Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперациий во время вооруженных конфликтов

Лоран Жизель, Тильман Роденхойзер и Кнут Дёрман*

Лоран Жизель возглавляет отдел по вопросам вооружений и ведения военных действий в Правовом управлении Международного Комитета Красного Креста (МККК) в Женеве. В период между 2013 и 2020 гг. он был старшим юридическим советником МККК, руководителем группы по вопросам кибернетизации и норм, регулирующих ведение военных действий

* Более ранняя версия настоящей статьи была опубликована теми же авторами под заголовком «The Applicability and Application of International Humanitarian Law to Cyber Warfare» («Применимость и применение международного гуманитарного права к военным действиям в кибернетическом пространстве») в журнале *Chinese Review of International Law*, Vol. 32, No. 4, 2019. Она была значительно обновлена и расширена для публикации в этом номере журнала. Настоящая статья написана в личном качестве и не обязательно отражает точку зрения МККК.

в соответствии с международным гуманитарным правом, включая их применение во время войны в городских условиях, операций в киберпространстве и космическом пространстве.

Д-р Тильман Роденхойзер является юридическим советником в МККК, его работа связана с вопросами операций в кибернетическом пространстве во время вооруженных конфликтов, с проблемами негосударственных вооруженных групп и передачи задержанных лиц.

Д-р Кнут Дёрман — глава делегации МККК в ЕС, НАТО и Королевстве Бельгия (Брюссель), ранее занимал пост главного юрисконсульта и главы Правового управления (2007–2019 гг.). До этого он был заместителем главы Правового управления МККК (2004–2007 гг.) и юридическим советником МККК (1999–2004 гг.), в том числе по вопросам операций в кибернетическом пространстве.

Аннотация

Использование операций в кибернетическом пространстве и вопрос о том, как международное гуманитарное право (МГП) применяется к таким операциям, получили значительное развитие за последние два десятилетия. Авторы настоящей статьи, занимая различные должности в Правовом управлении Международного Комитета Красного Креста (МККК), внимательно следили за этим развитием и участвовали в правительственных и неправительственных совещаниях экспертов по этим вопросам. В настоящей статье мы анализируем соответствующие гуманитарные, правовые и политические вопросы. Прежде всего мы показываем, что осуществление операций в кибернетическом пространстве во время вооруженных конфликтов стало реальностью таких конфликтов и в дальнейшем таких операций будет еще больше. Таким образом, возникает целый ряд причин для обеспокоенности в сегодняшних все более киберзависимых обществах, в которых вредоносные кибероперации могут привести к серьезным повреждениям и причинить ущерб людям. Во-вторых, мы предлагаем краткий обзор многосторонних дискуссий, касающихся правовых и нормативных положений, регулирующих операции в киберпространстве во время вооруженных конфликтов, обращая особое внимание на различные аргументы, касающиеся применимости МГП к таким операциям во время вооруженных конфликтов и взаимодействия МГП и Устава ООН. Мы подчеркиваем, что, по нашему мнению, нет сомнений в том, что кибероперации во время вооруженных конфликтов, или кибервойна, регулируются МГП в точности так же, как любое оружие, средства и методы ведения войны, применяемые воюющими сторонами в конфликте, — как старые, так и новые. В-третьих, внимание в основной части настоящей статьи сосредоточено на том, как МГП применяется к кибероперациям. Анализируя правовые позиции, занимаемые государствами и экспертами в последнее время, мы заново

пересматриваем некоторые из наиболее характерных аргументов последнего десятилетия, например, какие кибероперации являются «нападением» по определению МГП и пользуются ли гражданские данные такой же защитой, как и «гражданские объекты». Мы также исследуем нормы МГП, применимые к кибероперациям, которые не являются нападениями, и особые защитные режимы для определенных категорий лиц и инфраструктуры, например медицинских учреждений и гуманитарных организаций.

Ключевые слова: операции в кибернетическом пространстве (кибероперации), вооруженный конфликт, кибервойна, гуманитарные последствия, международное гуманитарное право.

Использование киберопераций во время вооруженных конфликтов и вопрос о том, как международное гуманитарное право (МГП) применяется к таким операциям, получили значительное развитие за последние два десятилетия. Это необходимо учитывать на оперативном, правовом и политическом уровне. С оперативной точки зрения использование киберопераций во время вооруженных конфликтов стало реальностью вооруженных конфликтов, и, по всей вероятности, в дальнейшем таких операций будет еще больше. Такое положение вызывает определенные опасения в сегодняшних все более киберзависимых обществах, где злонамеренные кибероперации могут стать причиной серьезных повреждений и причинить ущерб людям. На политическом и правовом уровне в результате многосторонних процессов государства пришли к согласию по некоторым аспектам правовых и нормативных оснований, регулирующих кибероперации; однако применение МГП к кибероперациям во время вооруженных конфликтов остается предметом активного обсуждения. Несколько государств обнародовали свою позицию касательно применения МГП к кибероперациям во время вооруженных конфликтов, кроме того, есть большой объем научных исследований по этой теме, и все же основные проблемы остаются спорными — по ним не достигнуто согласия среди государств и экспертов, и они требуют дальнейшего изучения. К таким проблемам относятся понятие «нападение», вопрос о том, как гражданские данные защищены от вредоносных киберопераций, и какие нормы МГП применяются к кибероперациям, которые не являются нападением. Авторы настоящей статьи, занимая различные должности в Правовом управлении Международного Комитета Красного Креста (МККК), с самого начала внимательно следили за развитием событий и дебатами в этой области и принимали участие в дискуссиях правительственных и неправительственных экспертов о применимости и применении МГП к кибероперациям во время вооруженных конфликтов.

В недавней публикации МККК изложил всестороннюю позицию организации по вопросу о международном гуманитарном праве и кибероперациях во время вооруженных конфликтов, которая была представлена

Группе правительственных экспертов и РГОС Организации Объединенных Наций (ООН)[1]. В настоящей статье мы подробно рассматриваем эту позицию и сначала разъясняем, почему возможные гуманитарные последствия кибероперациий вызывают серьезную озабоченность. Затем мы подчеркиваем, что МГП применяется к кибероперациям во время вооруженных конфликтов и, следовательно, налагает на них ограничения, и рассматриваем точки зрения различных государств по этому вопросу. В-третьих, мы анализируем, в каких случаях кибероперации могут стать причиной начала вооруженного конфликта и как этот порог связан с запретом на применение силы и с правом на самооборону в соответствии с Уставом ООН и обычным международным правом. В последней и самой существенной части этой статьи мы подробно рассматриваем отдельные давно поставленные вопросы о том, как МГП применяется к кибероперациям во время вооруженных конфликтов и какую точку зрения приняли государства по некоторым ключевым вопросам.

На оперативном уровне использование кибернетической технологии стало реальностью сегодняшних вооруженных конфликтов, и, вероятно, такое использование получит еще большее распространение в будущем. Некоторые государства публично признали, что они проводили кибероперации в происходивших вооруженных конфликтах. В частности, Соединенные Штаты, Соединенное Королевство и Австралия сообщили, что они использовали кибероперации в своих конфликтах с группой «Исламского государства»[2]. В открытых источниках были также сообщения, в которых высказывались предположения, что Израиль проводил кибероперации против ХАМАС, а также утверждения, что ХАМАС использовал кибероперации против Израиля[3]. Кроме того, кибероперации осущест-

1 «Международное гуманитарное право и кибероперации во время вооруженных конфликтов. Изложение позиции МККК» (далее — Изложение позиции МККК). Документ представлен Рабочей группе открытого состава по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группе правительственных экспертов по вопросу о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. Ноябрь 2019 г., доступно по адресу: https://www.icrc.org/ru/document/mezhdunarodnoe-gumanitarnoe-pravo-i-kiberoperacii-vo-vremya-vooruzhennyh-konfliktov (все интернет-ресурсы были доступны в августе 2020 г.). См. также раздел «Доклады и документы» в этом номере журнала.

2 См., в частности: Mike Burgess, Australian Signals Directorate, "Offensive Cyber and the People Who Do It", speech given to the Lowy Institute, 27 March 2019, www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm; Paul M. Nakasone, "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services", 14 February 2019, www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf; Jeremy Fleming, GCHQ, "Director's Speech at CyberUK18", 12 April 2018, www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf.

3 "Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions", *BBC News*, 15 May 2019, www.bbc.co.uk/news/technology-48280902; Zak Doffman, "Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First", *Forbes*, 6 May 2019, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#1c692f73afb5. Хотя о намеченной цели предполагаемых кибероперациий ХАМАС открыто не сообщалось, нападение на здание ХАМАС с применением кинетической силы, как говорилось, основывалось на разведывательных данных, полученных в результате действий Сил обороны Израиля по обеспечению киберзащиты.

влялись против других стран, участвующих в вооруженных конфликтах, например против Грузии в 2008 г.[4], против Украины в 2015–2017 гг.[5] и против Саудовской Аравии в 2017 г.[6], хотя те, кто планировал эти операции, остались неизвестными и присвоение ответственности оспаривается. Поэтому неясно, имели ли эти операции связь с соответствующими вооруженными конфликтами и, таким образом, применяется ли МГП. Более того, сообщалось о кибероперациях, осуществляемых государствами в других ситуациях, где правовая классификация не может быть простой, в том числе в тех областях, которые иногда называют «серой зоной»[7]. Эти примеры показывают рост числа военных кибероперациий за последние десять лет — изменение в области ведения военных действий, которое может иметь продолжение. Действительно, как утверждается, все больше государств, включая пять постоянных государств — членов Совета Безопасности ООН[8], имеют

4 David Hollis, "Cyberwar Case Study: Georgia 2008", *Small War Journal*, 2010, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

5 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017, www.wired.com/story/russian-hackers-attack-ukraine/; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired,* 22 August 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

6 Blake Johnson *et al.*, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", *Fireeye Blogs*, 14 December 2017, www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

7 Например, в средствах массовой информации были различные сообщения, из анонимных официальных источников, о том, что Соединенные Штаты осуществляли кибероперации, направленные на цели в России и Иране, а Израиль проводил кибероперацию, имея целью порт в Иране. См.: Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms", *Washington Post*, 27 February 2019, https://tinyurl.com/yxs8twyv; David E. Sanger and Nicole Perlroth,"U.S. Escalates Online Attacks on Russia's Power Grid", *New York Times*, 15 June 2019, www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; Julian E. Varnes and Thomas Gibbons-Neff, "U.S. Carried out Cyberattacks on Iran", *New York Times*, 22 June 2019, www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility", *Washington Post*, 18 May 2020, https://tinyurl.com/y4onsrt9. О так называемых «серых зонах» и кибертехнологии см.: Camille Faure, "Utilisation contemporaine et future des technologies cyber/numériques dans les conflits armés", in Gabriella Venturini and Gian Luca Beruto (eds), *Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare*, 42nd Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2020; Gary Corn, "Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses", *Just Security,* 11 February 2020, www.justsecurity.org/68622/punchingon-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/. О пороге применимости МГП см. далее раздел «Кибероперации, которые регулируются МГП».

8 Кроме Соединенных Штатов и Соединенного Королевства, Франция поставила перед собой задачу «создать оборонный киберпотенциал» для защиты от «иностранных государств или террористических групп, [которые] могут осуществить нападение на критически важные объекты инфраструктуры» (France, Agence Nationale de la Sécurité des Système d'Information, *Information System Defence and Security: France's Strategy*, 2011, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf). В 2015 г. в «Белой книге» о военной стратегии Китая утверждалось, что, «реагируя на все более интенсивную разработку военного киберпотенциала в других странах, Китай будет создавать оборонительный военный киберпотенциал» (Government of China, *White Paper on China's Military Strategy,* 2015, www.gov.cn/zhengce/2015-05/26/content_2868988.htm). Россия не столь явно высказывается по этому вопросу, но Доктрина информационной безопасности Российской Федерации предусматривает «совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов,

или развивают военный киберпотенциал. К примерам использования кибероперациий во время конфликтов относятся шпионаж, опознавание целей, информационные операции для воздействия на моральное состояние противника и его желание сражаться, создание помех для функционирования системы коммуникации противника, введение его в заблуждение или искажение смысла сообщений с целью не допустить координации сил и кибероперации в поддержку кинетических операций[9]. Примером последнего является выведение из строя военных радиолокаторов противника, чтобы облегчить нанесение ударов с воздуха[10]. Более того, как можно судить по целому ряду кибероперациий за последнее десятилетие, которые не обязательно имели место в контексте вооруженных конфликтов, кибероперации, направленные против сетей электроснабжения, систем здравоохранения, ядерных установок или других критически важных объектов инфраструктуры, могут стать причиной нанесения серьезного ущерба людям[11]. С правовой точки зрения дискуссии о том, применяется ли международное гуманитарное право к кибероперациям во время вооруженных конфликтов, а если применяется, то каким образом и какие ограничения устанавли-

включающей в себя силы и средства информационного противоборства» в качестве основного направления «обеспечения информационной безопасности в области обороны страны» (Министерство иностранных дел Российской Федерации, Доктрина информационной безопасности Российской Федерации, 5 декабря 2016 г., https://www.mid.ru/documents/10180/2563110/Ukaz_Prezidenta_Rossiiskoi_Federatsii_ot_05122016.pdf/b579d736-cb99-46ac-b4f7-a0b6bc102ed1). См. также: Министерство обороны Российской Федерации «Операторы Западного военного округа отразили кибернападение условного противника в ходе учений "Щит Союза — 2015"», 2015 г., https://eng.mil.ru/en/news_page/country/more.htm?id=12056193@egNews. Общую оценку распространения информационных инструментов см.: Anthony Craig, "Understanding the Proliferation of Cyber Capabilities", Council on Foreign Relations, 2018, www.cfr.org/blog/understanding-proliferation-cyber-capabilities. Согласно Кибериндексу Института ООН по исследованию проблем разоружения (UNIDIR) в 2012 г. у 47 государств имелись программы кибербезопасности, в которых определенная роль отводилась вооруженным силам (UNIDIR, *The Cyber Index: International Security Trends and Realities*, UN Doc. UNIDIR/2013/3, Geneva, 2013, p. 1), в то время как в 2020 г. в рамках инициативы Digital Watch Observatory было зарегистрировано 23 и 30 государств соответственно, в отношении которых имеются либо свидетельства, либо признаки того, что они располагают наступательным киберпотенциалом (Digital Watch Observatory, "UN GGE and OEWG", https://dig.watch/processes/un-gge).

9 ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts* (готовится к публикации).

10 Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", *Wired*, 4 October 2007, www.wired.com/2007/10/how-israel-spoo/; Lewis Page, "Israeli Sky-Hack Switched Off Syrian Radars Countrywide", *The Register*, 22 November 2007, www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/.

11 В ноябре 2018 г. МККК созвал Совещание экспертов, чтобы выработать реалистичный способ оценки киберпотенциала и его возможные последствия в гуманитарном плане в свете его технических характеристик (см.: Laurent Gisel and Lukasz Olejnik (eds), *ICRC Expert Meeting: The Potential Human Cost of Cyber Operations*, ICRC, Geneva, 2019, www.icrc.org/en/download/file/96008/the-potentialhuman-cost-of-cyber-operations.pdf). См. также: Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", *Humanitarian Law and Policy Blog*, 3 December 2019, https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/. В Докладе 2020 г. Всемирного экономического форума (ВЭФ) «Глобальные риски» кибератаки названы в числе десяти самых высоких рисков — в плане как их вероятности, так и воздействия (см.: WEF, *The Global Risks Report 2020*, 2020, p. 3, www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf).

вает, начались более двух десятилетий назад[12]. Во время составления двух Таллинских руководств по международному праву, применимому к кибероперациям (Таллинские руководства), стало очевидно, что эксперты во многом единодушны в отношении того, что МГП применяется в кибернетическом пространстве и что его основные нормы и принципы могут и должны применяться при осуществлении кибероперации во время вооруженных конфликтов[13]. Однако, как позволяют понять различные точки зрения, высказанные в Таллинских руководствах, а также все увеличивающееся число позиций государств и множество научных публикаций по вопросам, связанным с кибернетикой, некоторые аспекты применения определенных норм МГП в этой области остаются недостаточно исследованными; существуют разногласия и по другим вопросам, включая некоторые из наиболее исследованных (см. далее раздел «Ограничения, налагаемые МГП на использование киберпотенциала во время вооруженных конфликтов»). На политическом уровне недавние и ведущиеся в настоящее время дискуссии в ООН показали, что достижение согласия по вопросу о применимости МГП к кибероперациям и дальнейшему изучению того, как его нормы должны толковаться, остается проблематичным[14]. Дискуссии по вопросам, связанным с информационной безопасностью, начались, когда Российская Федерация внесла первую резолюцию по этому вопросу на Генеральной Ассамблее ООН в 1998 г. Обсуждения стали более оживленными за последние несколько лет. После 2004 г. правительственные эксперты провели заседания в шести последовательно созываемых Группах правительственных экспертов по вопросам, касающимся информатики и телекоммуникаций в контексте международной безопасности. В 2018 г. Генеральная Ассамблея ООН также создала Рабочую группу открытого состава, которая работает одновременно с Группами правительственных экспертов (ГПЭ). И те, и другие имеют полномочие среди прочего изучить, «как международное право применяется к использованию информационно-коммуникационных технологий государствами»[15]. Эти дискуссии должны основываться на важных выводах, сделанных ранее Группами правительственных экспертов. В 2013 и 2015 гг. государства, представленные в ГПЭ, подтвердили, что «между-

12 См.: US Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 1999, https://fas.org/irp/eprint/io-legal.pdf; об одном из первых научных анализов этих вопросов см.: Knut Dörmann, "Computer Network Attack and International Humanitarian Law", 2001, www.icrc.org/en/doc/resources/documents/article/other/5p2alj.htm.

13 См.: Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, Cambridge, 2013 (Tallinn Manual); Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0).

14 См., в частности: OEWG, "Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and telecommunications in the Context of International Security", 11 March 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

15 Резолюция ГА ООН 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Док. ООН A/RES/73/27, 11 декабря 2018 г., п. 5; резолюция ГА ООН 73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности». Док. ООН A/RES/73/266, 2 января 2019 г., п. 3.

народное право, в частности Устав Организации Объединенных Наций, применимо» в области информационно-коммуникативных технологий, и сослались на «существующие принципы международного права, в том числе, в соответствующих случаях, принципы гуманности, необходимости, пропорциональности и [проведения различия]»[16]. И все же, как показали недавние обсуждения в ходе этих процессов в ООН и как об этом говорится далее, достижение согласия по вопросу о применимости МГП к кибероперациям и о дальнейшем исследовании толкования его норм остается проблематичным.

На региональном уровне уже в 2009 г. государства — члены Шанхайской организации сотрудничества (ШОС) определили среди основных угроз в области международной информационной безопасности «разработку и применение информационного оружия» и «подготовку и ведение информационной войны», но ничего не сказали о применимых правовых основаниях[17]. Дискуссии о применении международного права, включая МГП, состоялись среди прочего в Афро-азиатской консультативно-правовой организации (ААКПО) (которая создала Рабочую группу открытого состава по международному праву в киберпространстве в 2015 г.)[18], странах Содружества[19], Европейского союза[20], Организации Североатлантического договора (НАТО)[21] и рганизации американских государств (ОАГ)[22].

Возможные гуманитарные последствия кибероперации

Развитие информационно-коммуникационной технологии, включая коммуникацию посредством компьютерных сетей (киберпространство), создает огромные возможности для государств, обществ и отдельных лиц, в том числе в социальной, экономической, информационной и коммуникационной сферах. Международное сообщество, отдельные страны и граждане все сильнее зависят от цифровых инструментов. Эта тенденция, которая

16 Генеральная Ассамблея ООН. «Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря». Док ООН A/70/174, 22 июля 2015 г., пп. 24, 28(d).

17 Соглашение между правительствами государств — членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 г. (Соглашение ШОС), ст. 1; см. также, например: J. Fleming (примечание 2 выше), p. 5.

