Санкт-Петербургский государственный университет

Уровень образования:

Направление 40.04.01 «Юриспруденция»

Основная образовательная программа BM.5814

«Международное публичное право»

***Книжникова Злата Сергеевна***

Выпускная квалификационная работа

**Предотвращение ущерба гражданскому населению**

**от военных киберопераций**

**во время вооруженных конфликтов**

**Научный руководитель**:

доцент кафедры международного права,

кандидат юридических наук

**Иваненко Виталий Семенович**

**Научный консультант:**

советник, Департамент права и политики, Международный Комитет Красного Креста

**Кушлейко Анастасия Станиславовна**

**Рецензент:**

Ведущий юрисконсульт ПАО «МТС-Банк»,

**Сидорова Мария Евгеньевна**

Санкт-Петербург

2023

ОГЛАВЛЕНИЕ

[**ВВЕДЕНИЕ** 3](#_Toc135258059)

[**ГЛАВА 1. ПРИМЕНИМОСТЬ НОРМ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА К КИБЕРОПЕРАЦИЯМ** 7](#_Toc135258060)

[1.1. Понятие киберопераций 7](#_Toc135258061)

[1.2. Кибероперации в международном вооруженном конфликте 1](#_Toc135258062)

[1.3. Кибероперации в немеждународном вооруженном конфликте 1](#_Toc135258063)

[1.4. Кибероперации в случаях, когда ситуация не достигла 7](#_Toc135258064)

[степени конфликта 7](#_Toc135258065)

[**ГЛАВА 2. ИСПОЛЬЗОВАНИЕ КИБЕРОПЕРАЦИЙ В ХОДЕ КОНФЛИКТА** 10](#_Toc135258066)

[2.1. Кибероперации против гражданского населения 10](#_Toc135258067)

[2.2 Кибероперации против гражданских объектов 18](#_Toc135258068)

[**ГЛАВА 3. СПОСОБЫ ПРЕДОТВРАЩЕНИЯ УЩЕРБА ГРАЖДАНСКОМУ НАСЕЛЕНИЮ ОТ ВОЕННЫХ КИБЕРОПЕРАЦИЙ** 32](#_Toc135258069)

[**ЗАКЛЮЧЕНИЕ** 40](#_Toc135258070)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 44](#_Toc135258071)

# **ВВЕДЕНИЕ**

**Актуальность темы исследования.** Государства всегда использовали информацию для достижения политических и экономических целей, поэтому конфликты никогда не ограничивались военной сферой. Учитывая быстрый прогресс в области военных информационно-коммуникационных технологиях (*далее – ИКТ*), киберпространство является идеальным местом для проведения различных операций, возможно даже более привлекательным, чем реальное место боя. Киберпространство предлагает многочисленные возможности для такого проведения, от манипулирования и кражи персональных данных до вмешательства в работу ИКТ противника.

В течение многих лет эксперты выражали обеспокоенность тем, что критически важные инфраструктуры уязвимы для киберопераций практически в любой точке мира. Удаленно передаваемые вредоносные программы и вирусы могут поставить под угрозу взаимосвязанные энергосистемы, аэропорты, больницы, военные системы и в целом любой объект, где подключенные к Интернету компьютеры используются для управления критически важными функциями. Уже сейчас в литературе отмечается, что вопросы безопасности от незаконных действий, нарушающих целостность, доступность и конфиденциальность информации в киберпространстве, которые могут нанести ущерб информационным ресурсам и системам связи, станут центральной темой в цифровом мире[[1]](#footnote-1). Особую озабоченность вызывает использование киберпространства для продвижения конкретных политических, социальных и военных целей.

Нельзя не согласиться со следующим высказыванием В.В. Путина: «Вопрос с кибербезопасностью является одним из самых важных на сегодняшний день, потому что всякие отключения целых систем ведут к очень тяжелым последствиям, а это, оказывается, возможно»[[2]](#footnote-2). Аналогичную позицию занимает и Международный Комитет Красного Креста (далее – МККК), который обеспокоен потенциальными гуманитарными последствиями растущего использования киберопераций во время вооруженных конфликтов[[3]](#footnote-3). Безусловно, международное гуманитарное право (далее – МГП) может применяться и в киберпротсранстве, однако защищает ли оно в полной мере гражданское население и гражданскую инфраструктуру? Для ответа на эти вопросы необходимо провести комплексное исследование, изучив, что понимается под «кибероперацией», как МГП работает в международном и немеждународном вооруженном конфликте, а также проанализировать, как право защищает гражданское население от киберопераций.

**Цель и задачи исследования**. Целью настоящего исследования является анализ основных проблем, существующих в рамках предотвращения ущерба гражданскому населению от военных кибереропераций во время вооруженных конфликтов, и предложения о путях и способах их решения.

Для достижения указанной цели поставлены **следующие задачи**:

1) Проанализировать нормы международного гуманитарного права на предмет возможности их применения к различным вооруженным конфликтам, происходящим в контексте киберпространства;

2) Изучить существующую практику государств по защите гражданского населения в рамках проведения киберопераций;

3) На основе проведенного анализа разработать предложения по предотвращению ущерба гражданскому населению от военных кибереропераций во время вооруженных конфликтов.

**Объектом настоящего исследования** являются общественные отношения, связанные с защитой гражданского населения от последствий кибеопераций, осуществляемых в рамках вооруженных конфликтов.

**Предметом исследования являются**:

1) применение права вооруженных конфликтов к киберпространству;

2) правовая квалификация кибератаки;

3) применение принципов МГП к киберпространству;

4) ограничение средств и методов ведения военных действий в целях защиты гражданского населения;

5) способы предотвращения ущерба гражданскому населению.

**Теоретическая значимость исследования обусловлена** тем, что многие исследования посвящены общему анализу проблемы применения норм МГП к киберпространству, либо отдельно взятым проблемам в данной сфере и не затрагивают таких узких вопросов как различные способы предотвращения ущерба гражданскому населению от военных кибереропераций во время вооруженных конфликтов. Кроме того, данный вопрос является мало разработанным как в зарубежной доктрине, так и в российской, а научные статьи и диссертационные исследования посвящены в основном применению международного гуманитарного права к кибероперациям, а не вопросам предотвращения ущерба гражданскому населению от военных киберопераций.

В своем исследовании автор опирался на работы отечественных и зарубежных ученых в области теории международного права и специальные работы по рассматриваемой проблеме.

С.И. Кузнецов, В.В. Анисимов, С.П. Тесля и И.В. Морозов изучали вопрос о том, какие действия могут считаться кибероперациями, а также отдельно рассмотрели вопрос о кибероперациях, используемых в вооруженных конфликтах[[4]](#footnote-4).

В.Н. Русинова проанализировала вопрос о том, можно ли вредоносное использование ИКТ рассматривать в качестве «вооруженного нападения»[[5]](#footnote-5).

П.В. Навиченок изучал проблемы ответственности государств за кибероперации во время вооружённого конфликта, а также отражал способы совершения кибератак. Он отметил в исследовании, что необходимо регулировать ответственность государств за кибероперации, поскольку в процессе их осуществления происходит хищение информации в огромных объемах, а также постоянно появляются новые способы совершения данных атак[[6]](#footnote-6).

В. Ю. Фицнер исследовала вопрос о применимости норм международного гуманитарного права при ведении военных действий в киберпространстве, а также она анализировала, какие кибероперации являются нападениями в соответствии с правом вооруженных конфликтов[[7]](#footnote-7).

В. Н. Плакса также посвятил исследование вопросам применимости норм и принципов международного гуманитарного права при использовании новых технологий ведения военных действий[[8]](#footnote-8).

Автором также были проанализированы работы таких иностранных ученых, как К. Дрёге, М. Н. Шмитт, Дж. Р. Хитон, Г. Корн, П. Паскуччи, Д. Фидлер, Н. Мельзер и др.

Несмотря на многочисленные исследования на эту тему, научных работ, посвященных комплексному, углубленному и последовательному анализу проблем, возникающих по вопросу предотвращения ущерба гражданскому населению от военных кибереропераций во время вооруженных конфликтов, в российской доктрине международного права не проводилось.

Практическая значимость: выводы, сделанные в настоящем исследовании, могут быть использованы как государственными органами, так и негосударственными субъектами при планировании/оценивании их деятельности в киберпространстве.

# **ГЛАВА 1. ПРИМЕНИМОСТЬ НОРМ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА К КИБЕРОПЕРАЦИЯМ**

## **1.1. Понятие киберопераций**

Как справедливо отметил С. Ю. Гаркуша-Божко, «в современном мире вооруженный конфликт в киберпространстве перестал быть выдумкой писателей-фантастов – теперь это потенциально возможный конфликт, который может начаться из-за столкновения интересов двух и более государств в киберсфере»[[9]](#footnote-9). Рассматривая содержание понятия кибероперации, нельзя не упомянуть тот факт, что само явление киберпространства, несмотря на его частые обсуждения и комментарии, все еще плохо изучено[[10]](#footnote-10). Международный комитет Красного Креста (далее – МККК) отмечает, что кибероперации стали реальностью в условиях современных вооруженных конфликтов[[11]](#footnote-11), хотя большая часть его норм создавалась достаточно давно[[12]](#footnote-12). Вследствие этого возникают трудности в понимании такого явления как «кибероперации».

Для начала, следует понять, что понимается под «киберпространством» в целом. При этом, не следует отождествлять Интернет и киберпространство[[13]](#footnote-13)

В наиболее полной форме киберпространство можно описать с помощью пяти взаимосвязанных (под)слоев[[14]](#footnote-14). Базис составляет географический слой, то есть физическое расположение физических элементов (объектов и людей) сети. Как следствие, эти физические элементы подчиняются правовым системам, в том числе юрисдикциям различных государств. Далее идет физический сетевой уровень со связанным аппаратным обеспечением и физической инфраструктурой, такой как компьютеры, маршрутизаторы, кабели, серверы и т. д., другими словами: материальные объекты. Поверх упомянутых двух слоев «реального мира» идут два виртуальных слоя. Во-первых, логический уровень, включающий в себя операционные системы, приложения, другое программное обеспечение и данные, информацию и контент[[15]](#footnote-15). Во-вторых, уровень киберперсонажа с его адресами электронной почты, учетными записями в социальных сетях и т. д., а также идентификаторами умного дома и электросети[[16]](#footnote-16).

П. Розенцвейг полагает, что представление киберпространства в виде набора виртуальных и физических уровней позволяет правильно понять кибероперации и связанные с ними юридические аспекты. Такую точку зрения можно объяснить, лишь взглянув на оперативные параметры цели, средства и методы, эффекты[[17]](#footnote-17), ведь кибероперации могут служить различным целям или задачам, начиная от сбора информации, обмана и сдерживания и заканчивая разрушением[[18]](#footnote-18).

Следует отметить, что кибероперации часто называют кибервойной[[19]](#footnote-19). Однако некоторые авторы отмечают, что кибервойна представляет собой более узкую форму киберопераций[[20]](#footnote-20). Государства[[21]](#footnote-21), неправительственные организации (МККК)[[22]](#footnote-22) и различные ученые[[23]](#footnote-23) предпринимали попытки к определению данного термина, однако все сводилось к смешению кибервойны или войны и кибер-операции или операций в киберпространстве.

Так, например, МККК понимает «кибервойну» и «кибероперацию» как операции против компьютера, компьютерной системы или сети, или другого подключенного устройства, через поток данных, когда они используются в качестве средства или метода ведения войны в контексте вооруженного конфликта[[24]](#footnote-24). Кибервойна поднимает вопросы о том, как именно некоторые положения международного гуманитарного права (МГП) применяются к этим операциям, покрывают ли нормы МГП все возможные вариации киберопреций и их последствий или его положения могут потребовать дальнейшего развития с целью освещения новых пятен в области кибервойны.

В свою очередь в научной литературе под «военными кибероперациями» понимается «использование вооруженными силами кибернетических возможностей с основной целью достижения военных целей в киберпространстве или с его использованием»[[25]](#footnote-25).

При определении содержания понятия «кибероперации»[[26]](#footnote-26) можно увидеть три основных подхода. Первый фокусируется на виртуальном, цифровом и логическом уровнях, в основном концентрируясь на данных и программном обеспечении[[27]](#footnote-27). Второй подход также признает физический уровень с материальной инфраструктурой ИКТ, используемой для связи и соединения[[28]](#footnote-28), а некоторые также признают социальный слой с людьми как частью киберпространства[[29]](#footnote-29). Указанные подходы нашли отражение в многоуровневых представлениях киберпространства, используемых некоторыми государствами[[30]](#footnote-30).

Кибероперации отличаются от кинетических или информационных операций, поскольку они направлены против виртуальных слоев киберпространства: они непосредственно воздействуют на кибер-объекты и/или кибер-субъектов[[31]](#footnote-31).  Однако они могут также производить вторичные физические эффекты, косвенно воздействуя на людей, физические объекты на физическом сетевом уровне и физические объекты за пределами киберпространства[[32]](#footnote-32).

Д. Мюррей делит кибероперации на две широкие категории: кибероперации, включающие деятельность по мониторингу, и кибероперации, включающие деятельность, основанную на воздействии[[33]](#footnote-33). Первые собирают информацию, но никоим образом не изменяют и не вмешиваются в нее, т.е. своего рода пассивные операции. К ним можно отнести массовый сбор информации, например, посредством прослушивания или копирования; скрытая установка программного обеспечения и проч. Кибероперации, основанные на эффектах, - те операции, которые дают ощутимый эффект либо в киберпространстве, либо в материальном мире. Они могут повредить, уничтожить или изменить данные или помешать нормальной работе системы. Ярким примером является червь *Stuxnet,* который (а) повлиял на частоту вращения двигателя целевых центрифуг, что привело к их физическому повреждению, и (б) вмешался в программное обеспечение[[34]](#footnote-34).

Следует отметить, что в литературе также рассматривается два вида киберопераций – кибератака и киберэксплуатация. Под *киберэксплуатацией* понимается несанкционированный доступ к компьютерам, компьютерным системам или сетям с целью извлечения информации, но без ущерба для функциональности системы, к которой осуществляется доступ, или изменения/удаления содержащихся в ней данных[[35]](#footnote-35). Как было замечено, «основное техническое различие между кибератакой и киберэксплуатацией заключается в характере выполняемой полезной нагрузки — полезная нагрузка кибератаки является разрушительной, тогда как полезная нагрузка киберэксплуатации получает информацию неразрушающим образом»[[36]](#footnote-36). Хотя в прессе они часто обозначаются как «кибератаки», операции по киберэксплуатации отличаются тем, что они не влияют на работу системы. Они сосредоточены на сборе разведданных, наблюдении и рекогносцировке, а не на разрушении системы, и могут предшествовать кинетической операции или кибератаке, которую они стремятся осуществить, например, путем сопоставления архитектуры сети или операционной системы, подлежащей атаке, или путем выявления ранее неизвестных уязвимостей.

Под «кибератаками» понимаются кибероперации, будь то в целях нападения или защиты, предназначенные для изменения, удаления, искажения или отказа в доступе к компьютерным данным или программному обеспечению в целях (а) пропаганды или обмана; и/или (б) частичного или полного нарушения функционирования компьютерной системы или сети и связанная с ними управляемая компьютером физическая инфраструктура (если таковая имеется); и/или (c) причинение физического ущерба, внешнего по отношению к компьютеру, компьютерной системе или сети[[37]](#footnote-37).

Кибератака может варьироваться от относительно безобидных «психологических» операций, таких как порча веб-сайта, до действий, которые вызывают хаос в военных кампаниях путем распространения дезинформации, или даже действий, приводящих к серьезному нарушению работы служб и материальному ущербу имуществу, и гибели людей. Во всех случаях кибератака включает в себя действие в виде нападения или защиты, которое осуществляется в киберпространстве или через него, хотя и не обязательно через сеть, и может быть нацелено либо на информационные системы, либо на системы управления инфраструктурой[[38]](#footnote-38). В этой связи следует согласиться с позицией С. Ю. Гаркуша-Божко, который отметил, что «логично квалифицировать кибератаки в качестве нападения даже в том случае, когда они привели к временному нарушению нормального функционирования инфраструктуры без ее физического разрушения или повреждения»[[39]](#footnote-39).

Наиболее часто используемыми методами проведения кибератаки являются повреждение аппаратного обеспечения («чипирование») или программного обеспечения, или затопление системы таким количеством информации, что это приводит к ее краху. Популярными программными средствами, предназначенными для вмешательства в нормальное функционирование компьютера, являются троянские кони, логические бомбы, вирусы и черви, которые могут быть установлены в компьютер путем чипирования, взлома, через портативное запоминающее устройство или путем непреднамеренной загрузки их с веб-сайта или вложения электронной почты[[40]](#footnote-40).

*Вирус* – это самовоспроизводящаяся программа, которая обычно присоединяется к законной программе на целевом компьютере, модифицируя ее и впоследствии воздействуя на другие программы и, если компьютер подключен к сети, потенциально также на другие компьютеры. Вирус обычно несет полезную нагрузку, представляющую собой код, который повреждает или удаляет компьютерные данные на зараженном компьютере.

*Червь* полностью реплицируется на другие компьютеры, но, в отличие от вирусов, обычно не изменяет другие программы: он захватывает адреса целевого компьютера и повторно рассылает сообщения по всей системе, что приводит к общему замедлению работы системы и, возможно, к сбою. В отличие от вируса, червь может распространяться без вмешательства человека[[41]](#footnote-41). Вирусы и черви могут быть скрыты в *троянских конях,* внешне безобидном фрагменте кода, который на самом деле скрывает вредоносную программу или позволяет внешнему пользователю осуществлять удаленный доступ к компьютеру.

