Международное гуманитарное право и кибероперации во время вооруженных конфликтов

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.

Содержание

Краткое изложение

- **В современных вооруженных конфликтах кибероперации стали реальностью.** Международный Комитет Красного Креста (МККК) обеспокоен **потенциальными гуманитарными последствиями** растущего использования кибероперациий во время вооруженных конфликтов.
- **По мнению МККК, международное гуманитарное право (МГП) ограничивает применение кибероружия** во время вооруженного конфликта так же, как любого другого оружия, средств и методов ведения войны — и новых, и старых.
- Утверждение о применимости МГП не легитимизирует кибервойну, как и любой другой вид войны. **Любое применение государствами силы — будь то кибероружие или кинетическое оружие — по–прежнему регулируется Уставом Организации Объединенных Наций (ООН) и соответствующими нормами обычного международного права,** в частности запретом на применение силы. Международные споры должны разрешаться мирными средствами во всех областях, в том числе в киберпространстве.
- Сейчас крайне важно, чтобы **международное сообщество подтвердило применимость МГП** к кибероперациям во время вооруженных конфликтов. МККК также призывает **провести среди правительственных и иных экспертов обсуждение того, *как* именно применяются имеющиеся нормы МГП** и являются ли существующие правовые нормы адекватными и достаточными. В связи с этим **МККК приветствует межправительственные обсуждения,** проходящие в настоящее время в рамках двух процессов, санкционированных Генеральной Ассамблеей ООН.
- События последних лет показывают, что кибероперации — как связанные с вооруженными конфликтами, так и не имеющие к ним отношения — могут подорвать работу жизненно важных объектов гражданской инфраструктуры и помешать предоставлению основных услуг населению. **В ситуации вооруженного конфликта объекты гражданской инфраструктуры защищены от кибератак существующими принципами и нормами МГП,** в частности принципами проведения различия, соразмерности и принятия мер предосторожности во время нападения. МГП также предоставляет особую защиту больницам и объектам, необходимым для выживания гражданского населения.
- **Во время вооруженных конфликтов запрещено применение киберсредств, которые распространяются неизбирательно и при этом наносят неизбирательный ущерб.** С технической точки зрения, некоторые киберинструменты можно проектировать и использовать таким образом, чтобы они направлялись против конкретных целей и наносили вред конкретным объектам, а не распространялись неизбирательно или причиняли неизбирательный ущерб. Однако в киберпространстве всё взаимосвязано, поэтому любой объект, подключенный к интернету, может подвергнуться нападению из любой точки мира и кибератака на одну систему может иметь последствия для многих других. В результате существует

реальная опасность того, что при проектировании и применении киберинструментов не будут учтены нормы МГП — преднамеренно или по ошибке.

- **Толкование государствами существующих норм МГП определит, в какой степени МГП защищает от последствий кибероперaций.** В частности, государства должны занять четкую позицию относительно своей готовности толковать МГП так, чтобы уберечь объекты гражданской инфраструктуры от серьезных повреждений и защитить данные гражданского назначения. Наличие такой позиции также повлияет на оценку того, достаточно ли существующих норм или же требуются новые. Если государства сочтут необходимым разработать новые нормы, они должны **взять за основу и укрепить существующую правовую базу, включая МГП.**

I. Вступление

Осуществление кибероперацій во время вооруженных конфликтов стало реальностью[1]. Хотя лишь несколько государств публично признались в ведении таких операций, все большее число стран развивает военный киберпотенциал, использование которого в будущем, по всей вероятности, будет расти.

Кроме того, технологии шагнули далеко вперед в разработке наступательных киберсредств: события последних лет свидетельствуют, что кибероперации могут оказывать серьезное воздействие на гражданскую инфраструктуру и причинять вред людям.

В соответствии со своими целями, задачами и мандатом Международный Комитет Красного Креста (МККК) в первую очередь озабочен использованием кибероперацій в качестве средства или метода ведения войны во время вооруженных конфликтов и защитой от последствий кибероперацій, которую предоставляет МГП.

