# МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО И КИБЕРОПЕРАЦИИ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

МККК

# МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО И КИБЕРОПЕРАЦИИ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

ИЗЛОЖЕНИЕ ПОЗИЦИИ МККК

Перевод с английского
с приложением оригинального текста

# СОДЕРЖАНИЕ

# 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.

## КРАТКОЕ ИЗЛОЖЕНИЕ

- **В современных вооруженных конфликтах кибероперации стали реальностью.** Международный Комитет Красного Креста (МККК) обеспокоен **потенциальными гуманитарными последствиями** растущего использования кибероперации 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 м**еждународное 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 кибер-средств, 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.**

## ВСТУПЛЕНИЕ

Осуществление кибероперaций 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 кибероперaций в качестве средства или метода ведения войны во время вооруженных конфликтов и защитой от последствий кибероперaций, 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 кибероперaций во время вооруженного конфликта. В нем не рассматриваются вопросы, касающиеся правовых норм, которые применимы к кибероперациям, не имеющим отношения к вооруженным конфликтам.

---

[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.

## 1. ПОТЕНЦИАЛЬНЫЕ ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ КИБЕРОПЕРАЦИЙ

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 кибероперации 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 кибероперации 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 или нарушена. После консультаций с экспертами со всего мира и проведения собственных исследований МККК особенно обеспокоен потенциальными гуманитарными последствиями кибероперации, 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 попрежнему известно крайне мало: каковы самые продвинутые киберсредства и инструменты, уже созданные или находящиеся в разработке; как технологии могут эволюционировать; в какой степени ведение кибероперации 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

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

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.

## 2. 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 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.

---

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-intconference-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/document/mezhdunarodnoe-gumanitarnoe-pravo-i-vyzovy-sovremennyh-vooruzhennyh-konfliktov; 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.

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

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 кибероперацій. 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.

## 3. 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 раз-

---

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.

личие 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 технически сложно, для этого может потребоваться тщательное планирование при разработке и ведении кибероперациий. 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

[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.

[9] Обычное МГП, норма 71.

[10] Ст. 48, 51 и 52 ДП I; Обычное МГП, нормы 1 и 7.

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 кибернетическихсредств 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 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 кибероперациий во время вооруженных конфликтов[16].

---

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.

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.

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].

## 4. 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 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

[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.

его автоматически военным объектом[19]. Если это все же происходит, 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 попрежнему 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

---

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/document/international-expert-meeting-report-principle-proportionality, 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

«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 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

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.

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.

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 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.

---

[25] См. примечание 16.

[26] См. текст, к которому относятся примечания 10–15 выше.

[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.

## 5. 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 киберопераций 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;
- деяния частных лиц или групп, которые государство признает и принимает как свои собственные[29].

---

[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.

## 6. ЗАКЛЮЧЕНИЕ

Существует реальная опасность того, что при использовании кибероперациий 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 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 кибероперациий 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.

# INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS DURING ARMED CONFLICTS

## ICRC POSITION PAPER

Submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'

## EXECUTIVE SUMMARY


- **Cyber operations have become a reality in contemporary armed conflict.** The International Committee of the Red Cross (ICRC) is concerned **by the potential human cost** arising from the increasing use of cyber operations during armed conflicts.
- **In the ICRC's view, international humanitarian law (IHeL) limits cyber operations during armed conflicts** just as it limits the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.
- Affirming the applicability of IHL does not legitimize cyber warfare, just as it does not legitimize any other form of warfare. **Any use of force by States – cyber or kinetic –remains governed by the Charter of the United Nations and the relevant rules of customary international law,** in particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.
- It is now critical **for the international community to affirm the applicability of international humanitarian law** to the use of cyber operations during armed conflicts. The ICRC also calls for **discussions among governmental and other experts on how existing IHL rules apply** and whether the existing law is adequate and sufficient. In this respect, the **ICRC welcomes the intergovernmental discussions** currently taking place in the framework of two United Nations General Assembly mandated processes.
- Events of recent years have shown that cyber operations, whether during or outside armed conflict, can disrupt the operation of critical civilian infrastructure and hamper the delivery of essential services to the population.