*Логические бомбы* – это разновидность троянского коня, предназначенного для запуска в определенное время или при определенных обстоятельствах, соответственно. Атаки типа «отказ в обслуживании» (DoS), примером которых являются «флуд-атаки», отличаются тем, что они обычно не проникают в систему, а направлены на то, чтобы завалить цель чрезмерными вызовами, сообщениями, запросами или запросами, чтобы перегрузить ее и принудительно закрыть[[42]](#footnote-42). Постоянные DoS-атаки это особенно серьезные атаки, которые повреждают систему и вызывают ее замену или переустановку оборудования. Когда DoS-атака осуществляется большим количеством компьютеров, организованных в ботнеты, это называется DDoS-атакой.

Таким образом, кибероперации могут принимать разные формы, но в любых вооруженных конфликтах стороны будут использовать их в качестве средства или метода ведения войны для совершения как операции против компьютера, компьютерной системы или сети.

## **1.2. Кибероперации в международном вооруженном конфликте**

Общепринятые критерии наличия международного вооруженного конфликта, которые отражают обычное международное право, вытекают из общей статьи 2 Женевских конвенций 1949 года[[43]](#footnote-43). Статья предусматривает: «настоящая Конвенция будет применяться в случае объявленной войны или всякого другого вооруженного конфликта, возникающего между двумя или несколькими Высокими Договаривающимися Сторонами, даже в том случае, если одна из них не признает состояния войны. Конвенция будет применяться также во всех случаях оккупации всей или части территории Высокой Договаривающейся Стороны, даже если эта оккупация не встретит никакого вооруженного сопротивления».

Существование международного вооруженного конфликта рассматривается как объективный факт, вытекающий из вооруженного столкновения между силами двух государств и не зависящий от того, как квалифицирует это столкновение та или иная сторона[[44]](#footnote-44).

Любой спор, возникающий между двумя государствами и вызывающий введение в действие вооруженных сил, является вооруженным конфликтом по смыслу ст. 2, даже если одна из сторон оспаривает наличие состояния войны. Ни длительность конфликта, ни степень разрушительности не играют никакой роли[[45]](#footnote-45).

В определенных случаях даже действия негосударственного субъекта – организованной вооруженной группы – могут быть присвоены государству, если находится под «общим контролем» государства. Вопрос о том, могут ли действия негосударственной организованной вооруженной группы против одного государства быть приписаны другому государству, так что конфликт признается международным, был прямо рассмотрен в решении Апелляционной камеры Международного уголовного трибунала по бывшей Югославии по делу *Тадича*[[46]](#footnote-46).

Апелляционная камера сформулировала критерий «общего контроля», когда анализировала действия боснийских сербов и могут ли их действия присваиваться Союзной Республике Югославия, чтобы сделать вывод о существовании международного вооруженного конфликта[[47]](#footnote-47). Так, контроль государства над подчиненными вооруженными силами, ополченцами или военизированными формированиями может носить общий характер (и должен включать нечто большее, чем простое предоставление финансовой помощи или военного снаряжения или обучение). При этом от государства также не требуется выдавать конкретные распоряжения или руководить каждой отдельной операцией.

Считается, что государство осуществляет общий контроль, когда играет определенную роль в организации, координации или планировании военных действий военной группы, в дополнение к финансированию, обучению и оснащению или предоставлению оперативной поддержки к этой группе[[48]](#footnote-48).

Международный суд ООН[[49]](#footnote-49) и Международный уголовный суд[[50]](#footnote-50) отмечают, что тест на общий контроль является достаточным для определения квалификации международного вооруженного конфликта. Однако следует иметь в виду, что простой финансовой поддержки недостаточно для того, чтобы признать конфликт международным. Апелляционная камера в деле *Тадича* установила, что финансирование государством, подготовка, оснащение и предоставление оперативной поддержки негосударственной группе не были, помимо прочего, достаточными для того, чтобы охарактеризовать ситуацию между двумя заинтересованными государствами как международную[[51]](#footnote-51). Если поддержка государства не достигает уровня общего контроля, то вмешательство не может быть присвоено государству.

Аналогично в *Таллиннском руководстве* Группа экспертов согласилась с тем, что международный вооруженный конфликт возникает всякий раз, когда между двумя или более государствами происходят военные действия, которые могут включать кибероперации или ограничиваться ими[[52]](#footnote-52).

В *Таллиннском руководстве* Группа экспертов рассмотрела следующий пример. Операция *Stuxnet* 2010 года против систем *SCADA* в Иране, в результате которой были физически повреждены центрифуги на заводе по переработке ядерного топлива, иллюстрирует трудность принятия окончательного решения. Международная группа экспертов разделилась во мнениях относительно того, достаточен ли ущерб для соответствия критерию вооруженности. Определение характеристик было дополнительно осложнено тем фактом, что остаются вопросы относительно того, проводилась ли операция *Stuxnet* государством или отдельными лицами, чье поведение приписывается государству, в целях установления международного вооруженного конфликта.

Как показал инцидент со *Stuxnet*, на пути окончательного вывода о том, что кибероперация привела к международному вооруженному конфликту, стоят значительные юридические и практические проблемы. На сегодняшний день ни один международный вооруженный конфликт не был публично охарактеризован как спровоцированный исключительно в киберпространстве. Тем не менее, Международная группа экспертов согласилась с тем, что кибероперации сами по себе потенциально могут перешагнуть порог международного вооруженного конфликта[[53]](#footnote-53).

## **1.3. Кибероперации в немеждународном вооруженном конфликте**

Право немеждународного вооруженного конфликта (далее – НМВК) применяется ко всем вооруженным конфликтам, не имеющим международного характера[[54]](#footnote-54). Как было установлено в деле *Тадича*, НМВК представляет собой ситуацию «длительного вооруженного насилия между правительственными властями и организованными вооруженными группами или между такими группами внутри государства»[[55]](#footnote-55). Правило 23 Таллиннского руководства также использует определение МТБЮ и адаптирует его к киберконтексту[[56]](#footnote-56).

Классическое установление наличия НМВК основывается на двух факторах - интенсивности боевых действий и организации негосударственной группы[[57]](#footnote-57). Считается, что эти же критерии применимы в ситуациях, включающих кибероперации[[58]](#footnote-58). В комментарии к 1 ЖК отмечается, что «для определения существования немеждународного вооруженного конфликта, включающего кибероперации, применяются те же критерии, что и в отношении кинетического насилия»[[59]](#footnote-59).

Во-первых, боевые действия между сторонами должны достичь определенного уровня интенсивности, на что может указывать, среди прочих факторов, серьезность и частота нападений и военных столкновений, масштабы разрушений или развертывание правительственных вооруженных сил[[60]](#footnote-60). В контексте киберпространства группа может рассматриваться в качестве «вооруженной», «если она имеет возможность совершать кибератаки»[[61]](#footnote-61).

Cогласно Таллиннскому руководству, «постоянные, хотя и не непрерывные кибератаки, происходящие в течение относительно определенного периода, могут быть охарактеризованы как затяжные»[[62]](#footnote-62). Относительно того, могут ли многочисленные атаки в совокупности достичь минимального уровня интенсивности, зависит от обстоятельств каждого конкретного дела[[63]](#footnote-63). Что касается подрывных киберопераций, не приводящих к физическим последствиям, то, вероятно, только многочисленные скоординированные кибероперации, осуществляемые в течение длительного времени и серьезно нарушающие функционирование нескольких или всех критических инфраструктур государства, в значительной степени зависящего от цифровых технологий, могут рассматриваться как достижение требования «интенсивности», необходимого для применения права НМВК в отсутствие сопутствующих кинетических боевых действий[[64]](#footnote-64).

Во-вторых, негосударственная группа должна иметь определенный минимальный уровень организации, показателями которого могут быть наличие командной или руководящей структуры, способность определять единую военную стратегию и выступать единым фронтом, соблюдение военной дисциплины, а также способность соблюдать МГП[[65]](#footnote-65).

Если критерий организации еще может быть гипотетически выполнен негосударственным субъектом в киберпространстве, то возникает вопрос с определением того, когда кибероперации достигнут требуемого порога «интенсивности». Отмечается, что сами по себе кибероперации лишь в редких случаях будут соответствовать необходимому уровню интенсивности, чтобы рассматриваться в качестве НМПК[[66]](#footnote-66). Поэтому далее в работе будут рассматриваться кибероперации, проводимые в контексте уже начатого НМВК. Указанные операции также подпадают под действие *jus in bello*, применимого к этому типу конфликтов, в той мере, в какой они связаны с таким конфликтом[[67]](#footnote-67).

Кроме того, стоит отметить, что те же проблемы, которые были упомянуты в отношении международных вооруженных конфликтов, применимы также и по отношению к НМВК. Как справедливо отмечает В.Н. Русинова, «большинство известных киберопераций не достигали минимального порогового уровня, который позволил бы квалифицировать их в качестве хотя бы простого «применения силы»[[68]](#footnote-68). Более того, трудности с НМВК и кибер-операциями в их контексте сводятся к тому, что может быть сложно провести различие между кибероперациями, приравниваемыми к актам военных действий, и обычными преступлениями. Другая проблема состоит в том, что, в отличие от государств и международных организаций, не существует правил присвоения действий или бездействия вооруженным группировкам[[69]](#footnote-69). Ученые отмечают, что, по крайней мере, некоторые положения об ответственности государств могут быть применены по аналогии к вооруженным группам, имеющим структуру, подобную государству[[70]](#footnote-70). В отношении других вооруженных групп было высказано предположение о том, что эффективный контроль группы над отдельными членами определяет ответственность группы[[71]](#footnote-71).

*Право, применимое к кибероперациям в рамках НМВК*

Общая статья 3 Женевских конвенций 1949 г. является основополагающим положением, принятым для применения «в случае вооруженного конфликта немеждународного характера, происходящего на территории одной из Высоких Договаривающихся Сторон»[[72]](#footnote-72). В деле «Военная и полувоенная деятельность в Никарагуа и против нее (Никарагуа против Соединенные Штаты Америки)» Международный суд ООН установил, что «общая статья 3 отражает "элементарные соображения гуманности" и представляет собой "минимальный критерий", применимый ко всем вооруженным конфликтам[[73]](#footnote-73). Поскольку указанная статья обычно понимается как отражающая обычное МГП[[74]](#footnote-74), ограничение ее применения только государствами-участниками Женевских конвенций уже устарело.

Тот факт, что кибероперации происходят в киберпространстве и посредством него, а не, строго говоря, на «территории» государства, не препятствует применению общей статьи 3, если рассматривать кибероперации как «сведение информации к электронному формату и фактическое перемещение этой информации между физическими элементами кибер-инфраструктуры»[[75]](#footnote-75) различных воюющих сил.

Общая статья 3 развивается и дополняется положениями Дополнительного протокола II (далее - ДП II), к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв немеждународных вооруженных конфликтов[[76]](#footnote-76). Проблема применения протокола заключается в том, что то или иное воюющее государство должно быть его участником[[77]](#footnote-77). Например, в конфликте между правительством Шри-Ланки и военизированным движением «Тигры освобождения Тамил-Илама», Шри-Ланка не являлась стороной ДП II[[78]](#footnote-78), поэтому применимым правом была только статья 3 и общее международное гуманитарное право. Кроме того, Протокол не применяется в ситуации НМВК, который существует между вооруженными группами внутри одного государства[[79]](#footnote-79).

Кроме того, критерии, при соблюдении которых возможно применение ДП II, отличаются от тех, что необходимы при применении общей статьи 3. Согласно МТБЮ, степень организации, необходимая для проведения «устойчивых и согласованных военных операций», выше, чем та, которая требуется для участия в «длительном насилии» для целей общей статьи 3[[80]](#footnote-80). Действительно, «общая статья 3 отражает основные гуманитарные меры защиты, и стороне вооруженного конфликта требуется лишь минимальная степень организации для обеспечения их применения»[[81]](#footnote-81). Более высокая степень организации, которой должна обладать вооруженная группа согласно ДП II, вытекает из более подробных правил, содержащихся в нем, которые требуют стабильного территориального контроля для его применения[[82]](#footnote-82).

Если вышеуказанные требования применяются в киберконтексте, то следует отметить, что ДП II вряд ли в этом случае когда-либо распространится на отдельные кибер-операции между правительством и вооруженной группой, существующей только в Интернете. В частности, некоторые авторы высказывают предположение о том, что будет трудно представить, как такая группа сможет обеспечить дисциплину и получить территориальный контроль только с помощью киберсредств[[83]](#footnote-83). Однако авторы отмечают, что с учетом современных технологических достижений в области ведения войны способность проводить «устойчивые и согласованные» военные операции не обязательно зависит от контроля над территорией[[84]](#footnote-84).

В этом ключе также важно отметить позицию некоторых авторов, которые отмечают, что «разница в пороговых значениях [между Общей статьей 3 и ДП II] в значительной степени теряет свою актуальность, поскольку большинство, если не все, нормы ДП II были перенесены на НМВК в рамках обычного права»[[85]](#footnote-85). Указывается, что если принять эту точку зрения, то обычные нормы ДП II будут применяться к кибероперациям на тех же более широких условиях, которые были выделены в отношении Общей статьи 3[[86]](#footnote-86).

Примеры применения киберопераций встречаются в практике государств. Например, относительно вооруженных конфликтов в Чечне в 1994 – 1996 гг.[[87]](#footnote-87), а также в 1999 г., которые квалифицировались многими в качестве немеждународных[[88]](#footnote-88), исследователи отмечали, что как во время первого, так и второго конфликта, прочеченские и пророссийские силы вели виртуальную войну в Интернете одновременно с их конфликтом на местах[[89]](#footnote-89). Чеченское сепаратистское движение, в частности, считается неким первооткрывателем в использовании Интернета в качестве инструмента для распространения мощных пиар-сообщений[[90]](#footnote-90). Сроки и изощренность, по крайней мере, некоторых нападений, наводили исследователей на мысль о причастности государства. Например, сайт kavkaz.org (сервера которого были размещены в США), как сообщается, был отключен одновременно со штурмом российским спецназом московского театра на Дубровке с мюзиклом «Норд-Ост», осажденного чеченскими террористами[[91]](#footnote-91).

Аналогично в конфликте между правительством Шри-Ланки и военизированным движением «Тигры освобождения Тамил-Илама», который рассматривался в качестве немеждународного[[92]](#footnote-92), использовались кибероперации для ослабления сил противника. Так, в 1997 г. «Тигры» провели ряд киберопераций по отключению серверов и систем электронной почты посольств Шри-Ланки[[93]](#footnote-93).

Утверждается также, что Сирийское правительство использует кибернетические возможности против повстанцев с начала 2012 г. Однако эти операции, по сути, представляют собой киберэксплуатацию, направленную на получение доступа к личной информации[[94]](#footnote-94).

## **1.4. Кибероперации в случаях, когда ситуация не достигла**

## **степени конфликта**

В упомянутом выше деле *Тадича* было отмечено, что закрепление элементов НМВК, позволяет отличить «вооруженный конфликт от бандитизма, неорганизованных и кратковременных восстаний или террористической деятельности, которые не подпадают под действие международного гуманитарного права»[[95]](#footnote-95). Таким образом, если какая-либо ситуация внутренней напряженности не имеет упомянутых выше критериев, то отличительной чертой рассматриваемых в ее контексте киберопераций будет то, что они не попадают под регулирование норм МГП. В этом ключе на них будет распространяться право прав человека и национальное законодательство.

МККК в комментарии 1973 года к проектам дополнительных протоколов к Женевским конвенциям привел другие примеры внутренних беспорядков и напряженности, не достигших порога немеждународного вооруженного конфликта:

– беспорядки, то есть все хаотичные действия, которые с самого начала не направляются каким-либо лидером и не имеют согласованных действий;

– изолированные и спорадические акты насилия, в отличие от военных операций, проводимых вооруженными силами или организованными вооруженными группами;

– другие акты аналогичного характера, которые влекут, в частности, массовые аресты лиц из-за их поведения или политических убеждений[[96]](#footnote-96).

В контексте киберпространства, например, Германия согласилась с подходом, предложенным *Таллинским руководством* о том, что такие действия, как «крупномасштабное вторжение в иностранные киберсистемы, значительная кража данных, блокировка интернет-сервисов и взлом правительственных каналов или веб-сайтов, как правило, сами по себе не приводят к немеждународному вооруженному конфликту»[[97]](#footnote-97).

В свете вышеизложенного применение силы государством против кибератак, равносильных «актам насилия» со стороны неорганизованных хакеров, может квалифицироваться как борьба с внутренними беспорядками. Тот же вывод будет иметь место и в отношении применения силы правительством против кибератак, приравниваемых к «актам насилия» со стороны организованной вооруженной группы, если такие атаки не достигают интенсивности, необходимой для того, чтобы быть вооруженным конфликтом. Если применение силы правительством является превентивной мерой для поддержания правопорядка, то ситуацию следует квалифицировать как внутреннюю напряженность.

DDoS-атаки 2007 года против Эстонии нельзя отнести ни к одной описанной выше ситуации, поскольку атаки не были «актами насилия» в описанном выше смысле, и эстонское правительство не использовало кинетическую или кибернетическую силу для реагирования на них: вместо этого использовались пассивная киберзащита и уголовные расследования[[98]](#footnote-98).

В контексте упомянутого применения права прав человека стоит отметить, что угроза правам человека заключается не в кибератаках, которые государство пытается предотвратить или контролировать[[99]](#footnote-99). Наоборот, некоторые авторы утверждают, что угроза заключается в посягательстве такого государства на «пространство прав» в киберпространстве, особенно на права на неприкосновенность частной жизни, свободу выражения мнения, и свободу собраний[[100]](#footnote-100).

Подводя итог, стоит отметить, что кибероперации подпадают под действие права вооруженных конфликтов в тех ситуациях, когда они происходят в контексте международного или немеждународного вооруженного конфликта и квалифицируются как акты военных действий, или когда они сами по себе приравниваются к международному или немеждународному вооруженному конфликту. Когда же кибероперации не достигают установленных МГП критериев, то их регулирование будет ограничиваться национальным законодательством государств и правом прав человека.