МККК приветствует межправительственные обсуждения, проходящие в настоящее время в рамках двух процессов, санкционированных Генеральной Ассамблеей ООН: Рабочей группы открытого состава по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов по вопросу о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. Обеим группам поручено изучить, «как международное право применяется к использованию ИКТ государствами»[2]. МККК передает настоящий документ обеим группам, чтобы поддержать обсуждение этого вопроса государствами.

Данный документ ограничивается правовыми и гуманитарными вопросами, которые встают в связи с ведением кибероперацій во время вооруженного конфликта. В нем не рассматриваются вопросы, касающиеся правовых норм, которые применимы к кибероперациям, не имеющим отношения к вооруженным конфликтам.

II. Потенциальные гуманитарные последствия кибероперацій

Во время вооруженного конфликта кибероперации ведутся в поддержку операций с применением кинетического оружия или параллельно с ними. Кибероперации предлагают решения, которые не могут предложить другие средства и методы ведения войны, но осуществление кибероперацій также сопряжено с рисками. С одной стороны, кибероперации потенциально могут позволить сторонам в вооруженном конфликте достичь их военных целей, не причиняя вреда гражданским лицам и не нанося физического ущерба гражданской инфраструктуре. С другой стороны, недавние кибероперации, в большинстве своем не связанные с вооруженным конфликтом, показывают, что в наше время акторы, обладающие новейшими киберсредствами, способны помешать предоставлению основных услуг гражданскому населению.

Посредством кибероперацій воюющие стороны могут проникнуть в систему и собрать, изъять, изменить, зашифровать или уничтожить данные. Также возможно использовать взломанную компьютерную систему для запуска и изменения процессов, которые она контролирует, или для иного манипулирования этими процессами. Работа разнообразных «целей», существующих в реальном мире, — например, производств, объектов инфраструктуры и линий связи, транспортной, правительственной или финансовой системы — может быть подорвана, изменена

[1] В настоящем документе выражение «кибероперации во время вооруженных конфликтов» обозначает операции, осуществляемые посредством потока данных против компьютера, компьютерной системы или сети либо другого подключенного к интернету устройства, когда такие операции используются в качестве средства или метода ведения войны в ситуации вооруженного конфликта. В кибероперациях используются информационно-коммуникационные технологии.

[2] Резолюции ООН A/RES/73/27, п. 5; A/RES/73/266, п. 3.

или нарушена. После консультаций с экспертами со всего мира и проведения собственных исследований МККК особенно обеспокоен потенциальными гуманитарными последствиями кибероперaций, направленных против жизненно важных объектов гражданской инфраструктуры, включая систему здравоохранения[3].

В последние годы кибератаки обнажили уязвимость систем жизнеобеспечения. По сообщениям, такие нападения происходят все чаще, а их последствия становятся все тяжелее — и эти изменения происходят быстрее, чем ожидали эксперты. Более того, о некоторых вещах нам по-прежнему известно крайне мало: каковы самые продвинутые киберсредства и инструменты, уже созданные или находящиеся в разработке; как технологии могут эволюционировать; в какой степени ведение кибероперaций во время вооруженных конфликтов может отличаться от тенденций, которые мы наблюдали до сих пор.

Кроме того, есть ряд опасений, связанных с особыми свойствами киберпространства. К примеру, кибероперации сопряжены с риском эскалации ситуации, которая повлечет за собой соответствующие гуманитарные последствия, — по той простой причине, что стороне, которая подвергается нападению, бывает сложно понять, какова цель нападающего — сбор разведданных или причинение более серьезного ущерба. В результате объект нападения, ожидая самого худшего, может отреагировать жестче, чем необходимо.

Киберинструменты также распространяются особым образом. Будучи задействованными, они могут быть перенацелены или широко использованы не только разработчиком или исходным пользователем, но и другими лицами или организациями.