18 См.: AALCO, *International Law in Cyberspace,* Doc. No. AALCO/58/DAR ES SALAAM/2019/SD/17, www.aalco.int/Final%20Cyberspace%202019.pdf.

19 См.: The Commonwealth Cyber Declaration issued at the Commonwealth Heads of Government Meeting, London, 16–20 April 2018, https://thecommonwealth.org/commonwealth-cyber-declaration.

20 См., например: EU Council Conclusions, General Affairs Council meeting, Doc. No. 11357/13, 25 June 2013.

21 См., например: the Wales Summit Declaration issued by the heads of State and government participating in the meeting of NATO in Wales, 5 September 2014, para. 72, www.nato.int/cps/en/natohq/official_texts_112964.htm.

22 См.: OAS, *Improving Transparency: International Law and State Cyber Operations: Fourth Report*, OAS Doc. CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, www.oas.org/en/sla/iajc/docs/CJI_doc_ 603-20_rev1_corr1_eng.pdf.

может стать еще более заметной в результате пандемии COVID-19, распространяющейся в момент написания настоящей статьи, увеличивает нашу зависимость от беспрепятственного функционирования этих технологий, что делает нас только более уязвимыми перед кибероперациями. Быстро развивающиеся киберпространство и кибертехнологии и потенциальные гуманитарные последствия кибероперациий делают поэтому необходимым постоянный мониторинг и анализ.

Использование киберинструментов в качестве средств или методов ведения войны дает военным возможность достигать своих целей без необходимости причинять непосредственный ущерб гражданским лицам или физически повреждать объекты гражданской инфраструктуры. В зависимости от обстоятельств кибероперации могут давать возможность определять в качестве цели военный объект, снижая при этом ожидаемый сопутствующий ущерб гражданским объектам по сравнению с применением других средств ведения войны. В состоявшихся недавно межправительственных дискуссиях некоторые государства подчеркивали, что при ответственном использовании в соответствии с международным правом «применение ИКТ [информационно-коммуникационной технологии] в военных контекстах может быть предпочтительным по сравнению с использованием кинетического оружия и может способствовать деэскалации»[23]. В отличие от этого, как уже было сказано, государства — члены ШОС предупреждали об опасности «разработки и применения информационного оружия» и «подготовки и ведения информационной войны»[24].

Проведение кибероперациий, в ходе которых вполне возможно проводить различие, что соответствует МГП, и щадить гражданское население, может быть крайне трудным технологически. Взаимосвязанность, которой характеризуется киберпространство, означает, что кибероперации, осуществляемые в любой точке мира, могут воздействовать на все, что подключено к Интернету. Кибернападение на конкретную систему может воздействовать на различные другие системы, независимо от того, где эти системы находятся. Существует реальная опасность, что киберинструменты — преднамеренно или ошибочно — могут вызвать крупномасштабные и разнообразные последствия для критически важной гражданской инфраструктуры. Взаимосвязанность киберпространства означает также, что все государства должны озаботиться эффективным регулированием: «…нападения, осуществляемые на одно государство, могут иметь последствия для многих других, где бы они ни были расположены и независимо

23 "UK Response to Chair's Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf. См. также: ICRC (примечание 9 выше); Gary Corn, "The Potential Human Costs of Eschewing Cyber Operations", *Humanitarian Law and Policy Blog*, 31 May 2019, https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/.

24 Соглашение ШОС (примечание 17 выше), ст. 2.

от того, участвуют ли они в конфликте»[25]. Кибероперации, проведенные в последние годы, — в основном вне рамок вооруженных конфликтов, — показали, что вредоносные программные средства могут распространяться моментально по всему миру, поражая гражданскую инфраструктуру, и влиять на предоставление основных услуг[26]. Поэтому некоторые авторы предупреждают, что кибернападения на промышленные предприятия представляют собой «гуманитарный кризис, подготавливаемый на наших глазах»[27].

Представляется, что сектор здравоохранения особенно уязвим для кибератак[28]. Он развивается в сторону все большей цифровизации и взаимосвязанности, что увеличивает его зависимость от цифровых технологий и возможные масштабы поражения в случае нападения — тенденция, которая, вероятно, получит развитие в ближайшие годы. Слишком часто эти явления не сопровождались соответствующими улучшениями в области кибербезопасности[29].

Эта уязвимость стала особенно заметной во время пандемии COVID-19, когда больницы и другие учреждения здравоохранения в различных государствах сталкивались с нарушением своей деятельности в результате враждебных кибероперациий. Поскольку сектор здравоохранения исключительно важен для уменьшения страданий в любое время, но особенно во время вооруженных конфликтов и кризисов в области охраны здоровья, МККК призвал все государства уважать и предоставлять защиту медицинским службам и медицинским учреждениям от кибернападений любого рода, как в мирное время, так и в ситуации конфликтов, и подтвердить свою приверженность международным нормам, которые запрещают такие действия[30]. Хотя этот призыв отражает существующие обязательства

25 Helen Durham, "Cyber Operations during Armed Conflict: 7 Essential Law and Policy Questions", *Humanitarian Law and Policy Blog*, 26 March 2020, https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

26 К примерам относятся вредоносная программа CrashOverride, программа-вымогатель WannaCry, стирающая программа NotPetya и вредоносная программа Triton. CrashOverride повлияла на электроснабжение на Украине; WannaCry затронула больницы в нескольких странах; NotPetya нанесла ущерб очень большому числу предприятий; целью программы Triton было нарушение функционирования систем управления промышленностью, по имеющимся сведениям она использовалась в нападениях на нефтехимические заводы Саудовской Аравии. Немаловажный анализ см.: Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation", *Humanitarian Law and Policy Blog*, 14 November 2018, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

27 См.: S. Caltagirone (примечание 11 выше).

28 L. Gisel and L. Olejnik (eds) (примечание 11 выше), pp. 18–22.

29 См.: Aaron F. Brantly, "The Cybersecurity of Health", *Council on Foreign Relations Blog*, 8 April 2020, https://tinyurl.com/yxc4oc9j.

30 См.: "Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 May 2020, https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/. В конкретных рамках работы вышеупомянутой Рабочей группы открытого состава МККК предложил государствам принять норму, в силу которой они взяли бы на себя обязательство «не осуществлять и намеренно не поддерживать кибероперации, которые бы причиняли вред медицинским службам или медицинским учреждениям, и принять меры для защиты медицинских служб от ущерба». В этом предложении сочетается «отрицательный» элемент, а именно — государства не должны осуществлять или намеренно оказывать поддержку деятельности в кибернетическом пространстве, которая

в соответствии с МГП, как оно применяется к кибероперациям во время вооруженных конфликтов[31], его цель заключается в том, чтобы подтвердить и, возможно, усилить запреты, существующие согласно применяемому во всякое время публичному международному праву[32].

Кибероперации, направленные против других важнейших объектов гражданской инфраструктуры, таких как электросети, объекты водоснабжения и санитарии, также могут причинить значительный вред людям[33]. Часто функционирование этой инфраструктуры обеспечивают отраслевые системы управления (ОСУ). Кибернападения на такие системы требуют особых обширных знаний и опыта и зачастую созданных по специальным требованиям заказчика вредоносных программных средств, их цель — нарушение нормальной работы ПК. Хотя подобные нападения случались реже, чем другие виды кибероперций, их частотность по имеющимся сообщениям возрастает, и серьезность угрозы увеличивается быстрее, чем это ожидалось всего лишь несколько лет назад[34]. Специалисты в области кибербезопасности указывали, что «в силу того, что киберфизические нападения могут иметь кинетический эффект и привести к жертвам, очень важно, чтобы международное сообщество специалистов в области IT-безопасности, правительства и юристы в гуманитарной области срочно обсудили вопрос о том, как регулировать применение киберфизических нападений»[35].

Как сказано далее в настоящей статье, во время вооруженных конфликтов МГП предоставляет довольно полную защиту сектору здравоохранения и запрещает нападения на гражданскую инфраструктуру, если такая инфраструктура не становится военным объектом.

может причинить вред медицинским службам или учреждениям, и «позитивный» элемент, то есть государства должны принять меры для защиты медицинских служб от причинения ущерба (см.: ICRC, "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law", 11 February 2020, www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law).

31 См. далее раздел, озаглавленный «Нормы МГП, предоставляющие защиту объектам, необходимым для выживания гражданского населения, медицинским службам и операциям по оказанию гуманитарной помощи».

32 Подробнее о том, как международное право применяется к таким операциям, см.: Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?", *Just Security,* 27 March 2020, www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/. См. также: the Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector, May 2020 (Oxford Statement), www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

33 L. Gisel and L. Olejnik (eds) (примечание 11 выше), pp. 23–28. См. также: Aron Heller, "Israeli Cyber Chief: Major Attack on Water Systems Thwarted", *ABC News*, 28 May 2020, https://abcnews.go.com/International/wireStory/israeli-cyber-chief-major-attack-water-systems-thwarted-70920855.

34 Ibid., p. 25.

35 Marina Krotofil, "Casualties Caused through Computer Network Attacks: The Potential Human Costs of Cyber Warfare", 42nd Round Table on Current Issues of International Humanitarian Law, 2019, http://iihl.org/wp-content/uploads/2019/11/Krotofil1.pdf.

Если говорить о воздействии кибероперацій не только на конкретную инфраструктуру, можно выделить по крайней мере три их характерные черты, которые также вызывают озабоченность[36].

Во-первых, хотя это и не является невозможным, все-таки присвоение кибернападений государству или негосударственному актору оказалось проблематичным[37]. Затруднительно и определить акторов, которые нарушают МГП в киберпространстве, и привлечь их к ответственности, что является единственным способом обеспечить соблюдение МГП. Правдоподобные опровержения и надежда остаться необнаруженным могут также изменить политические расчеты, связанные с проведением кибернападений, — и с проведением их в нарушение международного права.

Во-вторых, как, например, отмечалось Китаем, «увеличение числа вредоносных кибернетических инструментов и технологий происходит все быстрее»[38]. Количество кибернетических инструментов и методов действительно может увеличиваться так быстро, что это трудно контролировать. Сегодня кибернападения на современном уровне могут осуществлять только наиболее квалифицированные акторы, располагающие достаточными ресурсами. После того как вредоносная программа использована, украдена, произошла ее утечка или она стала иным образом доступной, те акторы, которые не занимались ее разработкой, могут найти ее онлайн, восстановить исходный код и использовать ее для своих целей.

В-третьих, кибероперации опасны тем, что могут вызвать чрезмерную ответную реакцию пострадавших государств и последующую эскалацию насилия. Тем, против кого направлено кибернападение, обычно трудно узнать, является ли целью нападающего шпионаж или причинение иного, возможно физического, ущерба. Цель кибероперации может быть установлена с определенностью только тогда, когда будет достигнута конечная цель или получен желаемый эффект. Поэтому существует риск, что жертва операции будет ожидать самого пагубного ее воздействия и отреагирует сильнее, чем в случае, когда есть понимание того, что целью нападающего было просто осуществление шпионской деятельности.

К моменту написания настоящей статьи кибероперации не причинили серьезного вреда людям. Однако был нанесен значительный экономический ущерб[39]. Что касается возможных гуманитарных последствий

36 См. также: ICRC. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* Geneva, 2019 (ICRC Challenges Report 2019), p. 27, www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts; L. Gisel and L. Olejnik (eds) (примечание 11 выше), p. 7.

37 Подробнее о дискуссии по вопросу присвоения поведения, включая соответствующие нормы международного права, см. далее раздел, озаглавленный «Вопрос о присвоении поведения».

38 Statement by Counsellor Sun Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UN General Assembly, 23 October 2017), www.china-un.org/eng/chinaandun/disarmament_armscontrol/unga/t1505683.htm.

39 Общая стоимость ущерба в результате только преступлений в кибернетическом пространстве измеряется в триллионах долларов США: по существующим оценкам это было 3 триллиона долларов США в 2015 г., и эта цифра, как прогнозируется, будет удвоена к 2021 г. (Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation", Herjavec Group, 17 August 2016, www.herjavecgroup.

кибероперациий, то многое еще неизвестно, если говорить о технологическом развитии, возможностях и инструментах, разрабатываемых наиболее квалифицированными акторами, включая военных, и того, в какой степени использование кибероперациий во время вооруженных конфликтов может отличаться от наблюдаемых до сих пор тенденций. Другими словами, пока опасность гуманитарных последствий не представляется крайне высокой, если основываться на имеющихся в настоящее время наблюдениях, особенно с учетом разрушений и страданий, которые всегда являются результатом конфликтов, эволюция кибероперациий требует пристального внимания из-за существующей неопределенности и очень быстрого темпа изменений.

Применимость МГП к кибероперациям во время вооруженных конфликтов

С правовой точки зрения основным сводом норм, налагающим ограничения на использование кибероперациий во время вооруженных конфликтов и предоставляющим защиту гражданскому населению от возможного вреда, является международное гуманитарное право.

В МГП нет определения кибероперации, кибернетических военных действий или кибервойны. Нет его и в других областях международного права. Различные определения кибероперациий имеются в военных и других документах некоторых государств[40]. Другие государства говорят об информационных военных действиях или информационной войне и определяют это понятие таким образом, что оно включает по крайней мере несколько аспектов того, что часто понимается как военные действия в кибернетическом пространстве или кибервойна[41]. Независимо от того, как кибероперации, кибервойна или информационная война определяются государствами

com/hackerpocalypse-cybercrime-report/). Воздействие программы NotPetya оценивалось в сумму, превышающую 1 миллиард, а по некоторым оценкам достигало 10 миллиардов долларов (Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue", *Cybereason*, 9 November 2017, https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue; A. Greenberg, примечание 5 выше). Финансовые системы также часто подвергаются кибернападениям, см., например: Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks", *New York Times*, 20 March 2013, www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

40 См., например: US Department of Defense, *DOD Dictionary of Military and Associated Terms*.

41 Соглашение ШОС (примечание 17 выше) определяет «информационную войну» как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны». Вооруженные Силы Российской Федерации определяют информационную войну аналогичным образом, устанавливая, что «Вооруженные Силы Российской Федерации руководствуются нормами международного гуманитарного права» в ходе «военной деятельности в глобальном информационном пространстве» (Министерство обороны Российской Федерации. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, 2011, раздел 2.1, доступно по адресу: https://ens.mil.ru/science/publications/more.htm?id=10845074%40cmsArticle).

и кем-то еще, решение вопроса о том, применяется ли МГП к таким операциям, должно приниматься на основании особенностей и воздействия таких операций, а также обстоятельств их осуществления.

Выражение «кибероперации во время вооруженных конфликтов» МККК понимает как означающее операции против компьютерной системы, или сети, или иного подключенного к сети устройства через поток данных, когда такие операции применяются в качестве средства или метода войны в контексте вооруженного конфликта[42].

Хотя продолжаются споры о том, применяется ли МГП к кибероперациям во время вооруженных конфликтов и, следовательно, налагает ли оно ограничения на такие операции, МККК с самого начала занял ясную и твердую позицию[43]. По мнению МККК, вообще нет сомнения в том, что кибероперации во время вооруженных конфликтов, или кибервойна, регулируются международным гуманитарным правом, — в точности так же, как и любое оружие, средство и метод ведения войны, используемые воюющими сторонами в конфликте, как новые, так и старые. Тот факт, что кибероперации используют новые и постоянно развивающиеся технологии, не препятствует применению МГП в случае использования таких технологий в качестве средства или метода ведения войны. Это справедливо, независимо от того, считается ли киберпространство новой средой ведения военных действий, аналогично воздушному пространству, суше, морю и космосу, или средой иного типа, потому что она создана человеком, а прежние являются естественными, или вообще не является средой как таковой.

Мы считаем, что такое мнение находит убедительное подтверждение в договорах по МГП, в судебной практике Международного суда (МС) и в позициях целого ряда государств и международных организаций.

Сами объект и цель МГП заключаются в том, чтобы регулировать конфликты будущего, то есть те, которые будут происходить после принятия договора по МГП. Принимая такие договоры, государства включали нормы, в которых предвидится развитие новых средств и методов ведения военных действий, и предполагали, что МГП будет применяться и к ним. Уже в 1868 г. в Санкт-Петербургской декларации предполагалось, что устанавливаемые ею принципы должны сохраняться в силе в отношении «усовершенствований, произведенных науками в вооружении войск»[44]. Важная в этом отношении и более поздняя норма МГП находится в статье 36 Дополнительного протокола I 1977 г. (ДП I)[45], которая устанавливает:

42 См.: Изложение позиции МККК (примечание 1 выше).

43 См.: ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva, 2011 (ICRC Challenges Report 2011), pp. 36–39, www.icrc.org/en/doc/assets/files/red-crosscrescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; K. Dörmann (примечание 12 выше).

44 Декларация об отмене употребления взрывчатых и зажигательных пуль, Санкт-Петербург, 29 ноября 1868 г.

45 Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов (Протокол I), 8 июня 1977 г. (вступил в силу 7 декабря 1978 г.).

> При изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне.

Это обязательство, несомненно, основывается на той презумпции, что МГП применяется к таким новым видам оружия, средствам и методам, иначе не было бы необходимости оценивать их законность в соответствии с существующим правом. Сюда относятся и оружие, средства и методы войны, которые используют кибертехнологии.

Тот вывод, что МГП применимо к кибероперациям во время вооруженных конфликтов, подтверждается и далее мнениями, высказанными Международным судом. В своем Консультативном заключении о законности угрозы ядерным оружием или его применения Суд напомнил, что общепризнанные принципы и нормы гуманитарного права, применимого во время вооруженного конфликта, относятся «ко всем формам военных действий и всем видам оружия», включая оружие «будущего»[46]. Конечно, это включает и кибероперации. Такая точка зрения широко признается экспертами[47].

Все больше государств признают, что международное право применяется в кибернетическом пространстве и, в частности, что МГП применяется к кибероперациям во время вооруженных конфликтов — следовательно, налагает на них ограничения. Как уже было сказано, в 2013 и 2015 гг. в докладах Группы правительственных экспертов ООН был сделан вывод, что «международное право, в частности Устав Организации Объединенных Наций, применимо» в сфере информационно-телекомму-

46 МС, Законность угрозы ядерным оружием или его применения. Консультативное заключение. 8 июля 1996 г., п. 86.

47 См.: Tallinn Manual 2.0 (примечание 13 выше), Rule 80; Oxford Statement (примечание 32 выше), point 5. См. также статью «Применение принципа проведения различия к информационным технологиям: опыт Китая» (авторы — Чжисюн Хуан и Яохой Ин) в настоящем выпуске журнала; кроме того, см.: Ма Синьминь, тогдашний заместитель генерального директора Департамента международных договоров и права Министерства иностранных дел Китайской Народной Республики, который писал в личном качестве: «Сфера применимости норм МГП была расширена… Она также стала охватывать киберпространство. Группа правительственных экспертов ООН по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности подтвердила в своих докладах 2013 и 2015 гг., что международное право, в частности Устав ООН, применимо в кибернетическом пространстве. Поэтому МГП должно, в принципе, быть применимо к кибернападениям, но методы его применения все еще подлежат обсуждению» (неофициальный перевод, Ma Xinmin, "International Humanitarian Law in Flux: Development and New Agendas — In Commemoration of the 40th Anniversary of the 1977 Adoption Protocols to the Geneva Conventions", *Chinese Review of International Law*, Vol. 30, No. 4, 2017, p. 8).

никационной технологии[48]. Этот вывод сначала был одобрен[49], а затем подтвержден[50] Генеральной Ассамблеей ООН. В Докладе 2015 г., кроме того, делается ссылка на «существующие принципы международного права, в том числе, в соответствующих случаях, принципы гуманности, необходимости, пропорциональности и [проведения различия]»[51]. Хотя в этом перечне принципов МГП не упоминается явным образом, комментаторы указывали, что эти принципы являются «главными принципами МГП»[52].

