

ПРОЕКТ ДЛЯ ЧЕТВЕРТОЙ КОНСУЛЬТАЦИИ С  
ГОСУДАРСТВАМИ

# **Направление деятельности 6. СОБЛЮДЕНИЕ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ**

СОПРЕДСЕДАТЕЛИ: Гана, Люксембург, Мексика, Швейцария и  
Международный Комитет Красного Креста

## **Краткий обзор**

Информационно-коммуникационные технологии (ИКТ) стали неотъемлемой частью жизни людей по всему миру. В нашем цифровом и взаимосвязанном мире предоставление гражданскому населению критически важных услуг, а также возможность людей общаться с близкими и заниматься экономической деятельностью зависят от целостности и доступности ИКТ. В затронутых конфликтами районах надежные ИКТ имеют решающее значение для

обеспечения доступа гражданского населения к основным товарам и услугам, для предоставления услуг государствами, а также для поддержки медицинской и гуманитарной деятельности, в том числе деятельности Международного движения Красного Креста и Красного Полумесяца. Несмотря на то что с помощью ИКТ воюющие стороны способны достигать военных целей, не причиняя гражданским лицам и объектам вреда или причиняя им меньший вред по сравнению с операциями с использованием кинетического оружия, применение ИКТ в современных конфликтах также имеет разрушительные последствия, затрагивающие гражданское население и инфраструктуру и нередко носящие трансграничный характер.

Участники дискуссий в рамках данного направления деятельности подчеркнули необходимость защищать гражданское население и обеспечивать сохранение человеческого достоинства в условиях как современных, так и будущих конфликтов. Для этого крайне важно добиться более строгого соблюдения международного гуманитарного права (МГП) при использовании ИКТ во время вооруженных конфликтов, с тем чтобы обеспечить бесперебойное функционирование инфраструктуры, сетей и коммуникаций, защитить данные от уничтожения и предотвратить паралич нормальной жизни общества.

В рамках этого направления деятельности также были выработаны практические рекомендации. В частности, было рекомендовано:

- защищать гражданское население, данные гражданского назначения и гражданскую инфраструктуру от наносящей вред деятельности в сфере ИКТ;
- защищать медицинские службы и гуманитарные организации от цифровых угроз и обеспечить соблюдение запрета на применение сексуального насилия, а также запрета на вербовку детей и их вовлечение в военные действия, в том числе с помощью цифровых средств;
- устранить риск распространения информации в нарушение норм МГП;
- свести к минимуму риски причинения вреда гражданскому населению в результате использования гражданской ИКТ-инфраструктуры в военных целях, а также принимать меры, для того чтобы гражданские лица (включая хакеров и сотрудников технологических компаний), участвующие в деятельности в сфере ИКТ, не допускали нарушения норм МГП и не подвергали неосознанно себя риску.

Участники дискуссий в рамках данного направления подчеркнули, что в целях обеспечения соблюдения МГП в ходе деятельности в сфере ИКТ важно:

- признать, что в затронутых конфликтами районах надежные ИКТ имеют крайне важное значение для гражданских лиц, государственных органов и гуманитарных организаций, и что деятельность в сфере ИКТ может иметь гуманитарные последствия (приводя к страданиям, ранениям и гибели людей), даже не причиняя при этом физического ущерба, что подчеркивает необходимость соблюдения гуманитарных принципов и обеспечения сохранения человеческого достоинства в ходе военных действий;
- обеспечивать применение норм МГП и разъяснять, каким образом применять их в ходе деятельности в сфере ИКТ, а также принимать практические индивидуальные и коллективные меры для минимизации рисков для гражданского населения и обеспечения того, чтобы деятельность в сфере ИКТ при любых обстоятельствах

осуществлялась в соответствии с нормами и принципами МГП, гарантирующими защиту;

- продолжать изучать и обсуждать то, каким образом МГП применяется к деятельности в сфере ИКТ, опираясь на выводы, сделанные по итогам обсуждений, уже состоявшихся в рамках данного направления, в целях выработки общего понимания относительно способов защиты гражданских лиц от причинения им вреда;
- повысить прозрачность в отношениях между государствами за счет обнародования ими своих позиций по вопросам применения международного права, включая МГП, к деятельности в сфере ИКТ, а также за счет обмена опытом и полезными наработками в части минимизации рисков причинения вреда гражданскому населению;
- поддерживать наращивание потенциала на двустороннем, региональном и глобальном уровнях для обеспечения более эффективного соблюдения государствами норм МГП применительно к деятельности в сфере ИКТ.