Кроме того, несмотря на применимость МГП к киберпространству, следует согласиться с А.А. Данельян в том, что в настоящее время требуется универсализация существующего международно-правового регулирования применительно к киберпространству «с учетом его определенной специфики и в целях эффективного правового противодействия использованию информационно-коммуникационных технологий в незаконных целях»[[101]](#footnote-101).

# **ГЛАВА 2. ИСПОЛЬЗОВАНИЕ КИБЕРОПЕРАЦИЙ В ХОДЕ КОНФЛИКТА**

## **2.1. Кибероперации против гражданского населения**

Запрещение нападать на гражданских лиц, выступающее как выражение принципа проведения различия, - очень старая норма. Первым многосторонним договором, в котором она присутствовала, была Санкт-Петербургская декларация, где во второй мотивировке четко определяется, что «единственная законная цель, которую должны иметь государства во время войны, состоит в ослаблении военных сил неприятеля»[[102]](#footnote-102).

Женевская конвенция о защите гражданского населения во время войны[[103]](#footnote-103) посвящена в основном защите лиц, находящихся в руках неприятеля, в т.ч. в условиях оккупации, и содержит очень мало положений об общей защите от последствий военных действий населения, проживающего на территории противника (ч. II Женевской конвенции IV). В этом отношении основополагающее положение содержится в Дополнительном протоколе I (далее – ДП I) к Женевским конвенциям (1977 г.), в котором также дается определение гражданского населения. Однако следует отметить, что ДП I не ратифицирован таким же количеством государств, как и Женевские конвенции[[104]](#footnote-104).

Прежде всего, необходимо определить, какие лица подпадают под категорию «гражданского населения». В соответствии с ДП I в ситуациях международного вооруженного конфликта гражданские лица определяются через отрицание как все лица, не принадлежащие к личному составу вооруженных сил стороны в конфликте и не являющиеся участниками ополчения[[105]](#footnote-105). Хотя в договорном МГП, предшествующем ДП I, гражданские лица явным образом не определялись, терминология, использованная в Гаагском положении и в четырех Женевских конвенциях, подводит к заключению, что понятия гражданского лица, вооруженных сил и ополчения являются взаимоисключающими и что любое лицо, участвующее в военных действиях или затронутое ими, принадлежит к одной из указанных трех категорий.

Например, в ст. 22 Брюссельской декларации (1874 г.) и ст. 29 Гаагской конвенции IV (1907 г.) «гражданские лица» упоминаются в противопоставлении «военнослужащим». Аналогичным образом, Женевские конвенции 1949 г. оперируют категорией «гражданские лица» (ЖК IV), которая выступает как дополнительная по отношению к личному составу «вооруженных сил» (ЖК I и ЖК II). Хотя сфера применения каждой Конвенции не точно соответствует общим категориям, обозначенным в их названиях, категории «гражданское лицо» и «вооруженные силы» используются как взаимоисключающие во всех четырех Конвенциях. Например, в ЖК I, ЖК II и ЖК IV раненые, больные и потерпевшие кораблекрушение «гражданские лица» (ст. 22 ЖК I; ст. 35 ЖК II; ст. 20, 21, 22 ЖК IV) противопоставляются общим категориям, находящимся под покровительством ЖК I и ЖК II, а именно, раненым и больным в действующих армиях и раненым, больным и лицам, потерпевшим кораблекрушение из состава вооруженных сил на море (ЖК I и ЖК II).

Ст. 51 ДП I устанавливает, что «гражданское население как таковое, а также отдельные гражданские лица не должны быть объектом нападения». Международный суд ООН подчеркивал в своих решениях, что это первый из «главных принципов, которые составляют основу гуманитарного права»[[106]](#footnote-106). Аналогичным образом Совет Безопасности «решительно осуждает преднамеренные действия против гражданских лиц в ситуациях вооруженного конфликта»[[107]](#footnote-107). МТБЮ в деле Милошевича заявил; «запрещено любое нападение, направленное против гражданских лиц, какими бы ни были мотивировавшие его военные соображения»[[108]](#footnote-108).

Как было отмечено выше, в киберпространстве правила ведения боевых действий особенно актуальны. Эти правила, в частности, направлены и на защиту гражданского населения от последствий военных действий. Они основаны на важнейшем *принципе различия*, который требует, чтобы воюющие стороны всегда проводили различие между гражданским населением и комбатантами.

МККК в своей позиции отмечает, что МГП, включая принципы различия, соразмерности и предосторожности, применяется к кибероперациям во время вооруженных конфликтов, и это означает, что:

* запрещены кибернетические возможности, которые квалифицируются как оружие и по своей природе являются неизбирательными[[109]](#footnote-109);
* запрещены прямые нападения на гражданских лиц и гражданские объекты, в том числе при использовании киберсредств или методов ведения войны[[110]](#footnote-110);
* акты или угрозы насилия, основной целью которых является распространение террора среди гражданского населения, запрещены, в том числе, когда они осуществляются с помощью киберсредств или методов ведения войны[[111]](#footnote-111);
* запрещены неизбирательные нападения, а именно нападения, направленные на поражение военных целей и гражданских лиц без различия, запрещены, в том числе, когда использование киберсредств или методов ведения войны[[112]](#footnote-112);
* запрещены непропорциональные атаки, в том числе при использовании киберсредств или методов ведения войны. Непропорциональные нападения - это те, которые, как можно ожидать, приведут к случайным жертвам среди гражданского населения, ранениям гражданских лиц, повреждению гражданских объектов или их сочетанию, что было бы чрезмерным по отношению к ожидаемому конкретному и прямому военному преимуществу.
* должны быть приняты все возможные меры предосторожности, чтобы избежать или, по крайней мере, свести к минимуму случайный ущерб гражданскому населению при проведении атак, в том числе с помощью киберсредств и методов ведения войны[[113]](#footnote-113). Такими мерами предосторожности могут быть: отделение военной кибер-инфраструктуры и сетей от гражданской; отделение компьютерных систем от Интернета, от которого зависит важнейшая гражданская инфраструктура; должна проводиться идентификацией в киберпространстве с целью определение сетей, обслуживающих особо охраняемые объекты, такие как больницы[[114]](#footnote-114).

Так, комбатантам разрешается принимать участие в боевых действиях, в то время как гражданским лицам предоставляется защита до тех пор, пока они не принимают непосредственного участия в боевых действиях[[115]](#footnote-115). Прямое участие может включать нанесение ущерба воюющей стороне или снабжение вооруженных сил противника[[116]](#footnote-116). МККК опубликовал руководящие принципы, в которых устанавливается трехсторонний тест на непосредственное участие.

Во-первых, должно производиться в качестве вероятного результата негативное воздействие на военные операции или военный потенциал стороны в конфликте либо причинить смерть, ранение или разрушение соответственно лиц или объектов, пользующихся защитой от непосредственного нападения (*порог вреда*).

Во-вторых, должна существовать непосредственная причинная связь между действием и вредом, который может стать вероятным результатом действия или скоординированной военной операции, составной частью которой является указанное действие (*непосредственное причинение*).

В-третьих, действие должно быть специально предназначено для достижения установленного порога вреда и быть совершено в поддержку одной стороны в конфликте и во вред другой (*связь с воюющей стороной*)[[117]](#footnote-117).

Из-за особенностей современных систем вооружения и ИТ-систем компьютерная инфраструктура редко эксплуатируются исключительно военнослужащими, зачастую обслуживание осуществляется гражданскими лицами. Однако не все гражданские лица, которые сотрудничают с воюющими сторонами, принимают непосредственное участие в боевых действиях. Все больше гражданских лиц и гражданских экспертов нанимается в вооруженные силы для выполнения так называемых невоенных обязанностей и предоставления необходимых ноу-хау для повышения эффективности операций.

Другая сторона медали заключается в том, что ИТ-операторы могли бы географически располагаться за тысячи миль от поля боя и проводить операции исключительно с помощью компьютерных экранов и удаленной аудиопередачи[[118]](#footnote-118). Эта пространственная разобщенность с реальным боевым пространством могла бы способствовать развитию так называемого менталитета *PlayStation*[[119]](#footnote-119), когда оператор не осознает последствий своих действий, которые затем также могут привести к злоупотреблению властью и нарушениям закона.

В настоящее время есть тенденция к тому, что гражданские лица или субподрядчики сопровождают вооруженные силы, по-видимому, чаще из-за сложности технологий, используемых вооруженными силами. Необходимость понятна, но также увеличивает риск того, что гражданские лица, работающие в вооруженных силах, особенно в районе операций, будут рассматриваться как непосредственные участники боевых действий[[120]](#footnote-120). И даже более того, когда гражданские лица или подрядчики проводят операции по приказу командиров и инициируют кибератаки или контролируют их. Таким образом, гражданские ИТ-специалисты рискуют стать законными целями. Эта неопределенность создает опасную ситуацию для МГП, поскольку она может подорвать гуманитарные гарантии, установленные для гражданского населения и для гражданских лиц, сопровождающих вооруженные силы, т.к. воюющие стороны не могут проводить разумное различие между комбатантами и гражданскими лицами[[121]](#footnote-121). В идеале кибератаки должны проводить военнослужащие вооруженных сил, но это, по-видимому, нереалистичное ожидание.

Недавние конфликты привели к появлению спорных примеров участия гражданского населения в военных действиях. Например, в качестве примера можно привести червь *Conficker*, который направлен на участие по незнанию, и в этом случае захватываются либо домашние компьютеры, либо компьютеры компаний, а пропускная способность используется для облегчения кибератак. Проект *Grey Goose* подготовил два отчета о грузино-российском конфликте 2008 г., в которых указывается, что ботнеты использовались для проведения DDoS-атак на грузинские веб-сайты, и большинство владельцев захваченных компьютеров не знали, что они участвуют в боевых действиях[[122]](#footnote-122).

Другая сторона медали - это так называемый «патриотический взлом», когда пользователи компьютеров добровольно и сознательно разрешают использовать свои компьютеры или сами совершают действия, наносящие ущерб воюющей стороне. Это было применено во время грузино-российского конфликта 2008 г., когда некоторые российские доски объявлений содержали простые инструкции, как атаковать грузинские веб-сайты. Так, Евгений Морозов описывает свой опыт определенной личной заинтересованности в участии в кибератаке: «Не зная точно, как подписаться на кибервойну, я начал с обширного опроса российской блогосферы. Так я узнал из этого поста в блоге все, что мне нужно было сделать - это сохранить копию определенной веб-страницы на свой жесткий диск, а затем открыть ее в своем браузере p. Менее чем за час я превратился в интернет-солдата. Я не получал никаких звонков; мне также не пришлось покупать веб-сервер или каким-либо существенным образом модифицировать свой компьютер. Если то, что я делал, было кибервойной, у меня есть некоторые опасения по поводу количества детей-солдат, которые могут просто счесть это слишком забавным и доступным»[[123]](#footnote-123).

Следующий вопрос, который возникает при изучении кибероперации, – соответствуют ли кибероперация, использующая механизмы прикрытия или другие средства сокрытия, МГП? Ряд ученых полагают, что это можно квалифицировать как вероломство. Вероломство – это, по определению, акт обмана[[124]](#footnote-124). Оно заключается в том, чтобы заставить противника поверить, что он обязан предоставить защиту по праву вооруженных конфликтов с намерением предать это доверие[[125]](#footnote-125).

В МГП запрещенное вероломство должно удовлетворять четырем критериям: (1) действие вызывает особое доверие противника, (2) есть намерение предать это доверие, (3) у лица есть особая защита, предусмотренная международным правом, и (4) наступили смерть или увечье противника[[126]](#footnote-126). Часто приводимые примеры такого вероломства включают убийство или ранение противника посредством симуляции капитуляции с целью приблизить противника, симулирование статуса раненого или не участвующего в боевых действиях или нейтрального статуса[[127]](#footnote-127).

Но в большинстве случаев маловероятно, что кибероперации будут удовлетворять всем четырем элементам вероломства. Во-первых, грань между вероломным и не вероломным обманом (уловками) может быть весьма неуловимой[[128]](#footnote-128). Даже если военная инфраструктура будет имитировать гражданскую инфраструктуру или использовать другие методы для сокрытия кибернетических возможностей, то в любом случае будет «нелегко установить причинно-следственную связь между вероломным [кибернетическим] актом... и последствиями боевых действий»[[129]](#footnote-129).

Во-вторых, для того, чтобы представлять собой нарушение запрета, вероломный акт должен быть непосредственной причиной предполагаемого вреда[[130]](#footnote-130). Так, физические последствия для лица должны быть именно из-за вероломного акта[[131]](#footnote-131). Хотя кибероперации могут служить средством распространения вероломного обмана, в целом они сами по себе не могут непосредственно убить, ранить или захватить противника в плен. С простой технической точки зрения кибероперации могут быть направлены только против физических и логических компонентов киберпространства или данных и причинять им вред. Вред отдельным лицам может быть причинен только вторично, и ни Гаагские правила, ни ДП I, ни обычное международное право не включают в сферу запрещенного вероломства причинение вреда только объектам[[132]](#footnote-132). Следовательно, если только вероломная кибероперация не проводится с целью проведения отдельной атаки, любое полученное в результате повреждение или смерть должны были быть либо специально запланированы, либо разумно предсказуемы, чтобы операция представляла собой запрещенное вероломство. Например, кибероперация, которая одновременно подделывает гражданский IP-адрес для доступа к системе жизнеобеспечения и приводит к сбою в работе этой системы с намерением убить вражеского пациента, скорее всего, будет противоречить МГП[[133]](#footnote-133). Однако изменчивый характер киберпространства и быстрые изменения в данных и архитектуре серьезно затрудняют определение непосредственной причины.

Как отмечается в комментарии 1987 года к ДП I, «запрет на вероломство имеет свои слабые стороны»[[134]](#footnote-134). Главным из них является размытая грань между вероломным обманом и уловками, особенно в отношении использования или имитации гражданских объектов для проведения операций.

Подводя итог, можно отметить, что государства все активнее используют кибервозможности и оперативные конструкции в качестве средств и методов ведения войны, в том числе благодаря тому, что это является «серой зоной» международного права. Использование прикрытия и маскировок в киберпространстве затрагивает традиционные нормы МГП, призванные обеспечить уважение принципа проведения различия и защиты гражданского населения. Эти правила должны интерпретироваться в свете уникальных аспектов киберпространства и тех особых проблем, которые оно создает.

## **2.2 Кибероперации против гражданских объектов**

Большинство кибератак, которые осуществляются в настоящее время против гражданской инфраструктуры, выходят за рамки каких-либо вооруженных конфликтов. В марте 2021 года государства-члены ООН признали, что кибероперации могут серьезно повлиять на гражданскую инфраструктуру и, таким образом, привести к «разрушительным гуманитарным последствиям»[[135]](#footnote-135). Например, в феврале 2023 г. власти Национального центра кибербезопасности Нидерландов заявили, что пророссийские хакеры осуществили DDoS-атаки на веб-сайты больниц в Нидерландах и других странах Европы[[136]](#footnote-136). К наиболее узнаваемым атакам относят вирус *Stuxnet*, приостановивший ядерную программу Ирана[[137]](#footnote-137), а также кибератаки против Эстонии, направленные, в том числе, на частный сектор (банки, телекоммуникационные операторы, новостные организации страны и др.). Несмотря на их разрушительный характер, DDoS-атаки не нанесли существенного физического ущерба и не достигли уровня реальной кибервойны.

В ключе же вооруженных конфликтов, гражданские объекты и их данные остаются более уязвимыми. Неоспорим также и тот факт, что кибероперации стали неотъемлемой частью стратегий многих государств и иных субъектов по достижению военных и стратегических целей[[138]](#footnote-138). Мобильные телефоны являются таким же оружием XXI века, как и любое другое огнестрельное вооружение, а электронная почта и текстовые сообщения стали широко распространенными средствами военной коммуникации.

Прежде чем рассматривать возможность или невозможность проведения киберопераций, направленных на объекты гражданской инфраструктуры, стоит отметить, что правовые режимы, регулирующие международные и немеждународные вооруженные конфликты, в отношении ведения военных действий становятся все более похожими. Таким образом, говоря о применимых нормах, следует оговориться об отсутствии необходимости проводить различие между осуществлением киберопераций против гражданских объектов в контексте МВК или НМВК. По большей части, защита их проведения будет регулироваться нормами обычного МГП.

При этом, как было отмечено МТБЮ, распространение норм, разработанных для МВК, на конфликты немеждународного характера «не произошло в форме полного и механического переноса этих норм; скорее, общая суть указанных норм, а не детальное регулирование, которое они могут содержать, стало применимо к внутренним конфликтам»[[139]](#footnote-139).

Базовое для МГП определение гражданского объекта содержится в ст. 52 (1) ДП I, которая закрепляет, что «гражданскими объектами являются все те объекты, которые не являются военными объектами». В то время как ст. 52 (2) конкретизирует, что «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».

Оба определения подразумевают некую осязаемость объектов. Подобная подразумеваемая осязаемость, физическая материальность, была четко сформулирована в комментарии МККК к Дополнительным протоколам[[140]](#footnote-140), где указывалось, что «в английском тексте используется слово "objects", которое означает "нечто, расположенное перед глазами, или представленное зрению или другому чувству, отдельная вещь, видимая или воспринимаемая, или которая может быть увидена или воспринята; материальная вещь". Во французском тексте используется слово "biens", что означает "осязаемая вещь, способная к присвоению"». Очевидно, что и в английском, и во французском языках это слово означает нечто видимое и осязаемое[[141]](#footnote-141).

В этой связи возникает вопрос о возможности наличия «гражданских объектов» в контексте киберпространства. Так, например, эксперты Таллиннского руководства единодушно согласились с тем, что «компьютеры, компьютерные сети и другие материальные компоненты киберинфраструктуры представляют собой объекты»[[142]](#footnote-142). Однако как среди разработчиков Таллиннского руководства, так и среди ученых возникают споры о том, как квалифицировать нападения на различные гражданские данные, выразившееся в их удалении или изменении.

