cyber Pearl Harbor" (примечание 4 выше); J. J. Wirtz, "The Cyber Pearl Harbor Redux" (примечание 4 выше).