**In the context of armed conflicts, civilian infrastructure is protected against cyber attacks by existing IHL principles and rules,** in particular the principles of distinction, proportionality and precautions in attack. IHL also affords special protection to hospitals and objects indispensable to the survival of the civilian population, among others.

- **During armed conflicts, the employment of cyber tools that spread and cause damage indiscriminately is prohibited.** From a technological perspective, some cyber tools can be designed and used to target and harm only specific objects and to not spread or cause harm indiscriminately. However, the interconnectivity that characterises cyberspace means that whatever has an interface with the internet can be targeted from anywhere in the world and that a cyber attack on a specific system may have repercussions on various other systems. As a result, there is a real risk that cyber tools are not designed or used – either deliberately or by mistake – in compliance with IHL.
- **States' interpretation of existing IHL rules will determine the extent to which IHL protects against the effects of cyber operations.** In particular, States should take clear positions about their commitment to interpret IHL so as to preserve civilian infrastructure from significant disruption and to protect civilian data. The availability of such positions will also influence the assessment of whether the existing rules are adequate or whether new rules may be needed. If States see a need to develop new rules, they should **build on and strengthen the existing legal framework – including IHL.**

## 1. INTRODUCTION

The use of cyber operations during armed conflicts is a reality.[1] While only a few States have publicly acknowledged using such operations, an increasing number of States are developing military cyber capabilities, and their use is likely to increase in future.

Moreover, there have been significant technological advances in offensive cyber capabilities: in recent years, cyber operations have shown that they can seriously affect civilian infrastructure and might result in human harm.

In line with its mission and mandate, the International Committee of the Red Cross (ICRC) is primarily concerned with cyber operations used as means and methods of warfare during an armed conflict and the protection that international humanitarian law (IHL) affords against their effects.

---

[1] In this position paper, the term 'cyber operations during armed conflicts' is used to describe operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means and methods of warfare in the context of an armed conflict. Cyber operations rely on information and communication technologies.

The ICRC welcomes the intergovernmental discussions currently taking place in the framework of the two United Nations General Assembly mandated processes, namely the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Both groups are mandated to study "how international law applies to the use of information and communications technologies by States".[2] The ICRC submits this position paper to both groups to support States' deliberation on this matter.

This position paper is limited to legal and humanitarian questions arising from the use of cyber operations during armed conflict. It does not address questions relating to the legal framework applicable to cyber operations unrelated to armed conflict.

## 2. THE POTENTIAL HUMAN COST OF CYBER OPERATIONS

**During armed conflict, cyber operations have been used in support of or alongside kinetic operations. The use of cyber operations may offer alternatives that other means or methods of warfare do not, but it also carries risks. On the one hand, cyber operations have the potential to enable parties to armed conflicts to achieve their military aims without harming civilians or causing physical damage to civilian infrastructure. On the other hand, recent cyber operations – which have been mostly conducted outside the context of armed conflict – show that sophisticated actors have developed the capability to disrupt the provision of essential services to the civilian population.**

By means of cyber operations, it is possible for belligerents to infiltrate a system and collect, exfiltrate, modify, encrypt, or destroy data. It is also possible to trigger, alter or otherwise manipulate processes controlled by a compromised computer system. A variety of "targets" in the real world can be disrupted, altered or damaged, such as industries, infrastructures, telecommunications, transport, or governmental and financial systems. Based on discussions with experts from all parts of the world and its own research, the ICRC is particularly concerned about the potential human cost of cyber operations on critical civilian infrastructure, including health infrastructure.[3]

In recent years, cyber attacks have exposed the vulnerability of essential services. They are reportedly becoming more frequent and their severity is increasing more rapidly than experts had anticipated. Moreover, much is unknown with respect to the most sophisticated cyber capabilities and tools that have been or are being developed, how

---

2 A/RES/73/27, OP 5; A/RES/73/266, OP 3.

3 See ICRC, The Potential Human Cost of Cyber Operations, 2019;available at https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

technology may evolve, and the extent to which the use of cyber operations during armed conflicts might be different from the trends observed so far.