В соответствии с этим выводом все больше государств и международных организаций публично утверждали, что МГП применяется к кибероперациям во время вооруженных конфликтов. К таковым относятся, например, ЕС[53] и НАТО[54]. Более того, Парижский призыв к доверию и безопасности в киберпространстве (его поддержали 78 государств на апрель 2020 г.) еще раз подтвердил применимость МГП к кибероперациям во время вооруженных конфликтов[55]; главы правительств 54 государств Содружества «обязуются содействовать дальнейшему обсуждению вопроса о том, как… применимое международное гуманитарное право применяется к кибероперациям во всех своих аспектах»[56]; и ответы государств на исследование, проведенное Юридическим комитетом ОАГ, — все это «свидетельствует о поддержке применимости МГП» в киберпространстве[57].

В то же самое время в контексте дискуссий о применимости МГП к кибероперациям во время вооруженных конфликтов целый ряд госу-

48 Генеральная Ассамблея ООН, «Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: Записка Генерального секретаря». Док. ООН A/68/98, 24 июня 2013 г., п. 19, и док. ООН A/70/174, 22 июля 2015 г., п. 24.

49 Резолюция ГА ООН 70/237, «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности». Док. ООН A/RES/70/237, 30 декабря 2015 г., преамбула, ч. 16.

50 Резолюция ГА ООН 73/27 (примечание 15 выше), преамбула, ч. 17; резолюция ГА ООН 73/266 (примечание 15 выше), преамбула, ч. 12.

51 Док. ООН A/70/174 (примечание 48 выше), п. 28(d).

52 Michael N. Schmitt, "France Speaks Out on IHL and Cyber Operations: Part I", *EJIL: Talk!*, 30 September 2019, www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/.

53 EU Council Conclusions (примечание 20 выше).

54 Wales Summit Declaration (примечание 21 выше), para. 72.

55 См.: "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", *France Diplomacy*, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

56 Commonwealth Cyber Declaration (примечание 19 выше), p. 4, para. 4.

57 См.: OAS (примечание 22 выше), para. 43 (где упоминаются Боливия, Чили, Гайана, Перу и Соединенные Штаты); может показаться, что ответ Эквадора подразумевает такую поддержку (см. также: paras 19–21, 25). Другие государства — члены ОАГ выразили свою позицию в контексте деятельности Рабочей группы открытого состава. См. замечания Бразилии, Колумбии и Уругвая по первоначальному проекту доклада Группы, www.un.org/disarmament/open-ended-working-group/. См., однако, мнения Кубы, Никарагуа и Венесуэлы, которые отмечают, среди прочего, что пока еще нет общего согласия относительно применимости МГП в киберпространстве и что прямое упоминание МГП в докладе может обосновывать или легитимизировать милитаризацию киберпространства.

дарств возражали против милитаризации киберпространства или гонки вооружений в киберпространстве. Государства также выразили обеспокоенность в связи с возможной легитимизацией использования киберопераций в военных целях[58], призвали к осторожности при обсуждении применимости МГП[59] и отметили, что МГП «должно применяться с учетом особенностей кибервойны»[60]. Это важные соображения, но их не следует понимать как несовместимые с применением МГП к кибероперациям во время вооруженного конфликта.

Однако, по нашему мнению, утверждение, что МГП применяется к кибероперациям во время вооруженных конфликтов, не является поощрением милитаризации кибернетического пространства и не должно в любом случае пониматься как легитимизация кибервойны[61]. Любое применение государствами силы, как кибернетической, так и кинетической природы, всегда регулируется Уставом ООН и обычным международным

58 См. недавние заявления Китая, Кубы, Ирана, Никарагуа, России и других по вопросу о первоначальном проекте доклада РГОС, www.un.org/disarmament/open-ended-working-group/. См. также: People's Republic of China, *Position Paper of the People's Republic of China for the 73rd Session of the United Nations General Assembly,* 2018 (Китайская Народная Республика, меморандум, излагающий позицию Китая для 73-й сессии Генеральной Ассамблеи Организации Объединенных Наций), p. 10, https://tinyurl.com/y4qquywp; "Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 23 June 2017, p. 2; Министерство иностранных дел Российской Федерации, «Ответ Специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности Андрея Крутских на вопросы ТАСС, касающиеся состояния международного диалога в этой сфере», 29 июня 2017 г.

59 «К применимости права вооруженных конфликтов и *jus ad bellum* необходимо относиться с осторожностью. Законность кибервойны нельзя признавать ни при каких обстоятельствах. Государства не должны превращать киберпространство в новое поле битвы» ("China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", September 2019, p. 6, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf). «Мы должны быть крайне осмотрительны в отношении любой попытки применять силу любого вида в киберпространстве, давать трезвую оценку возможных конфликтов и противостояний в результате неизбирательного применения права вооруженных конфликтов в киберпространстве и воздерживаться от того, чтобы дать миру неправильный сигнал» ("China's Contribution to the Initial Pre-Draft of OEWG Report", April 2020, p. 5, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf). «Без практики государств мы должны быть очень осторожны при обсуждении применения гуманитарного права в так называемых "кибервойнах". Причина очень проста, но крайне важна: во-первых, кибервойны не должны допускаться; и во-вторых, кибервойна будет совершенно новой формой высокотехнологичной войны» (Заявление Китая на 58-й ежегодной сессии Афро-Азиатской консультативно-правовой организации, стенографический отчет обсуждений: Fifty-Eighth Annual Session, Doc No. AALCO/58/DAR ES SALAAM/2019/VR, 2019, p. 176, www.aalco.int/Verbatim%20(FINAL)%2020200311.pdf).

60 На заседании Рабочей группы по международному праву в киберпространстве Афро-Азиатской консультативно-правовой организации представитель Китая заявил, что «режимы jus ad bellum и jus in bello должны применяться с учетом особенностей кибервойны» (AALCO, Summary Report of the Fourth Meeting of the Open-Ended Working Group on International Law in Cyberspace, 3 September 2019, www.aalco.int/Summary%20Report%20as%20Adopted.pdf).

61 Это мнение выражалось среди прочего в заявлениях Австралии, Бразилии, Чили, Дании и Соединенного Королевства, касающихся первоначального проекта доклада РГОС, www.un.org/disarmament/open-ended-working-group/.

правом, в частности запретом на применение силы[62]. Разногласия между государствами должны быть урегулированы мирным способом. Этот принцип применяется в киберпространстве, как и во всех других сферах. Кроме требований Устава ООН и независимо от него МГП предусматривает ограничения на ведение военных действий, если и в тех случаях, когда государства или негосударственные стороны используют кибероперации во время вооруженного конфликта. В частности, МГП предоставляет гражданским лицам и гражданским объектам защиту от военных действий, ограничивая выбор средств и методов ведения войны воюющими сторонами, независимо от того, было ли применение силы законным. Это означает, что, не легитимизируя кибероперации (как и любые другие военные действия) во время вооруженного конфликта, МГП — jus in bello — предусматривает ограничения в дополнение к тем, которые предусмотрены в Уставе ООН и обычном международном праве — jus ad bellum. Более того, МГП фактически налагает некоторые ограничения на милитаризацию киберпространства. Например, оно запрещает разрабатывать киберпотенциал, который может квалифицироваться в качестве оружия и быть неизбирательным по своей природе или который в силу своих особенностей может причинять чрезмерные или излишние страдания[63].

Если согласиться с тем, что в целом МГП применимо к кибероперациям во время вооруженных конфликтов, возникает следующий вопрос — все или только некоторые нормы МГП применяются? В этом отношении нормы МГП, касающиеся средств и методов ведения войны, могут широко быть разделены на нормы, которые применяются ко всем видам оружия, средствам и методам ведения войны, где бы они ни применялись (например, принцип проведения различия, соразмерности и принятия мер предосторожности), и нормы, которые касаются конкретных видов оружия (договоры о конкретных видах оружия) или конкретных областей применения оружия (например, предназначенные специально для регулирования войны на море). Все основные обычные принципы и нормы, регулирующие ведение военных действий, принадлежат к первой категории и применяются к кибероперациям во время вооруженных конфликтов[64]. В отличие от этого более подробный анализ потребуется в отношении применимости норм МГП, которые касаются конкретных видов оружия или конкретных областей его применения.

Тот факт, что МГП применимо, не мешает государствам развивать и далее международное право, согласовывая нормы, не имеющие обязательной силы, или работая над общим толкованием существующих норм.

62 Устав ООН, ст. 2(4).

63 См.: *Хенкертс, Жан-Мари и Досвальд-Бек, Луиза.* Обычное международное гуманитарное право. Том I: Нормы. МККК, 2006 (далее — Обычное МГП). Нормы 70, 71, https://www.icrc.org/rus/resources/documents/publication/pcustom.htm.

64 Принципы и нормы, регулирующие ведение военных действий, освещаются далее в разделе «Ограничения, налагаемые МГП на использование киберпотенциала во время вооруженных конфликтов».

Например, когда в 2018 г. была создана РГОС ООН, большинство государств на Генеральной Ассамблее ООН приветствовали «нормы, правила и принципы ответственного поведения государств», которые основывались на нормах, разработанных за годы работы Группой правительственных экспертов[65]. Еще один пример возможных новых норм в области информационной безопасности включен в Международный кодекс поведения для обеспечения информационной безопасности, представленный в 2011 г. ООН государствами — членами ШОС. Согласно Кодексу государства должны взять на себя обязательство среди прочего «не распространять информационное оружие и связанные с ним технологии»[66]. Существуют также предложения исследователей, в том числе связанные с дальнейшими правовыми и политическими ограничениями на кибероперации во время вооруженных конфликтов[67].

Подводя итог, можно сказать, что хотя убедительные правовые аргументы и все возрастающая международная поддержка подтверждают вывод о том, что МГП применяется к кибероперациям во время вооруженного конфликта, по этому вопросу все-таки еще нет всеобщего согласия. Однако, как показано в настоящем разделе, тщательный анализ различных аргументов, выдвигаемых в ходе многосторонних дискуссий, свидетельствует о том, что подтверждение применимости МГП не легитимизирует ни милитаризации киберпространства, ни использования вредоносных кибероперациий. Более того, ничто не мешает разработке возможных новых норм, но, скорее, МГП предоставляет надежную правовую основу, на которой могут — и должны — разрабатываться возможные новые нормы.

65 Резолюция ГА ООН 73/27 (примечание 15 выше).

66 Правила поведения в области обеспечения международной информационной безопасности. Док. ООН A/66/359): они были представлены Китаем, Российской Федерацией, Таджикистаном и Узбекистаном в 2011 г., а в 2013 г. к ним присоединились Казахстан и Киргизстан (см. док. ООН A/68/98 (примечание 48 выше), с. 10, п. 18). Аналогичным образом в 2011 г. Министерство иностранных дел Российской Федерации представило проект Конвенции по международной информационной безопасности (22 сентября 2011 г., https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU), где среди «Основных мер по предотвращению военных конфликтов в информационном пространстве» перечислены «меры по ограничению распространения “информационного оружия” и технологий его создания» (ст. 6(10)), которые будут принимать государства. В ст. 7(2) предусматривается также, что «в случае любого международного конфликта право государств-участников, находящихся в конфликте, выбирать методы или средства ведения “информационной войны” ограничено применимыми нормами международного гуманитарного права».

67 Среди многих других Паскуччи, например, предложил подумать о принятии Дополнительного протокола IV, в котором могли бы быть рассмотрены отдельные вопросы, встающие в результате применения принципа проведения различия и соразмерности в киберпространстве: Peter Pascucci, “Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution”, *Minnesota Journal of International Law*, Vol. 26, No. 2, 2017. Между тем Шмитт выдвинул предложения, касающиеся политики, которую могли бы принять государства: Michael N. Schmitt, “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations”, *International Review of the Red Cross*, Vol. 101, No. 910, 2019, pp 333–355.

Могут ли кибероперации сами по себе переступить через «порог»? Разъяснение разницы между соответствующими порогами согласно МГП и Уставу ООН

Поскольку ежедневно сообщается о многообразии кибероперациий, важно помнить, что МГП применяется только к кибероперациям, которые являются частью вооруженного конфликта, ведущегося во всех других отношениях с применением традиционных видов оружия или, что менее вероятно, к тем кибероперациям, которые уже сами по себе являются вооруженным конфликтом в отсутствие кинетических операций. Как подчеркивалось в предыдущем разделе, вопрос о том, применяется ли МГП к кибероперациям во время вооруженных конфликтов, следует проанализировать отдельно от вопроса о том, были ли нарушены нормы, регулирующие применение силы в соответствии с Уставом ООН. В контексте применения МГП и Устава ООН ключевой проблемой является присвоение кибероперациий государствам. Эти три пункта — какие кибероперации регулируются МГП[68], взаимодействие между МГП и Уставом ООН и вопрос о присвоении — рассматриваются в настоящем разделе.

Кибероперации, которые регулируются МГП

Когда кибероперации осуществляются в контексте существующего международного или немеждународного вооруженного конфликта, ведущегося при помощи кинетических средств, или имеют связь с таким конфликтом, ко всем сторонам в конфликте и их действиям применяются соответствующие нормы МГП[69]. Кибероперации, осуществляемые одновременно с кинетическими операциями и в поддержку таких операций во время вооруженных конфликтов, являются единственным видом операций, которые государства признают и считают, что они регулируются МГП[70].

Отдельный вопрос заключается в том, могут ли только кибероперации, если не ведутся кинетические операции, регулироваться МГП. Другими словами, может ли кибероперация быть первым и, возможно, единственным выстрелом в вооруженном конфликте, как он определяется в МГП? Это должно определяться в соответствии с общими статьями 2 и 3 четырех Женевских конвенций 1949 г.[71] для международных и немежду-

68 Подробнее об этих дебатах см.: "Scenario 13: Cyber Operations as a Trigger of the Law of Armed Conflict", in Kubo Mačák, Tomáš Minárik and Taťána Jančárková (eds), *Cyber Law Toolkit*, https://cyberlaw.ccdcoe.org/.

69 См.: МККК, Комментарий к Женевской конвенции I: Конвенция об улучшении участи раненых и больных в действующих армиях (далее — Комментарий МККК к ЖК I) (готовится к публикации на русском языке), п. 254; Tallinn Manual 2.0 (примечание 13 выше), Rule 80.

70 См. ссылки в примечании 2 выше.

71 Женевская конвенция от 12 августа 1949 года об улучшении участи раненых и больных в действующих армиях (вступила в силу 21 октября 1950 г.) (ЖК I); Женевская конвенция от 12 августа 1949 года об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море (вступила в силу 21 октября 1950 г.) (ЖК II); Женевская

народных вооруженных конфликтов соответственно[72]. Эти два типа вооруженных конфликтов различаются особенностями сторон, которые в нем участвуют, уровнем интенсивности насилия, который обусловливает применимость МГП, и некоторыми применимыми нормами МГП.

Относительно международных вооруженных конфликтов общая статья 2 устанавливает, что «настоящая Конвенция будет применяться в случае объявленной войны или всякого другого вооруженного конфликта, возникающего между двумя или несколькими Высокими Договаривающимися Сторонами, даже в том случае, если одна из них не признает состояния войны». Сегодня все согласны с тем, что «вооруженный конфликт имеет место всегда, когда в отношениях между государствами применяется вооруженная сила»[73]. Что же касается вопроса о том, существует ли порог интенсивности в связи с международными вооруженными конфликтами, то имеется определенная практика государств и некоторые сильные гуманитарные и концептуальные аргументы в пользу того, что МГП применяется, когда вооруженная сила используется в отношениях между государствами, независимо от интенсивности насилия. МГП в основном защищает лиц, пострадавших от вооруженного конфликта. Таким образом, как только государства применяют вооруженную силу, они должны направлять свои нападения на военные объекты, а не на гражданских лиц или гражданские объекты, их необходимо постоянно щадить. Не имеет значения, одно или много гражданских лиц нуждается в защите от нападения[74]. По крайней мере, если использование кибероперацій в отношениях между государствами приводит к последствиям, схожим с последствиями использования более традиционных средств и методов войны, применяется МГП.

Эксперты в целом согласны с тем, что кибероперации сами по себе могут достичь уровня международного вооруженного конфликта согласно МГП[75]. МККК разделяет это мнение[76]. Государства редко выражают свою позицию по этому вопросу, однако Франция заявила, что «кибероперации,

конвенция от 12 августа 1949 года об обращении с военнопленными (вступила в силу 21 октября 1950 г.) (ЖК III); Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны (вступила в силу 21 октября 1950 г.) (ЖК IV).

72 Общая ст. 2(1): «…настоящая Конвенция будет применяться в случае объявленной войны или всякого другого вооруженного конфликта, возникающего между двумя или несколькими Высокими Договаривающимися Сторонами, даже в том случае, если одна из них не признает состояния войны». Общая ст. 3(1): «В случае вооруженного конфликта, не носящего международного характера и возникающего на территории одной из Высоких Договаривающихся Сторон…»

73 International Criminal Tribunal for the former Yugoslavia (ICTY), *The Prosecutor v. Duško Tadić*, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70; Комментарий МККК к ЖК I (примечание 69 выше), п. 218.

74 Аналогичным образом, если применение вооруженной силы приводит, например, к повреждениям или захвату лица из состава вооруженных сил другого государства, нормы МГП о защите раненых и больных или о статусе и обращении с военнопленными актуальны, независимо от того, идет ли речь об одном или о многих пленных, одном или многих раненых, которым полагается уход (см.: Комментарий МККК к ЖК I (примечание 69 выше), пп. 236–244).

75 Tallinn Manual 2.0 (примечание 13 выше), Rule 82, para. 16.

76 См.: Комментарий к ЖК I (примечание 69 выше), пп. 253–256.

которые представляют собой военные действия между двумя или более государствами, могут указывать на существование международного вооруженного конфликта»[77].

Вопрос о том, где точно находится этот уровень, остается нерешенным[78]. По мнению МККК, нет никаких причин рассматривать одну или несколько кибероперациий, приведших к разрушению гражданского или военного имущества или к смерти и ранению солдат или гражданских лиц, иначе, чем равнозначное нападение, осуществленное посредством более традиционных средств и методов войны. Однако кибероперации могут вывести из строя объекты, не нанося им физических повреждений. Предстоит еще увидеть, могут ли и при каких условиях государства считать, что такие операции достигают уровня применения вооруженной силы, как это понимается в МГП, и поэтому регулируются этим сводом права[79].

Что касается немеждународных вооруженных конфликтов, то ситуации насилия внутри страны могут считаться немеждународным вооруженным конфликтом, «когда имеет место продолжительное вооруженное насилие между государственными властями и организованными вооруженными группами или между такими группами в пределах государства»[80]. Два критерия, которые вытекают из этого определения, — организация сторон в конфликте и интенсивность насилия, — поднимают целый ряд вопросов касательно кибероперациий. Во-первых, в то время как государственные вооруженные силы удовлетворяют критерию организации, определить степень организации вооруженной группы сложнее, нужно оценивать конкретный факт; это становится тем более проблематичным — хотя и не является невозможным, — когда такая группа организована только онлайн[81]. Во-вторых, в отличие от МГП, применимого к международным вооруженным конфликтам, которое регулирует любое применение вооруженной силы в отношениях между государствами независимо от ее интенсивности[82], немеждународный вооруженный конфликт будет существовать,

77 French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 2019, p. 12, www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. В этом документе уточняется, что «хотя вооруженный конфликт, заключающийся исключительно в цифровой деятельности, нельзя, в принципе, исключать, он может квалифицироваться в качестве такового, если потенциал автономных кибероперациий позволяет достичь требуемого для этого порога насилия».

78 Tallinn Manual 2.0 (примечание 13 выше), Rule 82, paras 11–16; как видно из пп. 12–13, вопрос не решен и в отношении кинетических операций, и эта же неопределенность характерна для обсуждений того, могут ли кибернетические операции сами по себе достичь порога международного вооруженного конфликта, а не оставаться только проблемами специфически цифровой области.