*Данные как гражданский объект*

При признании гражданских данных «объектом» в понимании МГП, нападение против них в форме кибероперации (например, их удаление) будут защищаться использованием принципов проведения различия, пропорциональности и принятия мер предосторожности и защитой, которую они предоставляют гражданским объектам[[143]](#footnote-143). И наоборот, если данные не будут рассматриваться в качестве «объекта», то гражданские массивы данных будут пользоваться ограниченной защитой во время вооруженного конфликта[[144]](#footnote-144).

Вопрос о том, пользуются ли гражданские данные такой же защитой, как и гражданские объекты, остается нерешенным. Их защита от угроз киберопераций во время вооруженного конфликта становится все более важной, поскольку они являются важнейшим компонентом цифровой сферы. К гражданским данным относят: данные социального обеспечения, налоговые записи, банковские счета, файлы клиентов компаний, медицинские данные отдельных лиц, избирательные списки и протоколы, которые являются ключевыми для функционирования большинства аспектов жизни граждан и т. п.

В отношении данных, относящихся к определенным категориям объектов и пользующихся особой защитой в соответствии с МГП, правила защиты носят всеобъемлющий характер. Например, обязательства по уважению и защите медицинских учреждений и операций по оказанию гуманитарной помощи должны распространяться также и на медицинские данные, принадлежащие этим учреждениям и гуманитарным организациям, которые необходимы для их деятельности. Аналогичным образом, удаление или иное вмешательство в данные таким образом, чтобы сделать бесполезными объекты, необходимые для выживания гражданского населения, такие как, например, сооружения для снабжения питьевой водой и ирригационные системы, запрещено[[145]](#footnote-145).

В широком смысле можно отметить два общих подхода. Согласно первому, в соответствии с которым данные считаются объектами МГП, операция, направленная на удаление или какое-либо изменение данных, будет являться нападением, регулируемым всеми соответствующими нормами МГП, поскольку она будет равносильна уничтожению или повреждению объекта (данных). Так было бы и в том случае, если бы такое удаление или изменение не привело к повреждению или выведению из строя физического объекта. Однако даже при таком подходе операция, направленная исключительно на получение доступа к (возможно, конфиденциальным) данным без их удаления или изменения - например, шпионаж - не будет рассматриваться в качестве атаки[[146]](#footnote-146). И наоборот, если данные не являются объектами согласно МГП, то операция, направленная на их удаление или изменение без причинения ущерба объекту, не будет регулироваться правилами, обеспечивающих защиту гражданских объектов[[147]](#footnote-147).

Большинство экспертов, участвовавших в процессе подготовки Таллиннского руководства, считают, что обычное значение термина «объект», рассмотренное в Комментарии МККК 1987 года к ДП I, не может быть истолковано как включающее в себя данные, поскольку объекты являются материальными, видимыми и осязаемыми. Поэтому кибероперации с данными не подпадают под действие соответствующих норм МГП, если только рассматриваемая операция не привела к какому-либо физическому эффекту и/или потере функциональности целевой системы или сети[[148]](#footnote-148). Некоторые государства, в том числе Дания[[149]](#footnote-149), Чили[[150]](#footnote-150) и Израиль[[151]](#footnote-151), также поддерживают эту точку зрения.

В это же время другие ученые утверждают, что либо все, либо некоторые типы данных должны рассматриваться как объекты в рамках МГП[[152]](#footnote-152). Например, относительно экспертов Таллинского руководства: меньшинство придерживались мнения о том, что «позиция большинства является недостаточно содержательной в том смысле, что если не включить кибероперации, направленные на данные как таковые, в объем термина «нападение», то это будет означать, что даже удаление основных совокупностей данных гражданского населения, таких как данные социального обеспечения, налоговые записи и банковские счета, потенциально может выйти из сферы регулирования права вооруженного конфликта, тем самым противореча принципу о том, что гражданское население пользуется общей защитой от последствий военных действий»[[153]](#footnote-153). Для этих экспертов ключевым фактором, исходя из основного объекта и цели статьи 52 Дополнительного протокола I, является тяжесть и последствия операции, а не характер ущерба. Таким образом, они придерживались мнения, что, как минимум, гражданские данные, которые «необходимы» для благополучия гражданского населения, охватываются понятием гражданских объектов и должны защищаться как таковые[[154]](#footnote-154).

В этом ключе учеными приводятся примеры с нацеливанием на данные, которые по своей сути являются гражданскими, «такие как медицинские карты, хранящиеся в конкретной больнице»[[155]](#footnote-155). Отмечается, что «если бы эти данные были тайно стерты или изменены, жизнь и здоровье пациентов в больнице оказались бы под угрозой; их уничтожение повлияло бы на целостность гражданского объекта (самих данных) и безопасность гражданского населения (пациентов в больнице). . . . Оба этих примера объединяет тот факт, что прямым следствием рассмотренных атак было бы исключительно уничтожение данных»[[156]](#footnote-156). Исходя из подхода Таллинского руководства, такие нападения, как правило, выходят за рамки МГП, если они не нарушают функциональность системы управления до такой степени, что требуется замена физических компонентов. Однако как отмечали сами эксперты Таллинского руководства, «данные, которые являются неотъемлемой частью операций или управления медицинскими подразделениями и транспортом, должны уважаться и защищаться и, в частности, не могут быть объектом нападения»[[157]](#footnote-157).

Некоторые государства (включая Финляндию[[158]](#footnote-158), Германию[[159]](#footnote-159), Норвегию[[160]](#footnote-160) и Румынию[[161]](#footnote-161)) поддерживают точку зрения о том, что защита гражданских объектов распространяется на гражданские данные. Франция прямо указывает на то, что «особая защита, предоставляемая определенным объектам, распространяется на системы и данные, которые обеспечивают их функционирование»[[162]](#footnote-162), поэтому «учитывая нынешнее состояние цифровой зависимости, данные о содержимом (такие как гражданские, банковские или медицинские данные и т.д.) защищаются в соответствии с принципом проведения различия»[[163]](#footnote-163).

Также важно отметить позицию одного из создателей Таллинского руководства Майкла Н. Шмитта[[164]](#footnote-164), который прямо признал, что международное право может быстро эволюционировать в ответ на вопрос о том, являются ли данные объектом. Он указал следующее: «я буду рабски придерживаться *lex lata*. Хотя я считаю, что закон о понятии объектов будет развиваться достаточно быстро, спекуляции в этой области не являются моей целью. Я понимаю, что толкование объектов, предложенное большинством, приводит к нежелательным результатам в том смысле, что открывает двери для кибер-операций против данных, которые могут оказать значительное негативное воздействие на гражданское население. Однако всеобъемлющая трактовка данных как объекта, […] была бы чрезмерной. Пока государства не определят соответствующий баланс, [для экспертов Таллинского руководства] было бы опрометчиво расширять значение объектов до такой степени»[[165]](#footnote-165).

Похожее предложение заключается в проведении различия между «данными операционного уровня» (*operational-level data*), или «кодом», и «данными уровня содержания» (*content-level data*)[[166]](#footnote-166). Согласно предложенному различию, данные уровня содержания будут включать такие данные как «содержание медицинских баз данных, библиотечных каталогов и т.д.», в то время как данные на операционном уровне будут описывать «по сути "душу машины"», то есть «тип данных, которые придают оборудованию его функциональность и способность выполнять те задачи, которые нам требуются»[[167]](#footnote-167). В этом ключе утверждается, что, в частности, если данные операционного уровня могут квалифицироваться как военный объект, то это подразумевает, что такой тип данных также может квалифицироваться как гражданский объект[[168]](#footnote-168).

Позиция МККК относительно данных, принадлежащих к определенным категориям объектов и которые пользуются особой защитой в соответствии с МГП, сводится к тому, что правила защиты являются всеобъемлющими. Например, обязательство уважать и защищать медицинские учреждения следует понимать как распространяющееся и на медицинские данные, принадлежащие этим учреждениям[[169]](#footnote-169). При этом МККК уточняет, что «было бы важно уточнить, в какой степени гражданские данные, которые не подпадают под такую конкретную защиту, такие как данные социального страхования, налоговые отчеты, банковские счета, файлы клиентов компаний или избирательные списки или записи, уже защищены существующими общими правилами ведения военных действий. Удаление или фальсификация таких данных может быстро привести к полной остановке государственных служб и частного бизнеса и нанести гражданскому населению больший вред, чем уничтожение физических объектов»[[170]](#footnote-170).

В целом позиция о том, что замена бумажных документов цифровыми данными не должна снижать уровень защиты, предоставляемой им МГП[[171]](#footnote-171), логична и обоснована. МККК в этом отношении также подчеркнул важность того, чтобы «государства договорились о том, что гражданские данные должны быть защищены» нормами МГП, регулирующими ведение военных действий[[172]](#footnote-172). Однако очень немногие государства предоставили позиции относительно вопроса о том, являются ли данные «объектом»[[173]](#footnote-173).

В настоящее время отсутствуют примеры вооруженных конфликтов, когда кибероперации были бы направлены против гражданских данных без пагубных физических последствий, и, следовательно, отсутствуют прецеденты того, как государства реагируют на правовую характеристику таких инцидентов. Отсутствие соответствующей практики государств делает возможные ответные меры умозрительными, поскольку, в конечном счете, именно государства должны будут определить, являются ли гражданские данные объектом для целей закона о целеуказании в контексте вооруженного конфликта. Однако подводя итог, следует отметить, что гражданские данные должны рассматриваться в качестве объекта для предоставления им достаточного уровня защиты в рамках МГП.

*Средства и методы ведения киберопераций против гражданских объектов*

Как отметил С. Ю. Гаркуша-Божко, «киберпространство представляет собой не совсем обычный театр войны, т. к. средства и методы ведения военных действий, применяемых в нем, никак не связаны с традиционным применением вооруженной силы»[[174]](#footnote-174). Сильная зависимость современных обществ от компьютеров, компьютерных систем и сетей значительно расширила средства и методы, имеющиеся в распоряжении воюющих сторон для нанесения ущерба друг другу. Как следствие, использование киберопераций в современной войне быстро становится стратегически столь же важным, как и авиация в традиционных формах конфликтов[[175]](#footnote-175).

Важно помнить, что правила ведения военных действий применяются к кибероперациям только в той мере, в какой они квалифицируются как «акты военных действий». Руководство МККК по толкованию понятия прямого участия в военных действиях определяет «военные действия» как «(коллективное) обращение сторон конфликта к средствам и методам нанесения вреда врагу»[[176]](#footnote-176). Таллиннское руководство также определяет «военные действия» как «коллективное применение средств и методов ведения войны»[[177]](#footnote-177).

В частности, военные действия охватывают не только акты насилия, но также любое действие, которое негативно влияет на военный потенциал противника, включая «операции, направленные на повышение собственных возможностей»[[178]](#footnote-178), такие как эксплуатация киберзащиты для защиты военных объектов и сбор тактических разведданных.

Кибероперации, направленные против гражданских данных (например, их удаление), будут регулироваться принципами проведения различия, соразмерности и принятия мер предосторожности, а также полным объемом защиты, которую они обеспечивают физическим гражданским объектам[[179]](#footnote-179).

Статья 48 ДП 1 гласит о том, что «для обеспечения уважения и защиты […] гражданских объектов стороны, находящиеся в конфликте, должны всегда проводить различие между […] гражданскими объектами и военными объектами». Аналогичным образом статья 52 Протокола 1 подтверждает, что «гражданские объекты не должны являться объектом нападения или репрессалий».

Принцип проведения различия означает запрет использовать средства или методы кибервойны, которые являются неизбирательными по своей природе[[180]](#footnote-180). Такими средствами могут быть вирусы и черви, которые не различают какой-либо конкретной цели. Чтобы следовать этому правилу, те, кто осуществляет кибератаку в виде вируса или червя, могут внедрить их в какую-либо закрытую систему, или разработчик кибератаки может запрограммировать ее на проверку определенных условий, существующих в сети или системе до заражения[[181]](#footnote-181). Другими возможными мерами может быть такая разработка вируса или червя, чтобы он действовал только в течение определенного времени.

Реализация принципов проведения различия и пропорциональности, а также запрета на неизбирательные атаки требует, чтобы атака могла быть и была направлена на военную цель и не причиняла чрезмерного случайного вреда гражданским объектам. Вопреки предположению, что эти принципы могут потерять смысл в киберпространстве из-за характерной для него взаимосвязанности, анализ киберопераций показывает, что такие операции по своей сути не являются неизбирательными. Например, если кибероперация проводится операторами, которые знают цель операции, и, исходя из этого знания, они проводят ее, то такие операторы будут знать, в каком «пространстве» они «находятся» и какая деятельность им предстоит. Аналогичным образом, анализ киберсредств показывает, что они не обязательно являются неизбирательными. Те, кто разрабатывает вредоносные программы или планирует кибератаки, могут создавать их без функций самораспространения. В этом случае вредоносное программное обеспечение не может распространяться без дополнительного вмешательства человека.

Даже если вредоносная программа запрограммирована на широкое распространение, она может быть разработана таким образом, чтобы наносить ущерб только конкретной цели или определенному набору целей. В частности, для кибератак, направленных на нанесение физического ущерба промышленным системам управления, могут потребоваться кибернетические инструменты, разработанные для этой конкретной цели и задачи. Характеристики, наблюдаемые в ряде киберопераций, показывают, что они могут быть очень точно приспособлены для оказания воздействия только на конкретные цели, и поэтому такие операции могут соответствовать принципам и правилам МГП.

Как уже было установлено, одним из основных положений в МГП является строгое разделение гражданских и военных объектов. Как отметила советник по правовым вопросам МККК М. С. Гаврилова, «если мы имеем дело с киберпространством, когда один и тот же объект используется и в гражданских, и в военных целях, то соблюсти это различие становится достаточно трудно. Например, та же GPS-навигация и банальный кабель может использоваться и в гражданских, и в военных целях»[[182]](#footnote-182). Таким образом, одной из дополнительных проблем применения МГП в контексте киберпространства является трудность применения принципа проведения различия в ситуации объекта двойного назначения.

Своеобразным «спасительным кругом» в такой ситуации может выступить позиция, на которую указал С. Ю. Гаркуша-Божко: «применение в киберпространстве принципа проведения различия вряд ли сможет обеспечить защиту объектов двойного назначения. Более важным для защиты таких объектов в киберпространстве является принцип соразмерности»[[183]](#footnote-183). Таким образом, государствам необходимо приоритизировать имеющиеся принципы МГП в целях их эффективного использования.

МГП запрещает нападения с использованием средств и методов ведения войны, включая киберсредства и методы, которые не могут быть направлены на конкретную военную цель или, как можно ожидать, выйдут из-под контроля пользователя,[[184]](#footnote-184) или - будучи направленными на военную цель - могут, как можно ожидать, причинить случайный ущерб гражданскому населению, чрезмерный по сравнению с ожидаемым конкретным и прямым военным преимуществом.[[185]](#footnote-185)

Также отмечается, что при применении всех известных МГП средств и методов ведения военных действий к кибердеятельности следует руководствоваться требованиями разумности[[186]](#footnote-186). Например, тот факт, что военные отправляют электронную почту через Интернет, не делает весь Интернет законной целью для нападения. Наконец, гражданский объект может стать военной целью благодаря «цели», которая относится к предполагаемому будущему использованию объекта в военных целях. Например, если есть достоверная информация о том, что гражданская серверная фирма вскоре начнет хранить военные данные, то фирма является военным объектом, который может быть атакован еще до начала хранения данных[[187]](#footnote-187).

Подводя итог, текущее состояние МГП, регулирующего кибероперации, не является удовлетворительным в части защиты гражданских объектов. Отсутствует ясность относительно определения гражданского объекта, а также относительно того, как защитить гражданских лиц, ставших жертвами в результате нападения на гражданские данные, в отношении которых нет устоявшейся позиции по их признанию в качестве гражданского объекта. Вследствие этого возникает «правовая лакуна», когда указанные данные каким-либо образом изменяются, что приводит к ущербу гражданскому населению, однако регулирование таких атак не попадает под положения МГП. Подобная «серая зона» открывает двери для государств, желающих воспользоваться имеющейся двусмысленностью для проведения крайне разрушительных киберопераций против гражданского населения. Более того, некоторые кибероперации, которые не будут квалифицироваться как нападение, тем не менее, могут вызвать хаос среди гражданского населения.

Также можно прийти к выводу о том, что операция с гражданскими данными иногда может представлять собой атаку. В этой связи, для обеспечения максимально возможной защиты гражданского населения и гражданской инфраструктуры, крайне необходимо признать, что такие операции не происходят в правовом вакууме, а регулируются имеющимися нормами МГП, применимыми в киберпространстве.

# **ГЛАВА 3. СПОСОБЫ ПРЕДОТВРАЩЕНИЯ УЩЕРБА ГРАЖДАНСКОМУ НАСЕЛЕНИЮ ОТ ВОЕННЫХ КИБЕРОПЕРАЦИЙ**

В рамках данной научной работы важно отметить ст. 58 Дополнительного протокола I, которая устанавливает три важных требования к сторонам конфликта. В «максимально возможной степени» стороны должны:

a) стремиться удалить гражданское население, отдельных гражданских лиц и гражданские объекты, находящиеся под их контролем, из районов, расположенных вблизи от военных объектов;

b) избегать размещения военных объектов в густонаселенных районах или вблизи от них;

c) принимать другие необходимые меры предосторожности для защиты гражданского населения, отдельных гражданских лиц и гражданских объектов, находящихся под их контролем, от опасностей, возникающих в результате военных операций.

Хотя в строгом смысле это применимо только к государствам-участникам Дополнительного протокола I, некоторые считают, что ст. 58 отражает обычное международное право, применимое как к международным, так и к немеждународным вооруженным конфликтам[[188]](#footnote-188). Однако на практике в киберпространстве данная статья вряд ли будет работать.