Moreover, the characteristics of cyberspace raise specific concerns. For example, cyber operations entail a risk for escalation and related human harm for the simple reason that it may be difficult for the targeted party to know whether the attacker's aim is intelligence collection or more harmful effects. The target may thereby react with greater force than necessary out of anticipation of a worst-case scenario.

Cyber tools also proliferate in a unique manner. Once used, they can be repurposed and widely used by actors other than the one that developed or used them initially.

## 3. THE APPLICATION OF IHL TO CYBER OPERATIONS DURING ARMED CONFLICTS

For the ICRC, there is no question that IHL applies to, and therefore limits, cyber operations during armed conflict – just as it regulates the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.[4] This holds true whether cyberspace is considered as a new domain of warfare similar to air, land, sea and outer space; a different type of domain because it is man-made while the former are natural; or not a domain as such.

When States adopt IHL treaties, they do so to regulate present and future conflicts. States have included rules that anticipate the development of new means and methods of warfare in IHL treaties, presuming that IHL will apply to them. For instance, if IHL did not apply to future means and methods of warfare, it would not be necessary to review their lawfulness under existing IHL, as required by Article 36 of the 1977 First Additional Protocol.

This conclusion finds strong support in the International Court of Justice's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons: the Court recalled that the established principles and rules of IHL applicable in armed conflict apply 'to all forms of warfare and to all kinds of weapons', including 'those of the future'.[5] In the ICRC's view, this finding applies to the use of cyber operations during armed conflict.

---

4 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, 31IC/11/5.1.2, pp. 36-37; available at 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; *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2015, 32IC/15/11, p. 40; available at: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, 33IC/19/9.7, p. 18; available at: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report__EN.pdf.

5 International Court of Justice, Legality of the threat or the use of nuclear weapons, Advisory Opinion, 8 July 1996, para. 86.

The ICRC welcomes that an increasing number of States and international organizations have affirmed that IHL applies to cyber operations during armed conflicts and welcomes discussion on how IHL applies.

States may also decide to impose additional limits to those found in existing law and develop complementary rules, in particular in order to strengthen the protection of civilians and civilian infrastructure against the effects of cyber operation. In the ICRC's view, any new rules need to build on and strengthen the existing legal framework, including IHL.

In cases not covered by existing rules of IHL, civilians and combatants remain protected by the so-called "Martens clause", meaning they remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[6]

It is important to underline that affirming the application of IHL to cyber operations during armed conflict does not legitimize cyber warfare or encourage the militarization of cyberspace. In fact, IHL imposes some limits to the militarization of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL.[7] Moreover, any use of force by States – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law, in particular, the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

## 4. THE PROTECTION AFFORDED BY EXISTING IHL

Existing IHL treaties and customary law provide rules on a number of issues during armed conflict. In cyberspace, the rules on the conduct of hostilities are particularly relevant. These rules aim to protect the civilian population against the effects of hostilities. They are based on the cardinal principle of distinction, which requires that belligerents distinguish at all times between the civilian population and combatants and between civilian objects and military objectives, and direct their operations only against military objectives.[8]

Notwithstanding the interconnectivity that characterizes cyberspace, a careful

---

6 See Art. 1(2) of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I); paragraph 9 of the preamble to the 1899 Hague Convention (II); paragraph 8 of the preamble to the 1907 Hague Convention (IV).

7 See, among others, Henckaerts and Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. I: Rules, ICRC, Cambridge University Press, Cambridge, 2005 (hereinafter ICRC Customary IHL Study), Rules 70 and 71; see also Art. 36 AP I.

8 Art. 48 AP I; Rules 1 and 7 ICRC Customary IHL Study. International Court of Justice, *Legality of the threat or the use of nuclear weapons*, Advisory Opinion, 8 July 1996, para. 78.

examination of the functioning of cyber tools shows that they are not necessarily indiscriminate. Many of the recent cyber attacks that have been reported in public sources appear to have been rather "discriminate" from a technical point of view: they have been designed and actually used to target and harm only specific objects and have not spread or caused harm indiscriminately. Ensuring that cyber operations affect only the targeted object may, however, be technically challenging and require careful planning in their design and use. Moreover, it must be noted that a cyber operation that is technically discriminate is not necessarily lawful, whether during or outside of an armed conflict.