III. Применение МГП к кибероперациям во время вооруженных конфликтов

МККК не сомневается, что нормы МГП применимы к кибероперациям во время вооруженного конфликта и, соответственно, ограничивают их так же, как применение любого другого оружия, средств и методов ведения войны — и новых, и старых[4]. Это справедливо вне зависимости от того, считать ли киберпространство новой сферой ведения войны, аналогичной воздуху, земле, морю и космическому пространству; иного вида сферой ведения войны, поскольку оно создано человеком в отличие от перечисленных выше пространств, созданных природой; или же не считать его сферой ведения войны вовсе.

Принимая договоры в области МГП, государства стремятся регулировать конфликты в настоящем и в будущем. Государства включают в договоры по МГП нормы, которые предвосхищают разработку новых средств и методов ведения войны, предполагая, что МГП будет применимо и к ним. К примеру, не будь МГП применимо к будущим средствам и методам ведения войны, не было бы необходимости определять их законность в соответствии с существующими нормами МГП, как этого требует статья 36 Дополнительного протокола I от 8 июня 1977 г.

Этот вывод находит решительную поддержку в Консультативном заключении Международного суда ООН относительно законности угрозы ядерным оружием или его применения: Суд

---

[3] См.: ICRC, *The Potential Human Cost of Cyber Operations*, 2019: https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

[4] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, 31IC/11/5.1.2, pp. 36–37: https://www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; МККК, Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015 г., 32IC/15/11, с. 70-71: https://www.icrc.org/ru/download/file/20891/mezhdunarodnoe_gumanitarnoe_pravo_i_vyzovy_sovremennyh_konfliktov.pdf; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, 33IC/19/9.7, p. 18: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.

напомнил, что установленные принципы и нормы МГП, применимые в ситуации вооруженного конфликта, относятся «ко всем формам военных действий и всем видам оружия», включая оружие будущего[5]. По мнению МККК, данное заключение касается и ведения кибероперациий во время вооруженного конфликта.

МККК приветствует тот факт, что все больше государств и международных организаций подтверждают применимость МГП к кибероперациям во время вооруженных конфликтов, и надеется на обсуждение вопроса о том, как именно применяется МГП.

Государства также могут принять решение о введении ограничений на кибероперации в дополнение к тем, которые можно найти в действующих положениях права, и могут разработать дополнительные нормы, в частности для усиления защиты гражданских лиц и гражданской инфраструктуры от последствий кибероперациий. С точки зрения МККК, любые предполагаемые новые нормы должны взять за основу и укрепить существующую правовую базу, включая МГП.

В случаях, не предусмотренных существующими нормами МГП, гражданские лица и комбатанты остаются под защитой так называемой оговорки Мартенса, то есть на них по-прежнему распространяется защита и действие принципов международного права, вытекающих из установившихся обычаев, принципов гуманности и требований общественного сознания[6].

Важно подчеркнуть, что подтверждение применимости МГП к кибероперациям во время вооруженного конфликта не легитимизирует кибервойну и не содействует милитаризации киберпространства. На самом деле, МГП налагает некоторые ограничения на милитаризацию киберпространства, запрещая разрабатывать киберсредства военного назначения, которые нарушили бы нормы МГП[7]. Более того, любое применение силы государствами — будь то кибератака или кинетическое оружие — по-прежнему регулируется Уставом ООН и соответствующими нормами обычного МГП, в частности запретом на применение силы. Международные споры должны разрешаться мирными средствами во всех областях, в том числе в киберпространстве.

IV. Защита, предоставляемая существующими нормами МГП

Ведение вооруженного конфликта регулируют многочисленные положения обычного права и существующих договоров в области МГП. В киберпространстве особенно актуальны нормы, регулирующие ведение военных действий. Эти нормы направлены на защиту гражданского населения от последствий военных действий. Они основаны на главном принципе — принципе проведения различия, который требует от воюющих сторон во всякое время проводить различие между гражданскими лицами и комбатантами и между гражданскими и военными объектами, а также осуществлять нападения только на военные объекты[8].