## Ожидаемые результаты

### **1. Защита гражданского населения, данных гражданского назначения и гражданской инфраструктуры от вреда, причиняемого им в результате деятельности в сфере ИКТ во время вооруженных конфликтов.**

Современные вооруженные конфликты показывают, что деятельность в сфере ИКТ может создавать риски для гражданского населения, данных гражданского назначения и гражданской инфраструктуры. Она может иметь серьезные последствия для гражданского населения, а также для других покровительствуемых лиц и объектов, в том числе в случаях нарушения функционирования основных гражданских служб (таких как электро- и водоснабжение, канализация, телекоммуникации, здравоохранение, гуманитарная деятельность, службы экстренной помощи, финансовые услуги), даже в отсутствие физического ущерба.

Деятельность в сфере ИКТ, осуществляемая в условиях вооруженных конфликтов и в связи с ними, при любых обстоятельствах должна соответствовать нормам и принципам МГП, включая принцип гуманности, принцип настоящей военной необходимости, принцип проведения различия, принцип соразмерности и принцип принятия мер предосторожности.

Операции в сфере ИКТ, которые, как ожидается, приведут к гибели или ранению людей либо к повреждению или уничтожению тех или иных объектов, в соответствии с МГП квалифицируются как «нападения». К ним относятся операции, способные привести к выходу из строя оборудования или систем, для восстановления функционирования которых могут потребоваться их замена, переустановка или ремонт. Подобные операции в сфере ИКТ должны проводиться с соблюдением всех принципов и норм МГП, касающихся ведения военных действий, включая нормы, запрещающие нападения на гражданских лиц и гражданские объекты, неизбирательные и несоразмерные нападения, а также принцип принятия мер предосторожности.

Данные являются ключевым ресурсом в современном мире в условиях всё большей цифровизации, обеспечивают функционирование основных гражданских служб и играют важную роль в вопросах ведения гуманитарной деятельности. Способы использования данных

во время вооруженных конфликтов могут напрямую влиять на человеческие жизни и достоинство. В частности, медицинские, биометрические и финансовые данные, а также данные, собираемые гуманитарными организациями, имеют важное значение для целей предоставления государственных и социальных услуг. Уничтожение или изменение таких данных, ограничение доступа к ним или их несанкционированное разглашение могут нарушить функционирование критически важных систем и подвергнуть отдельных лиц и целые сообщества серьезному риску в плане причинения им вреда.

Защита гражданского населения, данных гражданского назначения и гражданской инфраструктуры от опасностей, возникающих в результате деятельности в сфере ИКТ во время вооруженного конфликта, обеспечивается с помощью целого ряда принципов и норм МГП, включая:

- принцип, согласно которому сторона в вооруженном конфликте может прибегать только к тем средствам и методам ведения войны, которые необходимы для ослабления военных сил противника;
- принципы и нормы, регулирующие ведение военных действий, включая нормы, запрещающие нападения на гражданских лиц и гражданские объекты, неизбирательные и несоразмерные нападения, а также принцип принятия мер предосторожности;
- обязательство на постоянной основе обеспечивать защиту гражданского населения, гражданских лиц и гражданских объектов при проведении военных операций;
- нормы, обеспечивающие защиту собственности от мародерства, захвата и уничтожения.

При этом нормы МГП не запрещают деятельность по сбору информации как таковую, в том числе деятельность, в рамках которой осуществляется доступ к тем или иным данным.