79 См.: Комментарий МККК к ЖК I (примечание 69 выше), п. 255; Tallinn Manual 2.0 (примечание 13 выше), Rule 82, para.11.

80 ICTY, Tadić (примечание 73 выше), para. 70.

81 Комментарий МККК к ЖК I (примечание 69 выше), п. 437; Tallinn Manual 2.0 (примечание 13 выше), Rule 83, paras 13–15. Подробный анализ вопроса см.: 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.

82 См.: Комментарий к ЖК I (примечание 69 выше), пп. 236–244.

только если уровень интенсивности насилия между двумя или несколькими организованными сторонами достаточно высок. И снова, хотя, вероятно, это не является невозможным в исключительных обстоятельствах, вряд ли только кибероперации будут удовлетворять критерию интенсивности для существования немеждународного вооруженного конфликта[83]. Полагая, что длительные кибероперации могут, в принципе и в зависимости от обстоятельств, являться немеждународным вооруженным конфликтом, Франция считала, что уровень развития технологии, как представляется, пока исключает такую возможность[84].

Справедливо подчеркивалось, что право вооруженных конфликтов «не регулирует кибероперации, которые осуществляются не в ситуации вооруженного конфликта»[85]. Однако есть разные точки зрения относительно того, должны ли всегда применяться некоторые или все принципы этого права к кибероперациям.

Соединенные Штаты недавно заявили, что «даже если право войны формально не применяется, потому что предполагаемые военные кибероперации будут осуществляться не в контексте вооруженного конфликта, [Министерство обороны] тем не менее применяет принципы права войны»[86], как оно вообще поступает в отношении всех своих операций[87]. В отличие от этого Россия предупредила, что «потенциально опасным видится навязывание принципа полной и автоматической применимости МГП к информпространству в мирное время»[88].

Хотя политические дебаты по этому вопросу, скорее всего, будут продолжаться, с правовой точки зрения не вызывает сомнений тот факт, что МГП не применяется вне контекста вооруженного конфликта. Совершенно справедливо, что некоторые нормы МГП, такие как закрепленные в общей

83 Там же, п. 437. Дополнительный анализ см.: Tallinn Manual 2.0 (примечание 13 выше), Rule 83, paras 7–10; *Дрёге, Кордула*. Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц // Международный журнал Красного Креста. Т. 94, № 866, 2012. С. 23–25; Michael N. Schmitt, "Classification of Cyber Conflict", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 260.

84 French Ministry of the Armies (примечание 77 выше), p. 12.

85 New Zealand Defence Force, Manual of Armed Forces Law, Vol. 4: *Law of Armed Conflict*, 2nd ed., DM69, 2017 (New Zealand Military Manual), para. 5.2.23, www.nzdf.mil.nz/assets/Publications/DM-69-2ed-vol4.pdf.

86 Paul C. Ney Jr., US Department of Defence General Counsel, Remarks at US Cyber Command Legal Conference, 2 March 2020, www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

87 См.: US Department of Defense (DoD), Directive 2311.01E, "DoD Law of War Program", 2006 (amended 2011), paras 4–4.1 («Политика МО заключается в том, что… лица из состава всех компонентов МО соблюдают право войны во время всех вооруженных конфликтов, как бы такие конфликты ни квалифицировались, *и в ходе всех других военных операций*» (*курсив наш*)). См. также: US Department of Defense (DoD), *Law of War Manual,* 2015 (DoD Law of War Manual), para. 3.1.1.2, https://tinyurl.com/y6f7chxo.

88 Российская Федерация, «Комментарий Российской Федерации по первоначальному проекту доклада Рабочей группы ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности», апрель 2020, https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-rus.pdf.

статье 3 и предоставляющие защиту лицам, не принимающим или прекратившим принимать участие в военных действиях, а также усиленная защита учреждений здравоохранения или объектов, необходимых для выживания гражданского населения, могли бы иметь положительный эффект, если применять их постоянно. В отличие от этого более проблематичным будет применение других норм МГП не в контексте вооруженного конфликта — речь идет о тех, которые вытекают из принципов проведения различия и соразмерности. Эти нормы основаны на той предпосылке, что нападения на военные объекты являются законными согласно МГП во время вооруженного конфликта. Однако вне рамок вооруженного конфликта понятие «военные объекты», на которые можно осуществлять нападения на законных основаниях, не существует, нападения даже на военнослужащих другого государства запрещены. Хотя принцип соразмерности существует и вне рамок вооруженного конфликта, у него иное значение согласно другим сводам права, и поэтому он действует по-разному во время вооруженного конфликта и вне его контекста[89]. Если речь не идет о вооруженном конфликте, споры между государствами и применение силы регулируются исключительно другими отраслями международного права, такими как Устав ООН и право прав человека.

Взаимодействие между МГП и Уставом ООН

Государство, которое рассматривает осуществление кибероперации против другого государства, должно проанализировать законность такой операции в соответствии с jus ad bellum (как оно отражено в Уставе ООН и обычном международном праве) и jus in bello (МГП). Когда речь идет о защите людей от войны и ее последствий, Устав ООН и МГП дополняют друг друга, хотя они являются отдельными отраслями международного права. У них взаимодополняющие цели: в то время как в преамбуле Устава ООН говорится, что его цель — «избавить грядущие поколения от бедствий войны», в преамбуле ДП I сказано, что цель МГП — обеспечить «защиту жертв вооруженных конфликтов». Говоря более конкретно, Устав ООН запрещает применение силы иначе, как только с целью самообороны или в соответствии с санкцией Совета Безопасности. Применимость МГП не заменяет и не отменяет основные нормы Устава ООН, но если конфликт начинается, МГП определяет нормы защиты тех, кто не принимает (гражданские лица) или прекратил принимать участие в военных действиях (например, раненые солдаты или задержанные лица), и ограничивает воюющих в выборе средств и методов ведения войны. Таким образом, если Устав ООН устанавливает — за редкими исключениями — запрет на применение силы, МГП налагает ограничения на то, как военные действия могут вестись, если конфликт начался.

89 Краткий анализ см. в ICRC Challenges Report 2019 (примечание 36 выше), pp. 18–22.

В то же самое время МГП и Устав ООН являются разными областями международного права со своими собственными концепциями и терминологией. Поскольку обе касаются регулирования применения силы, некоторая терминология, которую они используют, аналогична и иногда это приводит к путанице. Так, например, обстоит дело в отношении понятия «применение вооруженной силы в отношениях между государствами» для классификации конфликта в соответствии с МГП и запрет на «угрозу силой или ее применения» и право на самооборону в случае «вооруженного нападения» согласно Уставу ООН. Хотя договоры по международному праву не определяют эти понятия — ни в целом, ни в отношении кибернетического пространства, — некоторые базовые элементы можно извлечь из судебной практики и комментариев.

Как уже сказано выше, МГП применяется с того момента, когда в отношениях между государствами используется вооруженная сила, независимо от уровня интенсивности насилия.

Устав ООН не определяет термин «применение силы» в статье 2(4), и вопрос о том, какой вид силы может этому соответствовать, остается предметом споров. Исходя из истории составления этого положения и последующей практики государств, можно прийти к выводу, что использование политического или экономического давления не включено в это понятие[90]. Вместо этого утверждалось, что запрет на применение силы согласно Уставу ООН «ограничен вооруженной силой»[91]. В отношении кибероперациий важно отметить, что МС установил, что в статье 2(4) запрет относится к «любому применению силы, независимо от используемого оружия»[92]. На основании этого заключения некоторые государства подчеркивали, что «превышение порога применения силы зависит не от используемых цифровых средств, а от последствий кибероперации», и пришли к выводу, что «кибероперация, осуществленная одним государством против другого государства, нарушает запрет на применение силы, если ее последствия аналогичны последствиям применения обычных видов оружия»[93]. Целый ряд приведенных государствами примеров применения силы в киберпространстве, как представляется, отражает такое понимание, например кибероперации, приводящие к ранению и гибели людей или

90 См.: Oliver Dörr and Albrecht Randelzhofer, "Article 2(4)", in Bruno Simma et al. (eds), *The Charter of the United Nations: A Commentary*, Vol. 1, Oxford University Press, Oxford, 2016, paras 17–20 of the commentary on Art. 2(4). Соответственно, эксперты пришли к выводу, что «не приводящие к разрушениям информационные психологические операции, предназначенные исключительно для подрыва доверия к правительству, или запрет государства на электронную торговлю с другим государством с целью вызвать негативные экономические последствия не квалифицируются как применение силы» (Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 69, para. 3).

91 O. Dörr and A. Randelzhofer (примечание 90 выше), p. 208, para. 16.

92 МС (примечание 46 выше), п. 39.

93 French Ministry of the Armies (примечание 77 выше), p. 7. См. также: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 69. para. 1.

к повреждению и уничтожению имущества[94]; запуск процесса расплавления тепловыделяющего элемента ядерной установки; открытие дамбы в населенном районе, что вызывает разрушения; прекращение функционирования служб управления воздушным движением, что приводит к авиакатастрофам; и выведение из строя военных систем материально-технического снабжения[95]. Как представляется, некоторые государства толкуют запрет на применение силы даже еще шире, утверждая, что нельзя исключить, что «кибероперация без физического эффекта может характеризоваться и как применение силы»[96] и что «кибероперация с очень серьезными финансовыми или экономическими последствиями может квалифицироваться как применение силы»[97].

Переходя к праву на самооборону в соответствии с Уставом ООН и обычным международным правом, напомним, что это право может осуществляться только в случае «вооруженного нападения». Исходя из решения МС, что только «наиболее серьезные случаи применения силы» могут квалифицироваться как вооруженные нападения и что такие операции должны иметь определенные «масштаб и последствия»[98], можно прийти к выводу, что применение силы должно достичь определенного уровня интенсивности, чтобы квалифицироваться в качестве «вооруженного нападения»[99]. Опять же, эксперты утверждали, что «некоторые кибероперации могут быть достаточно серьезными, чтобы квалифицироваться в качестве "вооруженного нападения" по смыслу Устава»[100], а именно те, последствия которых можно сравнить с последствиями более традиционных вооруженных нападений. Эта точка зрения нашла отражение и в публичной позиции некоторых государств[101].

94 См.: Estonia, "President of the Republic at the Opening of CyCon 2019", 29 May 2019, www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html. Australian Department of Foreign Affairs and Trade, "Australia's International Cyber Engagement Strategy", 2019, www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

95 DoD Law of War Manual (примечание 87 выше), para. 16.3.1.

96 French Ministry of the Armies (примечание 77 выше), p. 7. Примеры действий, которые приводит Франция и которые могут «рассматриваться как применение силы», это «проникновение в военные системы с целью поставить под угрозу оборонный потенциал Франции, финансирование или даже подготовка отдельных лиц для выполнения кибернападений на Францию».

97 Dutch Ministry of Foreign Affairs, "Letter to the Parliament on the International Legal Order in Cyberspace", 5 July 2019, p. 4, www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legalorder-in-cyberspace/; French Ministry of the Armies (примечание 77 выше), p. 7. Последний обзор позиций государства см.: Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views,* Policy Brief, Hague Program for Cyber Norms, 2020. Иллюстрацию этих обсуждений см., например: Kenneth Kraszewski, "Scenario 14: Ransomware Campaign", in K. Mačák, T. Minárik and T. Jančárková (eds) (примечание 68 выше), paras L5–L13.

98 ICJ, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, 27 June 1986, paras 191, 195.

99 Однако эта точка зрения признается не всеми государствами. Соединенные Штаты, например, считают, что любое применение силы является вооруженным нападением.

100 Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 71, para. 4.

101 Dutch Ministry of Foreign Affairs (примечание 97 выше), p. 4; French Ministry of the Armies (примечание 77 выше), p. 7.

Эволюционирует понимание того, как толкуются в связи с действиями в киберпространстве уровень интенсивности вооруженной силы, который обусловливает применимость МГП, запрет на использование силы в соответствии с Уставом ООН и понятие «вооруженные нападения», которые влекут за собой наступление неотъемлемого права на самооборону. Хотя кое-какие выводы можно сделать на основании судебной практики МС, прецедентного права международных уголовных трибуналов и судов, практики государств и мнений экспертов, многие вопросы пока что остаются неясными.

Тем не менее важно подчеркнуть, что эти три понятия и концепции берут свое начало из разных сводов международного права и имеют разное значение. Как уже говорилось, по мнению МККК, кибероперации, которые достигают уровня применения вооруженной силы в отношениях между государствами в соответствии с МГП, регулируются этим сводом права, даже если отсутствует вооруженный конфликт. На практике такая операция может также являться запрещенным применением силы согласно Уставу ООН. Однако каждый из данных выводов требует отдельного правового анализа: заключение, что порог был достигнут в соответствии с одним сводом права, не обязательно исключает другой вывод в соответствии с другим сводом права. Это особенно важно при проведении различия между применимостью МГП и правом на самооборону согласно Уставу ООН. Ввиду той позиции, что только самые серьезные формы применения силы, — то есть те, которые имеют определенный масштаб и последствия, — могут квалифицироваться в качестве вооруженных нападений, совершенно очевидно, что не каждый случай использования вооруженной силы, к которому применяется МГП, является вооруженным нападением согласно Уставу ООН, обусловливая возникновение права на самооборону[102]. Эти различия имеют серьезные правовые и практические последствия. Поэтому, анализируя любую ситуацию, в которой государство применяет кибероперации против другого государства, надлежит проводить четкое различие между разными понятиями, их не следует объединять одним неопределенным «порогом».

Вопрос о присвоении поведения

Во время войны вообще — и в киберпространстве в частности — государства иногда будут использовать негосударственных акторов, таких как негосударственные вооруженные группы или частные военные и охранные компании, для выполнения определенных действий, включая кибероперации. Особые характеристики киберпространства, такие как разнообразие возможностей для акторов скрыть или фальсифицировать свою идентичность, осложняют присвоение поведения конкретным лицам и сторонам

102 H. Durham (примечание 25 выше).

в вооруженном конфликте[103]. Это связано с серьезными проблемами при определении применимости МГП в конкретной ситуации. Если актора, осуществившего данную операцию, и, следовательно, связь между операцией и вооруженным конфликтом невозможно установить, очень трудно определить, применяется ли вообще МГП к этой операции[104]. Во-первых, как уже было сказано, различные пороговые уровни интенсивности насилия имеют значение для квалификации государственного или негосударственного кибернападения в качестве вооруженного конфликта. Таким образом, если неизвестно, какое государство или негосударственный актор осуществил кибероперацию не в ситуации вооруженного конфликта, непонятно, какой порог применяется. Во-вторых, даже если вооруженный конфликт имеет место, кибернападения, у которых нет связи с конфликтом (например, преступные деяния, не связанные с конфликтом), не регулируются МГП, и невозможность установить автора кибероперации может затруднить выяснение вопроса, существует ли связь с конфликтом. Эти примеры показывают, что определение авторства кибероперации и того, может ли операция присваиваться государству или негосударственной стороне в конфликте, имеет важные правовые последствия.

Присвоение кибероперации важно также для привлечения к ответственности акторов, которые нарушают международное право, в том числе МГП. Понимание того, что будет легко отрицать ответственность за незаконные нападения, также может ослаблять запрет на такие действия — и может позволить акторам быть менее щепетильными в отношении проведения операций в нарушение международного права[105].

С учетом этого присвоение не является проблемой с точки зрения акторов, которые осуществляют кибероперации, руководят ими или контролируют их: у них в распоряжении есть все данные, чтобы определить, в рамках системы какой отрасли международного права они действуют и какие обязательства они должны выполнять[106].

В соответствии с международным правом государство несет ответственность за поведение, которое может быть присвоено ему, в том числе возможные нарушения МГП. Сюда входят:

a) нарушения, совершенные его органами, в том числе вооруженными силами;
b) нарушения, совершенные лицами или объединениями, которых оно уполномочило осуществлять элементы государственной власти;

103 Исследование технических проблем в деле присвоения кибернападений конкретным акторам см.: Vitaly Kamluk, "Know Your Enemy and Know Yourself: Attribution in the Cyber Domain", *Humanitarian Law and Policy Blog*, 3 June 2019, https://blogs.icrc.org/law-and-policy/2019/06/03/know-your-enemy-know-yourself-cyber-domain-attribution/.
104 ICRC Challenges Report 2011 (примечание 43 выше), p. 36.
105 Изложение позиции МККК (примечание 1 выше), с. 9.
106 Там же.

c) нарушения, совершенные лицами или группами лиц, действующими фактически по указаниям государства или под его руководством или контролем; и
d) нарушения, совершенные частными лицами или группами, которые государство признает в качестве своих собственных действий[107].

Эти принципы применяются независимо от того, было нарушение МГП совершено с применением кибернетических или любых других средств[108].

Ограничения, налагаемые МГП на использование киберпотенциала во время вооруженных конфликтов

Признание того, что МГП применяется к кибероперациям, имеющим связь с вооруженным конфликтом, — это только первый шаг. Конкретные характеристики этой новой технологии ставят несколько проблем для толкования норм МГП, в том числе тех, которые касаются ведения военных действий.

Частично нефизический (то есть цифровой) характер киберпространства и взаимосвязанность военных и гражданских сетей вызывают практические и правовые проблемы при применении общих норм МГП, предоставляющих гражданским лицам и гражданским объектам защиту от кибероперациий, в частности тех, которые приравниваются к нападениям согласно МГП. Выдвигается даже предположение, что иногда, вероятно, не будет возможности применять основные принципы МГП в киберпространстве. Как продемонстрировано далее, эта трудность, возможно, преувеличена. Тем не менее ключевые вопросы возникают в отношении защиты важнейших гражданских объектов кибернетической инфраструктуры от военных нападений. Поскольку многие нормы МГП, регулирующие ведение военных действий, применяются только к военным операциям, которые являются «нападениями» по определению МГП, в настоящем разделе прежде всего рассматриваются различные вопросы, касающиеся кибероперациий, которые квалифицируются в качестве нападений, включая существенный вопрос о том, *какие* операции квалифицируются в качестве нападений в соответствии с МГП. Во-вторых, в нем рассматриваются обязательства сторон в вооруженном конфликте в ходе военных операций,

107 См.: Обычное МГП (примечание 63 выше), норма 149. См. также: Комиссия международного права. Ответственность государств за международно-противоправные деяния, 2001 г., в частности ст. 4–11.

108 Изложение позиции МККК (примечание 1 выше), с. 11; Tallinn Manual 2.0 (примечание 13 выше), Rules 15–17. Иную точку зрения см. в выступлении Китая о первоначальном проекте доклада РГОС, где говорится, что «нет никаких правовых оснований для какой-либо дискуссии о применимости в киберпространстве концепции ответственности государств, в отношении которой, в отличие от права вооруженных конфликтов или прав человека, пока еще не достигнут международный консенсус» (Comments by China on the initial pre-draft of the OEWG report, www.un.org/disarmament/open-ended-working-group/).

которые не являются «нападениями». В-третьих, в разделе анализируются некоторые проблемы, касающиеся правовой экспертизы киберпотенциала.

Кибероперации, которые являются нападениями согласно МГП

МГП излагает основные нормы, ограничивающие кибероперации, которые приравниваются к «нападениям», как они определены в МГП. В настоящем разделе рассматриваются эти нормы и принципы, которые подвергались самым бурным обсуждениям. В нем прежде всего анализируется, могут ли кибернападения с технологической точки зрения быть направлены на конкретные военные объекты, как это требует принцип проведения различия. Во второй части исследуется вопрос о том, как понятие нападения в соответствии с МГП должно толковаться в киберпространстве. В третьей части обсуждается близко связанная с этим тема — должны ли данные гражданского характера пользоваться такой же защитой, что и гражданские «объекты» для целей МГП. В последней части речь идет о продолжающейся дискуссии о том, как нормы МГП по ведению военных действий применяются к объектам, используемым одновременно для гражданских и военных целей (их часто называют объекты двойного назначения), которых особенно много в киберпространстве.