This being said, some known cyber tools have been designed to self-propagate and indiscriminately affect widely used computer systems. They have not done so by chance: the ability to self-propagate needs to be specifically included in the design of such tools. The interconnectivity that characterises cyberspace means that whatever has an interface with the internet can be targeted from anywhere in the world. Moreover, an attack on a specific system may have repercussions on various other systems and cause indiscriminate effects. As a result, there is a real risk that cyber tools are not designed or used – either deliberately or by mistake – in compliance with IHL.

Affirming that IHL – including the principles of distinction, proportionality, and precautions – applies to cyber operations during armed conflicts means that under existing law, among many other rules:

- cyber capabilities that qualify as weapons and are by nature indiscriminate are prohibited;[9]
- direct attacks against civilians and civilian objects are prohibited, including when using cyber means or methods of warfare;[10]
- acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited, including when carried out through cyber means or methods of warfare;[11]
- indiscriminate attacks, namely those of a nature to strike military objectives and civilians or civilian objects without distinction, are prohibited, including when using cyber means or methods of warfare;[12]
- disproportionate attacks are prohibited, including when using cyber means or

[9] Rule 71 ICRC Customary IHL Study.

[10] Arts 48, 51 and 52 AP I; Rules 1 and 7 ICRC Customary IHL Study.

[11] Art. 51(2) AP I; Rule 2 ICRC Customary IHL Study.

[12] Art. 51(4) AP I; Rules 11 and 12 ICRC Customary IHL Study. Indiscriminate attacks are those: (a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) which employ a method or means of combat the effects of which cannot be limited as required by international humanitarian law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

methods of warfare. Disproportionate attacks are those which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[13]

- during military operations, including when using cyber means or methods of warfare, constant care must be taken to spare the civilian population and civilian objects; all feasible precautions must be taken to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare;[14]
- attacking, destroying, removing or rendering useless objects indispensable to the survival of the population is prohibited, including through cyber means and methods of warfare;[15]
- medical services must be protected and respected, including when carrying out cyber operations during armed conflicts.[16]

In addition, all feasible precautions must also be taken to protect civilians and civilian objects against the effects of attacks conducted through cyber means and methods of warfare, which is an obligation that States must already implement in peacetime.[17] Measures that could be considered include, among others: segregating military from civilian cyber infrastructure and networks; segregating computer systems on which essential civilian infrastructure depends from the internet; work on the identification in cyberspace of the cyber infrastructure and networks serving specially protected objects like hospitals.[18]

## 5. THE NEED TO DISCUSS HOW IHL APPLIES

Affirming that IHL applies to cyber operations in armed conflict is an essential first step to avoid or minimize the potential human suffering that cyber operations might cause. However, the ICRC also encourages States to work towards a common understanding of how IHL principles and rules apply to cyber operations. This is necessary because the interconnected nature of cyberspace and its largely digital

---

13 Arts 51(5)(b) and 57 AP I; Rule 14 ICRC Customary IHL Study.

14 Art. 57 AP I; Rules 15 - 21 ICRC Customary IHL Study.

15 Art. 54 AP I; Art. 14 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II); Rule 54 ICRC Customary IHL Study.

16 See, for instance, Art. 19 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GCI); Art. 12 Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GCII); Art. 18 Convention (IV) relative to the Protection of Civilian Persons in Time of War (GCIV); Art. 12 AP I; Art. 11 AP II; Rules 25, 28, 29 ICRC Customary IHL Study.

17 Art. 58 AP I; Rules 22 to 24 ICRC Customary IHL Study.

18 ICRC, *International humanitarian law and the challenges of contemporary armed conflicts,* 2015, p. 43.

character pose challenges for the interpretation of key IHL principles and concepts on the conduct of hostilities.

Among the various issues, in this position paper the ICRC emphasizes three.

## THE MILITARY USE OF CYBERSPACE AND THE EFFECT ON ITS CIVILIAN CHARACTER

Except for some specific military networks, cyberspace is predominantly used for civilian purposes. However, civilian and military networks may be interconnected. Furthermore, military networks may rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping and air traffic controls increasingly rely on navigation satellite systems that may also be used by the military. Civilian logistical supply chains and essential civilian services use the same web and communication networks through which some military communications pass.