Для усиления защиты гражданского населения, данных гражданского назначения и гражданской инфраструктуры от вреда, причиняемого в результате деятельности в сфере ИКТ во время вооруженного конфликта, государства и стороны в вооруженном конфликте должны:

- a) разработать и применять строгие протоколы выбора целей при проведении операций в сфере ИКТ для обеспечения соблюдения МГП, включая проверку объектов на предмет их соответствия критериям военного объекта и отсутствия предоставленной им особой защиты, а также оценку рисков причинения случайного вреда гражданскому населению и предотвращение или, во всяком случае, сведение к минимуму таких рисков;
- b) при проведении операций в сфере ИКТ (в том числе при применении протоколов выбора целей) руководствоваться полной информацией из всех доступных при существующих обстоятельствах источников, включая надежные разведывательные и другие данные, с привлечением юридических консультантов, как того требуют нормы МГП; а также в максимально возможной степени консультироваться со специалистами в области кибербезопасности и другими профильными техническими специалистами по таким вопросам, как структура ИКТ-инфраструктуры, взаимосвязанность ее отдельных объектов и зависимость гражданского населения от их функционирования;

- c) в тех случаях, когда ИКТ-инфраструктура согласно МГП квалифицируется как военный объект, но при этом продолжает выполнять гражданские функции — при планировании и проведении нападений учитывать все разумно прогнозируемые прямые и косвенные случайные последствия полной или частичной утраты возможности использования такой ИКТ-инфраструктуры в гражданских целях для гражданского населения, данных гражданского назначения и гражданской инфраструктуры, в том числе последствия для основных гражданских служб, функционирование которых зависит от данной ИКТ-инфраструктуры, руководствуясь принципом соразмерности и принципом принятия мер предосторожности;
- d) при соблюдении обязательства принимать все возможные меры предосторожности при выборе средств и методов ведения боевых действий выбирать те средства и методы, которые, как ожидается, причинят наименьший случайный вред гражданскому населению, в том числе посредством проведения тщательной оценки того, позволят ли средства и методы ведения боевых действий, в основе которых лежит использование ИКТ (или другие средства и методы, не предполагающие применение кинетического оружия), снизить риск причинения вреда гражданским лицам по сравнению с использованием кинетического оружия;
- e) при проведении операций в сфере ИКТ использовать надлежащие ограничения в части территории и сроков проведения операций, а также в части выбора конкретных систем, которые будут подвергнуты нападению, с тем чтобы предотвратить или, во всяком случае, свести к минимуму риск причинения случайного вреда гражданскому населению;
- f) на постоянной основе осуществлять мониторинг операций в сфере ИКТ и обеспечить возможность скорректировать или прекратить их, с тем чтобы предотвратить причинение непреднамеренного вреда гражданскому населению (или вреда, которое перевешивает конкретное и явное военное преимущество). По возможности, внедрять технические средства защиты (например, системы экстренного аварийного отключения), позволяющие останавливать, ограничивать или изолировать операции в сфере ИКТ при возникновении риска того, что их последствия затронут не только намеченную цель, но и гражданские сети или инфраструктуру, а также сети или инфраструктуру третьих государств.

## **2. Минимизация риска причинения вреда гражданскому населению в результате использования гражданской ИКТ-инфраструктуры в военных целях во время вооруженного конфликта.**

За исключением некоторых военных сетей, среда ИКТ является преимущественно гражданской. Однако взаимосвязанность гражданских и военных сетей и использование гражданской ИКТ-инфраструктуры в военных целях порождают ряд проблем в связи с ее защитой.

Использование ИКТ-инфраструктуры (включая инфраструктуру, предоставляемую технологическими компаниями) в военных целях не превращает ее или даже отдельные ее части автоматически в военный объект согласно МГП. Тем не менее подобное использование повышает риск того, что данная инфраструктура станет объектом для нападения, в результате

чего гражданские лица и гражданские объекты, находящиеся вблизи такой инфраструктуры, подключенные к ней или зависящие от нее, могут подвергнуться непреднамеренному ущербу.

МГП запрещает нападения на гражданские объекты, в том числе на гражданскую ИКТ-инфраструктуру. Однако использование такой инфраструктуры или ее части в военных целях может привести к тому, что они будут признаны военными объектами.

При нападении на такие военные объекты государства и стороны в вооруженном конфликте должны соблюдать запреты на неизбирательные и несоразмерные нападения и принцип принятия мер предосторожности, в том числе в тех случаях, когда гражданское население зависит от данной ИКТ-инфраструктуры, обеспечивающей предоставление критически важных услуг. По возможности они должны совершать операции в отношении только тех компонентов ИКТ-инфраструктуры, которые используются для военных целей, не затрагивая при этом компоненты, используемые для обслуживания гражданского населения.