С технической точки зрения кибернападения могут быть направлены на конкретные военные объекты

Соблюдение принципов проведения различия и соразмерности и запрет на неизбирательные нападения требуют, чтобы нападение могло направляться и направлялось на военный объект и не причиняло чрезмерного сопутствующего ущерба гражданским лицам или гражданским объектам. В отличие от предположения, что эти принципы могут стать бессмысленными в киберпространстве из-за характеризующей его взаимосвязанности, внимательное изучение кибероперций показывает, что такие операции не являются по своей природе неизбирательными. Например, если кибероперация осуществляется операторами, которые указывают цель и выполняют операцию, они должны знать, где они находятся и что они делают. Аналогичным образом анализ киберинструментов показывает, что они не обязательно являются неизбирательными. Однако составление вредоносной программы, которая проводит различие между гражданскими объектами и военными объектами, и проведение кибероперации без причинения чрезмерного сопутствующего ущерба требуют современных высокотехнологичных возможностей и испытаний.

Те, кто разрабатывает вредоносные программы или планирует кибернападения, могут создавать свои инструменты без функций самораспространения. В этом случае вредоносная программа не может распространяться без дополнительного вмешательства человека. Даже если программа является самораспространяющейся, нападения, имевшие место за послед-

ние годы, показали, что вредоносные программы могут создаваться для нападений только на конкретные аппаратные средства или программное обеспечение. Это означает, что даже если вредоносная программа создана для широкого распространения, она может быть разработана так, чтобы причинять ущерб только конкретной цели или конкретному набору целей. Для кибернападений, цель которых заключается в причинении ущерба промышленным системам управления, могут потребоваться киберинструменты, которые создаются для этой конкретной цели и задачи. Во многих случаях потребность в таких несерийных и специально для этой цели созданных инструментах будет эффективно препятствовать — с технической точки зрения — возможности осуществить масштабное или неизбирательное кибернападение. Тот факт, что кибернападения могут технически быть точно направленными, не означает, что они обязательно будут законными, если осуществляются во время конфликта. Однако их особенности, как это можно наблюдать в ходе целого ряда кибероперациий, показывают, что они могут быть выполнены очень точно, чтобы воздействовать только на конкретные цели, — значит, такие операции могут осуществляться в соответствии с принципами и нормами МГП.

Некоторые из известных киберинструментов были разработаны для самораспространения и вызвали пагубные последствия в широко используемых гражданских компьютерных системах, но этот факт не говорит в пользу того аргумента, что взаимосвязанность киберпространства делает очень проблематичным, если не невозможным соблюдение основных норм МГП. Напротив, во время вооруженных конфликтов применение таких киберинструментов было бы запрещено МГП[109]. МГП запрещает нападения, в ходе которых применяются средства и методы ведения войны, включая кибернетические средства и методы, если их нельзя направить против конкретных военных объектов, или которые, как можно предположить, выйдут из-под контроля тех, кто их применяет[110], или, будучи направлены на военный объект, как можно ожидать, причинят гражданским объектам сопутствующий ущерб — чрезмерный по отношению к конкретному и непосредственному военному преимуществу, которое предполагается получить[111].

109 Аналогичным образом в Руководстве по праву войны Министерства обороны США (DoD Law of War Manual (примечание 87 выше), para. 16.6) делается вывод: «Например, разрушительный компьютерный вирус, который был запрограммирован распространяться и бесконтрольно вызывать нарушения в гражданских интернет-системах, будет запрещен как оружие неизбирательного по своей природе действия».

110 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), para. 1963.

111 Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов, 8 июня 1977 г. (вступил в силу 7 декабря 1978 г.) (ДП I), ст. 51(4)–(5); Обычное МГП (примечание 63 выше), нормы 11, 14.

Понятие «нападение» в соответствии с МГП и его применение к кибероперациям

Вопрос о том, доходит ли операция до уровня «нападения», как это определено в МГП, очень важен для применения многих норм, вытекающих из принципов проведения различия, соразмерности и принятия мер предосторожности, которые предоставляют важную защиту гражданским лицам и гражданским объектам. Конкретнее, такие нормы, как запрет на *нападения* на гражданских лиц и гражданские объекты[112], запрет на неизбирательные[113] и несоразмерные *нападения*[114] и обязательства принять все возможные меры предосторожности, чтобы избежать или по крайней мере уменьшить случайный вред гражданским лицам и ущерб гражданским объектам при осуществлении *нападения*[115], применяются к тем операциям, которые квалифицируются как «нападения» по определению МГП. Поэтому вопрос о том, как широко или узко понятие «нападение» толкуется в случае кибероперациий, крайне важен для применимости к кибероперациям ключевых норм и защиты, которую они предоставляют гражданским лицам и гражданской инфраструктуре.

Статья 49 ДП I определяет нападения как «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне». Давно установлено, что понятие насилия в этом определении может относиться как к средствам военных действий, так и к последствиям их применения, — это означает, что операция, вызывающая крайне негативные последствия, может быть нападением, даже если средства, использованные для этого, как таковые не предназначены для совершения насилия[116]. На основании такого понимания Таллинское руководство 2.0 предлагает следующее определение кибернападения: «Кибернападением является кибероперация как наступательного, так и оборонительного характера, которая, как можно ожидать на разумных основаниях, станет причиной ранения или смерти лиц или ущерба объектам или их уничтожения»[117].

Широко признано государствами, которые заняли позицию по этому вопросу, МККК и экспертами, что по крайней мере те кибероперации, которые приведут к гибели, ранению или физическому повреждению, будут считаться нападением в соответствии с МГП[118]. Некоторые государ-

112 См.: ДП I, ст. 52; Обычное МГП (примечание 63 выше), нормы 7–10.
113 См.: ДП I, ст. 51 (4)(c); Обычное МГП (примечание 63 выше), норма 11.
114 См.: ДП I, ст. 51(5)(b); Обычное МГП (примечание 63 выше), норма 14.
115 См.: ДП I, ст. 57(1); Обычное МГП (примечание 63 выше), норма 15.
116 См.: *Дрёге* (примечание 83 выше), с. 31; William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 384. Как отмечает Дрёге, «не вызывает разногласий тот факт, что применение биологических, химических или радиоактивных веществ является нападением, даже несмотря на то, что нападение не связано с физической силой».
117 Tallinn Manual 2.0 (примечание 13 выше), Rule 92.
118 См.: МККК, доклад «Международное гуманитарное право и вызовы современных вооруженных конфликтов». Женева, 2015 г. (Доклад МККК 2015 г.), с. 71–75, https://www.icrc.org/ru/download/file/40074/mezhdunarodnoe_gumanitarnoe_pravo_i_vyzovy_sovremennyh_konfliktov.pdf;

ства явным образом включают сюда вред из-за косвенных (или отдаленных) последствий нападений[119], такую точку зрения разделяет и МККК[120]. Такие последствия могут иметь место, если, например, пациенты в палатах интенсивной терапии умирают в результате кибероперации, направленной на сеть электроснабжения, что приводит к отключению электричества в больнице.

За пределами этого базового консенсуса существуют различные мнения относительно того, доходит ли кибероперация, которая выводит из строя объект, не причиняя ему физических повреждений, до уровня нападения согласно МГП[121]. Проходили продолжительные дискуссии по этому вопросу в процессе составления Таллинского руководства. Большинство экспертов придерживались мнения, что кибероперация является нападением, если, как ожидается, она нарушит работу системы или оборудования и если восстановление их функционирования потребует замены физических компонентов. Некоторые эксперты считали также, что кибероперация будет являться нападением, если восстановление функциональности потребует переустановки операционной системы или конкретных данных.

МККК занял такую позицию: операция, предназначенная для выведения из строя компьютера или компьютерной сети во время вооруженного конфликта, является нападением по определению МГП, независимо от того, выведен ли объект из строя в результате уничтожения или каким-либо иным способом[122].

Две главные причины обусловливают позицию МККК. Первая вытекает из толкования понятия «нападение» в его контексте[123]. С учетом того, что определение военных объектов в статье 52(2) ДП I относится не только к уничтожению или захвату, но также к «нейтрализации», которая может быть результатом нападения, то понятие «нападение» согласно статье 49 ДП I должно пониматься как включающее операции, предназна-

Tallinn Manual 2.0 (примечание 13 выше), Rule 92. О государствах, которые выразили свою точку зрения относительно того, как понятие нападения в соответствии с МГП применяется к кибероперациям, см., в частности: Australian Department of Foreign Affairs and Trade (примечание 94 выше), Annex A; Danish Ministry of Defence, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations, 2016* (Danish Military Manual), pp. 290–291, https://forsvaret.dk/en/publications/military-manual/; French Ministry of the Armies (примечание 77 выше), p. 13; Norway, *Manual i krigens folkerett,* 2013 (Norwegian Military Manual Руководство для вооруженных сил Норвегии), para. 9.54, https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/194213/manual_krigens_folkerett.pdf?sequence=1&isAllowed=y; New Zealand Military Manual (примечание 85 выше), para 8.10.17; DoD Law of War Manual (примечание 87 выше), para. 16.5.1.

119 Danish Military Manual (примечание 118 выше), p. 677 (в Руководстве говорится о нападениях на компьютерные сети); New Zealand Military Manual (примечание 85 выше), para 8.10.22; Norwegian Military Manual (примечание 118 выше), para. 9.54.

120 Изложение позиции МККК (примечание 1 выше), с. 7.

121 См., например: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 92, paras 10–12.

122 См.: Доклад МККК 2015 г. (примечание 118 выше), с. 71–75. См. также: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 92, para. 12.

123 См.: Венская конвенция о праве международных договоров, ст. 31(1).

ченные нарушить функционирование объекта (то есть нейтрализовать его), не нанося физического ущерба и не уничтожая его. Действительно, утверждалось, что явное упоминание нейтрализации в статье 52(2) было бы иначе излишним[124]. Во-вторых, излишне ограничительное понимание понятия «нападение» было бы трудно сочетать с объектом и целью норм, касающихся ведения военных действий, которые должны обеспечить защиту гражданского населения и гражданских объектов от последствий военных действий. Действительно, согласно излишне ограничительному пониманию, кибероперация, которая направлена на то, чтобы нарушить функционирование гражданской сети (электроснабжения, банковской или коммуникационной), или связана с риском вызвать такие последствия случайно, может и не попадать в сферу действия основных норм МГП, предоставляющих защиту гражданскому населению и гражданским объектам[125].

Аналогичным образом комментаторы из числа экспертов высказывали мнение, что важно «толковать положение [статьи 49 ДП I], принимая во внимание происходящее в последнее время технологическое развитие, и расширить понятие "насилие" таким образом, чтобы оно включало не только материальный ущерб объектам, но и выведение из строя объектов инфраструктуры, не разрушая их»[126].

Поскольку кибероперации могут серьезно нарушить функционирование жизненно важных служб, не обязательно причиняя физические повреждения, это является важнейшим аргументом в пользу предоставления защиты гражданским лицам от последствий кибероперацій. Поэтому государства обязательно должны выразить свое мнение по этому вопросу и постараться прийти к взаимопониманию. В настоящее время у государств, которые публично высказали свою позицию, существуют разные мнения.

Определения понятия «нападение» в военных руководствах Норвегии и Новой Зеландии отражают определение, принятое в Таллинском руководстве 2.0. Однако неясно, должны ли были эти руководства выражать какую-то позицию по этому вопросу, потому что комментарий к норме 92 Таллинского руководства 2.0 отмечает разные мнения относительно того, как «ущерб» должен пониматься в киберконтексте. Австралия заявила, что кибероперации квалифицируются в качестве нападений, если они доходят

124 Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", 2004, p. 4, www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf; *Дрёге* (примечание 83 выше), с. 30–32. Другую точку зрения см.: Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", *International Law Studies*, Vol. 87, 2011, pp. 95–96; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 198.

125 См. также: M. N. Schmitt (примечание 67 выше), p. 339.

126 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 181. См. также: Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare — A Critical First Assessment of the New Tallinn Manual", *Journal of Conflict and Security Law*, Vol. 18, No. 2, 2013, p. 341: «Было бы действительно совсем неубедительно настаивать на том, что значение термина "нападение" должно быть ограничено актами, непосредственно причиняющими ущерб или приводящими к физическому уничтожению, когда то же самое действие может, например, привести к срыву поставок важнейших припасов в больницы или к повреждению других важных объектов гражданской инфраструктуры».

«до такого же порога, что и кинетическое “нападение согласно МГП”»[127], но неясно, было ли это утверждение сделано в качестве выражения позиции в ходе дебатов.

Некоторые государства для квалификации кибероперации в качестве нападения сосредоточивают внимание на физическом ущербе. Согласно одному исследованию, проведенному ОАГ, Перу высказало мнение, что для квалификации операции в качестве нападения люди или объекты должны получить «физические повреждения»[128]. Военное руководство Дании уточняет в отношении термина «нападение»: «…что касается ущерба объектам, термин охватывает любой физический ущерб. Однако этот термин не означает временного неработоспособного состояния и иной нейтрализации, которая не влечет за собой физического ущерба (например, цифровой “заморозки” системы управления связью)»[129]. В выступлении на заседании Группы правительственных экспертов в 2014 г. Соединенные Штаты отмечали:

> При определении того, является ли нападением деятельность в киберпространстве по смыслу jus in bello, государства должны рассмотреть, inter alia, вопрос о том, приводит ли такая деятельность к кинетическим и необратимым последствиям для гражданских лиц, гражданских объектов или гражданской инфраструктуры или к некинетическим и обратимым последствиям для них[130].

Руководство Министерства обороны США по праву войны на основании таких же соображений приводит пример «кибернападения, которое может уничтожить компьютерную систему противника», и отмечает, что «к факторам, которые свидетельствуют о том, что кибероперация не является нападением, относится причинение ею лишь обратимых или только временных последствий»[131]. К сожалению, эти документы не проясняют, что имеется в виду под словами «обратимые» и «временные» последствия или в чем заключается разница — если она вообще есть — между этими двумя понятиями[132]. В них не анализируется, может ли последствие не считаться более временным — а если так, то по окончании какого периода, — или как рассматривать повторяющиеся операции, каждая из которых будет иметь временный, но преднамеренно накапливающийся эффект. В них также

127 Australian Department of Foreign Affairs and Trade (примечание 94 выше), Annex A.
128 OAS (примечание 22 выше), para. 43.
129 Danish Military Manual (примечание 118 выше), p. 290. В отношении нападений на компьютерную сеть Руководство уточняет: «…это значит, например, что сетевые операции должны рассматриваться как нападения в соответствии с МГП, если последствием будет причинение физического ущерба» (Ibid., p. 291).
130 United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2014–15, p. 5.
131 См. также: DoD Law of War Manual (примечание 87 выше), paras 16.5.1, 16.5.2.
132 Gary Brown and Kurt Sanger, “Cyberspace and the Law of War”, *Cyber Defense Review*, 6 November 2015, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136032/cyberspace-and-the-law-of-war/.

ничего не говорится о том, относится ли термин «обратимый» только к операциям, когда их автор может обратить вспять эффект нападения[133], или также к операциям, в результате которых придется предпринять шаги для восстановления функционирования пораженной системы или иным образом устранить последствия нападения. В этом отношении следует помнить, что возможность устранить физический ущерб, причиненный военной операцией (как кибернетической, так и кинетической), обычно не считается критерием для того, чтобы не квалифицировать операцию в качестве нападения в соответствии с МГП[134]. Это так, даже если непосредственное последствие операции устранимо и функционирование объекта восстанавливается [135].

Франция выразила более четкое и широкое понимание понятия «кибернападение». Она считает, что,

> кибероперация является нападением, если оборудование или системы, являющиеся объектом нападения, более не предоставляют услуги, ради которых они были созданы, независимо от того, временное это явление или постоянное, обратимо это или нет. Если последствия носят временный и (или) обратимый характер, нападение характеризуется как таковое, если необходимы действия другой стороны для восстановления инфраструктуры или системы (ремонт оборудования, замена его части, переустановка сети и т. п.)[136].

Комментируя эту позицию, Шмитт отметил, что «эта точка зрения очень оправданна с правовой точки зрения, поскольку простое значение термина "ущерб" вполне разумно распространяется на системы, которые не действуют должным образом и требуют какого-то ремонта для восстановления функциональности»[137]. Аналогичным образом согласно упомянутому выше исследованию ОАГ Чили предлагает, чтобы для квалификации операции в качестве нападения ее результат должен требовать от пострадавшего государства «предпринять действия для ремонта или восстановления пораженной инфраструктуры или компьютерной системы, поскольку в таких случаях последствия нападения аналогичны тем, которые опи-

133 Например, самораспространяющиеся нападения типа «отказ в обслуживании», в которых сеть или система, которые являются целью, будут автоматически возвращаться к нормальной работе, когда нападающий завершит нападение и если никаких косвенных последствий не возникнет за тот период времени, пока сеть или система была поражена.

134 Laurent Gisel, "The Use of Cyber Technology in Warfare: Which Protection Does IHL afford and Is It Sufficient?", in G. Venturini and G. L. Beruto (eds) (примечание 7 выше).

135 Например, Майкл Льюис говорит о практике нападений на мосты в продольном направлении во время войны в Персидском заливе 1991 г. и среди прочего отмечает, что «повреждения моста тогда будут ближе к середине пролета, и поэтому будет легче его отремонтировать», не утверждая, что это помешает квалифицировать операцию как нападение (см.: Michael Lewis, "The Law of Aerial Bombardment in the 1991 Gulf War", *American Journal of International Law*, Vol. 97, No. 3, 2003, p. 501).

136 French Ministry of the Armies (примечание 77 выше), p. 13.

137 M. N. Schmitt (примечание 52 выше). См. также: W. H. Boothby (примечание 116 выше), p. 386.

саны выше, в частности причинение физического ущерба имуществу»[138]. Кроме того, в исследовании указывалось, что и Гватемала выразила свою позицию, полагая, что кибероперация, которая «приводит только к утрате функциональности», должна считаться нападением; эту позицию разделяет и Эквадор[139]. Боливия, Эквадор и Гайана уточнили также, что такие кибероперации могут являться нападением согласно МГП, если они, в частности, выводят из строя критическую инфраструктуру или срывают предоставление основных услуг населению[140].

В любом случае не все кибероперации во время вооруженных конфликтов будут являться «нападениями», как этот термин понимается в МГП. Во-первых, понятие «нападение» в МГП не включает разведывательную деятельность. Во-вторых, нормы, касающиеся ведения военных действий, не запрещают все операции, которые мешают функционированию гражданских коммуникационных систем: глушение радио или телепередач традиционно не считалось нападением по определению МГП. Однако проведение различия между нападениями и помехами для коммуникации, которые не достигают уровня нападения, является, возможно, менее понятным в случае кибероперации, чем в случае традиционных кинетических или электромагнитных операций[141]. В-третьих, понятие «военные операции» согласно МГП, в том числе операции, осуществляемые кибернетическими средствами, шире, чем понятие «нападения», как будет показано далее.

Защита данных как «гражданского объекта»

Кроме основополагающего вопроса о том, какие кибероперации являются нападениями согласно МГП, предметом серьезного обсуждения был и остается нерешенным вопрос о том, пользуются ли такой же защитой, что и гражданские объекты, гражданские данные. Защита гражданских данных от вредоносных кибероперации во время вооруженных конфликтов становится все более важной, поскольку данные — это важнейший компонент цифровой сферы и краеугольный камень жизни во многих обществах: личные медицинские данные, данные органов социального обеспечения, налоговые сведения, банковские счета, файлы клиентов компаний и списки избирателей крайне важны для функционирования большинства систем гражданской жизни. Поскольку, как ожидается, эта тенденция будет разви-

138 OAS (примечание 22 выше), para. 43.

139 Эквадор уточнил, что «кибероперация может квалифицироваться в качестве нападения, если она выводит из строя критически важные объекты инфраструктуры государства или если она угрожает безопасности государства» (ibid., para. 44).