Во-первых, основное внимание в ст. 58 уделяется эвакуации гражданских лиц из районов, которые могут подвергнуться нападению. Единственный пример, когда данная норма будет работать в киберпространстве – это удаление гражданских лиц или подвижных гражданских объектов из непосредственной близости от очевидных военных «кибернетических» установок и сил[[189]](#footnote-189), поэтому применение этой меры предосторожности в киберпространстве практически неосуществимо.

Кибероперации предполагают виртуальное маневрирование на физических и виртуальных уровнях киберпространства, где отдельные базы данных, которые могут дать определенное военное преимущество другой стороне, могут «соседствовать» с широко рассредоточенной гражданской инфраструктурой. Так, за считанные наносекунды любой объект потенциально превращается в военную цель[[190]](#footnote-190). Более того, военные данные и возможности могут храниться в «облачной» среде, объединяться с гражданскими данными и инфраструктурой, а также динамически передаваться с одного сервера на другой, опять же за считанные наносекунды. Оставляя в стороне гуманитарные соображения, можно говорить о том, что государства физически не смогут эвакуировать гражданских лиц или переместить их данные.

Второй пункт ст. 58 Дополнительного протокола I еще менее применим к киберпространству. Во-первых, по своим условиям он узок по охвату. Содержащийся в нем призыв избегать размещения военных объектов в непосредственной близости от гражданских лиц применим только в густонаселенных районах, что является относительным понятием, которое плохо соотносится с киберпространством[[191]](#footnote-191). Во-вторых, основное внимание в ст. 58, когда она была составлена, было сосредоточено на материальных объектах, а не на виртуальные объектах и нематериальных вещах, таких как данные[[192]](#footnote-192). Таким образом, по многим из тех же причин, которые были сформулированы ранее, эта мера предосторожности практически невыполнима в киберпространстве.

Природа киберпространства такова, что отделить военные кибернетические возможности, инфраструктуру и операции от гражданской инфраструктуры часто невозможно, и составители Дополнительного протокола I ясно дали понять, что в отношении пассивных мер предосторожности «ни от кого нельзя требовать невозможного»[[193]](#footnote-193). Современные боевые действия часто требуют «локализации или размещение вооруженных сил [и техники] в городских районах или других районах, где присутствуют гражданские лица» по военным причинам[[194]](#footnote-194). То же самое особенно верно в отношении физической и виртуальной кибернетической инфраструктуры и возможностей, и составители Дополнительного протокола I понимали, что «нельзя ожидать, что сторона в конфликте расположит свои вооруженные силы и объекты таким образом, чтобы они бросались в глаза противнику»[[195]](#footnote-195). В условиях кибер-войны безопасность операций и внезапность могут быть достигнуты только путем сокрытия инфраструктуры и возможностей с использованием оперативного прикрытия и других средств «технической» маскировки. В той мере, в какой «определение местоположения» этих кибер-объектов подпадает под ограниченную сферу действия ст. 58, и, как правило, будет невозможно отделить или каким-либо образом отметить и при этом добиться успеха в операциях.

Наконец, ст. 58 устанавливает бессрочное, «всеобъемлющее» обязательство «принимать другие необходимые меры предосторожности». На первый взгляд, это общее обязательство кажется довольно размытым, возможно, применяемым ко всем «военным операциям», которые создают какую-либо «опасность» для гражданских лиц или гражданских объектов и потенциально требующие принятия мер по снижению рисков в отношении подавляющего большинства киберопераций. Однако данный пункт применяются только к нападениям, а не к широкому кругу операций[[196]](#footnote-196).

Сфера применения данного пункта ограничивается снижением риска для гражданских лиц и гражданских объектов, находящихся под контролем стороны, и опять же, только в максимально возможной степени. Когда речь идет о гражданских кибер-объектах, применение правила осложняется территориальной концепцией контроля, предусмотренной разработчиками Дополнительного протокола I[[197]](#footnote-197). Вопрос о том, подлежит ли гражданская кибер-инфраструктура на территории государства ipso facto государственному контролю, является предметом некоторых дискуссий[[198]](#footnote-198). Независимо от этого, национальные законы могут сами по себе создают препятствия для принятия правительством превентивных или корректирующих мер в отношении частных систем, что, вероятно, делает такие меры неосуществимыми.

Таким образом, ст. 58(с) обычно рассматривается как не обязательно требующая, но «позволяющая государствам принимать дополнительные меры предосторожности в соответствии с такими обстоятельствами, как доступные государству средства и другие соображения, связанные с конфликтом»[[199]](#footnote-199). При её принятии разработчики имели в виду относительно ограниченные и конкретные примеры типов других мер предосторожности, которые могут быть «необходимыми». Они включали такие защитные меры, как строительство убежищ, создание организаций гражданской обороны, выявление и маркировка зон или объектов повышенного риска, и обеспечение систем раннего предупреждения и мер по исправлению положения, таких как оказание медицинской помощи раненым или служб пожаротушения для ограничения ущерба объектам[[200]](#footnote-200). Таллиннское руководство 2.0 предлагает аналогичные меры по снижению риска или смягчению ущерба кибер-инфраструктуре, такие как использование антивирусных программ для защиты гражданских систем, резервное копирование важных данных и восстановление поврежденных компьютеров и сетей[[201]](#footnote-201). Из характера представленных примеров очевидно, что какие бы превентивные меры ни были необходимы по смыслу статьи 58(c), данное положение не предназначалось для введения требований к разделению или маркировке сверх тех, которые охватываются конкретными обязательствами, предусмотренными подразделами (a) и (b), или другими применимыми положениями положения МГП. В конечном счете, статья 58(c), как представляется, представляет собой не более чем традиционный, основанный на конкретных фактах баланс гуманитарных интересов и военной необходимости.

По сравнению с кинетическими операциями понимание возможных побочных эффектов военных киберопераций и риска для гражданского населения может быть затруднено из-за взаимосвязанного и динамического характера целевых систем и сетей, а также потенциальной неопытности вооруженных сил в проведении таких операций. В настоящее время предлагается несколько способов для того, чтобы избежать или хотя бы снизить риск причинения вреда гражданскому населению в результате военных киберопераций[[202]](#footnote-202). В целом, все приведенные способы так или иначе коррелируют с уже упомянутыми выше принципами МГП, применимыми к проведению киберопераций.

Прежде всего, ответственность за проведение кибеопераций должна лежать как на тех, кто предпринимает наступательные действия, так и на тех, чьи сети и системы подвергаются риску атаки. Подобная двойственность ответственности также отражена в нормах ответственного поведения государств в киберпространстве, принятых ГА ООН[[203]](#footnote-203). В частности, одна из норм предписывает государствам не проводить кибероперации, которые могут нанести ущерб критической инфраструктуре[[204]](#footnote-204), в то время как другая норма предусматривает, что государства должны принимать соответствующие меры для защиты своей собственной критической инфраструктуры[[205]](#footnote-205). Таким образом, все государства несут ответственность за снижение риска причинения вреда гражданскому населению путем принятия соответствующих мер кибербезопасности. Например, Израильские военнослужащие отправляли текстовые сообщения гражданским лицам в секторе Газа, которые проживают в зданиях, предназначенных для неминуемого нападения, или вблизи них[[206]](#footnote-206).

Положения МГП устанавливают, что при проведении военных операций необходимо постоянно следить за тем, чтобы щадить гражданское население и гражданские объекты[[207]](#footnote-207). В частности, кибероператоры должны понимать, в какой степени целевые сети и программные системы взаимосвязаны, риск непреднамеренного распространения вредоносных программ и риск косвенных последствий. Государства должны иметь стратегии смягчения последствий для всех военных киберопераций, которые они рассматривают для применения.

Например, одним из способов предотвращения или уменьшения ущерба гражданскому населению от киберопераций является принятие мер предосторожности при нападении. Безусловно, такие меры будут применимы к операциям, в которых для достижения желаемого эффекта используется вредоносное программное обеспечение. Например, это может касаться разработки вредоносных программ, способных к «системному ограждению», т.е. к распознаванию среды, в которую они попадают, и последующему исполнению только в том случае, если целевая система точно соответствует этой среде[[208]](#footnote-208). Например, *Stuxnet* является наглядным примером использования такого подхода, поскольку он был разработан для работы только в системе с определенной конфигурацией[[209]](#footnote-209) и фактически не выходил за рамки запрограммированной системы[[210]](#footnote-210).

Также среди возможных методов смягчения последствий упоминается «гео-ограждение», под которым понимается техника, ограничивающая работу вредоносной программы только в определенном диапазоне IP-адресов[[211]](#footnote-211), а также «kill switch», представляющая собой техническую функцию, которая отключает вредоносную программу через определенный период времени или при использовании удаленной активации. Более того, вредоносная программа может содержать функцию автоудаления, при которой она стирает себя с целевой системы после достижения заданной цели[[212]](#footnote-212). Также важно отметить, что нужда в перечисленных мерах может отпасть в ситуации наличия непосредственного человеческого управления и контроля на всех этапах кибероперации. Таким образом, оптимальный подход к снижению риска заключается в следующем: чем более автономной является конкретная программа, тем более сильные встроенные гарантии она должен иметь.

Все государства так или иначе вносят свой вклад в снижение риска причинения вреда гражданскому населению путем принятия мер киберзащиты, поэтому важно прорабатывать также меры предосторожности против последствий кибератак. Среди экспертного сообщества обсуждаются возможности цифровой маркировки охраняемых гражданских объектов в качестве возможной пассивной меры предосторожности. Эксперты отмечают, что такая маркировка технически возможна, например, с помощью протокола Интернета версии 6 (IPv6), который позволяет обозначать определенные блоки IP-адресов как защищенные[[213]](#footnote-213). Однако другие эксперты выражают скептицизм в отношении эффективности такой практики в сдерживании вредоносной деятельности. В частности, было подчеркнуто, что преступные организации итак нацелены на больницы и прочие объекты гражданской инфраструктуры, и цифровая маркировка только облегчит эту задачу. Некоторые эксперты также предупредили, что такая система может быть использована для защиты критически важных военных систем несмотря на то, что это так же недопустимо, как рисовать красный крест на военных объектах[[214]](#footnote-214). Однако при всем при этом цифровая маркировка может рассматриваться как способ потенциального снижения риска случайного ущерба гражданскому населению в результате военных кибер-операций.

М. Шмитт в качестве одного из способа предотвращения ущерба гражданскому населению дополнительно предлагает государствам в качестве вопроса политики воздерживаться от проведения киберопераций, к которым не применяются нормы МГП, регулирующие нападения, когда ожидаемые конкретные негативные последствия для отдельных гражданских лиц или гражданского населения чрезмерны по сравнению с конкретной выгодой, связанной с конфликтом, которую предполагается получить в результате операции[[215]](#footnote-215).

Можно отметить, что государства и иные лица при осуществлении киберопераций должны принимать меры для защиты гражданского населения от опасностей, в том числе не нападать на ключевые объекты гражданской инфраструктуры, создавать резервные копии важных данных гражданского назначения, принимать повышенные меры антивирусной защиты. Однако нельзя не отметить, что в настоящее время существует реальность опасность того, что при использовании киберопераций может быть нанесен вред гражданским лицам. Многие нормы МГП, касающиеся защиты гражданского населения, применяются к кибероперациям, но возникают определённые сложности в их применении. Важно, чтобы все субъекты международного права подтвердили, что МГП применяется к кибероперациям во время вооруженных конфликтов, при этом, безусловно, исходя из понимания, что такое подтверждение не содействует «поощрению» проведения таких действий. Более того, государства, активно развивающее свои кибервозможности должно обеспечить, чтобы кибервозможности не нарушали нормы и принципы, защищающие гражданское население и гражданскую инфраструктуру в ходе вооруженного конфликта, как международного, так и немеждународного характера.

# **ЗАКЛЮЧЕНИЕ**

В рамках данной работы были достигнуты все поставленные задачи.

1. Автором были проанализированы нормы международного гуманитарного права на предмет возможности их применения к различным вооруженным конфликтам, происходящим в контексте киберпространства. Автор пришел к выводу о том, что кибероперации стали неотъемлемой частью современных вооруженных конфликтов как международного, так и немеждународного характера. Несмотря на то, что они могут принимать различные формы, во всех вооруженных конфликтах стороны будут использовать их в качестве средства или метода ведения войны для совершения операций против компьютера, компьютерной системы или сети.

Относительно международного вооруженного конфликта, автор отмечает, что гипотеза о том, что кибероперации само по себе могут привести к международному вооруженному конфликту, трудно доказуема по причине наличия значительных юридических и практических проблем. На сегодняшний день ни один международный вооруженный конфликт не был публично охарактеризован как спровоцированный исключительно в киберпространстве.

Относительно немеждународного вооруженного конфликта, автором был сделан вывод о том, что для квалификации наличия такого конфликта будут необходимы классические критерии НМВК, которые обладают определенной спецификой в киберпространстве. Таким образом, если какая-либо ситуация внутренней напряженности не будет иметь упомянутых критериев, то отличительной чертой рассматриваемых в ее контексте киберопераций будет то, что они не попадут под регулирование норм МГП.

1. В рамках поставленных задач автор также изучил существующую практику государств по защите гражданского населения во время проведения киберопераций. Автор отмечает, что в контексте киберпространства государства все активнее используют кибервозможности и оперативные конструкции в качестве средств и методов ведения войны, в том числе благодаря тому, что это является «серой зоной» международного права. Использование прикрытия и маскировок в киберпространстве затрагивает традиционные нормы МГП, призванные обеспечить уважение принципа проведения различия и защиты гражданского населения. Автор делает вывод о том, что указанные правила должны интерпретироваться в свете уникальных аспектов киберпространства и тех особых проблем, которые оно создает.

Автор отметил, что государства и иные лица при осуществлении киберопераций должны принимать меры для защиты гражданского населения от опасностей, в том числе не нападать на ключевые объекты гражданской инфраструктуры, создавать резервные копии важных данных гражданского назначения, принимать повышенные меры антивирусной защиты. Однако нельзя не отметить, что в настоящее время существует реальность опасность того, что при использовании киберопераций может быть нанесен вред гражданским лицам. Многие нормы МГП, касающиеся защиты гражданского населения, применяются к кибероперациям, но возникают определённые сложности в их применении. Важно, чтобы все субъекты международного права подтвердили, что МГП применяется к кибероперациям во время вооруженных конфликтов, при этом, безусловно, исходя из понимания, что такое подтверждение не содействует «поощрению» проведения таких действий. Более того, государства, активно развивающее свои кибервозможности должно обеспечить, чтобы кибервозможности не нарушали нормы и принципы, защищающие гражданское население и гражданскую инфраструктуру в ходе вооруженного конфликта, как международного, так и немеждународного характера.

Дополнительно автор изучил проведение киберопераций против гражданских данных, так как их повреждение иди удаление также будет оказывать негативный эффект на гражданское население. Автор отмечает, что текущее состояние МГП, регулирующего кибероперации, не является удовлетворительным в части защиты гражданских объектов. Отсутствует ясность относительно определения гражданского объекта, а также относительно того, как защитить гражданских лиц, ставших жертвами в результате нападения на гражданские данные, в отношении которых нет устоявшейся позиции по их признанию в качестве гражданского объекта. Вследствие этого возникает «правовая лакуна», когда указанные данные каким-либо образом изменяются, что приводит к ущербу гражданскому населению, однако регулирование таких атак не попадает под положения МГП. Подобная «серая зона» открывает двери для государств, желающих воспользоваться имеющейся двусмысленностью для проведения крайне разрушительных киберопераций против гражданского населения. Более того, некоторые кибероперации, которые не будут квалифицироваться как нападение, тем не менее, могут вызвать хаос среди гражданского населения.

Автор пришел к выводу о том, что операция с гражданскими данными иногда может представлять собой атаку. В этой связи, для обеспечения максимально возможной защиты гражданского населения и гражданской инфраструктуры, крайне необходимо признать, что такие операции не происходят в правовом вакууме, а регулируются имеющимися нормами МГП, применимыми в киберпространстве.

1. На основе проведенного анализа автор выдвинул предложения по предотвращению ущерба гражданскому населению от кибереропераций во время вооруженных конфликтов. Прежде всего, при проведении киберопераций государствам следует всегда принимать дополнительные меры предосторожности, которые будут зависеть от планируемой операции. Например, такие меры могут касаться разработки вредоносных программ, способных к «системному ограждению», т.е. к распознаванию среды, в которую они попадают, и последующему исполнению только в том случае, если целевая система точно соответствует этой среде. Также государства могут использовать «гео-ограждение», т.е. техника, ограничивающая работу вредоносной программы только в определенном диапазоне IP-адресов, и «kill switch», представляющая собой техническую функцию, которая отключает вредоносную программу через определенный период времени. Более того, вредоносная программа может содержать функцию автоудаления, при которой она стирает себя с целевой системы после достижения заданной цели. В качестве дополнительной меры по предотвращению ущерба может быть отказ государств от проведения кибератак, которые могут нанести ущерб критической гражданской инфраструктуре. В любом случае, государства также должны иметь стратегии смягчения последствий для всех военных киберопераций, а также предпринимать меры по обеспечению киберзащиты.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

**1. Нормативно-правовые акты и иные официальные документы**

**1.1. Международные нормативно-правовые акты и иные**

**официальные документы**

1. Декларация об отмене употребления взрывчатых и зажигательных пуль (Принята в г. Санкт-Петербурге 29.11.1868) // Действующее международное право. Т. 2.- М.: Московский независимый институт международного права, 1997. С. 573 - 574.
2. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов (Протокол I) // Сборник международных договоров СССР. Вып. XLVI. - М., 1993. С. 134 - 182.
3. Женевская конвенция о защите гражданского населения во время войны (Заключена в г. Женеве 12.08.1949) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XVI.- М., 1957. С. 204 - 278, 280.