Государства и стороны в вооруженных конфликтах должны в максимально возможной степени принимать все необходимые меры предосторожности для защиты гражданского населения и гражданских объектов, находящихся под их контролем, от опасностей, возникающих в результате проведения военных операций, в частности от последствий нападений.

С тем чтобы свести к минимуму риск причинения вреда гражданскому населению в результате использования гражданской ИКТ-инфраструктуры в военных целях во время вооруженного конфликта, и в дополнение к мерам, перечисленным в пункте 1 раздела «Ожидаемые результаты» выше, государства и стороны в вооруженном конфликте, под контролем которых данная инфраструктура находится, должны:

- a) выделять достаточные финансовые и технические ресурсы, а также принимать надлежащие меры по планированию, проектированию и конфигурации систем как до возникновения, так и во время вооруженного конфликта;
- b) по возможности физически или технически отделять компоненты ИКТ-инфраструктуры, используемые в военных целях, от ее компонентов, которые используются в гражданских целях, в том числе посредством сегментации сетей и конфигурации соответствующих систем. К таким мерам относится отделение данных, используемых в военных целях, от данных гражданского назначения, например посредством их отдельного хранения, отдельной работы с ними и разграничения доступа к ним;
- c) повышать устойчивость ключевой гражданской ИКТ-инфраструктуры и зависящих от нее основных гражданских служб, в том числе посредством резервирования систем, разработки планов действий в чрезвычайных ситуациях и принятия иных мер в целях снижения риска причинения случайного вреда гражданскому населению.

### **3. Минимизация рисков, связанных с участием в деятельности в сфере ИКТ во время вооруженного конфликта гражданских лиц, находящихся на территории того или иного государства или под его юрисдикцией или контролем.**

В последнее время участились случаи вовлечения гражданских лиц в деятельность в сфере ИКТ во время вооруженных конфликтов. В некоторых случаях государства терпимо относятся к

участию гражданских лиц в деятельности в сфере ИКТ в отношении противника (в том числе в деятельности, которая может затронуть гражданских лиц и гражданские объекты), содействуют такому участию или поощряют его.

Чем ближе гражданские лица оказываются к боевым действиям, тем больше они подвергаются опасности. Многие при этом могут не осознавать сопутствующие риски и потенциальные юридические последствия своих действий, а также не знать о нормах МГП, которые они должны соблюдать.

Гражданские лица, включая хакеров и сотрудников технологических компаний, при осуществлении деятельности в сфере ИКТ в условиях вооруженных конфликтов и в связи с ними, обязаны соблюдать МГП.

Государства и стороны в вооруженном конфликте несут ответственность за нарушения МГП, совершенные гражданскими лицами, в том числе хакерами и сотрудниками технологических компаний, чья деятельность в сфере ИКТ в условиях такого конфликта может быть присвоена данным государствам или сторонам. Государства должны принимать надлежащие меры для предотвращения нарушений МГП, совершаемых гражданскими лицами, находящимися на территории соответствующего государства или под его юрисдикцией или контролем, при осуществлении деятельности в сфере ИКТ, и пресекать любые такие нарушения, в соответствии со своими обязательствами в рамках МГП. Государства должны обеспечить осведомленность находящихся на их территории гражданских лиц о нормах МГП. Кроме того, они не должны поощрять гражданских лиц, участвующих в деятельности в сфере ИКТ, нарушать МГП, а также помогать или содействовать им в совершении таких нарушений.

В исключительных случаях участие гражданских лиц в деятельности в сфере ИКТ может быть приравнено к непосредственному участию в военных действиях; это означает, что такие гражданские лица утрачивают защиту от нападения, но лишь в подобных ситуациях. Однако в соответствии с нормами МГП при наличии сомнений гражданские лица должны считаться подпадающими под защиту от нападений.

При этом привлечение детей к участию в боевых действиях во время вооруженного конфликта, в том числе в рамках деятельности в сфере ИКТ, должно быть недопустимым.