140 Предложение Боливии заключалось в том, что кибероперация «может считаться нападением, если ее целью является выведение из строя основных служб государства (водоснабжения, электроснабжения или финансовой системы)»; Гайана предложила, чтобы «кибероперации, которые нарушают работу компьютерных сетей и инфраструктуры, необходимой для предоставления услуг и ресурсов гражданскому населению, считались нападением», среди таких объектов она назвала «ядерные установки, больницы, банки и системы управления воздушным движением» (ibid., paras 44–45).

141 Доклад МККК 2015 г. (примечание 118 выше), с. 72–75; *Дрёге* (примечание 83 выше), с. 35–36.

ваться, если не ускоряться, в ближайшие годы, все больше внимания уделяется безопасности таких важных гражданских данных.

Что касается данных, принадлежащих определенным категориям объектов, которые пользуются конкретной защитой согласно МГП, то нормы, предоставляющие им защиту, подробно разработаны. Как сказано далее, обязательства уважать и защищать медицинские учреждения и операции по предоставлению гуманитарной помощи должны распространяться на медицинские данные, принадлежащие этим учреждениям, и данные гуманитарных организаций, которые важны для их операций[142]. Аналогичным образом запрещено уничтожение данных или манипулирование данными, что может сделать непригодными к использованию объекты, необходимые для выживания гражданского населения, например сооружения для снабжения питьевой водой и ирригационные системы[143].

И все-таки важно прояснить, до какой степени существующие общие нормы по ведению военных действий обеспечивают защиту гражданских данных. В частности, спор возник в отношении того, являются ли данные объектом, как это понимается в МГП, и тогда кибероперации против этих данных (например, их уничтожение) будут регулироваться принципами проведения различия, соразмерности и принятия мер предосторожности, и данные будут пользоваться защитой, предоставляемой гражданским объектам[144].

Этот вопрос тесно связан с обсуждением понятия «нападение» (см. выше). Сначала можно сказать, что если данные уничтожены или подверглись манипуляциям, с тем чтобы непосредственно или косвенным образом причинить смерть или ранения лицу или ущерб физическому объекту (в том числе, как мы считаем, выведением его из строя), операция является нападением, независимо от того, представляют ли данные сами по себе объекты для целей МГП. Тогда последствия операции, направленной против данных, позволяют квалифицировать эту операцию как нападение согласно МГП, и поэтому она будет подлежать регулированию соответствующими нормами МГП. В отношении таких нападений не имеет значения тот факт, квалифицируются ли данные в качестве объекта в соответствии с МГП.

Однако вопрос о том, являются ли данные объектами для цели МГП, критически важен для операций, которые не предназначены для того, чтобы вызвать такие последствия, и не ожидается, что они станут их причиной.

142 См. анализ далее в разделе «Нормы МГП, предоставляющие защиту объектам, необходимым для выживания гражданского населения, медицинским службам и операциям по оказанию гуманитарной помощи».

143 ДП I, ст. 54; Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв вооруженных конфликтов немеждународного характера, 8 июня 1977 г. (вступил в силу 7 декабря 1978 г.) (ДП II), ст. 14; Обычное МГП (примечание 63 выше), норма 54.

144 См.: Tallinn Manual 2.0 (примечание 13 выше), paras 6–7 of the commentary on Rule 100. О научной дискуссии см.: *Israel Law Review,* Vol. 48, No. 1, pp. 39–132; M. N. Schmitt (примечание 67 выше).

В более широком плане можно рассмотреть два общих подхода. В соответствии с первым подходом, когда считается, что данные являются объектами согласно МГП, операция, предназначенная уничтожить данные или подвергнуть их манипулированию, или которая, как ожидается, может вызвать такой эффект, будет нападением, регулируемым всеми соответствующими нормами МГП, потому что это будет уничтожением или повреждением объекта (данных). Так же будет обстоять дело, если не ожидалось, что такое уничтожение данных или манипулирование ими приведет к смерти или ранению лица, к повреждению или выведению из строя физического объекта. Однако даже в соответствии с этой точкой зрения операция, предназначенная исключительно для получения доступа к (возможно, конфиденциальным) данным без уничтожения их или манипуляции ими — с целью шпионажа, — не будет нападением.

И напротив, если данные не считаются объектами согласно МГП, операция, предназначенная для уничтожения данных или манипулирования ими, не приводя к смерти или ранению лица или к повреждению объекта, не будет регулироваться нормами, касающимися нападений или некоторыми более общими нормами, предоставляющими защиту гражданским объектам (такими как обязанность постоянно щадить гражданских лиц и гражданские объекты, как сказано далее в разделе «Нормы, регулирующие военные операции, не являющиеся нападениями»). Однако операции могут регулироваться другими конкретными защитными режимами в соответствии с МГП, которые проанализированы далее в разделе «Нормы МГП, предоставляющие защиту объектам, необходимым для выживания гражданского населения, медицинским службам и операциям по оказанию гуманитарной помощи». Однако в защите важнейших гражданских данных, на которые не распространяется действие конкретного защитного режима, окажется пробел, и это вызывает обеспокоенность.

Эксперты придерживаются разных точек зрения на то, квалифицируются ли данные в качестве объектов для целей норм МГП, касающихся ведения военных действий[145]. Точка зрения, которой придерживаются большинство экспертов, участвовавших в составлении Таллинского руководства, такова: термин «объект» в своем обычном значении, как об этом говорится в Комментарии МККК 1987 г. к ДП I, не может толковаться как включающий в себя данные, потому что объекты материальны, видимы и осязаемы[146]. Однако соответствующее разъяснение в Комментарии МККК касается проведения различия между объектами и такими понятиями, как «цель» и «задача», а не проведения различия между осязаемыми и неосязаемыми предметами, и поэтому не может рассматриваться как определяю-

145 Подробнее об этих дебатах см.: "Scenario 12: Cyber Operations against Computer Data", in K. Mačák, T. Minárik and T. Jančárková (eds) (примечание 68 выше).

146 Напоминая обычное значение слова «объект», Комментарий МККК 1987 г. к Дополнительным протоколам описывает объект как «нечто видимое и осязаемое» (ICRC Commentary on the APs (примечание 110 выше), para. 2008). См. также: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 100, para. 6.

щее для дебатов по вопросу данных[147]. В отличие от этого другие эксперты заявляли, что либо все, либо некоторые виды данных должны считаться объектами согласно МГП. Есть мнение, что «современное значение» понятия «объекты» в сегодняшнем обществе и толкование термина в свете его цели и задачи должны привести к выводу, что «данные являются "объектом" по смыслу норм МГП, касающихся определения целей»[148]. Такое толкование подтверждается традиционным пониманием термина «объект» согласно МГП, которое шире, чем обычное значение слова, и охватывает также местоположение и животных. Другое предложение заключается в том, чтобы проводить различие между «данными, содержащими информацию о функционировании системы», или «кодами», и «данными содержательного уровня»[149]. В этой модели, как утверждалось, особенно данные, содержащие информацию о функционировании системы, могут квалифицироваться в качестве военного объекта — это подразумевает, что такой тип данных может также квалифицироваться и как гражданский объект[150]. Хотя рассмотрение таких данных в качестве объектов соответствовало бы вышеупомянутой точке зрения о том, что выведение объектов из строя является нападением, это, как представляется, не дает дополнительной защиты. В этих дебатах утверждалось, что ни одно из предлагаемых заключений не является полностью удовлетворительным, каждое из них либо недостаточно, либо излишне инклюзивно[151].

МККК, со своей стороны, говорил о необходимости сохранить важные гражданские данные, подчеркивая, что в киберпространстве уничтожение данных или их искажение может быстро привести к тому, что правительственные службы и частные предприятия полностью остановятся и тем самым гражданским лицам будет причинено больше вреда, чем разрушение физических объектов. Таким образом, по мнению МККК, вывод о том, что этот тип операций не будет запрещен МГП в сегодняшнем все более киберзависимом мире, как представляется, трудно согласуется

147 См. также: International Law Association (ILA) Study Group on the Conduct of Hostilities in the 21st Century, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", *International Law Studies*, Vol. 93, 2017 (ILA Report), pp. 338–339.

148 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, p. 80; Robert McLaughlin, "Data as a Military Objective", *Australian Institute of International Affairs*, 20 September 2018, www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

149 В соответствии с предлагаемым различением данные содержательного уровня будут включать такие данные, «как текст настоящей статьи или содержание медицинских баз данных, библиотечных каталогов и т. п.», в то время как коды будут описывать «главным образом "душу машины"», что означает «тип данных, который дает аппаратному средству его функциональность и способность решать задачи, выполнение которых нам требуется» (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).

150 Ibid., p. 54.

151 Поэтому Шмитт утверждает, что с точки зрения политики государства должны «предоставлять особую защиту некоторым "важнейшим гражданским функциям или службам", обязуясь воздерживаться от проведения кибероперaций против гражданской инфраструктуры или данных, которые оказывают на них негативное воздействие» (M. N. Schmitt (примечание 67 выше), p. 342).

с предметом и целью этого свода норм[152]. Совершенно логично, что замена бумажных досье и документов цифровыми данными не должна уменьшить защиту, которую им предоставляет МГП[153]. Как подчеркнул МККК, «исключение важных данных гражданского характера из сферы защиты, предоставляемой МГП гражданским объектам, привело бы к серьезному пробелу в защите»[154].

К настоящему времени небольшое число государств выразили свою точку зрения относительно того, должно ли понятие «объект» включать данные для целей применения норм, регулирующих ведение военных действий. В Руководстве для вооруженных сил Дании, например, сказано, что «(цифровые) данные в целом не являются объектом»[155]. И напротив, Руководство для вооруженных сил Норвегии утверждает, что данные должны считаться объектом и прямые нападения на них могут осуществляться, только если они квалифицируются в качестве законной цели[156]. Франция выразила мнение, которое можно рассматривать как промежуточную позицию, заявив, что «с учетом современного состояния цифровой зависимости содержательные данные (такие как гражданские, банковские или медицинские данные и т. д.) находятся под защитой согласно принципу проведения различия»[157]. Комментарий к позиции Перу в докладе ОАГ «Повышение уровня транспарентности», как представляется, отражает аналогичное мнение: Перу не занимает явным образом какую-либо позицию по вопросу о том, являются ли данные объектом, его точка зрения объясняется как оценка операций против данных согласно понятию «военный объект», это предполагает, что некоторые системы данных не должны подвергаться нападениям, поскольку такие нападения «не приведут к легитимному военному преимуществу»[158]. Поскольку определение военных объектов в статье 52(2) ДП I применяется, если речь «касается объектов», такая аргументация, как кажется, означает, что данные являются объектами. Чили предлагает рассмотреть последствия нападения на данные, делая вывод, что «в контексте кибероперациий должен поэтому быть принят во внимание принцип проведения различия, в силу которого государство должно воздерживаться от нападений на данные, если это может затронуть гражданское население». Как сообщалось, представитель Чили затем подчеркнул, что «нападе-

152 Доклад МККК 2015 г. (примечание 118 выше), с. 75–76.
153 ICRC Challenges Report 2019 (примечание 36 выше), p. 21.
154 См.: Изложение позиции МККК (примечание 1 выше), с. 10–11. См. также: P. Pascucci (примечание 67 выше). Автор отмечает, что позиция, занятая большинством экспертов в Таллинском руководстве в отношении данных, создает, «видимо, широкий пробел в понимании того, что является объектом», и затем добавляет, что «нереалистично в информационный век думать, будто данные окажутся за пределами области, которая представляет собой объект, ведь тогда не будет возможности пользоваться защитой МГП, связанной с принципами проведения различия и соразмерности».
155 Danish Military Manual (примечание 118 выше), p. 292.
156 Norwegian Military Manual (примечание 118 выше), para. 9.58.
157 French Ministry of the Armies (примечание 77 выше), p. 14.
158 OAS (примечание 22 выше), para. 49, fn. 115.

ние, направленное исключительно на компьютерные данные, вполне может вызвать негативные последствия, затронув гражданское население»[159].

В мире, который все более полагается на данные, вопрос о том, каким образом государства толкуют и применяют нормы МГП, чтобы защитить важнейшие данные от уничтожения, удаления или искажения, послужит лакмусовой бумажкой для определения адекватности существующих норм гуманитарного права.

Защита киберинфраструктуры, служащей одновременно военным и гражданским целям

Чтобы защитить критически важную гражданскую инфраструктуру, которая зависит от киберпространства, также важно обеспечить защиту инфраструктуре самого киберпространства. Проблема, однако, заключается во взаимосвязанности гражданских и военных сетей. Большинство военных сетей зависят от гражданской киберинфраструктуры, например подводные оптоволоконные кабели, спутники, маршрутизаторы и узловые модули. Управление движением гражданского наземного, морского и воздушного транспорта все чаще использует навигационное оборудование, которое зависит от спутников глобальной навигационной спутниковой системы (GNSS), таких как BeiDou, ГЛОНАСС, GPS и Galileo, которые могут использоваться и военными. Гражданские системы материально-технического снабжения (продукты и медицинские материалы) и другие предприятия используют тот же самый Интернет и коммуникационные сети, по которым проходят и некоторые военные линии связи. За исключением отдельных сетей, которые конкретно предназначены для использования военными, практически невозможно провести различие между чисто гражданскими и чисто военными объектами киберинфраструктуры.

В соответствии с МГП нападения должны быть строго ограничены военными объектами. Что касается объектов, то к военным объектам относятся только те, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и чье полное или частичное уничтожение, захват или нейтрализация при существующих в конкретный момент обстоятельствах дает явное военное преимущество. Все объекты, которые не являются военными объектами согласно этому определению, являются гражданскими объектами в соответствии с МГП и не могут становиться объектами нападения или репрессалий. В случае сомнения относительно того, не используется ли объект, который обычно используется с гражданскими целями, для внесения эффективного вклада в военные действия, следует предполагать, что этот объект остается под защитой в качестве гражданского объекта[160].

159 OAS (примечание 22 выше), para. 48.
160 См.: ДП I, ст. 52; Обычное МГП (примечание 63 выше), нормы 7–10.

Традиционно считается, что объект может стать военным объектом, если он таким образом используется для военных целей, что начинает соответствовать определению военного объекта, даже если он одновременно используется с гражданскими целями. Широкое толкование этой нормы может привести к заключению, что многие объекты, составляющие часть инфраструктуры киберпространства, окажутся военными объектами и поэтому не будут пользоваться защитой от нападений как кибернетических, так и кинетических. Это станет предметом серьезной обеспокоенности из-за все более широкого использования киберпространства в гражданских целях.

Однако такой вывод будет неполным. Во-первых, выяснить, когда гражданский объект становится военным объектом, вообще невозможно, если речь идет о киберпространстве или Интернете. Вместо этого воюющие стороны должны определить, какие компьютеры, узловые модули, маршрутизаторы или сети могли стать военным объектом. В этом отношении части сети, конкретные компьютеры или иное аппаратное обеспечение, которое отделено от сети или системы в целом, нужно проанализировать по отдельности. Используемые средства и методы должны давать возможность направлять нападение на конкретные военные объекты, которые были идентифицированы, и все возможные меры предосторожности следует принять, чтобы избежать или по крайней мере минимизировать опасность случайно воздействовать на оставшиеся гражданские объекты или части сети[161]. Утверждалось также, что запрещено рассматривать в качестве единой цели целый ряд явно отдельных кибернетических военных объектов в киберинфраструктуре, используемой в первую очередь для гражданских целей, если это причинит вред лицам или ущерб объектам, пользующимся защитой[162]. Во-вторых, киберпространство создано с высоким уровнем избыточности — это означает, что одной из его характеристик является возможность немедленно перенаправлять трафик данных. Эту встроенную устойчивость к внешнему воздействию следует принимать во внимание при оценке того, даст ли уничтожение или нейтрализация цели явное военное преимущество, как этого требует определение военного объекта. Если это не так, объект остается гражданским, и на него нельзя осуществлять нападение. И в-третьих, при совершении любого нападения должен соблюдаться запрет на неизбирательные нападения, а также нормы, касающиеся соразмерности и принятия мер предосторожности при нападении. Нападение, прекращающее гражданское использование объекта или создающее помехи такому использованию в нарушение одной из этих норм, будет незаконным, несмотря на тот факт, что объект стал военным объектом[163].

161 См.: ДП I, ст. 51(4), 57(2)(a)(ii); Обычное МГП (примечание 63 выше), нормы 12–17.

162 Tallinn Manual 2.0 (примечание 13 выше), Rule 112. Эта норма вытекает из запрета на бомбардировки по площади в ст. 51(5)(a) ДП I и обычном МГП (см.: Обычное МГП (примечание 63 выше), норма 13).

163 Признавая, что существует и другое мнение, Группа АМП по изучению вопроса ведения военных действий нашла это «более правильным мнением» на основании практики государств, официальных документов и доктрины (см.: ILA Report (примечание 147 выше), pp. 336–337). См. также: ICRC, *International Expert Meeting Report: The Principle of Proportionality in the Rules*

По сравнению с кинетическими военными операциями кибероперации могут, в зависимости от обстоятельств, воздействовать, причиняя меньший ущерб (цели или меньший сопутствующий ущерб другим объектам или системам) или такой ущерб, который может быть легче возмещен или при котором может быть восстановлена ранее существовавшая ситуация. Это соображение особенно актуально в отношении объектов двойного использования, как демонстрирует сценарий, когда воюющая сторона пытается нейтрализовать командный пункт противника, расположенный в подземном бункере, отключив линию электроснабжения, которая одновременно поставляет энергию в гражданскую инфраструктуру. Кибероперация может позволить оператору удаленно определить, какие части сети отключить[164]. Это могло бы дать возможность нападающей стороне достичь желаемого результата, избежав или по крайней мере минимизировав негативные последствия для энергоснабжения гражданских лиц. В таком случае и при том условии, что решение использовать кибероперацию вместо кинетической является практически возможным, осуществление кибероперации требовал бы принцип принятия мер предосторожности. Действительно, обязательство принять все возможные меры предосторожности при выборе средств и методов ведения военных действий с целью избежать случайного ущерба гражданским лицам и гражданским объектам или по крайней мере минимизировать его[165] является технологически нейтральным: это касается также средств и методов, в которых применяются новейшие технологии, и может даже потребовать их применения[166]. Является ли это практически возможным в конкретный момент, зависит от обстоятельств, сложившихся в данное время, включая соображения гуманитарного и военного характера[167].

Governing the Conduct of Hostilities under International Humanitarian Law, Geneva, 2018, p. 39, www.icrc.org/en/document/international-expert-meeting-reportprinciple-proportionality; Helen Durham, Keynote Address, in Edoardo Greppi (ed.), *Conduct of Hostilities: The Practice, the Law and the Future*, 37th Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2015, p. 31.

164 Как сообщалось, именно это было сделано в 2015 г. во время кибероперации против электроэнергетической системы на Украине (см.: Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, 3 March 2016, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid).

165 ДП I, ст. 57(2)(a)(ii); Обычное МГП (примечание 63 выше), норма 17.

166 См.: ILA Report (примечание 147 выше), p. 384.

167 В число военных соображений может входить «нестабильный характер» кибернетических средств и методов, но это не единственный фактор, определяющий практическую возможность. Нельзя исключить практическую возможность и, следовательно, необходимость использовать кибероперации, чтобы избежать сопутствующего ущерба гражданским лицам и объектам или минимизировать его, на том лишь основании, что используемые кибернетические средства и методы являются «нестабильными», не принимая во внимание всю ситуацию в целом, в том числе и все соответствующие соображения гуманитарного характера.

Ограничения на кибероперации, которые не достигают уровня нападений, включая предоставление особой защиты некоторым лицам и объектам

В то время как многие общие нормы, касающиеся ведения военных действий, ограничиваются действиями, достигающими уровня нападения, как это определено в МГП, некоторые нормы МГП, регулирующие ведение военных действий, применяются к более широкому перечню операций: во-первых, отдельные нормы применяются ко всем «военным операциям» и, во-вторых, особая защита, предоставляемая определенным категориям лиц и объектов, идет дальше защиты от нападений.