**1.2. Акты международных организаций, органов и конференций**

*1.2.1. Акты Генеральной Ассамблеи ООН*

Report of the Secretary-General’s Panel of Experts on accountability in Shi Lanka, 31 March 2011 // Режим доступа: https://www.refworld.org/docid/4db7b23e2.html (дата обращения 15.05.2023).

UN General Assembly, Resolution 70/237, Developments in the field of information and telecommunications in the context of international security, adopted on 23 December 2015 // Режим доступа: https://digitallibrary.un.org/record/816528 (дата обращения 15.05.2023).

*1.2.3. Иные международные официальные документы*

Human Rights Council. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions // Philip Alston. L Study on Targeted Killings. A/HRC/14/24/Add.6.

**1.3. Нормативно-правовые акты и иные официальные документы**

**иностранных государств**

Italy, National Strategic Framework for Cyberspace Security, Presidency of the Council of Ministers (December), 2013 // Режим доступа: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf (дата обращения 15.05.2023);

US Department of Defense, ‘Joint Publication Cyberspace Operations (JP 3-12 (R))’, Joint Chiefs of Staff, 2013 // Режим доступа: https://irp.fas.org/doddir/dod/jp3\_12.pdf (дата обращения 15.05.2023);

Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS, Improving Transparency: International Law and State Cyber Operations: Fifth Report, OAS Doc. CJI/doc. 615/20 rev.1 (7 August 2020) // Режим доступа: http://www.oas.org/en/sla/iajc/docs/CJI-doc\_615-20\_rev1\_ENG.pdf (дата обращения 15.05.2023);

French Ministry of the Armies, ‘International Law Applied to Operations in Cyberspace’, 9 September 2019, p. 12 // Режим доступа: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf (дата обращения 15.05.2023);

Germany, ‘On the Application of International Law in Cyberspace: Position Paper’, March 2021 // Режим доступа: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (дата обращения 15.05.2023);

Hungary, India, the International Organization for Standardization and International Electrotechnical Commission, the ITU, and CCDCOE // Режим доступа: https://ccdcoe.org/uploads/2018/10/NCSS-International-Cooperation.pdf (дата обращения 15.05.2023);

Ministry of Defence of Denmark, Military Manual on International Law Relevant to Danish Armed Forces in International Operations (2016) // Режим доступа: https://www.forsvaret.dk/en/publications/military-manual/ (дата обращения 15.05.2023);

**2. Материалы судебной практики**

*2.1. Акты Международного Суда ООН*

1. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America, ICJ Judgment of 27 June 1986 (Merits) // I.C.J. Reports. – 1986. – Р. 14;
2. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), ICJ Judgment of 26 February 2007(Merits) // I.C.J. Reports. – 2007. - Р. 43.

*2.2. Акты Международного Трибунала по бывшей Югославии*

Prosecutor v Boškoski and Tarčulovski (Trial Judgment) IT-04-82-T (10 July 2008) // Режим доступа: https://www.icty.org/ (дата обращения: 15.05.2023);

Prosecutor v Limaj, Bala and Musliu (Trial Judgment) IT-03-66-T (30 November 2005) // Режим доступа: https://www.icty.org/ (дата обращения: 15.05.2023);

Prosecutor v Tadić (Decision on Jurisdiction) IT-94-1-AR72 (2 October 1995)

Prosecutor v. Thomas Lubanga Dyilo (Trial Judgment) ICC-01/04-01/06-2842 (5 April 2012) // Режим доступа: https://www.icty.org/ (дата обращения: 15.05.2023);

**3. Специальная литература**

**3.1. Литература на русском языке**

Фицнер, В.Ю. Проблемы применения норм и принципов международного гуманитарного права к кибератакам // Тенденции развития современной юриспруденции : материалы VII Всероссийской студенческой научно-практической конференции Юридического института Балтийского федерального университета имени Иммануила Канта, Калининград, 19–21 апреля 2019 года / под общ. ред. О. А. Заячковского. – Калининград: Издательство балтийского федерального университета имени Иммануила Канта, 2019. – С. 53-59.

Плакса В.Н., Применимость норм международного гуманитарного права к новым технологиям, используемым при ведении военных действий / В. Н. Плакса // Актуальные проблемы сравнительного правоведения и юридической лингвистики: Сборник материалов IV международной научно-практической конференции, Москва, 10–12 декабря 2019 г. – Московский государственный лингвистический университет, 2020. – С. 26-34.

Гаврилова, М.С., Демидов, О.В., Козик, А. Л., Стрельцов, А. А. Применение международного права в киберпространстве // Индекс безопасности. – 2015. – Том 21. – № 4 (115).

Гаркуша-Божко, С.Ю. Международное гуманитарное право в киберпространстве: ratione materiae, ratione temporis и проблема квалификации кибератак // Цифровое право. – 2021. – Т. 2. – № 1. – С. 66.

Гаркуша-Божко, С. Ю. Применение принципов международного гуманитарного права (принципы проведения различия, соразмерности и предосторожности) к вооруженным конфликтам в киберпространстве // Российский журнал правовых исследований. – 2021. – Т. 8. – № 3. – С. 73 - 90.

Давид Э. Принципы права вооруженных конфликтов: курс лекций, прочитанных на юридическом факультете Открытого Брюссельского университета / пер. с фр. – 2-е рус. изд.. – М.: МККК, 2011. – 1144 с.

Данельян, А.А. Международно-правовое регулирование киберпространства // Образование и право. – 2020. – № 1. – С. 267.

Дрёге, К. Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц // Международный журнал Красного Креста. – 2014. – Том 94. – С. 1 – 60.

Навиченок, П.В. Проблема ответственности государств за кибероперации во время вооружённого конфликта // ЦИФРОВЫЕ ТЕХНОЛОГИИ в НАУКЕ, БИЗНЕСЕ, ОБРАЗОВАНИИ : сборник статей Международной научно-практической конференции, Пенза, 30 июля 2020 года. Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2020. С. 38-41. EDN SVPJYR.

Русинова В.Н. Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса // Московский журнал международного права. 2022. № 1. С. 46 - 48.

Русинова, В.Н. Международно-правовой принцип невмешательства и кибероперации: неоправданные ожидания? // Международное правосудие. – 2018. – № 1 (25). – С. 38 – 52.

Сассоли М., Бувье А. Правовая защита во время войны: в 4-х тт. Т. I. Международное гуманитарное право: краткий очерк. Варианты учебных курсов / пер. с англ. – М.: МККК, 2008. – 672 с.

Хенкертс Ж.-М., Досвальд-Бек Л. Обычное международное гуманитарное право. Том I. Нормы / пер. с англ. – М.: МККК, 2006. – LXVII, 819 с.

**3.2. Литература на иностранных языках**

Segal, The Hacked World Order // Public Affairs. - New York. – 2016. –P. 320.

Andreas Paulus and Mindia Vashakmadze, ‘Asymmetrical War and the Notion of Armed Conflict—A Tentative Conceptualization’// International Review of the Red Cross. – 2009. – Р. 95-125.

Bullough, Oliver , ‘Russians Wage Cyber War on Chechen Websites’, Reuters, November 15, 2002 // Режим доступа: <http://archive.cert.unistuttgart.de/isn/2002/11/msg00064.html> (дата обращения: 15.05.2023).

Raymond D., ‘Key Terrain in Cyberspace: Seeking the High Ground’, in P. Brangetto et al. in 6th CCDCOE Proceedings, 292, and The Netherlands (updated) Defence Cyber Strategy (2015), in Kamerstukken II (Parliamentary Papers) 2014–2015, 33 321.

Betz D.J. and Stevens T., Cyberspace and the State // Adelphi Series. – 2011. – P. 36.

Daragh Murray, Practitioners' Guide to Human Rights Law in Armed Conflict, Part II // Oxford Scholarly Authorities on International Law. – 17 November 2016.

David P. Fidler, Cyberattacks and international human rights law in Weapons Under International Human Right’s Law // Cambridge University Press. – 2014. – P. 633.

Dino Kritsiotis, ‘Enforced Equations’ // European Journal of International Law. – 2013.

Droege Cordula, ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians’ // International Review of the Red Cross. –2012. – P. 140-149.

Morozov, E. An Army of Ones and Zeroes: How I Became a Soldier in the Georgian-Russian Cyberwar // Режим доступа: https://slate.com/technology/2008/08/how-i-became-a-soldier-in-the-georgia-russia-cyberwar.html (дата обращения: 15.05.2023).

Gary P. Corn, Peter P. Pascucci, The Impact of Emerging Technologies on the Law of Armed Conflict // Oxford University Press. – 2019. – P. 290.

Georg Kerschischnig, Cyberthreats and international law // Eleven International Publishing. – 2012. – P. 365.

H. Harrison Dinniss, The Nature of Objects: Targeting Networks and the challenge of defining Cyber Military Objectives // 48 Israel Law Review. – 2015. – P. 39-54.

H. Harrison Dinniss, Cyber Warfare and the Laws of War // Cambridge. – Cambridge University Press. – 2012. – P. 360.

Herbert S Lin, Offensive Cyber Operations and the Use of Force // Journal of National Security Law and Policy 4. – 2010.

ICRC statement on International Law in the second session of the OEWG on security of and in the use of information and communications technologies, 01 April 2022 // URL: https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations.

ICRC, Avoiding civilian harm from military cyber operations during armed conflicts, report of ICRC expert meeting, 21–22 January 2020, Geneva.

ICRC, German Bundestag, letter of the Federal Ministry of Foreign Affairs, Document 13/437 - The Federal Government’s position on Russian action in the Chechen conflict March 2, 1995.

ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts’, Report prepared by the ICRC for the 31st International Conference of the Red Cross and Red Crescent (2011(31IC/11/512)).

ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva, 2015 (ICRC Challenges Report 2015).

ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Geneva, 2009 (prepared by Nils Melzer), p 43.

ICRC, The Potential Human Cost of Cyber Operations (Электр. ресурс) / Режим доступа: https://www.icrc.org/en/download/file/ 96008/the‐potential‐human‐cost‐of‐cyber‐operations.pdf.

Int’l Comm. Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949

J. R. Heaton, Civilians At War: Reexamining the Status of Civilians Accompanying the Armed Forces. L Air Force Law Review, Vol. 57

Jean-Francois Queguiner, Precautions Under the Law Governing the Conduct of Hostilities // 88 Int’l Rev. Red. Cross 793. – 818. – 2006.

John Ricou Heaton, Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces // – Air Force Law Review 57. – 2005.

Justin Salhani, In Syria, the Cyberwar Intensifies, Defense News, 18 January 2013 // URL: http://rpdefense.over-blog.com/article-in-syria-the-cyberwar-intensifies-114545428.html.

K. Dörmann, Applicability of the Additional Protocols to Computer Network Attacks. L ICRC. Conduct of Hostilities, Information Warfare. 19 November.

Kasandra Adams, Geofencing as applied within the field of cybersecurity: an overview of potential risks and advantages // California State University. – 2020.

Katherine J. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, in Alessandro Acquisti et al. (eds.), Digital Privacy: Theory, Technologies, and Practices, Auerbach Publications, Boca Raton, 2007.

Kubo Mačák and Laurent Gisel, ‘Grammar: Rules in a Cyber Conflict’, in Patryk Pawlak and François Delerue (eds), Cyber Defence in the European Union (EUISS 2022).

Kubo Mačák, ‘Unblurring the lines: military cyber operations and international law’ (2021) 6(3) Journal of Cyber Policy.

Kubo Mačák, Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law, 48 ISRAEL LAW REVIEW 55 (2015).

Laurent Gisel, Tilman Rodenhauser and Knut Dormann, Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts, International Review of the Red Cross (2020), 102 (913), 287–334.

Liesbeth Zegveld, Accountability of Organized Armed Groups, in Non-state Actors and International Humanitarian Law, edited by Marco Odello and Gian Luca Beruto (Milano: Franco Angeli, 2010).

M. Roscini, Cyber Operations and the Use of Force in International Law (Oxford: Oxford University Press, 2014).

M. Schmitt, Wired Warfare: Computer Network Attack and Jus In Bello. L International Review of the Red Cross, Vol 84, No 846.

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

Marko Milanović and Vidan Hadzi-Vidanović, ‘A Taxonomy of Armed Conflict’, in Research Handbook of International Conflict and Security Law, edited by Nigel D White and Christian Henderson (Cheltenham: Elgar, 2013).

Markus Maybaum, ‘Technical Methods, Techniques, Tools and Effects of Cyber Operations’, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy (NATO CCDCOE, 2013).

Marta Mísová, The legal character of the conflict in Chechnya, 18 May 2001 // URL: https://reliefweb.int/report/russian-federation/legal-character-conflict-chechnya.

Michael N Schmitt, ‘Cyber Operations and the Jus in Bello: Key Issues’, International Law Studies 87 (2011).

Michael N. Schmitt, “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations”, International Review of the Red Cross, Vol. 101, No. 910, 2019, pp 333–355; ICRC, General Assembly official records, 66th session: 1st Committee, 9th meeting, Tuesday, 11 October 2011, New York.

Michael N. Schmitt, The Nature of ‘Objects’ During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision, 48 ISRAEL LAW REVIEW 81 (2015).

Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. Geneva: ICRC.

P. Rosenzweig, Cyber Warfare—How Conflicts in Cyberspace Are Challenging America and Changing the World (Santa Barbara: Praeger, 2013).

P. Shakarian, J. Shakarian, and A. Ruef, Introduction to Cyber-Warfare: A Multidisciplinary Approach (Amsterdam etc.: Elsevier/Syngress, 2013).

Paul A.L. Ducheine and Jelle van Haaster, ‘Fighting Power, Targeting and Cyber Operations’, in P. Brangetto, M. Maybaum, and J. Stinissen (eds), Proceedings of the 6th International Conference on Cyber Conflict (CCDCOE, 2014).

Paul A.L. Ducheine, ‘The Notion of Cyber Operations in International Law’, in N. Tsagourias and R. Buchan (eds), The Research Handbook on the International Law and Cyberspace (Cheltenham: Edward Elgar Publishing, 2015).

Paul Cornish, On Cyber Warfare, A Chatham House Report, November 2010 quoted in Marco Sassòli, Antoine A Bouvier, and Anne Quintin, How Does Law Protect in War? // 3rd edn. – Geneva: ICRC. – 2011.

Richard E. Overill, ‘Denial of Service Attacks: Threats and Methodologies’ // Journal of Financial Crime 6. – 1999.

Robert Kolb and Richard Hyde, An Introduction to the International Law of Armed Conflicts // – Oxford and Portland: Hart. – 2008.

Robert McLaughlin, “Data as a Military Objective” // Australian Institute of International Affairs. – 20 September 2018.

Robin Geiss and Henning Lahmann, ‘Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space’ // Israel Law Review 45. – 2012.

Roy Schondorf, ‘Israel’s perspective on key legal and practical issues concerning the application of international law to cyber operations’ // 97 International Law Studies. – 2021.

S. Watts, Combatant Status and Computer Network Attack // L Virginia Journal of International Law. –Vol. 50. – No. 2.

Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.) Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. // Geneva: International Committee of the Red Cross. – Martinus Nijholf Publications.

Schindler, D., The Different Types of Armed Conflicts according to the Geneva Conventions // RCADI, 1979, II, T. 163.

Schmitt, M. Wired warfare 3.0: protecting the civilian population during cyber operations // International Review of the Red Cross. – 2019.

Stephen J Cox, Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War // Houston Law Review 42. – 2005.

Schmitt, M. Tallinn Manual on the International Law Applicable to Cyber Warfare // Cambridge. – 2013.

Tawfiq M. Aljohani, “Cyberattacks on Energy Infrastructures: Modern War Weapons” // Режим доступа: https://www.researchgate.net/publication/363128927\_Cyberattacks\_on\_Energy\_Infrastructures\_Modern\_War\_Weapons.

Terry D. Gill, Dieter Fleck, The Handbook of the International Law of Military Operations (2nd Edition) // Oxford Scholarly Authorities on International Law. – 10 December 2015.

Thomas, Timothy L. “Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?” Foreign Military Studies Office, Fort Leavenworth, 2002, and in Chapter 11 of Russian Military Reform 1992-2002, Frank Cass Publishers, 2003.

Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified.

Tim McCormack, ‘International Humanitarian Law and the Targeting of Data // International Law Studies. – 2012.

W. Jackson, Stuxnet shut down by its own kill switch // GCN. – 26 June 2012.

William H Boothby, The Law of Targeting // Oxford: Oxford University Press. –2012.

Yoram Dinstein, Non-International Armed Conflicts in International Law // Cambridge University Press. – 2014.

Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict 145 (2d ed. 2010)

Yves Sandoz, Christophe Swinarski & Bruno Zimmermann, Commentary on the Additional Protocols of 8 June 1977 to the Geneva conventions of 12 august 1949, 1987.