Для сведения к минимуму рисков, связанных с участием гражданских лиц в деятельности в сфере ИКТ во время вооруженного конфликта, государства и стороны в вооруженном конфликте должны:

- a)** принимать конкретные меры для информирования гражданских лиц, участвующих в деятельности в сфере ИКТ в условиях вооруженного конфликта и в связи с ним, о правовых и практических рисках участия в данной деятельности. Такие меры могут включать распространение информации о нормах МГП через социальные сети, специальные приложения, радио и другие средства массовых коммуникаций либо разработку соответствующих МГП типовых кодексов поведения, соблюдение которых следует рекомендовать гражданским лицам, осуществляющим деятельность в сфере ИКТ;
- b)** для защиты гражданского населения от опасностей, возникающих в результате военных действий, по возможности избегать вовлечения гражданских лиц в операции в сфере ИКТ, представляющие собой прямое участие в военных действиях. Если же избежать этого не удастся, соответствующие гражданские лица должны быть по возможности интегрированы в состав официальных вооруженных сил;

- с) принимать все возможные меры для предотвращения вовлечения детей в военные действия посредством их участия в деятельности в сфере ИКТ. Такие меры могут включать образовательные программы и мероприятия по повышению информированности для детей и лиц, осуществляющих за ними уход; принятие и обеспечение применения национальных законов и политики, вводящих запрет на вербовку детей и их вовлечение в военные действия, в том числе с помощью цифровых средств; изучение возможности введения возрастных ограничений на доступ к цифровым инструментам, использование которых может быть приравнено к непосредственному участию в военных действиях.

#### **4. Защита относящихся к сфере ИКТ продуктов и сервисов гражданского назначения, доступ к которым предоставляется технологическими компаниями во время вооруженного конфликта.**

Технологические компании всё чаще предоставляют сторонам в вооруженном конфликте услуги и продукты в области обеспечения кибербезопасности, а также доступ к другим продуктам и сервисам, относящимся к сфере ИКТ. В подобных случаях гражданские лица и гражданские объекты, использующие такие продукты и сервисы или имеющие к ним отношение, могут подвергнуться опасности.

При этом относящиеся к сфере ИКТ продукты и сервисы, доступ к которым предоставляется технологическими компаниями, широко используются гражданским населением, государственными органами и беспристрастными гуманитарными организациями, в том числе во время вооруженных конфликтов. Поэтому сбои в работе данных продуктов и сервисов, ухудшение их качества или их ненадлежащее использование могут иметь серьезные гуманитарные последствия. В соответствии с нормами МГП такие гражданские продукты и сервисы, относящиеся к сфере ИКТ, а также гражданский персонал, занимающийся их поддержкой, пользуются защитой.

Для усиления защиты подобных продуктов и сервисов, предоставляемых технологическими компаниями во время вооруженного конфликта, эти компании должны:

- а) понимать, что предоставление сторонам в вооруженном конфликте доступа к продуктам и сервисам, относящимся к сфере ИКТ, сопряжено с правовыми и практическими рисками;
- б) осознавать риски причинения вреда гражданскому населению и гражданским объектам (в том числе сотрудникам и имуществу технологических компаний, а также лицам и объектам, находящимся вблизи соответствующей ИКТ-инфраструктуры, зависящим от нее или подключенным к цифровым сервисам), оценивать такие риски и принимать меры для их минимизации. В частности, технологические компании должны по возможности физически или технически отделять свою инфраструктуру и свои сервисы и продукты, используемые для обеспечения военных операций, от инфраструктуры, сервисов и продуктов, которые используются в гражданских целях;
- с) предотвращать участие или соучастие своего персонала в совершении нарушений МГП (в том числе заключающееся в предоставлении доступа к соответствующим продуктам или сервисам сторонам в вооруженном конфликте) и надлежащим образом реагировать на любые подобные случаи.

## **5. Защита медицинских служб, гуманитарных организаций и других пользующихся особой защитой лиц, объектов и видов деятельности от вреда, причиняемого в результате осуществления деятельности в сфере ИКТ во время вооруженного конфликта.**

Сектор здравоохранения и беспристрастные гуманитарные организации особенно уязвимы перед последствиями деятельности в сфере ИКТ во время вооруженных конфликтов. Ввиду того что медицинские службы и гуманитарные организации всё сильнее зависят от взаимосвязанных систем и цифровых данных, сбои в функционировании ИКТ-инфраструктуры или связанных с ней сервисов могут напрямую повлиять на жизненно важную деятельность медицинских учреждений, привести к компрометации конфиденциальных данных, помешать работе беспристрастных гуманитарных организаций и их сотрудников, а также поставить под угрозу оказание необходимой помощи нуждающимся.