Несмотря на взаимосвязанность всех объектов, характерную для киберпространства, тщательное изучение работы киберинструментов показывает, что они не всегда действуют неизбирательно. Многие из недавних кибератак, о которых сообщалось публично, с технической точки зрения, по всей видимости, носили довольно избирательный характер: они были спланированы и использованы так, чтобы выбирать конкретные цели и нанести вред конкретным объектам, а не распространяться неизбирательно или причинять неизбирательный ущерб. Однако сделать так, чтобы были затронуты только конкретные объекты, может быть

[5] Международный суд ООН (МС), Консультативное заключение относительно законности угрозы ядерным оружием или его применения, 8 июля 1996 г., п. 86.

[6] См. ст. 1(2) Дополнительного протокола I к Женевским конвенциям от 8 июня 1977 г. (ДП I); п. 9 преамбулы к Гаагской конвенции II 1899 г.; п. 8 преамбулы к Гаагской конвенции IV 1907 г.

[7] См.: *Хенкертс, Жан-Мари и Досвальд-Бек, Луиза*. Обычное международное гуманитарное право. Том I: Нормы. МККК, 2006 (далее — Обычное МГП). Нормы 70 и 71. См. также ст. 36 ДП I.

[8] Ст. 48 ДП I; Обычное МГП, нормы 1 и 7; МС, Консультативное заключение международного суда относительно законности угрозы ядерным оружием или его применения, 8 июля 1996, п. 78.

технически сложно, для этого может потребоваться тщательное планирование при разработке и ведении кибероперaций. Следует также отметить, что кибероперация, даже будучи технически избирательной, совсем не обязательно законна — будь то в ходе вооруженного конфликта или в ситуации, не имеющей к нему отношения.

При этом некоторые уже существующие киберинструменты спроектированы таким образом, что могут самостоятельно распространяться и неизбирательно воздействовать на широкий круг компьютерных систем. И это не случайность: способность к самостоятельному распространению при проектировании таких инструментов может быть заложена только умышленно. В киберпространстве всё взаимосвязано, поэтому любой объект, подключенный к интернету, может подвергнуться нападению из любой точки мира. Более того, атака на конкретную систему может сказаться на многих других системах и привести к неизбирательным последствиям. В результате существует реальная опасность того, что при проектировании и применении киберинструментов не будут учтены нормы МГП — преднамеренно или по ошибке.

Подтверждение того, что нормы МГП, в том числе принципы проведения различия, соразмерности и принятия мер предосторожности, применимы к кибероперациям во время вооруженных конфликтов, означает, что в соответствии с существующими положениями права, среди прочего:

- запрещаются киберсредства, которые квалифицируются как оружие и по своей природе являются неизбирательными[9];
- запрещаются непосредственные нападения на гражданских лиц и гражданские объекты, в том числе с использованием кибернетических средств и методов ведения войны[10];
- запрещаются акты насилия и угрозы насилием, главная цель которых — терроризировать гражданское население, в том числе когда они осуществляются посредством кибернетических средств и методов ведения войны[11];
- запрещаются неизбирательные нападения, а именно нападения, которые поражают военные объекты и гражданских лиц или гражданские объекты без всякого различия, в том числе при использовании кибернетических средств и методов ведения войны[12];
- запрещаются несоразмерные нападения, в том числе при использовании кибернетических средств или методов ведения войны. Несоразмерные нападения — это нападения, которые, как можно ожидать, попутно повлекут за собой потери жизни среди гражданского населения, ранения гражданских лиц, ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить[13];
- во время военных операций, в том числе при использовании кибернетических средств или методов ведения войны, необходимо постоянно проявлять заботу о том, чтобы щадить гражданское население и гражданские объекты; должны приниматься все возможные меры предосторожности, чтобы избежать случайного вреда гражданским лицам и объектам или