Not every use for military purposes renders a civilian object a military objective under IHL.[19] If it does, however, the object is no longer protected by the prohibition to direct attacks on civilian objects. It would be a matter of serious concern if the military use of cyberspace led to the conclusion that many objects forming part thereof would no longer be protected as civilian objects. This could lead to large-scale disruption of the ever-increasingly important civilian usage of cyberspace.

This being said, even if certain parts of the cyberspace infrastructure were no longer protected as civilian objects during armed conflicts, any attack would remain governed by the prohibition of indiscriminate attacks and the rules of proportionality and precautions in attack. Precisely because civilian and military networks are so interconnected, assessing the expected incidental civilian harm of any cyber operation is critical to ensure that the civilian population is protected against its effects.[20]

## THE NOTION OF 'ATTACK' UNDER IHL AND CYBER OPERATIONS

Critical civilian infrastructure enabling the provision of essential services increasingly relies on digitalized systems. Safeguarding such infrastructure and

[19] See Art. 52(2) AP I; Rule 8 Customary IHL Study: "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." For more details on the limits to cyber infrastructure becoming military objectives under IHL, see ICRC, *International humanitarian law and the challenges of contemporary armed conflicts,* 2015, p. 42.

[20] See ICRC, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law,* 2018, available at https://www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality, pp. 37–40.

services against cyber attacks or incidental damage is essential to protect the civilian population.

IHL provides specific protection for certain infrastructure, such as medical services and objects indispensable to the survival of the population, regardless of the type of harmful operation.[21] However, most rules stemming from the principles of distinction, proportionality and precautions – which provide general protection for civilians and civilian objects – apply only to military operations that qualify as 'attacks' as defined in IHL.[22] Article 49 of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'.[23] The question of how widely or narrowly the notion of 'attack' is interpreted with regard to cyber operations is therefore essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.

It is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL. In the ICRC's view, this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply.

Beyond this, attacks that significantly disrupt essential services without necessarily causing physical damage constitute one of the most important risks for civilians. Diverging views exist, however, on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL. In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[24] If the notion of attack is interpreted as only referring to operations that cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities. It is therefore essential that States find a

---

21 See text in relation to footnotes 16 and 15 above. With regard to the latter, they must not be attacked, destroyed, removed or rendered useless.

22 The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of jus ad bellum. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

23 For rules that apply specifically to attacks, see text in relation to footnotes 10 to 14 above.

24 See 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*, 2015, pp. 41-42.

common understanding in order to adequately protect the civilian population against the effects of cyber operations.

### CIVILIAN DATA AND THE NOTION OF 'CIVILIAN OBJECTS'

Essential civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records – are an essential component of digitalized societies. Such data are key to the functioning of most aspects of civilian life, be it at individual or societal level. There is increasing concern about safeguarding such essential civilian data.

Some of the specific protection afforded by IHL extends to essential data, such as data belonging to medical units, which are encompassed in the obligation to respect and protect such units.[25]

More generally, the main IHL principles and rules governing the conduct of hostilities protect civilians and civilian objects.[26]It would therefore be important for States to agree on an understanding that civilian data is protected by these rules.

Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill. Such operations could cause more harm to civilians than the destruction of physical objects. While the question of whether and to what extent civilian data constitute civilian objects remains unresolved, in the ICRC's view the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL. The replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them.[27] Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.

## 6. ATTRIBUTION OF CONDUCT IN CYBERSPACE FOR THE PURPOSES OF STATE RESPONSIBILITY

Cyberspace provides various technical possibilities for actors to hide or falsify their identity, which increases the complexity of attribution by other actors. This creates major difficulties. For example, even during armed conflict, IHL only applies to operations that are linked to the conflict. If the author of a cyber operation – and thus the link of the operation to an armed conflict – cannot be identified, it may be

---

[25] See footnote 16 above.

[26] See text in relation to notes 10 to 15 above.