Медицинский персонал, медицинские формирования и санитарно-транспортные средства, а также сотрудники гуманитарных организаций и объекты, используемые в рамках гуманитарной деятельности, должны при любых обстоятельствах пользоваться уважением и защитой в соответствии с нормами МГП, в том числе защитой от вреда, причиняемого в результате деятельности в сфере ИКТ. Деятельность в сфере ИКТ во время вооруженного конфликта не должна приводить к ненадлежащему нарушению функционирования медицинских служб и гуманитарных организаций и, в частности, не должна затрагивать принадлежащие им данные, ИКТ-системы и коммуникационное оборудование.

При этом в соответствии с нормами МГП должна быть обеспечена конфиденциальность медицинских данных и данных, собираемых гуманитарными организациями. Это крайне важно для сохранения доверия к работе медицинских служб и беспристрастных гуманитарных организаций.

Стороны в вооруженном конфликте должны также принимать все возможные (при существующих обстоятельствах и с учетом имеющихся у них ресурсов) меры для защиты медицинских служб и гуманитарных организаций от причинения им вреда, в том числе от негативных последствий деятельности в сфере ИКТ, которая осуществляется третьими лицами (например, киберпреступниками или другими негосударственными акторами) и не может быть присвоена той или иной стороне в конфликте.

Некоторые другие объекты и виды деятельности, в соответствии с нормами МГП пользующиеся особой защитой, в том числе объекты, необходимые для выживания гражданского населения, установки и сооружения, содержащие опасные силы, культурные объекты и объекты гражданской обороны, также могут подвергаться серьезным рискам негативных последствий деятельности в сфере ИКТ. Им должно быть обеспечена особая защита, в том числе при осуществлении деятельности в сфере ИКТ во время вооруженных конфликтов. Защита распространяется также и на принадлежащие этим объектам данные и ИКТ-инфраструктуру, необходимую для их функционирования.

Деятельность в сфере ИКТ может также использоваться для совершения или облегчения совершения актов сексуального насилия либо для вербовки детей и их вовлечения в военные действия. Нормы МГП запрещают сексуальное насилие, а также вербовку детей и их вовлечение в военные действия, в том числе с использованием для этих целей ИКТ.

Для защиты медицинских служб, гуманитарных организаций и других пользующихся особой защитой лиц, объектов и видов деятельности от вреда, причиняемого в результате осуществления деятельности в сфере ИКТ во время вооруженного конфликта, государства и стороны в вооруженном конфликте должны:

- a) поддерживать дискуссии и усилия, направленные на то, чтобы медицинские службы и гуманитарные организации, в соответствии с нормами МГП пользующиеся особой защитой, были легко идентифицируемыми и распознаваемыми, в том числе с помощью разрабатываемой в настоящее время «цифровой эмблемы», а также продолжать взаимодействие с МККК для проработки правовых, технических и дипломатических способов ее внедрения;
- b) недвусмысленно подтвердить свое обязательство уважать и защищать медицинские службы и гуманитарные организации (в том числе принадлежащие им данные, ИКТ-системы и коммуникационное оборудование), содействовать их работе в среде ИКТ, а также обеспечивать особую защиту для объектов, необходимых для выживания гражданского населения (в том числе в отношении принадлежащих им данных и ИКТ-инфраструктуры, необходимой для их функционирования). Эти обязательства должны быть закреплены в национальных законах, политике и военной доктрине и применяться на практике;
- c) по возможности содействовать разработке достаточных мер в области обеспечения кибербезопасности и защиты данных в интересах медицинских служб и беспристрастных гуманитарных организаций, а также оказывать им помощь в повышении устойчивости перед лицом опасностей, связанных с использованием ИКТ и затрагивающих их системы и деятельность;
- d) укреплять соответствующие национальные правовые и политические механизмы, регулирующие поведение в сети интернет, которое может представлять собой нарушения МГП (или содействовать совершению таких нарушений) в части сексуального насилия либо в части вербовки детей и их привлечения к участию в вооруженных конфликтах, а также обеспечить эффективное применение соответствующих механизмов и координацию усилий профильных государственных органов;
- e) закрепить конкретные меры защиты в военной доктрине, стандартных руководствах по проведению военных операций и правилах применения оружия в целях предотвращения и пресечения нарушений, совершаемых при осуществлении деятельности в сфере ИКТ, включая сексуальное насилие, а также вербовку детей и их вовлечение в военные действия. Возможные меры включают регулирование использования персональных ИКТ-устройств в ходе операций, ограничение распространения конфиденциальных изображений и данных, запрет использования ИКТ для вербовки детей и их вовлечения в военные действия, а также информирование детей и лиц, осуществляющих за ними уход, о сопутствующих рисках.