[9] Обычное МГП, норма 71.
[10] Ст. 48, 51 и 52 ДП I; Обычное МГП, нормы 1 и 7.
[11] Ст. 51(2) ДП I; Обычное МГП, норма 2.
[12] Ст. 51(4) ДП I; Обычное МГП, нормы 11 и 12. К нападениям неизбирательного характера относятся: а) нападения, которые не направлены на конкретный военный объект; б) нападения, при которых применяются методы или средства ведения военных действий, которые невозможно направить на конкретный военный объект; или в) нападения, при которых используются методы или средства ведения военных действий, последствия применения которых не могут быть ограничены, как того требует МГП; соответственно, в каждом таком случае эти нападения поражают военные объекты и гражданских лиц или гражданские объекты без различия.
[13] Ст. 51(5)(b) и 57 ДП I; Обычное МГП, норма 14.

хотя бы свести его к минимуму при осуществлении нападений, в том числе когда они осуществляются с использованием кибернетических средств и методов ведения войны[14];

- запрещаются нападения на объекты, необходимые для выживания гражданского населения, их уничтожение, вывоз или приведение в негодность, в том числе посредством использования кибернетических средств и методов ведения войны[15];
- необходимо защищать и уважать медицинские службы, в том числе при проведении кибероперaций во время вооруженных конфликтов[16].

Кроме того, необходимо принимать все возможные меры предосторожности для защиты гражданских лиц и объектов от последствий нападений, осуществляемых при помощи кибернетических средств и методов ведения войны, — это обязанность, которую государства должны выполнять уже в мирное время[17]. Можно рассмотреть такие меры, как разделение военной и гражданской киберинфраструктуры и сетей; отделение компьютерных систем, которые использует гражданская инфраструктура жизнеобеспечения, от интернета; определение киберинфраструктуры и сетей, которые обслуживают объекты, находящиеся под особой защитой, например больницы[18].

V. Необходимость обсудить, *как* применяется МГП

Подтверждение того, что МГП применяется к кибероперациям во время вооруженных конфликтов, — важнейший первый шаг к тому, чтобы избежать человеческих страданий, которые могут принести кибероперации, или свести их к минимуму. Однако МККК также призывает государства работать над достижением общего понимания того, *как* принципы и нормы МГП применяются к кибероперациям. Это необходимо, потому что взаимосвязь всех объектов в киберпространстве и его по большей части цифровой характер создают трудности для толкования основных принципов и понятий МГП, касающихся ведения военных действий.

В настоящем документе МККК хотел бы уделить особое внимание трем из множества различных проблем.

Использование киберпространства в военных целях и последствия такого использования для его гражданского характера

За исключением отдельных сетей военного назначения, киберпространство используется в основном в гражданских целях. Однако гражданские и военные сети могут быть связаны друг с другом; военные сети могут использовать гражданскую киберинфраструктуру: проходящие по морскому дну волоконно-оптические кабели, спутники, маршрутизаторы и узлы. И наоборот, гражданский транспорт, управление морскими перевозками и воздушным движением все больше зависят от спутниковых навигационных систем, которые могут использоваться и военными. Гражданские системы материально-технического снабжения и основные

[14] Ст. 57 ДП I; Обычное МГП, нормы 15–21.
[15] Ст. 54 ДП I; ст. 14 Дополнительного протокола II к Женевским конвенциям от 8 июня 1977 г. (ДП II); Обычное МГП, норма 54.
[16] См., например, ст. 19 Женевской конвенции об улучшении участи раненых и больных в действующих армиях от 12 августа 1949 г. (ЖК I); ст. 12 Женевской конвенции об улучшении участи раненых, больных и потерпевших кораблекрушение из состава вооруженных сил на море от 12 августа 1949 г. (ЖК II); ст. 18 Женевской конвенции о защите гражданского населения во время войны от 12 августа 1949 г. (ЖК IV); ст. 12 ДП I; ст. 11 ДП II; Обычное МГП, нормы 25, 28 и 29.
[17] Ст. 58 ДП I; Обычное МГП, нормы 22-24.
[18] МККК, Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015 г., с. 76-77.