1. Tawfiq M. Aljohani, Cyberattacks on Energy Infrastructures: Modern War Weapons, [Электронный ресурс] // URL: https://www.researchgate.net/publication/363128927\_Cyberattacks\_on\_Energy\_Infrastructures\_Modern\_War\_Weapons. (Дата обращения - 10.05.2023) [↑](#footnote-ref-1)
2. ТАСС, Путин назвал кибербезопасность одной из важнейших тем современности, [Электронный ресурс] // URL: https://tass.ru/politika/11637535. (Дата обращения - 10.05.2023) [↑](#footnote-ref-2)
3. См. об этом: ICRC statement on International Law in the second session of the OEWG on security of and in the use of information and communications technologies [Электронный ресурс], 01 April 2022 // URL: https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations. (Дата обращения: 10.05.2023) [↑](#footnote-ref-3)
4. Кузнецов, С. И. Анисимов, В. В. Тесля, С. П. Морозов, И. В. Кибероперация как вид боевых действий // Защита и безопасность. –– 2018. –– № 1(84). –– С. 5. [↑](#footnote-ref-4)
5. Русинова, В.Н. Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса // Московский журнал международного права. –– 2022. –– № 1. –– С. 46 – 48. [↑](#footnote-ref-5)
6. Навиченок, П.В. Проблема ответственности государств за кибероперации во время вооружённого конфликта // Цифровые технологии в науке, бизнесе, образовании: сборник статей Международной научно-практической конференции, Пенза, 30 июля 2020 г. Пенза: "Наука и Просвещение". –– 2020. – С. 38-41. [↑](#footnote-ref-6)
7. Фицнер, В.Ю. Проблемы применения норм и принципов международного гуманитарного права к кибератакам // Тенденции развития современной юриспруденции: материалы VII Всероссийской студенческой научно-практической конференции Юридического института Балтийского федерального университета им. Иммануила Канта, Калининград, 19–21 апреля 2019 г. / под общ. ред. О.А. Заячковского. – Калининград: Издательство Балтийского федерального университета им. Иммануила Канта. –– 2019. –– С. 53-59. [↑](#footnote-ref-7)
8. Плакса, В.Н. Применимость норм международного гуманитарного права к новым технологиям, используемым при ведении военных действий // Актуальные проблемы сравнительного правоведения и юридической лингвистики: Сборник материалов IV международной научно-практической конференции, Москва, 10–12 декабря 2019 г. – Московский государственный лингвистический университет. –– 2020. –– С. 26-34. [↑](#footnote-ref-8)
9. Гаркуша-Божко, С.Ю. Международное гуманитарное право в киберпространстве: ratione materiae, ratione temporis и проблема квалификации кибератак // Цифровое право. – 2021. – Т. 2. – № 1. – С. 66. [↑](#footnote-ref-9)
10. Paul A.L. Ducheine and Jelle van Haaster, Fighting Power, Targeting and Cyber Operations, Brangetto, P., Maybaum, M., Stinissen, J. (eds), Proceedings of the 6th International Conference on Cyber Conflict (CCDCOE, 2014). Р. 304. [↑](#footnote-ref-10)
11. ICRC statement on International Law in the second session of the OEWG on security of and in the use of information and communications technologies, [Электронный ресурс] 01 April 2022 // URL: https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations. (Дата обращения - 15.03.2023) [↑](#footnote-ref-11)
12. Гаврилова, М.С., Демидов, О.В., Козик, А.Л., Стрельцов, А.А. Применение международного права в киберпространстве // Индекс безопасности. – 2015. – Том 21. – № 4 (115). – С. 102. [↑](#footnote-ref-12)
13. Гаркуша-Божко, С.Ю. Международное гуманитарное право в киберпространстве. – С. 69. [↑](#footnote-ref-13)
14. Raymond, D. et al. (eds), Key Terrain in Cyberspace: Seeking the High Ground, Brangetto P. et al. in 6th CCDCOE Proceedings, P. 292. [↑](#footnote-ref-14)
15. Harrison Dinniss, The Nature of Objects: Targeting Networks and the challenge of defining Cyber Military Objectives // 48 *Israel Law Review* 2015, P. 53. [↑](#footnote-ref-15)
16. Rosenzweig, P. Cyber Warfare — How Conflicts in Cyberspace Are Challenging America and Changing the World // Santa Barbara: Praeger. – 2013. – P.19. [↑](#footnote-ref-16)
17. Paul A.L. Ducheine, The Notion of Cyber Operations in International Law, Tsagourias N., Buchan R. (eds), The Research Handbook on the International Law and Cyberspace, Cheltenham: Edward Elgar Publishing. – 2015. – P 6. [↑](#footnote-ref-17)
18. Kerschischnig, G. Cyberthreats and international law // Eleven International Publishing. – 2012. – P. 26. [↑](#footnote-ref-18)
19. Cornish, P. On Cyber Warfare // A Chatham House Report. – 2010. – P. 22. [↑](#footnote-ref-19)
20. Roscini, M. Cyber Operations and the Use of Force in International Law // Oxford: Oxford University Press. – 2014. – P. 11. [↑](#footnote-ref-20)
21. Belgium, Cyber Security Strategy, Français-Dutch. – 2012; Italy, National Strategic Framework for Cyberspace Security, Presidency of the Council of Ministers. – December 2013; the US Department of Defense, Joint Publication Cyberspace Operations (JP 3-12 (R))’ // Joint Chiefs of Staff. – 2013. [↑](#footnote-ref-21)
22. ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts, Report prepared by the ICRC for the 31st International Conference of the Red Cross and Red Crescent, 31IC/11/512. – 2011– p. 36. [↑](#footnote-ref-22)
23. Maybaum, M. Technical Methods, Techniques, Tools and Effects of Cyber Operations, Ziolkowski, K.(ed.), Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy // NATO CCDCOE. – 2013. – p. 104; Ducheine, P. The Notion of Cyber Operations, Tsagourias N., Buchan R. (eds), The Research Handbook on the International Law and Cyberspace // Cheltenham: Edward Elgar. – 2015. – 211–232. – P. 213. [↑](#footnote-ref-23)
24. ICRC, The Potential Human Cost of Cyber Operations [Электронный Ресурс] // URL: https://www.icrc.org/en/download/file/ 96008/the‐potential‐human‐cost‐of‐cyber‐operations.pdf. (Дата обращения - 25.03.2023) [↑](#footnote-ref-24)
25. Gill, T. D., Fleck D., The Handbook of the International Law of Military Operations (2nd Edition) // Oxford Scholarly Authorities on International Law. – 10 December 2015. – p. [↑](#footnote-ref-25)
26. CCDCOE, 'Cyber Definitions', [Электронный Ресурс], 2014 // URL: <https://ccdcoe.org/cyber-definitions.html>, перечисляет 19 различных определений, используемых 16 государствами и 3мя негосударственными субъектами. (Дата обращения - 25.03.2023) [↑](#footnote-ref-26)
27. Betz, D.J., Stevens, T. Cyberspace and the State. – Adelphi Series. – 2011. – p. 36. [↑](#footnote-ref-27)
28. Ibid., p. 37. [↑](#footnote-ref-28)
29. Ibid., p. 37. [↑](#footnote-ref-29)
30. US Department of Defense, Joint Publication Cyberspace, I-3; Rosenzweig, P. Cyber Warfare—How Conflicts in Cyberspace Are Challenging America and Changing the World // Santa Barbara: Praeger. – 2013. – p. 19. [↑](#footnote-ref-30)
31. Harrison Dinniss, Cyber Warfare and the Laws of War // Cambridge: Cambridge University Press. – 2012. – p 185 – 187. [↑](#footnote-ref-31)
32. Shakarian, P., Shakarian, J., Ruef, A. Introduction to Cyber-Warfare: A Multidisciplinary Approach // Amsterdam etc.: Elsevier/Syngress. – 2013. – p. 224–235. [↑](#footnote-ref-32)
33. Murray, D. Practitioners' Guide to Human Rights Law in Armed Conflict, Part II, 15 Cyber Operations, Oxford Scholarly Authorities on International Law. – 17 November 2016. – p. 235. [↑](#footnote-ref-33)
34. Tallinn Manual on the International Law Applicable to Cyber Warfare // Cambridge University Press. – 2013. – p. 262, [‘*Tallinn Manual’*]. [↑](#footnote-ref-34)
35. Roscini, M. Cyber Operations and the Use of Force in International Law // Oxford University Press. – 2014. – p. 19, [‘Roscni, Cyber Operations]. [↑](#footnote-ref-35)
36. Lin, H. S. Offensive Cyber Operations and the Use of Force // Journal of National Security Law and Policy. – 4. – 2010. – p. 64. [↑](#footnote-ref-36)
37. Roscini, Cyber Operations, p. 19. [↑](#footnote-ref-37)
38. Heaton, J. R. Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces // Air Force Law Review 57. – 2005. – p 161. [↑](#footnote-ref-38)
39. Гаркуша-Божко, С.Ю. Международное гуманитарное право в киберпространстве. – С. 79. [↑](#footnote-ref-39)
40. Cox, S. J. Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War // Houston Law Review 42. – 2005–2006. – pp. 888–889. [↑](#footnote-ref-40)
41. Dinniss, H. Cyber Warfare, p. 296. [↑](#footnote-ref-41)
42. Overill, R. E. Denial of Service Attacks: Threats and Methodologies // Journal of Financial Crime 6. – 1999. – p. 353. [↑](#footnote-ref-42)
43. UK Manual, para. 3.2; DoD Manual, para. 3.3.1; Canadian Manual, at GL-9; German Manual, para. 202; AMW Manual, Rule 1(r). [↑](#footnote-ref-43)
44. Давид, Э. Принципы права вооруженных конфликтов. – Международный комитет Красного Креста. – 2011 г., – С. 117. [↑](#footnote-ref-44)
45. Conventions, сommentaire, op. cit., I, p. 34; 1959, II, p. 28; III, 1958, p. 29; 1956, IV, p. 26; Schindler, D., The Different Types of Armed Conflicts according to the Geneva Conventions, RCADI. – 1979. – II. – T. 163. – p. 131. [↑](#footnote-ref-45)
46. ICTY, Tadić, IT-94-1 // Appeals Chamber. – 15 July 1999. – para. 131–140, 145. [↑](#footnote-ref-46)
47. Ibid. [↑](#footnote-ref-47)
48. Ibid, para. 137. [↑](#footnote-ref-48)
49. ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) [2007] para. 404. [↑](#footnote-ref-49)
50. ICC, The Prosecutor v. Thomas Lubanga Dyilo // Trial Chamber. – 5 April 2012. – para. 541. [↑](#footnote-ref-50)
51. ICTY, Tadić, para. 137. [↑](#footnote-ref-51)
52. Tallinn Manual, p. 384. [↑](#footnote-ref-52)
53. Commentary on the First Geneva Convention, International Committee of the Red Cross, 2016, para. 255. [↑](#footnote-ref-53)
54. Общая статья 3, Женевские конвенции от 12 августа 1949 года и Дополнительные протоколы к ним. – 5-e изд., доп. – М.: МККК, 2011. – 302 с. [↑](#footnote-ref-54)
55. ICTY, Prosecutor v Tadić, Decision on Jurisdiction, IT-94-1-AR72. – 2 October 1995. – para 70. [↑](#footnote-ref-55)
56. Tallinn Manual*,* Rule 23, p 84. [↑](#footnote-ref-56)
57. ICTY, Prosecutor v Tadić, Trial Judgment. – para 562. [↑](#footnote-ref-57)
58. Cameron, L. et al, Article 3: Conflicts Not of an International Character // ICRC (ed), Commentary on the First Geneva Convention. – CUP 2016. – p. 158. [↑](#footnote-ref-58)
59. Ibid. [↑](#footnote-ref-59)
60. ICTY, Prosecutor v Boškoski and Tarčulovski, Trial Judgment, IT-04-82-T. – 10 July 2008. – para 177. [↑](#footnote-ref-60)
61. Tallinn Manual, p 88. [↑](#footnote-ref-61)
62. Ibid. [↑](#footnote-ref-62)
63. Roscini, Cyber Operations, p. 153. [↑](#footnote-ref-63)
64. Ibid. [↑](#footnote-ref-64)
65. ICTY, Prosecutor v Limaj, Bala and Musliu, Trial Judgment, IT-03-66-T. – 30 November 2005. – para 129; Prosecutor v Boškoski and Tarčulovski, Trial Judgment, IT-04-82-T. – 10 July 2008. – paras 199 – 203. [↑](#footnote-ref-65)
66. Tallinn Manual, Rule 83, para 7; Dinstein, Y. Non-International Armed Conflicts in International Law // CUP. – 2014. – 35. Позиция государств**:** French Ministry of the Armies, International Law Applied to Operations in Cyberspace. – 9 September 2019. – p. 12; Germany, On the Application of International Law in Cyberspace: Position Paper. – March 2021. – p. 7. [↑](#footnote-ref-66)
67. Roscini, Cyber Operations, p. 148. [↑](#footnote-ref-67)
68. Русинова, В. Н. Международно-правовой принцип невмешательства и кибероперации: неоправданные ожидания? // Международное правосудие. – 2018. – №1 (25). – С. 38 – 39. [↑](#footnote-ref-68)
69. Zegveld, L. Accountability of Organized Armed Groups, in Non-state Actors and International Humanitarian Law, edited by Marco Odello and Gian Luca Beruto // Milano: Franco Angeli. – 2010. – pp. 111–112. [↑](#footnote-ref-69)
70. Roscini, Cyber Operations, p. 148. [↑](#footnote-ref-70)
71. Liesbeth Zegveld, Accountability of Armed Opposition Groups in International Law // Cambridge: Cambridge University Press. – 2002. – pp. 112-113. [↑](#footnote-ref-71)
72. Общая статья 3 Женевских конвенций. [↑](#footnote-ref-72)
73. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) [Electronic resource]: ICJ Judgment of 27 June 1986 (Merits) // I.C.J. Reports. – 1986. – P. 14. – para 218. Access mode: https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (Дата обращения - 01.05.2023) [↑](#footnote-ref-73)
74. ICTY, Prosecutor v. Mladen Naletilic, para 249. [↑](#footnote-ref-74)
75. Melzer, N. Cyberwarfare and International Law // UNIDIR. – 2011. – p 5. [↑](#footnote-ref-75)
76. Статья 1 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 года, касающегося защиты жертв немеждународных вооруженных конфликтов (Протокол II). Женева, 8 июня 1977 года. [↑](#footnote-ref-76)
77. Paulus A., Vashakmadze, M. Asymmetrical War and the Notion of Armed Conflict — A Tentative Conceptualization // International Review of the Red Cross 9. – 2009. – p. 118. [↑](#footnote-ref-77)
78. Report of the Secretary-General’s Panel of Experts on accountability in Shi Lanka. – 31 March 2011. – para 182. – p. 52. [↑](#footnote-ref-78)
79. Статья 1 (1) Дополнительного протокола к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв немеждународных вооруженных конфликтов (Протокол II). Женева, 8 июня 1977 года. [↑](#footnote-ref-79)
80. ICTY, Boškoski and Tarčulovski, para 197. [↑](#footnote-ref-80)
81. Ibid. [↑](#footnote-ref-81)
82. Ibid.;Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.) Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 // Geneva: International Committee of the Red Cross, Martinus Nijholf Publications. – 1987. –para 4467. [↑](#footnote-ref-82)
83. Droege, C. Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians // International Review of the Red Cross. – 94. – 2012. – p. 550. [↑](#footnote-ref-83)
84. Boothby, W. H. The Law of Targeting // Oxford: Oxford University Press. – 2012. – p. 555; Dinniss, H. H. Cyber Warfare and the Laws of War // Cambridge: Cambridge University Press. – 2012. – p. 136. [↑](#footnote-ref-84)
85. Milanović, M., Hadzi-Vidanović V., A Taxonomy of Armed Conflict, Research Handbook of International Conflict and Security Law // White N. D., Henderson C. // Cheltenham: Elgar. – 2013. – p. 286; Kolb R., Hyde, R. An Introduction to the International Law of Armed Conflicts // Oxford and Portland: Hart. – 2008. – p. 79. [↑](#footnote-ref-85)
86. Roscini, Cyber Operations, p. 159. [↑](#footnote-ref-86)
87. Memorial Human Rights Center, By All Available Means: the Russian Federation Ministry of Internal Affairs Operation in the Village of Samashki. – April 7-8, 1995. – Moscow. – 1996; ICRC, German Bundestag, letter of the Federal Ministry of Foreign Affairs, Document 13/437 - The Federal Government’s position on Russian action in the Chechen conflict. – March 2 1995. [↑](#footnote-ref-87)
88. Mísová, M. The legal character of the conflict in Chechnya [Электронный ресурс], 18 May 2001 // URL: https://reliefweb.int/report/russian-federation/legal-character-conflict-chechnya. (Дата обращения - 28.04.2023) [↑](#footnote-ref-88)
89. Tikk, K., Rünnimeri, K., Cyber Attacks Against Georgia: Legal Lessons Identified. – November 2008. – p. 5. [↑](#footnote-ref-89)
90. Thomas, T. L. Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform? // Foreign Military Studies Office, Fort Leavenworth. – 2002; Chapter 11 of Russian Military Reform 1992-2002 // Frank Cass Publishers. – 2003. [↑](#footnote-ref-90)
91. Bullough, O. Russians Wage Cyber War on Chechen Websites // Reuters. – November 15. – 2002. [↑](#footnote-ref-91)
92. Report of the Secretary-General’s Panel of Experts on accountability in Shi Lanka. – 31 March 2011. – para. 182. – p. 52. [↑](#footnote-ref-92)
93. Kritsiotis, D. Enforced Equations // European Journal of International Law. – 24. – 2013. – p. 146. [↑](#footnote-ref-93)
94. Salhani, J. In Syria, the Cyberwar Intensifies [Электронный ресурс], Defense News, 18 January 2013 // URL: http://rpdefense.over-blog.com/article-in-syria-the-cyberwar-intensifies-114545428.html. (Дата обращения - 29.03.2023) [↑](#footnote-ref-94)
95. ICTY, Prosecutor v Tadić. Trial Judgment, para 562. [↑](#footnote-ref-95)
96. Bouvier, A. A., Quintin, A. How Does Law Protect in War? // Geneva: ICRC. – 2011. – Vol III. – p. 2. [↑](#footnote-ref-96)
97. Germany, On the Application of International Law in Cyberspace: Position Paper . – March 2021. – p. 7 со ссылкой на Tallinn Manual, Rule 83, paras. 2, 7 and 8. [↑](#footnote-ref-97)