## **6. Устранение риска распространения информации в нарушение норм МГП.**

В современных вооруженных конфликтах ИКТ всё чаще используются для распространения информации, которая может нарушать МГП. Хотя информационные операции уже давно представляют собой часть военных действий и не являются противозаконными как таковые,

использование ИКТ — особенно в социальных сетях или приложениях для обмена сообщениями либо в сочетании с искусственным интеллектом и другими новыми технологиями — способно существенно увеличить скорость и масштабы распространения вредоносной информации.

Государства должны воздерживаться от распространения информации в нарушение норм МГП, в том числе с использованием ИКТ, и принимать все возможные меры для предотвращения подобных случаев. Речь идет, в частности, о распространении информации, которая подстрекает к нарушениям МГП или поощряет их, подвергает лиц, лишенных свободы, оскорблениям или делает их уязвимыми, а либо имеет своей основной целью терроризирование гражданского населения.

Медицинские службы и гуманитарные организации должны быть защищены от дезинформации, распространяемой с помощью ИКТ с целью воспрепятствовать их работе во время вооруженных конфликтов, поскольку такие действия представляют собой необоснованное вмешательство и несовместимы с обязательством уважать и защищать сотрудников медицинских и гуманитарных организаций и их деятельность.

Для устранения риска распространения информации в нарушение норм МГП государства и стороны в вооруженном конфликте должны:

- a) принимать все возможные меры для оценки, предотвращения и сведения к минимуму риска осуществления информационных операций, которые могут нанести вред гражданскому населению и другим покровительствуемым лицам, например, ставя под угрозу их безопасность, посягая на их достоинство или лишая их доступа к критически важным услугам;
- b) воздерживаться от распространения информации, направленной на дегуманизацию противника или разжигающей ненависть к гражданскому населению, в том числе с помощью ИКТ, а также принимать надлежащие меры для предотвращения участия своих вооруженных сил, государственных органов и других лиц, действующих от имени соответствующего государства или стороны в вооруженном конфликте, в совершении подобных действий;
- c) по возможности оказывать медицинским службам и беспристрастным гуманитарным организациям содействие в повышении устойчивости к дезинформации и другим вредоносным информационным операциям, в том числе помогая им собирать, проверять и распространять достоверную информацию; повышая их готовность к реагированию на вредоносную информацию и содействуя им в разработке планов действий на случай распространения подобной информации; и содействуя разработке ими надлежащих мер реагирования на вредоносную информацию, затрагивающую гражданских лиц, находящихся на территориях, подконтрольных соответствующему государству или стороне в вооруженном конфликте;
- d) взаимодействовать с соответствующими субъектами, в том числе с представителями технологического сектора, в целях снижения риска использования онлайн-платформ или других ИКТ-сервисов для подстрекательства к нарушениям МГП, их поощрения или содействия их совершению, а также для причинения вреда гражданскому населению и гражданским объектам. В частности, следует разрабатывать надлежащие правовые и политические механизмы, а также рекомендовать технологическим компаниям внедрять меры, направленные на выявление и оценку вредоносной

информации, распространяемой в условиях вооруженного конфликта, и меры реагирования на подобные случаи;

- e) повысить устойчивость общества к вредоносным информационным операциям, в том числе посредством обеспечения доступа к надежным источникам, защиты журналистов и СМИ в соответствии с требованиями МГП и применимого законодательства, а также повышения готовности к оказанию помощи гражданскому населению в получении достоверной информации во время вооруженных конфликтов;
- f) воздерживаться от ограничения доступа гражданских лиц к сети интернет и другим ИКТ-сервисам, поскольку подобные меры способны навредить гражданскому населению. В тех случаях, когда введение подобных ограничений обусловлено настоятельной военной необходимостью, следует принимать меры по смягчению последствий для гражданского населения в максимально возможной степени.