Нормы, регулирующие военные операции, не являющиеся нападениями

Выявление и по возможности разъяснение норм, которые предоставляют общую защиту гражданскому населению и гражданским объектам от воздействия кибероперации, не достигающих уровня нападения, является вопросом, требующим повышенного внимания. Это тем более важно, если принимается та точка зрения, что только операции, которые причиняют физический ущерб, считаются нападениями: в таком случае к довольно широкой категории кибероперации применялось бы лишь ограниченное число норм МГП. Такой вывод вызвал бы сильную обеспокоенность в отношении защиты гражданских лиц и гражданской инфраструктуры.

Понятие «военная операция» появляется в целом ряде статей Женевских конвенций 1949 г. и в Дополнительных протоколах к ним 1977 г.[168] Наибольший интерес здесь представляют нормы, регулирующие ведение военных операций, в том числе тех, которые осуществляются киберсредствами. К ним относятся базовая норма, гласящая, что «стороны, находящиеся в конфликте, должны всегда… направлять свои действия только против военных объектов» (ДП I, статья 48), принцип, гласящий, что «гражданское население и отдельные гражданские лица пользуются общей защитой от опасностей, возникающих в связи с военными операциями» (ДП I, статья 51(1))[169], и обязательство, в силу которого «при проведении военных операций постоянно проявляется забота о том, чтобы щадить гражданское население, гражданских лиц и гражданские объекты» (ДП I, статья 57(1))[170].

Обычное значение термина «военная операция» и систематическое толкование этих статей приводят к выводу, что это понятие отличается от понятия «нападение», как оно определено в статье 49 ДП I[171]. Хотя

168 См.: ЖК III, ст. 23; ЖК IV, ст. 28; ДП I, ст. 3, 39, 44, 51, 56–60; ДП II, ст. 13.

169 См. также: ДП I, ст. 58; ДП II, ст. 13(1).

170 См. также: Обычное МГП (примечание 63 выше), норма 15; Tallinn Manual 2.0 (примечание 13 выше), Rule 114.

171 Толкование, при котором приравниваются понятия «операция» и «нападение», лишило бы нормы, применяющиеся к операциям, значимого содержания и сделало бы их, по сути, излишними. См.: *Дрёге* (примечание 83 выше), с. 31.

в Комментарии МККК к статье 48 ДП I отмечается, что понятие относится к военным операциям, во время которых применяется насилие, а не к идеологическим, политическим или религиозным кампаниям, там разъясняется, что это более широкое понятие, чем «нападение». Комментарий определяет «военные операции» для целей этих статей как «все передвижения, маневры и любая другая деятельность, осуществляемая вооруженными силами и связанная с военными действиями» — понимание, которое широко принято[172].

В основном это понятие обсуждается в связи с договорным и обычным обязательством постоянно проявлять заботу о том, чтобы щадить гражданское население, гражданских лиц и гражданские объекты при ведении военных операций. Франция однозначно заявила, что это обязательство применяется в киберпространстве[173]. Это обязательство требует, чтобы все участвующие в военных операциях постоянно помнили о последствиях военных операций для гражданского населения, гражданских лиц и гражданских объектов, предпринимали шаги для того, чтобы как можно менее тяжелыми были такие последствия, и стремились избегать любых не являющихся необходимыми последствий[174]. Оно описывалось как позитивное и постоянное обязательство, направленное на снижение риска и предотвращение ущерба, а также налагающее обязанности, которые становятся все более строгими по мере повышения уровня опасности для гражданских лиц[175]. В этом отношении Таллинское руководство разъясняет, что

172 ICRC Commentary on the APs (примечание 110 выше), paras 2191, 1936, 1875. В том же ключе см.: Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Leiden, 2013, para. 2.2.3 on Art. 48, para. 2.8.2 on Art. 57; UK Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004 (UK Military Manual), para 5.32, fn. 187; ILA Report (примечание 147 выше), p. 380. Руководство по международному праву, применимому к воздушной и ракетной войне (The *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Program on Humanitarian Policy and Conflict Research, Harvard University, 2009)) применяет обязательство постоянно проявлять заботу в случае «воздушных или ракетных боевых операций» (Rule 34), и это понятие шире, чем «нападение», поскольку включает среди прочего дозаправку, создание помех для функционирования радаров противника, использование бортовых систем оповещения и высадку авиадесантных войск (комментарий к норме 1(c), п. 3). См. также: Noam Neuman, "A Precautionary Tale: The Theory and Practice of Precautions in Attack", *Israel Yearbook on Human Rights*, Vol. 48, 2018, p. 28; Jean-François Quéguiner, "Precautions under the Law Governing the Conduct of Hostilities", *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 797; Chris Jenks and Rain Liivoja, "Machine Autonomy and the Constant Care Obligation", *Humanitarian Law and Policy*, 11 December 2018, https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/. Конкретно в отношении кибероперацій см.: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 114, para. 2 (в комментарии отмечается, что понятие военных действий, к которым применимо обязательство постоянно проявлять заботу, шире, нежели понятие нападений); H. Harrison Dinniss (примечание 124 выше), p. 199. Иную точку зрения, по крайней мере в отношении принципа проведения различия, см.: M. Roscini (примечание 126 выше), p. 178.

173 French Ministry of the Armies (примечание 77 выше), p. 15.

174 UK Military Manual (примечание 172 выше), para. 5.32.1; Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 114, para. 4; Dieter Fleck, *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 199; N. Neuman (примечание 172 выше), pp. 28–29.

175 ILA Report (примечание 147 выше), p. 381.

> право не допускает какой-либо ситуации или какого-то времени, когда лица, участвующие в планировании и осуществлении процесса, могут игнорировать последствия своих операций для гражданских лиц или гражданских объектов. В контексте кибероперации это требует постоянной оценки ситуации, а не только во время подготовительного этапа операции[176].

Более проблематичен вопрос о применении принципа проведения различия в отношении тех военных операций, которые не являются нападениями. Как уже отмечалось, статья 48 ДП I требует, чтобы военные операции направлялись только против военных объектов. Хотя в комментариях МККК и Боте, Партша и Зольфа[177] подчеркивается основополагающий характер этой статьи, авторы не проливают свет на точное значение и сферу действия данного обязательства, которое остается предметом обсуждений.

Статья 48 понимается иногда как общий принцип, который соблюдается посредством применения различных норм раздела Протокола, который она открывает. Некоторые комментаторы поэтому утверждают, что конкретные нормы, проистекающие из принципа проведения различия, применяются только к нападениям, а не к военным операциям, которые не являются нападениями[178]. Следовательно, отдельные военные наставления явным образом утверждают, что кибероперации, не являющиеся нападениями, могут направляться против гражданских лиц или гражданских объектов[179]. Это утверждение, как представляется, трудно привести в соответствие со статьей 48 для государств — участников Протокола или по крайней мере его надо тщательно сформулировать. Действительно, эксперты указывали, что «хотя… существует разница между военными операциями и нападениями, из этого не следует, что ненасильственные нападения на компьютерную сеть могут направляться против гражданских объектов»[180]. Такой вывод можно сделать из правил толкования договоров, которые требуют, чтобы положения толковались подобным образом, чтобы они имели «значимое содержание и не [были] излишними»[181].

Как уже отмечалось, «военные операции» понимаются как любое передвижение, маневры или любая другая деятельность, осуществляемая вооруженными силами с целью ведения боя или связанная с военными действиями. Маневрирование также является неотъемлемой частью киберо-

176 Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 114, para. 4.
177 M. Bothe, K. J. Partsch and W. A. Solf (примечание 172 выше).
178 M. Roscin (примечание 126 выше), p. 178. См. также, хотя это выражено посредством обычного права: Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 93, para. 5; Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict: Proceedings*, NATO CCD COE Publications, Tallinn, 2012, pp. 283–293, 289–290.
179 Norwegian Military Manual (примечание 118 выше), para. 9.57. См. также: DoD Law of War Manual (примечание 87 выше), para. 16.5.2.
180 H. Harrison Dinniss (примечание 124 выше), p. 199.
181 См. также: *Дрёге* (примечание 83 выше), с. 29.

пераций[182]. Например, установление удаленного доступа к одной системе или устройству может быть шагом к получению доступа или нападению на другую систему или устройство[183]. Предположив, что первая система или устройство имеет гражданский характер, а другая является военным объектом, можно столкнуться с вопросом, не будет ли установление доступа к гражданской системе или гражданскому устройству запрещенной военной операцией? По мнению авторов, при условии, что гражданская система или устройство не повреждено и не вышло из строя в процессе, такой сценарий не представляется противоречащим статье 48, потому что операция в конечном счете направлена на военный объект[184]. Такие военные операции могут на самом деле оцениваться так же, как и традиционные военные операции, — например, когда диверсионно-десантный отряд проходит через дом гражданского лица для осуществления нападения на военный объект, который находится за ним. И все же другие обязательства остаются актуальными, например обязательство постоянно проявлять заботу о том, чтобы щадить гражданские объекты.

По мнению авторов настоящей работы, статья 48, как сама по себе, так и в сочетании со статьями 51(1) и 57(1) ДП I, должна толковаться как запрет на кибероперации, предназначенные исключительно для прекращения интернет-услуг для гражданского населения, даже если такие кибероперации не выводят объекты из строя или иным образом не вызывают последствий, которые квалифицируют их как нападения. Гражданское использование Интернета является сегодня столь всепроникающим, что любое другое толкование оставило бы серьезный пробел в защите, которую МГП предоставляет гражданским лицам от последствий военных действий, осуществляемых киберсредствами[185].

Как уже говорилось выше, некоторые придерживаются мнения, что не все кибероперации, которые выводят из строя объекты или уничтожают

182 См., например: US DoD, *Cyberspace Operations*, Joint Publication 3–12, 8 June 2018, p. xii («Передвижение и маневр. Операции в киберпространстве дают возможность для проецирования силы без необходимости физического присутствия на иностранной территории. Маневры в DODIN (информационной сети Министерства обороны) или ином голубом [дружественном] киберпространстве включают размещение сил, сенсорной системы и оборонительных сооружений, чтобы наилучшим способом захватить территории киберпространства или осуществлять оборонительные действия по мере необходимости. Маневрирование в сером [нейтральном] и красном [противника] киберпространстве является деятельностью по развитию успеха в киберпространстве и включает такие действия, как получение доступа к каналам передачи данных и узловым модулям противника или посредника и формирование этого киберпространства для оказания поддержки дальнейшим действиям»).

183 L. Gisel and L. Olejnik (eds) (примечание 11 выше), p. 57.

184 Ср.: H. Harrison Dinniss (примечание 124 выше), p. 201.

185 Эксперты, которые составляли Таллинское руководство, обсуждали вопрос о том, является ли прерывание связи по электронной почте на всей территории страны во время вооруженного конфликта нападением (более узкое понятие, чем военные операции). Хотя меньшинство придерживалось мнения, что международное сообщество в целом сочло бы такую операцию нападением, точка зрения большинства заключалась в том, что МГП в настоящее время не распространяется так далеко, но тем не менее они считали, что была логика в рассмотрении этих операций в качестве нападений (Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 92, para. 13).

данные, или искажают их, являются нападениями. Вследствие такого толкования значительно более широкий диапазон кибероперацій не будет регулироваться нормами, касающимися нападений, включая операции, которые создают серьезную опасность причинения вреда. Поэтому тем более важно для защиты гражданского населения, чтобы те, кто узко толкует понятия «нападение» и «объекты», прояснили, считают ли они, что кибероперации, которые просто выводят из строя объекты или уничтожают данные, являются «военными операциями» и что это означает для применения принципа проведения различия в таких операциях, — в частности, с точки зрения требования статьи 48 ДП I относительно того, что стороны в вооруженном конфликте должны «направлять свои действия только против военных объектов». Например, по крайней мере некоторый уровень защиты будет сохранен, если те, кто толкует понятие «нападение» узко, согласны с тем, что кибероперация, которая просто выводит объекты из строя, является «военной операцией» и, следовательно, должна быть направлена только против военных объектов.

Даже кибероперации, которые не входят в понятие «военная операция», как это понимается в ДП I, могут регулироваться некоторыми нормами МГП, вытекающими из принципа проведения различия. Например, отмечалось, что применение психологических операций или других форм пропаганды в отношении гражданских лиц не будет нарушением статьи 48 ДП I, поскольку эти операции не охватываются значением термина «военные операции», как он понимается в статье 48[186]. Тем не менее психологические операции не находятся за пределами защитного действия других норм МГП. Например, они не должны достигать уровня запрещенных актов насилия или угроз насилием, основной целью которых является терроризировать гражданское население или поощрять нарушения МГП[187].

Ограничения на иные кибероперации, нежели нападения, также могут проистекать из принципа военной необходимости. Полагаясь на обычную норму, которую можно обнаружить еще в Гаагском положении 1907 г., Руководство по праву войны МО США устанавливает, что «кибероперация, которая не является нападением, но тем не менее захватывает или уничтожает имущество противника, должна настоятельно требоваться военной необходимостью»[188]. Руководство ссылается также на военную необходимость в более общем плане, уточняя, что кибероперации, которые не являются нападением, «не должны направляться против гражданских лиц или гражданских объектов противника, если только эти операции не осуществляются в силу военной необходимости»[189]. Аналогичным образом Австралия отмечает, что «применимые нормы МГП, включая принцип военной необходимости, применяются во время вооруженного конфликта и к кибероперациям, которые не являются или не достигают уровня напа-

186 *Дрёге* (примечание 83 выше), с. 29.
187 ICRC Challenges Report 2019 (примечание 36 выше), pp. 28–29.
188 DoD Law of War Manual (примечание 87 выше), para. 16.5.1.
189 Ibid., para. 16.5.2.

дения»[190]. Хотя эти ссылки на военную необходимость в качестве сдерживающего принципа приветствуются, требуется больше ясности относительно того, что точно предписывает принцип военной необходимости при проведении кибероперациий.

Этот краткий анализ свидетельствует о том, что кибероперации, не являющиеся нападениями, не остаются нерегулируемыми. Однако правовой режим, регулирующий военные операции, менее полный, точный и строгий, нежели правовой режим, регулирующий операции, которые в соответствии с МГП доходят до уровня нападения. Решая, хотя бы до какой-то степени, вопрос, касающийся этого пробела в защите, Шмитт выдвинул предложение, чтобы государства в качестве принципа своей политики применяли адаптированную оценку соразмерности к кибероперациям, которые не являются нападениями[191].

Особая защита, которую МГП предоставляет определенным лицам и объектам, как мы увидим далее, ограничивает сферу допустимых военных операций.

Нормы МГП, предоставляющие защиту объектам, необходимым для выживания гражданского населения, медицинским службам и операциям по оказанию гуманитарной помощи

Кроме общих норм, касающихся ведения военных действий, МГП устанавливает особые режимы для определенных объектов и служб, которые предоставляют дополнительную и более сильную защиту, чем защита, предоставляемая всем гражданским лицам и гражданским объектам.

Например, МГП конкретно устанавливает, что незаконно «подвергать нападению или уничтожать, вывозить или приводить в негодность объекты, необходимые для выживания гражданского населения»[192]. Защитой, предоставляемой этой нормой, пользуются, например, «продукты питания», «производящие продовольствие сельскохозяйственные районы», «сооружения для снабжения питьевой водой и запасы последней, а также ирригационные сооружения»[193]. Хотя эксперты, которые составляли Таллинское руководство, полагали, что Интернет как таковой не может считаться объектом, необходимым для выживания гражданского населения, они отмечали, что «киберинфраструктура, необходимая для функционирования электрогенераторов, ирригационных сооружений и установок, установок для снабжения питьевой водой, а также предприятий, осуществляющих продовольствен-

190 Australian Department of Foreign Affairs and Trade (примечание 94 выше), p. 4.

191 M. N. Schmitt (примечание 67 выше), p. 347: «Государства должны принять на себя обязательство в рамках своей политики воздерживаться от осуществления кибероперациий, к которым нормы МГП, регулирующие нападения, не применяются, если ожидаемые негативные последствия для гражданских лиц или гражданского населения являются чрезмерными по отношению к конкретному связанному с конфликтом преимуществу, которое ожидается получить в результате операции».

192 См.: ДП I, ст. 54(2); ДП II, ст. 14; Обычное МГП (примечание 63 выше), норма 54.

193 ДП I, ст. 54(2).

ное снабжение, может, в зависимости от обстоятельств, квалифицироваться в качестве таковой»[194]. Четкое использование выражения «приводить в негодность» должно пониматься как подразумевающее более широкий спектр операций, которые могут воздействовать на эти объекты, а не только нападения или уничтожение. Как отмечалось в Комментарии МККК к статье 54(2) ДП I, намерение составителей заключалось в том, чтобы «охватить все возможные способы», какими объекты, обеспечивающие средства существования гражданского населения, могут быть приведены в негодность[195]. Сегодня кибероперации, которые должны или могут вывести из строя объекты, необходимые для гражданского населения, запрещены, независимо от того, являются ли они нападением. Дебаты относительно того, представляют ли собой операции против этих объектов нападения (как говорилось выше), являются поэтому чисто теоретическими.

МГП предоставляет также особую защиту медицинским службам. Учитывая огромное значение здравоохранения для любого человека, пострадавшего от вооруженного конфликта, воюющие должны уважать и предоставлять защиту медицинским учреждениям и персоналу во всякое время[196]. Обязательство «уважать» медицинские учреждения и персонал понимается не только как предоставление им защиты от операций, которые достигают уровня нападения, — запрещено «причинять им вред любым способом. Это также означает, что не должно чиниться никаких препятствий их работе (например, не пропуская поставки материалов) и нельзя лишать их возможности продолжать лечение раненых и больных, которые находятся на их попечении»[197]. Особая защита медицинских учреждений

194 Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 141, para. 5.

195 ICRC Commentary on the APs (примечание 110 выше), paras 2101, 2103.

196 См., например: ЖК I, ст. 19; ЖК II, ст. 12; ЖК IV, ст. 18; ДП I, ст. 12; ДП II, ст. 11; Обычное МГП (примечание 63 выше), нормы 25, 28, 29; Tallinn Manual 2.0 (примечание 13 выше), Rules 131–132. Защита медицинских учреждений и персонала прекращается, только если они совершают не входящие в их гуманитарные обязанности действия или используются для совершения таких действий, которые причиняют вред противнику. Защита, однако, может быть утрачена только после должного предупреждения, в котором в соответствующих случаях указывается период времени для исправления ситуации и если такое предупреждение оставлено без внимания (см.: ЖК I, ст. 21; ЖК II, ст. 34; ЖК IV, ст. 19; ДП I, ст. 13; ДП II, ст. 11(2); Обычное МГП (примечание 63 выше), нормы 25, 28, 29; Tallinn Manual 2.0 (примечание 13 выше), Rule 134).

197 ICRC Commentary on the APs (примечание 110 выше), para. 517. См. также: Комментарий МККК к ЖК I (примечание 69 выше), п. 1799; Oxford Statement (примечание 32 выше), point 5 («Во время вооруженных конфликтов международное гуманитарное право требует, чтобы медицинские формирования, транспортные средства и персонал уважались и защищались во всякое время. Следовательно, стороны в вооруженных конфликтах не могут мешать функционированию учреждений здравоохранения посредством кибероперациий, они должны принимать все возможные меры предосторожности, чтобы избежать случайного вреда, причиняемого кибероперациями, и должны принять все возможные меры, способствующие функционированию учреждений здравоохранения, и не допускать причинения им ущерба, в том числе кибероперациями»); Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 131, para. 5. («Например, эта норма [норма 131, которая устанавливает, что "медицинский и духовный персонал, медицинские формирования и медицинские транспортные средства должны уважаться и защищаться, а также, в частности, не могут становиться объектами кибернападения"] запрещает изменение данных в GPS медицинского вертолета, чтобы перенаправить его, даже если операция не будет квалифицироваться как нападение на медицинский транспорт»).