98. Без объявления войны: С российскими хакерами будут бороться на высшем уровне [Электронный ресурс], 18 мая 2007 // URL: https://lenta.ru/articles/2007/05/17/hack/ (Дата обращения - 05.04.2023) [↑](#footnote-ref-98)
99. Fidler, D. P. Cyberattacks and international human rights law in Weapons Under International Human Right’s Law // Cambridge University Press. – 2014. – p. 301. [↑](#footnote-ref-99)
100. Strandburg, K. J. Surveillance of Emergent Associations: Freedom of Association in a Network Society, Acquisti A. et al. (eds.), Digital Privacy: Theory, Technologies, and Practices, Auerbach Publications // Boca Raton. – 2007. – pp. 435–458. [↑](#footnote-ref-100)
101. Данельян, А.А. Международно-правовое регулирование киберпространства // Образование и право. – 2020. – № 1. – С. 267. [↑](#footnote-ref-101)
102. Декларация об отмене употребления взрывчатых и зажигательных пуль (Принята в г. Санкт-Петербурге 29.11.1868) // Действующее международное право. Т. 2.- М.: Московский независимый институт международного права, 1997. С. 573 - 574. [↑](#footnote-ref-102)
103. Женевская конвенция о защите гражданского населения во время войны (Заключена в г. Женеве 12.08.1949) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XVI.- М., 1957. С. 204 - 278, 280. [↑](#footnote-ref-103)
104. По состоянию на 1 апреля 2023 г. 174 государств являлись участниками ДП I, а ратификация ЖК I-IV приобрела практически всемирный характер (194 государства-участников). [↑](#footnote-ref-104)
105. Ст. 50 (1) ДП I. Согласно Обычному МГП (Хенкертс Ж.-М., Досвальд-Бек Л. Обычное международное гуманитарное право. Том I. Нормы / пер. с англ. – М.: МККК, 2006.) , Норма 5, это определение гражданских лиц отражает обычное МГП в международном вооруженном конфликте. Категории, охваченные ст. 4 A [1], [2] и [3] ЖК III, включены в общее определение вооруженных сил в статье 43 (1) ДП I. См. также Sandoz et al. (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: ICRC, 1987), §§ 1916. [↑](#footnote-ref-105)
106. Консультативное заключение Международного суда относительно законности угрозы ядерным оружием или его применения, п. 78. [↑](#footnote-ref-106)
107. Резолюция СБ ООН 1265, 17 сентября 1999 г., п. 2; Резолюция СБ ООН 1296, 19 апреля 2000 г., п. 2. [↑](#footnote-ref-107)
108. TPIY, aff . IT-98-29/1-T, D. Milosevic, 12 Dec. 2007, § 906. [↑](#footnote-ref-108)
109. ICRC Customary Law Study, Rule 71. [↑](#footnote-ref-109)
110. ДП I, ст. 48, 51, 52; ICRC Customary Law Study, Rules 1, 7. [↑](#footnote-ref-110)
111. ДП I, ст. 51(2); ICRC Customary Law Study, Rule 2 [↑](#footnote-ref-111)
112. ДП I, ст. 51(4); ICRC Customary Law Study, Rules 11, 12. [↑](#footnote-ref-112)
113. ДП I, ст. 51(5)(b), 57; ICRC Customary Law Study, Rule 14. [↑](#footnote-ref-113)
114. CRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32IC/15/11, Geneva, 2015 (ICRC Challenges Report 2015), p. 40, available at: www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf [↑](#footnote-ref-114)
115. ДП I, ст. 48, 50(1), 51 (2) и 52(1). [↑](#footnote-ref-115)
116. ДП I, ст. 51(3). [↑](#footnote-ref-116)
117. Melzer, N. Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law // Geneva: ICRC. – 2009. – p. 46. [↑](#footnote-ref-117)
118. Human Rights Council. 2010. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston. L Study on Targeted Killings. A/HRC/14/24/Add.6, paras 84. [↑](#footnote-ref-118)
119. Schmitt, M. Wired Warfare: Computer Network Attack and Jus In Bello // International Review of the Red Cross, Vol 84. – No 846. – p. 384; Dörmann, K. Applicability of the Additional Protocols to Computer Network Attacks // ICRC. Conduct of Hostilities, Information Warfare. – 19 November 2004. – pp. 18-19. [↑](#footnote-ref-119)
120. Heaton, J. R. Civilians At War: Reexamining the Status of Civilians Accompanying the Armed Forces // Air Force Law Review. – Vol. 57. – p. 155. [↑](#footnote-ref-120)
121. Watts, S. Combatant Status and Computer Network Attack // Virginia Journal of International Law. – Vol. 50, No. 2. – p. 396. [↑](#footnote-ref-121)
122. Project Grey Goose, Phase I Report: Russia/Georgia Cyber War L Findings and Analysis. – 17 October 2007. [↑](#footnote-ref-122)
123. Morozov, E. An Army of Ones and Zeroes: How I Became a Soldier in the Georgian-Russian Cyberwar // Режим доступа: https://slate.com/technology/2008/08/how-i-became-a-soldier-in-the-georgia-russia-cyberwar.html. [↑](#footnote-ref-123)
124. Int’l Comm. Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. – p. 434. [↑](#footnote-ref-124)
125. ДП I, ст. 37 (1). [↑](#footnote-ref-125)
126. Tallinn Manual, p. 496; Henderson, I. et al., Emerging Technology and Perfidy in Armed Conflict // 91 Int’l L. Stud. 468, 471. – 2015. [↑](#footnote-ref-126)
127. U.S. Dep’t of Defense, Law of War Manual para. 5.21 (2015). [↑](#footnote-ref-127)
128. Corn, G. P., Pascucci, P.P. The Impact of Emerging Technologies on the Law of Armed Conflict. – p. 284. [↑](#footnote-ref-128)
129. ICRC Commentary, p. 432. [↑](#footnote-ref-129)
130. Tallinn Manual, p. 492. [↑](#footnote-ref-130)
131. Watts, S. Law-of-War Perfidy // 219 Mil. L. Rev. 106. – 165. [↑](#footnote-ref-131)
132. Tallinn Manual, p. 492 (Rule 122, comment 10); Bothe, M. New Rules for Victims of Armed Conflicts. – 1982. – p. 204. [↑](#footnote-ref-132)
133. Corn, G. P., Pascucci, P.P. The Impact of Emerging Technologies on the Law of Armed Conflict. – p. 286. [↑](#footnote-ref-133)
134. ICRC Commentary, at 432. [↑](#footnote-ref-134)
135. UN General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security. – 10 March 2021. – A/AC.290/2021/CRP.2. – para 18. [↑](#footnote-ref-135)
136. Dutch, European hospitals hit by pro-Russian hackers, [Электронный ресурс] 02 Feb 2023 // URL: https://www.thestar.com.my/tech/tech-news/2023/02/02/dutch-european-hospitals-hit-by-pro-russian-hackers (Дата обращения - 10.05.2023) [↑](#footnote-ref-136)
137. Broad, W. J., Markoff J., Sanger, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, [Электронный ресурс], New York Times, 15 Jan 11 // URL: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. (Дата обращения - 10.05.2023) [↑](#footnote-ref-137)
138. Significant Cyber Incidents Since 2006 (CSIS) [Электронный ресурс] // URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Дата обращения - 10.05.2023) [↑](#footnote-ref-138)
139. ICTY, *Tadić,* Decision on the Defence Motion, para 126. [↑](#footnote-ref-139)
140. Commentary on the Additional Protocols, para 2007. [↑](#footnote-ref-140)
141. Ibid., para 2008. [↑](#footnote-ref-141)
142. Tallinn Manual, Rule 100, para. 5, at 437. [↑](#footnote-ref-142)
143. Mačák, K. Unblurring the lines: military cyber operations and international law // Journal of Cyber Policy. – 2021. – 6(3). – p. 411, 421–422. [↑](#footnote-ref-143)
144. Mačák K., Gisel, L. Grammar: Rules in a Cyber Conflict, Pawlak P., Delerue F. (eds) // Cyber Defence in the European Union, EUISS. – 2022. – p. 67. [↑](#footnote-ref-144)
145. AP I, Art. 54; Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II), Art. 14; ICRC Customary Law Study, above note 63, Rule 54. [↑](#footnote-ref-145)
146. Gisel, L. Rodenhauser, T., Dormann, K. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts // International Review of the Red Cross. – 2020. – 102 (913). – pp. 287–334. – p. 318. [↑](#footnote-ref-146)
147. Ibid. [↑](#footnote-ref-147)
148. Tallinn Manual, Rule 100, para. 6. [↑](#footnote-ref-148)
149. Ministry of Defence of Denmark, Military Manual on International Law Relevant to Danish Armed Forces in International Operations. – 2016. – 292. [↑](#footnote-ref-149)
150. Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire. – 14 January 2020, cited in OAS, Improving Transparency: International Law and State Cyber Operations: Fifth Report, OAS Doc. CJI/doc. 615/20 rev.1. – 7 August 2020. – para 36. [↑](#footnote-ref-150)
151. Schondorf, R. Israel’s perspective on key legal and practical issues concerning the application of international law to cyber operations // International Law Studies. – 2021. – 97. – p. 401. [↑](#footnote-ref-151)
152. Mačák, K. Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law // Israel Law Review. – Vol. 48. – No. 1. – 2015. – p. 80; McLaughlin, R. Data as a Military Objective // Australian Institute of International Affairs. – 20 September 2018; Heather A Harrison Dinniss, The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives // 48 IsrLR 39. – 2015; McCormack, T. International Humanitarian Law and the Targeting of Data // 94 International Law Studies 222. – 2018. [↑](#footnote-ref-152)
153. Tallinn Manual, rule 100, p. 7, 437. [↑](#footnote-ref-153)
154. Ibid. [↑](#footnote-ref-154)
155. Mačák, K. Military Objectives 2.0, p. 76. [↑](#footnote-ref-155)
156. Ibid, p. 76–77. [↑](#footnote-ref-156)
157. Tallinn Manual 2.0, Rule 131. [↑](#footnote-ref-157)
158. Finland, International Law and cyberspace: Finland’s national positions. – 2020. – p. 7. [↑](#footnote-ref-158)
159. Federal Government of Germany, On the Application of International Law in Cyberspace // Position Paper. – March 2021. – p. 8. [↑](#footnote-ref-159)
160. Norway, Manual i krigens folkerett. – 2013. – para 9.58. [↑](#footnote-ref-160)
161. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136. – August 2021. – p. 78. [↑](#footnote-ref-161)
162. Ministere Des Armees, International Law Applied To Operations in Cyberspace. Paris: Delegation a l’information et a la communication de la defense. – 2019. – p. 15. [↑](#footnote-ref-162)
163. Ibid, p. 14. [↑](#footnote-ref-163)
164. Майкл Н. Шмитт является американским специалистом в области международного права, специализирующимся на международном гуманитарном праве, вопросах применения силы и международном праве, применимом к киберпространству; является профессором публичного международного права в Университете Рединга, почетным научным сотрудником Г. Нормана Либера в Институте Либера Военной академии США в Вест-Пойнте и почетным научным сотрудником Чарльза Х. Стоктона в резиденции Военно-морского колледжа США. Главный редактор Таллиннского руководства. [↑](#footnote-ref-164)
165. Schmitt, M. N. The Nature of ‘Objects’ During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision // 48 Israel law review. – 81. – 2015. – p. 84. [↑](#footnote-ref-165)
166. Dinniss, H. H. The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives // Israel Law Review. – Vol. 48. – No. 1. – 2015. – p. 41. [↑](#footnote-ref-166)
167. Ibid. [↑](#footnote-ref-167)
168. Ibid,*,* p. 54. [↑](#footnote-ref-168)
169. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts // Geneva, ICRC Challenges Report 2015. – 2015. – p. 43. [↑](#footnote-ref-169)
170. Ibid. [↑](#footnote-ref-170)
171. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts // Geneva, ICRC Challenges Report. – 2019. – p. 21. [↑](#footnote-ref-171)
172. ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts // ICRC position paper. – November 2019. – p. 8. [↑](#footnote-ref-172)
173. Помимо упомянутых выше стран стоит отметить также позицию Швейцарии, которая прямо указывает на то, что «вопрос о том, как именно защищаются данные при отсутствии физического повреждения, остается сложной задачей», Switzerland’s Position Paper on the Application of International Law in Cyberspace (Federal Department of Foreign Affairs. – 2021. – p. 10; В это же время Швеция уклоняется от прямого выражения позиции относительно данных, а просто ссылается на то, что «изменение данных и вмешательство в них без причинения физического вреда также может нарушать суверенитет», Position Paper on the Application of International Law in Cyberspace, Government Offices of Sweden. – July 2022. – p. 2. [↑](#footnote-ref-173)
174. Гаркуша-Божко, С. Ю. Международное гуманитарное право в киберпространстве. – С. 67. [↑](#footnote-ref-174)
175. Geiss, R., Lahmann, H. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space // Israel Law Review. – 45. – 2012. – p. 384. [↑](#footnote-ref-175)
176. ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law // Geneva. – 2009. – p. 43. [↑](#footnote-ref-176)
177. Tallinn Manual, p 82. [↑](#footnote-ref-177)
178. Schmitt, M. N. Cyber Operations and the Jus in Bello: Key Issues // International Law Studies 87. – 2011. – p. 101. [↑](#footnote-ref-178)
179. Schmitt, M. N. Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations // International Review of the Red Cross. – Vol. 101. – No. 910, 2019. – pp. 333–355; ICRC, General Assembly official records, 66th session: 1st Committee, 9th meeting. – 11 October 2011. – New York. – p. 21. [↑](#footnote-ref-179)
180. Tallinn Manual, Rule 43. [↑](#footnote-ref-180)
181. Dinniss, H. H. Cyber Warfare and the Laws of War, p. 203. [↑](#footnote-ref-181)
182. Гаврилова, М. Применение международного права в киберпространстве, с. 103. [↑](#footnote-ref-182)
183. Гаркуша-Божко, С. Ю. Применение принципов международного гуманитарного права (принципы проведения различия, соразмерности и предосторожности) к вооруженным конфликтам в киберпространстве // Российский журнал правовых исследований. – 2021. – Т. 8. – № 3. – С. 86. [↑](#footnote-ref-183)
184. Commentary on the Additional Protocols, para. 1963. [↑](#footnote-ref-184)
185. ДП I, ст. 51(4)–(5); ICRC Customary Law Study, Rules 11, 14. [↑](#footnote-ref-185)
186. Schmitt, M. N. The Law of Cyber Targeting // Naval War College Review. – Vol. 68. – No. 2. – 2015. – Article 3. – p. 8. [↑](#footnote-ref-186)
187. Ibid. [↑](#footnote-ref-187)
188. Dinstein, Y. The Conduct of Hostilities Under the Law of International Armed Conflict // 145 (2d ed.). – 2010; Tallinn Manual 2.0, 487. [↑](#footnote-ref-188)
189. Например, Киберкомандование США, основной штаб Министерства обороны по ведению кибервойн, расположено в Форт-Миде, штат Мэриленд, в пределах одной мили от гражданских объектов. [↑](#footnote-ref-189)
190. ДП I, ст. 52(2). [↑](#footnote-ref-190)
191. Tallinn Manual 2.0, p. 490. [↑](#footnote-ref-191)
192. Ibid, p. 437. [↑](#footnote-ref-192)
193. ICRC Commentary, p. 693. [↑](#footnote-ref-193)
194. U.S. Dep’t of Defense, Law of War Manual, para 5.14; Tallinn Manual 2.0, p. 487. [↑](#footnote-ref-194)
195. ICRC Commentary, at 693. [↑](#footnote-ref-195)
196. Tallinn Manual, p. 488. [↑](#footnote-ref-196)
197. ICRC Commentary, at 692; Tallinn Manual, p. 489. [↑](#footnote-ref-197)
198. Ibid. [↑](#footnote-ref-198)
199. Queguiner, J. Precautions Under the Law Governing the Conduct of Hostilities // 88 Int’l Rev. Red. Cross 793, 818. – 2006. [↑](#footnote-ref-199)
200. Ibid. [↑](#footnote-ref-200)
201. Tallinn Manual, p. 488. [↑](#footnote-ref-201)
202. См. об этом: ICRC, Avoiding civilian harm from military cyber operations during armed conflicts, report of ICRC expert meet-ing, 21–22 January 2020, Geneva (ICRC expert report). [↑](#footnote-ref-202)
203. UN General Assembly, Resolution 70/237, Developments in the field of information and telecommunications in the context of international security, adopted on 23 December 2015. [↑](#footnote-ref-203)
204. Ibid., p. 8 para. 13(f). [↑](#footnote-ref-204)
205. Ibid., p. 8 para. 13(g). [↑](#footnote-ref-205)
206. Goldman, L. IDF sends text message to Gaza mobile phones: ‘The next phase is on the way’, [Электронный ресурс], +972 Magazine, 16 November 2012 // URL: https://www.972mag.com/idf-sends-text-message-to-gaza-mobile-phones-the-next-phase-is-on-the-way/ (Дата обращения: 01.03.2023) [↑](#footnote-ref-206)
207. ICRC, Customary IHL, Rule 15, Principle of Precautions in Attack. [↑](#footnote-ref-207)
208. ICRC expert report. – p. 26. [↑](#footnote-ref-208)
209. Segal, A. The Hacked World Order // Public Affairs, New York. – 2016. – p. 3. [↑](#footnote-ref-209)
210. Jackson, W. Stuxnet shut down by its own kill switch, GCN. – 26 June 2012. [↑](#footnote-ref-210)
211. Kasandra Adams, Geofencing as applied within the field of cybersecurity: an overview of potential risks and advantages, California State University. – 2020. [↑](#footnote-ref-211)
212. ICRC expert report, p. 26. [↑](#footnote-ref-212)
213. Ibid, p. 27. [↑](#footnote-ref-213)
214. Ibid, p. 28. [↑](#footnote-ref-214)
215. Schmitt, M. N. Wired warfare 3.0: protecting the civilian population during cyber operations // International Review of the Red Cross. – 2019. – 101 (1). – p. 346. [↑](#footnote-ref-215)