#### **7. Сквозные меры по повышению эффективности применения МГП при осуществлении деятельности в сфере ИКТ.**

При исполнении предусмотренных МГП обязательств, касающихся осуществления деятельности в сфере ИКТ, государства должны (в том числе в мирное время):

- a) распространять информацию о нормах МГП среди военнослужащих и населения в целом (особенно среди лиц, занимающихся деятельностью в сфере ИКТ), а также закрепить принципы и нормы МГП (в том числе применимые к деятельности в сфере ИКТ) в национальных законах, военных доктринах, стандартных руководствах по проведению военных операций, правилах применения оружия и учебных программах;
- b) обеспечить военным подразделениям и командованию, отвечающим за операции в сфере ИКТ, возможность консультироваться с квалифицированными юридическими консультантами, в частности при планировании и проведении таких операций;
- c) проводить тщательный правовой анализ возможностей ИКТ как потенциальных новых видов оружия, методов или средств ведения войны, включая тестирование, оценку, проверку и подтверждение их эффективности, с целью всесторонней оценки их функционирования, распространения и воздействия на гражданские системы;
- d) принять все необходимые законодательные, регулятивные и другие меры (включая, при необходимости, криминализацию соответствующих действий) для предотвращения и пресечения нарушений МГП, совершаемых с помощью ИКТ теми или иными лицами или на той или иной территории, которые находятся под юрисдикцией или контролем данного государства;
- e) принять все возможные меры для предотвращения или ограничения распространения, перепрофилирования или ненадлежащего использования инструментов и возможностей ИКТ в тех случаях, когда существует явный риск того, что они могут способствовать нарушению МГП;
- f) содействовать принятию мер, направленных на добровольное распространение информации и укрепление доверия в целях снижения рисков для гражданской ИКТ-инфраструктуры, включая обмен передовыми наработками между государствами, налаживание каналов связи и создание других практических механизмов, способствующих минимизации рисков, а также добровольное информирование о

серьезных инцидентах, связанных с использованием ИКТ, приведших к причинению гражданским лицам непреднамеренного вреда, что способствовало бы взаимопониманию и снижению рисков;

- g)** повысить прозрачность и укрепить взаимопонимание в отношениях между государствами за счет выработки и обнародования ими своих позиций по вопросам применения международного права, включая МГП, к деятельности в сфере ИКТ, а также за счет обмена опытом и полезными наработками в части минимизации рисков причинения вреда гражданскому населению;
- h)** поддерживать наращивание потенциала на двустороннем, региональном и глобальном уровнях для обеспечения более эффективного соблюдения государствами норм МГП применительно к деятельности в сфере ИКТ;
- i)** содействовать сотрудничеству между государствами, технологическими компаниями, беспристрастными гуманитарными организациями и гражданским обществом в использовании ИКТ таким образом, чтобы усилить защиту гражданского населения, в том числе посредством разработки соответствующих рекомендаций и практических мер;
- j)** содействовать взаимодействию между технологическими компаниями и беспристрастными гуманитарными организациями в целях повышения готовности к реагированию на связанные с использованием ИКТ угрозы для лиц и объектов, пользующихся защитой, в том числе посредством обмена информацией и принятия мер по обеспечению кибербезопасности, с соблюдением при этом гуманитарных принципов нейтральности, беспристрастности и независимости;
- к)** закрепить в национальном законодательстве и внедрить в действующую практику подходы, учитывающие гендерные аспекты, возрастные особенности и особенности инвалидности, что способствовало бы более эффективному соблюдению МГП, в том числе в части выявления и обеспечения защиты от рисков, связанных с ИКТ.