[27] ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015, p. 43; ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2019, p. 21.

difficult to determine whether IHL is even applicable to the operation. Attribution of cyber operations is also important to ensure that actors who violate international law, including IHL, can be held accountable. The perception that it will be easier to deny responsibility for such attacks may also weaken the taboo against their use – and may make actors less scrupulous about using them in violation of international law.[28]

This being said, attribution is not a problem from the perspective of the actors who conduct, direct or control cyber operations: they have all the facts at hand to determine under which international legal framework they are operating and which obligations they must respect.

Under international law, a State is responsible for conduct attributable to it, including possible violations of IHL. This includes:

- conduct by State organs, including its armed forces or intelligence services;
- conduct by persons or entities, such as private companies, the State empowered to exercise elements of governmental authority;
- conduct by persons or groups, such as militias or group of hackers, acting in fact on the State's instructions, or under its direction or control; and
- conduct by private persons or groups which the State acknowledges and adopts as its own conduct.[29]

## 7. THESE PRINCIPLES APPLY WHETHER THE CONDUCT IS CARRIED OUT BY CYBER OR ANY OTHER MEANS. CONCLUSION

The use of cyber operations as means or methods or warfare in an armed conflict poses a real risk of harm to civilians. For the protection of the civilian population and civilian infrastructure, it is critical to recognize that such operations do not occur in a legal vacuum. The ICRC urges all States to affirm that IHL applies to cyber operations during armed conflicts, on the understanding that such affirmation neither encourages the militarization of cyberspace nor legitimizes cyber warfare.

At the same time, the ICRC believes that further discussion – especially among States – is needed on how IHL should be interpreted and applied in cyberspace. There is a pressing need for such discussion because States that decide to develop or acquire cyber capabilities that qualify as weapons, means and methods of warfare – whether for offensive or defensive purposes – must ensure that these capabilities can be used

---

[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] See Rule 149 ICRC Customary IHL Study. See also *International Law Commission, Responsibility of States for Internationally Wrongful Acts*, 2001, in particular Articles 4 to 11.

in accordance with their obligations under IHL.[30] Discussion should be informed by an in-depth understanding of the development of military cyber capabilities, their potential human cost, and the protection afforded by existing law. States need to determine whether existing law is adequate and sufficient to address the challenges posed by the interconnected and largely digital character of cyberspace, or whether it needs adaptation to the specific characteristics of cyberspace. If new rules are to be developed to protect civilians against the effects of cyber operations or for other reasons, they should build on and strengthen the existing legal framework – including IHL.

The ICRC welcomes the intergovernmental discussions currently taking place in the framework of two United Nations General Assembly mandated processes and it is grateful for the opportunity to share its views with the participating States. The ICRC also stands ready to lend its expertise to such discussions, as States deem appropriate.

[30] See ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2019, p. 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; Art. 36 AP I.

## ЦЕЛИ И ЗАДАЧИ МККК

МККК помогает людям, пострадавшим от вооруженных конфликтов и других ситуаций насилия по всему миру, делая все возможное, чтобы защитить их жизнь и достоинство и облегчить их страдания, часто в сотрудничестве со своими партнерами по Движению Красного Креста и Красного Полумесяца. Пропагандируя и укрепляя гуманитарное право, отстаивая универсальные гуманитарные принципы, организация стремится предотвратить страдания людей.

Люди знают, что могут рассчитывать на МККК, который осуществляет самые разные виды деятельности, спасая жизни в зонах конфликтов, и тесно сотрудничает с местным населением с тем, чтобы понимать и удовлетворять его потребности. Опыт и знания МККК позволяют ему реагировать быстро и эффективно, не отдавая предпочтения ни одной из сторон.

facebook.com/ICRCRu
twitter.com/MKKK
vk.com/icrc_rus

**Международный Комитет Красного Креста**
19, avenue de la Paix
1202, Женева, Швейцария
T +41 22 734 60 01
shop.icrc.org

**Русская версия издания подготовлена Региональной делегацией МККК в России, Беларуси и Молдове**
129090, Москва, Грохольский пер. 13, стр. 1
T +7 495 626 54 26 moscow@icrc.org


МККК