гражданские службы используют те же сети и системы коммуникации, через которые проходят отдельные сообщения военного характера.

Согласно МГП использование гражданского объекта в военных целях не делает его автоматически военным объектом[19]. Если это все же происходит, однако, то такой объект больше не находится под защитой запрета на непосредственные нападения на гражданские объекты. Если бы использование киберпространства в военных целях привело к тому, что многие входящие в него объекты утратили бы защиту как гражданские, это стало бы поводом для серьезного беспокойства и могло бы существенно подорвать использование киберпространства в гражданских целях, которое приобретает все большее значение в настоящее время.

При этом во время вооруженного конфликта, даже если определенные объекты инфраструктуры киберпространства утрачивают право на защиту как гражданские объекты, любое нападение по-прежнему ограничено запретом на неизбирательные нападения, а также принципами соразмерности и принятия мер предосторожности при нападении. Именно из-за такой взаимосвязанности гражданских и военных сетей, чтобы обеспечить защиту гражданского населения от последствий любой кибероперации, крайне важно оценить предполагаемый случайный вред, который она может нанести гражданским лицам и объектам[20].

Понятие «нападение» согласно МГП и кибероперации

Критически важные объекты гражданской инфраструктуры, позволяющие предоставлять населению основные услуги, все больше зависят от цифровых систем. Ограждать такую инфраструктуру и услуги от кибератак или случайного ущерба предельно важно для защиты гражданского населения.

МГП предусматривает защиту конкретных объектов инфраструктуры, таких как медицинские службы и объекты, необходимые для выживания гражданского населения, независимо от типа операции, которая может причинить им вред[21]. Однако большинство норм, вытекающих из принципов проведения различия, соразмерности и принятия мер предосторожности (которые обеспечивают общую защиту гражданских лиц и объектов), применимы лишь к военным операциям, которые квалифицируются как «нападения» согласно определению, содержащемуся в МГП[22]. Статья 49 ДП I определяет нападения как «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне»[23]. Поэтому вопрос о том, насколько широко или узко толкуется понятие «нападение» применительно к кибероперациям, представляется крайне важным в плане применимости этих

---

[19] См. ст. 52(2) ДП I; Обычное МГП, норма 8 («Что касается объектов, то военные объекты ограничиваются теми объектами, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество»). Более подробно об ограничениях, налагаемых МГП на превращение объектов киберинфраструктуры в военные объекты, см.: МККК, Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015 г., с. 75.

[20] См.: ICRC, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, 2018: https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf, pp. 37–40.

[21] См. выше текст к сноскам 16 и 15 выше. «Объекты, необходимые для выживания населения», нельзя подвергать нападению, уничтожать, вывозить или приводить в негодность.

[22] Понятие «нападение» в соответствии с МГП, определение которого дается в ст. 49 ДП I, отличается от понятия «вооруженное нападение» в ст. 51 Устава ООН (которая является частью jus ad bellum), и его не следует путать с последним. Подтверждение того, что конкретная кибероперация или тип кибероперации представляет собой нападение согласно МГП, не всегда означает, что эта кибероперация будет считаться вооруженным нападением в соответствии с Уставом ООН.

[23] Нормы, применимые конкретно к нападениям, можно найти в тексте, к которому относятся примечания 10–14 выше.

норм и в плане защиты, которую они предоставляют гражданскому населению и гражданской инфраструктуре.