распространяется на медицинские линии связи: хотя глушение линий коммуникации противника обычно считается допустимым, «преднамеренное лишение [медицинских] формирований возможности осуществлять связь с медицинскими целями» может оказаться недопустимым, даже если медицинские формирования осуществляют связь с вооруженными силами[198]. Более того, обязанность уважать и предоставлять защиту медицинским учреждениям включает запрет на удаление и изменение медицинских данных или другое негативное воздействие на них[199]. Он может также предоставлять защиту от кибероперaций, направленных на конфиденциальность медицинских данных. Такие операции, по крайней мере в некоторых обстоятельствах, было бы трудно сочетать с обязательством защищать и уважать медицинские учреждения[200]. Данные, о которых идет речь, включают «данные, необходимые для правильного использования медицинского оборудования или для отслеживания медицинских поставок», а также «личные медицинские данные, требующиеся для лечения пациентов»[201]. Обязательство «защищать» медицинские учреждения, включая их данные, влечет за собой позитивные обязанности. Стороны в конфликте должны по мере возможности энергично принимать меры для защиты медицинских учреждений от ущерба, в том числе от ущерба в результате кибероперaций[202].

МГП предписывает также, что персонал, оказывающий гуманитарную помощь, а также грузы помощи следует уважать и защищать[203]. Это обязательство определенно запрещает любые «нападения» на гуманитарные операции. Таким же образом, что и в случае обязательства уважать и защищать медицинский персонал и медицинские учреждения, соответствующие нормы необходимо понимать как запрещающие «другие виды опасного поведения, не являющегося частью военных действий», в отношении персонала, осуществляющего гуманитарную деятельность, или неправомерное вмешательство в его работу[204]. Более того, стороны в вооруженных конфлик-

198 ICRC Commentary on the APs (примечание 110 выше), para. 1804.

199 См.: Доклад МККК 2015 г. (примечание 118 выше), с. 75–76.

200 См.: L. Gisel and L. Olejnik (eds) (примечание 11 выше), p. 36. В работе обсуждаются гипотетические действия хакеров с целью получения незаконного доступа к медицинским или административным записям медицинского учреждения, для того чтобы узнать о медицинских назначениях командиру противника, выяснить его местонахождение и захватить его в плен или убить по пути в медицинское учреждение или из него. Это может действительно ненадлежащим образом помешать функционированию медицинского учреждения и препятствовать профессионалам-медикам в выполнении их этических обязанностей по сохранению медицинской конфиденциальности. Таллинское руководство (The Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 132, para. 2) предлагает следующий пример операции, которая не нарушила бы МГП: «…не наносящая разрушений кибернетическая разведка для определения того, не используется ли медицинское учреждение или транспортное средство (или их компьютеры, компьютерные сети или данные) для наносящих ущерб действий военного характера».

201 Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 132, para. 3.

202 Комментарий МККК к ЖК I (примечание 69 выше), пп. 1805–1808; Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 131, para. 6.

203 См.: ДП I, ст. 70(4), 71(2); Обычное МГП (примечание 63 выше), нормы 31, 32.

204 Комментарий МККК к ЖК I (примечание 69 выше), пп. 1358, 1799.

тах должны разрешать осуществление операций гуманитарной помощи и всячески им содействовать[205]. Следовательно, норма 145 Таллинского руководства 2.0 устанавливает, что «кибероперации не должны предназначаться или осуществляться для неправомерного вмешательства в беспристрастные действия по предоставлению гуманитарной помощи», и уточняет, что такие операции запрещены, «даже если они не достигают уровня "нападения"»[206]. Обязательство уважать и защищать персонал гуманитарных организаций и операции по оказанию гуманитарной помощи следует понимать как защищающее соответствующие данные[207]. По крайней мере для государств — участников ДП I защита гуманитарных данных должна распространяться на данные МККК, которые нужны организации, чтобы «выполнять гуманитарные функции, возложенные на нее [Женевскими] конвенциями и настоящим Протоколом с целью обеспечения защиты и помощи жертвам конфликтов»[208].

Эти особые защитные нормы показывают, что в МГП есть более строгие нормы для военных операций, направленных против определенных объектов и служб, которые крайне важны для выживания, здоровья и благополучия гражданского населения.

Важность правовой экспертизы кибернетических средств и методов ведения войны для обеспечения соблюдения МГП

В свете особых вызовов, которые обусловлены особенностями киберпространства и касаются толкования и применения некоторых принципов МГП во время военных действий, стороны в вооруженных конфликтах, которые разрабатывают, приобретают или принимают на вооружение оружие, средства или методы ведения войны, в которых используется кибертехнология, должны быть очень осмотрительны. В этом отношении государства — участники ДП I, которые разрабатывают или приобретают военный кибер-потенциал — как для наступательных, так и оборонительных целей, — обязаны определить, не будет ли применение кибернетического оружия, средств и методов ведения войны запрещено международным правом при некоторых или при всех обстоятельствах[209]. В более общем плане правовая экспертиза критически важна для всех государств для обеспечения соблюдения МГП их вооруженными силами[210], чтобы последние использо-

205 См., например: ЖК IV, ст. 59; ДП I, ст. 69–70; Обычное МГП (примечание 63 выше), норма 55.
206 Tallinn Manual 2.0 (примечание 13 выше), commentary on Rule 80, para. 4.
207 Дальнейший анализ см.: Tilman Rodenhäuser, "Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations against Cyber Operations", *EJIL: Talk!*, 16 March 2020, www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyberoperations/.
208 ДП I, ст. 81 (1). К таким данным относятся, например, те, которые нужны при учреждении агентств по розыску для сбора информации о лицах, пропавших без вести в контексте вооруженного конфликта, или данные, собранные МККК при посещении лиц, содержащихся под стражей, и беседах с ними без свидетелей.
209 ДП I, ст. 36.
210 См. общую ст. 1; Обычное МГП (примечание 63 выше), норма 139.

вали только виды оружия, средства и методы ведения войны, в том числе с применением кибертехнологии, которые соответствуют обязательствам государства согласно МГП[211]. Такой анализ должен осуществляться междисциплинарной группой, включающей юристов, военных и технических экспертов[212]. Эта правовая экспертиза должна проводиться раньше и быть более подробной и тщательной, чем оценка законности фактического применения инструмента в конкретных условиях нападения.

Ввиду новизны технологии очень важно, чтобы правовая экспертиза кибернетического оружия, средств и методов ведения войны проводилась с особенным вниманием. Запрет видов оружия, которые по своей природе являются неизбирательными, может быть особенно актуальным с учетом способности некоторых киберинструментов к автономному самораспространению[213]. Однако при правовой экспертизе кибернетического оружия, средств и методов ведения войны можно столкнуться с целым рядом проблем. Далее мы проиллюстрируем некоторые из них, перечень которых не будет исчерпывающим.

Во-первых, государство, осуществляющее правовую экспертизу, должно определить, в соответствии с какими правовыми стандартами оно оценивает киберинструмент. Другими словами, государство должно иметь ответы на некоторые вопросы, о которых говорилось выше, например, будет ли применение инструмента квалифицироваться в качестве нападения и, следовательно, должно ли оно соответствовать широкому спектру норм МГП. Потому что в областях, где право сформулировано неясно или где вопрос не урегулирован, осторожный подход может быть оправданным, чтобы избежать такой ситуации, когда впоследствии окажется, что применение киберинструмента было незаконным или должно бы было оцениваться как незаконное.

Во-вторых, государство обязано определить, что именно должно подвергнуться экспертизе. Это может и не быть очевидным в отношении киберинструментов или киберпотенциала, как было продемонстрировано широким использованием этих терминов вместо такого понятия, как кибероружие. Комментаторы обсуждали вопрос о том, являются ли киберинструменты и киберпотенциал оружием, средствами и методами ведения войны, и если являются, то какие из них, и что это означает для правовой экспертизы[214]. В любом случае, как уже отмечалось выше, государства — участники ДП I должны провести оценку всех киберинструментов и киберпотенциала, которые квалифицируются в качестве оружия, средств или

211 МККК. Руководство по проверке соответствия нормам права новых видов оружия, средств и методов ведения войны. Меры по имплементации статьи 36 Дополнительного протокола I 1977 г. (Руководство МККК), 2006, с. 1.

212 Там же, с. 22.

213 См.: Обычное МГП (примечание 63 выше), норма 71. Обсуждение некоторых вопросов, возникающих в связи с правовой оценкой кибероружия, см.: "Scenario 10: Cyber Weapons Review", in K. Mačák, T. Minárik and T. Jančárková (eds) (примечание 68 выше).

214 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, p. 219.

методов ведения войны. Для государств, которые не являются сторонами ДП I, обязательство соблюдать и обеспечивать соблюдение МГП их вооруженными силами и новизна использования кибертехнологий в качестве оружия, средств и методов ведения войны обусловили бы целесообразность учитывать как можно больше факторов и возможностей при проведении экспертизы[215].

В-третьих, оружие или средство ведения войны не должно оцениваться отдельно от того, каким образом оно будет применяться, то есть в ходе правовой экспертизы должно рассматриваться обычное или ожидаемое применение оружия или средства ведения войны. Военные возможности кибернетического потенциала могут, однако, быть менее стандартизированными, чем кинетические виды оружия, особенно если специально разработаны для конкретной операции. Это означает, что экспертиза должна проводиться с учетом конкретной кибернетической среды, в которой оружие будет вероятнее всего применяться.

В-четвертых, государство должно провести правовую экспертизу оружия, средства и метода ведения войны не только тогда, когда собирается их приобрести или принять на вооружение впервые, но также и тогда, когда оно модифицирует оружие, средство или метод, которые уже подвергались правовой экспертизе. Это может быть трудным в отношении киберинструментов, которые, скорее всего, часто подвергаются адаптации, в том числе для того, чтобы реагировать на повышение уровня безопасности программного обеспечения, которое осуществляется в отношении потенциальной цели. Хотя вопрос о типе и объеме изменений, которые бы потребовали новой правовой экспертизы, возможно, нуждается в дальнейшем прояснении, новую правовую экспертизу необходимо проводить, особенно когда оружие, средство или метод ведения войны модифицированы таким образом, что это изменяет их функции, или когда модификация может иным образом повлиять на соответствие применения оружия, средства или метода нормам права[216]. Касательно кибероружия отмечалось, что «оценка того, повлияет ли изменение на функционирование программы, должна быть, скорее, качественной, а не количественной по своему характеру»[217]. Чтобы правовая экспертиза была эффективной, государства, которые изучают, разрабатывают, приобретают или принимают на вооружение новые виды оружия, средства и методы, в которых применяются новые технологии, должны рассмотреть эти и другие сложности. Другими словами, тестовые режимы должны соответствовать уникальным характеристикам кибертехнологии. В свете вышеупомянутых сложностей хоро-

215 Например, в рамках политики МО США осуществлялась правовая экспертиза оружия, включая то, в котором используется киберпотенциал (DoD Law of War Manual (примечание 87 выше), para 16.6), а соответствующая Инструкция ВВС санкционирует экспертизу оружия и оценку киберпотенциала: US Department of the Air Force, *Legal Reviews of Weapons and Cyber Capabilities*, Air Force Instruction 51-402, 27 July 2011.

216 Руководство МККК (примечание 211 выше), с. 9.

217 Gary D. Brown and Andrew O. Metcalf, "Easier Said than Done: Legal Reviews of Cyber Weapons", *Journal of National Security Law and Policy*, Vol. 7, 2014, p. 133.

шим способом обеспечить соблюдение МГП всеми государствами был бы обмен информацией о механизмах правовой экспертизы, осуществляемой государствами, и, насколько это практически возможно, о существенных результатах правовых экспертиз[218]. Это было бы особенно важно в случае возникновения проблем относительно соответствия оружия международному гуманитарному праву — во избежание подобных проблем у других государств и для информирования их о выводах, сделанных в результате экспертизы о запрете таких инструментов согласно МГП. Обмен информацией о проведенных правовых экспертизах оружия, средств и методов, использующих новые технологии, может также способствовать накоплению знаний и опыта и выявлению передовой практики — это поможет государствам, которые захотят создать или усовершенствовать свои собственные механизмы экспертизы[219].

Заключение

Для защиты гражданского населения и гражданской инфраструктуры во время вооруженных конфликтов крайне важно признать, что кибероперации, осуществляемые во время вооруженных конфликтов, проводятся не в правовом вакууме — их регулирует международное право, главным образом МГП. Однако, как свидетельствует настоящая статья, признание применимости МГП не означает завершение переговоров. Необходимо дальнейшее обсуждение — особенно государствами — того, каким образом надлежит толковать МГП в киберпространстве. Участники любой такой дискуссии должны хорошо понимать процессы развития военного кибер-потенциала, возможные гуманитарные последствия его использования и защиту, предоставляемую существующим правом. Цель настоящей статьи заключается в том, чтобы послужить основой для подобной дискуссии. Пока применение кибероперациий во время вооруженных конфликтов изучается, выясняются его потенциальные гуманитарные последствия и разрабатываются правовые позиции государств по этому вопросу, анализ, проведенный в настоящей статье, позволяет сделать целый ряд выводов.

Во-первых, кибероперации во время вооруженных конфликтов — это реальность сегодняшних вооруженных конфликтов, и скорее всего использоваться такие операции будут все чаще. Они могут причинять значительный ущерб гражданскому населению, особенно в случае поражения критически важной гражданской инфраструктуры, такой как медицинские учреждения, сети электроснабжения, водоснабжения и канализационная система. Хотя риск причинить вред людям не представляется крайне высо-

218 Это предложила Хелен Дарем, директор Управления МККК по вопросам международного права и гуманитарной политики, во вступительном слове во время публичных слушаний, проведенных 22 января 2019 г. Глобальной комиссией по стабильности киберпространства (имеется в МККК).

219 ICRC Challenges Report 2019 (примечание 36 выше), p. 35.

ким на основании имеющихся наблюдений, особенно с учетом разрушений и страданий, которые неизбежно вызывают конфликты, эволюция кибероперациий требует повышенного внимания из-за существующей неопределенности и высокого темпа изменений.

Во-вторых, по мнению МККК, не вызывает сомнения тот вопрос, что кибероперации во время вооруженных конфликтов регулируются МГП — как и применение любого оружия, средств и методов ведения войны воюющими сторонами в конфликте, как старых, так и новых. Хотя по этому вопросу (еще) нет всеобщего согласия, тщательное исследование различных аргументов, выдвигаемых в ходе многосторонних дискуссий, свидетельствует о том, что подтверждение применимости МГП не легитимизирует ни милитаризацию киберпространства, ни применение злонамеренных кибероперациий. Государство, которое рассматривает возможность осуществить кибероперацию против другого государства, должно оценить законность этой операции согласно Уставу ООН и МГП. Эти две правовые системы дополняют друг друга, когда речь идет о защите людей от войны и ее последствий. Хотя подчас в них используется аналогичная терминология, две системы являются отдельными с правовой точки зрения и требуют отдельного анализа, поскольку схожая терминология (иногда) имеет разное значение. Например, вывод о том, что кибероперация вводит в действие МГП, не обязательно означает, что она является вооруженным нападением, приводящим к возникновению права на самооборону.

В-третьих, частично нефизическая, то есть цифровая природа киберпространства и взаимосвязанность военных и гражданских сетей создают практические и правовые проблемы при применении общих принципов и норм МГП, предоставляющих защиту гражданским лицам и гражданским объектам. Это особенно очевидно в отношении таких проблем, как понятие «нападение» в соответствии с МГП, вопрос о том, пользуются ли гражданские данные такой же защитой, что и гражданские объекты, и защита киберинфраструктуры двойного использования.

Вопрос о том, является ли операция нападением по определению МГП, крайне важен для применения многих норм, вытекающих из принципов проведения различия, соразмерности и мер предосторожности, которые предоставляют абсолютно необходимую защиту гражданским лицам и гражданским объектам. В течение многих лет позиция МККК была такова: операция, предназначенная для выведения из строя компьютера или компьютерной сети во время вооруженного конфликта, является нападением по определению МГП, независимо от того, выведен ли объект из строя посредством уничтожения или любым другим путем. Эта точка зрения нашла отражение и в позиции целого ряда государств.

Хотя многие из общих норм по ведению военных действий ограничиваются действиями, являющимися нападениями по определению МГП, некоторые нормы МГП, регулирующие ведение военных действий, применимы к более широкому диапазону операций. В МГП есть несколько норм, которые применяются ко всем военным операциям, например, обязанность

постоянно проявлять заботу, чтобы щадить гражданских лиц и гражданские объекты. Более того, МГП устанавливает особые правила по защите определенных категорий лиц и объектов, таких как объекты, необходимые для выживания гражданского населения, медицинские службы и операции по предоставлению гуманитарной помощи. Защита, которую они предусматривают, является более широкой, чем общая защита, предоставляемая гражданским лицам и гражданским объектам.

Защита данных от вредоносных кибероперациий во время вооруженных конфликтов становится все важнее, поскольку данные являются важнейшим компонентом цифровой сферы и краеугольным камнем жизни во многих обществах. По мнению МККК, серьезную обеспокоенность вызвал бы вывод о том, что в сегодняшнем, все более зависящем от цифровизации, мире МГП не будет содержать запрета на кибероперации, предназначенные для уничтожения важнейших данных гражданского характера, или на те, которые, как ожидается, могут сделать это. Как представляется, такой вывод трудно привести в соответствие с объектом и целью этого свода норм.

Чтобы защитить важнейшую гражданскую инфраструктуру, которая зависит от киберпространства, важно также защитить инфраструктуру самого киберпространства. Традиционно понимается, что гражданский объект может стать военным объектом, если он используется в военных целях таким образом, что это соответствует определению военного объекта, даже если он одновременно используется для гражданских целей. Однако сторона в конфликте, которая рассматривает возможность осуществить нападение на инфраструктуру киберпространства, должна проанализировать, какие именно части инфраструктуры вносят эффективный вклад в военные действия, и предоставит ли их уничтожение или нейтрализация в сложившихся в соответствующий момент обстоятельствах явное военное преимущество. Более того, эта сторона должна принять все практически возможные меры предосторожности, чтобы избежать или по крайней мере минимизировать случайный ущерб гражданским лицам и объектам, включая косвенный или отдаленный ущерб, и должна воздерживаться от осуществления нападения, если такой ущерб, как можно ожидать, будет чрезмерным.

В-четвертых, в свете особых вызовов, которые характеристики киберпространства ставят перед толкованием и применением отдельных принципов МГП при ведении военных действий, стороны в вооруженных конфликтах, которые принимают решение разрабатывать, приобретать или принимать на вооружение оружие, средства или методы ведения войны с использованием кибертехнологии, должны проявлять максимум внимательности и осторожности. Хотя правовая экспертиза новых видов оружия, средств и методов ведения войны является обязательной для государств — участников ДП I, такая экспертиза критически важна для всех государств, чтобы обеспечить применение их вооруженными силами такого оружия, средств и методов ведения войны, которые соответствуют обязательствам государства по МГП.

В заключение можно сказать, что признание применимости МГП в киберпространстве и участие в обсуждении вопросов о том, каким образом оно отвечает на различные вызовы, обусловленные особенностями кибернетической среды, и является ли существующее право адекватным и достаточным, не исключает того, что могут оказаться полезными и даже необходимыми новые нормы. По нашему мнению, ответ на этот вопрос зависит именно от того, как государства толкуют существующие обязательства по МГП. Если будут приняты узкие толкования, могут возникнуть серьезные пробелы в защите гражданского населения и инфраструктуры, и существующие правовые системы могут потребовать укрепления. Однако если будут разработаны новые нормы, то, по нашему мнению, очень важно, чтобы они развивали и укрепляли правовую систему, которая уже существует, а именно — МГП.