Широко признается, что кибероперации, которые, как ожидается, приведут к гибели, ранениям или физическому ущербу, согласно МГП представляют собой нападения. По мнению МККК, сюда относятся и кибероперации, которые причиняют вред своими прогнозируемыми прямыми и «непрямыми» (косвенными) последствиями: например, когда пациенты, находящиеся в реанимационном отделении больницы, умирают, потому что больница осталась без электричества в результате кибератаки на электроэнергетическую систему.

Помимо этого, нападения, которые серьезно подрывают оказание основных услуг, не обязательно причиняя при этом физический ущерб, представляют собой одну из самых серьезных опасностей для гражданских лиц. Мнения расходятся, однако, относительно того, считать ли кибероперацию, приводящую к потере функциональности без причинения физического ущерба, нападением по определению МГП. С точки зрения МККК, во время вооруженного конфликта операция, направленная на выведение из строя компьютера или компьютерной сети, является нападением согласно МГП, независимо от того, какими средствами объект был выведен из строя — кинетическими или кибернетическими[24]. Если толковать понятие «нападение» как относящееся только к операциям, приводящим к гибели, ранениям и физическому ущербу, то кибероперация, которая направлена на нарушение работы гражданской сети (например, электросети, банковской системы или системы связи) или, как можно ожидать, вызовет ее нарушение случайно, может не подпадать под действие основных норм МГП по защите гражданского населения и гражданских объектов. Такое чрезмерно ограничительное понимание понятия «нападение» с трудом согласуется с объектом и целью норм МГП, касающихся ведения военных действий. Поэтому чтобы обеспечить адекватную защиту гражданского населения от последствий кибероперациий, крайне важно, чтобы государства пришли к общему пониманию понятия «нападение».

Данные гражданского назначения и понятие «гражданские объекты»

Важнейшие данные гражданского назначения, такие как медицинские и биометрические данные, данные органов социального обеспечения, налоговая документация, банковские счета, клиентские базы компаний или списки избирателей и результаты выборов, — важный элемент общественной жизни в эпоху цифровых технологий. Такие данные имеют ключевое значение для функционирования большинства сфер жизни гражданина как на индивидуальном уровне, так и на уровне всего общества. Сохранение этих важнейших данных гражданского назначения становится предметом все большей озабоченности.

Часть особой защиты, предоставляемой МГП, распространяется на важнейшие данные, например данные медицинских учреждений, подпадающие под обязательство уважать и защищать такого рода учреждения[25].

В более широком плане гражданских лиц и гражданские объекты защищают основные принципы и нормы МГП, регулирующие ведение военных действий[26]. Поэтому государствам важно прийти к согласию относительно того, что данные гражданского назначения находятся под защитой этих норм.

Удаление или искажение важнейших данных гражданского назначения может быстро привести к полной остановке работы государственных служб и частных предприятий. Подобные действия могут причинить гражданскому населению больше вреда, чем уничтожение физических объектов. Вопрос о том, являются ли данные гражданского назначения гражданскими

[24] См.: ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, p. 37; МККК, Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015 г., с. 72–73.
[25] См. примечание 16.
[26] См. текст, к которому относятся примечания 10–15 выше.

объектами — и если да, то в какой степени, — остается без ответа. Как представляется МККК, утверждение о том, что в нашем мире, зависимом от данных, удаление или искажение таких важнейших данных гражданского назначения не запрещается МГП, с трудом согласуется с объектом и целью МГП. Замещение бумажных документов цифровыми не должно привести к снижению уровня защиты, предоставляемой МГП[27]. Лишение важнейших данных гражданского назначения защиты, которую МГП предоставляет гражданским объектам, означало бы значительный пробел в защите.

VI. Присвоение поведения в киберпространстве в целях установления ответственности государств

Киберпространство дает лицам и организациям различные технические возможности, позволяющие им скрывать или подделывать свою личность, что сильно затрудняет присвоение поведения. Это создает серьезные сложности. Например, даже во время вооруженного конфликта МГП применяется только к операциям, связанным с конфликтом. Если невозможно установить организатора кибероперации — и тем самым связь между кибероперацией и соответствующим вооруженным конфликтом, — может быть трудно определить, применимо ли к этой операции МГП. Установление личности организаторов кибероперации также имеет важное значение для привлечения к ответственности тех, кто нарушает нормы международного права, в том числе МГП. Помимо этого, ощущение, что ответственность за совершение кибератак легко отрицать, может ослабить табу на их использование и сделать акторов менее щепетильными в плане их совершения в нарушение международного права[28].

Вопрос присвоения поведения не создает, однако, проблемы для тех, кто проводит кибероперации, руководит ими или контролирует их: у них на руках есть все факты, чтобы определить, в каких международно-правовых рамках они действуют и какие обязательства должны соблюдать.

В соответствии с международным правом государство несет ответственность за действия, которые могут быть ему присвоены, включая возможные нарушения МГП. Сюда относятся:

- деяния государственных органов, в том числе вооруженных сил и разведывательных служб;
- деяния лиц и организаций, например частных компаний, уполномоченных государством выполнять функции государственных властей;
- деяния лиц и групп, например ополчений или групп хакеров, действующих, по сути, по указаниям государства или под его руководством или контролем; и
- деяния частных лиц или групп, которые государство признает и принимает как свои собственные[29].

Эти принципы применяются независимо от того, осуществляются ли деяния при помощи кибернетических или иных средств.

VII. Заключение

Существует реальная опасность того, что при использовании кибероперации в качестве средства или метода ведения войны во время вооруженного конфликта будет нанесен вред гражданским лицам. Чтобы защитить гражданское население и гражданскую инфраструктуру, крайне важно признать, что такие операции не происходят в правовом вакууме. МККК настоятельно призывает

[27] МККК, Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015 г., с. 76; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, p. 21.
[28] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, p. 37; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, p. 20.
[29] См.: Обычное МГП, норма 149. См. также: Комиссия ООН по международному праву, Ответственность государств за международно-противоправные деяния, 2001 г., в частности ст. 4–11.

все государства подтвердить, что МГП применяется к кибероперациям во время вооруженных конфликтов, исходя из понимания, что такое подтверждение не содействует милитаризации киберпространства и не легитимизирует кибервойну.

В то же время МККК полагает, что необходимо дальнейшее обсуждение — особенно среди государств — того, как следует толковать и применять МГП в киберпространстве. Существует настоятельная потребность в таком обсуждении, поскольку государства, решающие разрабатывать или приобретать — будь то для наступательных или оборонительных целей — киберинструменты, которые квалифицируются как оружие, средства или методы ведения войны, должны обеспечить возможность использования подобных инструментов в соответствии с обязательствами этих государств в области МГП[30]. Обсуждение этого вопроса должно быть основано на глубоком понимании путей развития киберсредств военного назначения, потенциальных гуманитарных последствий их использования и защиты, предоставляемой существующими нормами права. Государствам необходимо определить, являются ли действующие правовые нормы адекватными и достаточными для того, чтобы справиться с проблемами, которые возникают из-за цифрового — по большей части — характера киберпространства и взаимосвязанности всех объектов в нем, или же эти нормы необходимо адаптировать к особым свойствам киберпространства. Если разрабатывать новые нормы для защиты гражданских лиц от последствий кибероперации или с другими целями, необходимо взять за основу и укрепить существующую правовую базу, включая МГП.

МККК приветствует межправительственные обсуждения, которые сейчас проводятся в рамках двух процессов, санкционированных Генеральной Ассамблеей ООН, и благодарен за возможность рассказать о своем видении вопроса участвующим в них государствам. МККК также готов поделиться своим опытом и знаниями в ходе таких обсуждений, если государства сочтут это целесообразным.

[30] См.: ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, pp. 28–29; ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, 2006, p. 4; ст. 36 ДП I.