



Перевод подготовлен
Лингвистическим центром
Российского Красного Креста

Предотвращение и минимизация цифровых угроз для людей, пострадавших в результате вооруженного конфликта

ПРОЕКТ ЭЛЕМЕНТОВ РЕЗОЛЮЦИИ

Ноябрь 2023 г.

ОБЩАЯ ИНФОРМАЦИЯ

Проект элементов предлагаемой резолюции о предотвращении и минимизации цифровых угроз для людей, затронутых вооруженным конфликтом, направлен на то, чтобы дать общее представление о возможном содержании отдельных пунктов, не предоставляя при этом окончательного проекта текста. За каждым пунктом следует обоснование, объясняющее, почему было бы полезно включить такой пункт в резолюцию. Этот документ предоставляется для консультаций с членами Международной конференции Красного Креста и Красного Полумесяца, чтобы собрать первый раунд комментариев и отзывов, а также получить первоначальное понимание того, будет ли предлагаемый подход приемлемым и достичь консенсуса.

Предоставляя комментарии и отзывы по этому документу, пожалуйста, рассмотрите следующие вопросы:

- Согласны ли вы с предлагаемыми элементами преамбулы и постановляющей части предлагаемой резолюции?
- Есть ли какие-либо элементы, которые отсутствуют или должны быть включены в резолюцию?

Подробных комментариев по формулировкам проекта элементов данной резолюции на данном этапе не ожидается.

Возможность прокомментировать конкретные формулировки будет позже, как только будет готов нулевой проект резолюции.

ВВЕДЕНИЕ

Доступность и надежность цифровых технологий, инфраструктуры (включая подключение к Интернету) и данных имеют большое значение и могут спасти жизни во время чрезвычайных ситуаций, в частности вооруженных конфликтов. Это позволяет людям выжить, узнавая, где они могут получить, например, еду, воду и одеяла, а также безопасное место для проживания, а также позволяет им связаться и найти членов семьи, с которыми они потеряли связь. Это позволяет правительствам предоставлять основные услуги населению и поддерживать гражданское управление. Конфиденциальность, целостность и доступность цифровых технологий и данных также важны для функционирования медицинских служб – как военных, так и гражданских – и являются неотъемлемой частью гуманитарных операций, в том числе операций Международного движения Красного Креста и Красного Полумесяца (Движение).

Цифровизация вооруженных конфликтов несет новые угрозы для жизни, безопасности и достоинства гражданских лиц, медицинского персонала, вышедших из строя военнослужащих и тех, кто занимается их защитой и оказанием помощи.

В то время как государственные и негосударственные субъекты использовали цифровые средства и методы ведения войны для победы над своими противниками, такие средства и методы также использовались для вывода из строя критически важной гражданской инфраструктуры и служб, для подстрекательства к насилию в отношении гражданского населения, медицинского и военного персонала, за исключением боевых действий, а также срывать усилия по оказанию медицинской и гуманитарной помощи или подорвать доверие к последним. Злонамеренное использование цифровых технологий разжигает конфликты, подрывает доверие и усугубляет уязвимости.

Растущее использование искусственного интеллекта в таких операциях рискует усугубить их масштабы и последствия. МККК вместе с партнерами по Движению был в авангарде привлечения внимания к угрозам, которые представляет собой цифровизация военных операций для гражданского населения, медицинского персонала и военнослужащих, вышедших из строя, и работал над пониманием и распространением знаний о международных гуманитарное право, применимое в вооруженных конфликтах, в том числе в отношении кибер- и информационных операций.

Более того, Движение продвинуло понимание защиты данных в гуманитарных операциях

(см. «Руководство по защите данных в гуманитарных операциях»), сформировало международный консенсус относительно важности защиты данных в контексте восстановления семейных связей

(см. 33-ю Международную конференцию, «Восстановление семейных связей при соблюдении конфиденциальности, в том числе в том, что касается защиты персональных данных», и согласовали конкретные меры членов Движения по защите гуманитарных данных

(см. Совет делегатов 2022 года, «Защита гуманитарных данных». Правительства работали в Организации Объединенных Наций). Форумы по информации и телекоммуникациям в контексте международной безопасности и защиты прав человека в цифровом пространстве: Предлагаемая резолюция, выдвинутая на уникальном гуманитарном форуме, организованном

Международной конференцией Красного Креста и Красного Полумесяца, призвана привлечь внимание к возникновению цифровых угроз гражданскому населению, медицинскому персоналу и покинувшему строй/ раненому военнослужащему, а также определить меры, которые государства и члены Движения могли бы предпринять для предотвращения или минимизации таких угроз.

Пункты преамбулы (П)

П 1: В этом пункте преамбулы можно было бы подчеркнуть важность наличия и целостности цифровых технологий, инфраструктуры (включая подключение к Интернету) и данных для предоставления основных услуг – включая медицинские и гуманитарные услуги – гражданскому населению и для помощи гражданским лицам в предоставлении информации о том, где получить безопасность, предметы, необходимые для выживания, и поддерживать семейные контакты, особенно во время вооруженного конфликта.

Обоснование: Установление общего понимания важности цифровых технологий, инфраструктуры и данных для жизни, безопасности и достоинства людей, пострадавших в результате вооруженного конфликта. П 2: В этом пункте преамбулы можно было бы напомнить, что государства разрабатывают цифровые возможности для военных целей и что эти возможности используются в текущих вооруженных конфликтах, и их использование в будущих конфликтах становится все более вероятным, и выразить обеспокоенность по поводу использования таких технологий для нанесения вреда гражданскому населению, медицинскому персоналу, военнослужащему вне несения службы, гражданским объектам и другим защищаемым лицам и объектам или случайно причинить такой вред, а также о риске того, что такие возможности причинят чрезмерные травмы и ненужные страдания.

Обоснование: признание военных событий в этой области и потенциальных человеческих жертв во время вооруженного конфликта.

П 3: В этом пункте преамбулы можно было бы выразить особую обеспокоенность по поводу потенциальных человеческих жертв, вызванных прямыми и косвенными последствиями киберопераций, которые нарушают гражданскую инфраструктуру, услуги и данные, необходимые для безопасности и поддержания достоинства человека, а также функционирования общества.

Обоснование: Признание потенциальной угрозы киберопераций для человека.

П 4: В этом пункте преамбулы можно было бы выразить особую обеспокоенность по поводу масштабов, скорости и охвата операций с цифровой информацией, а также потенциального вреда, который они могут причинить, разжигая насилие и ненависть, повышая напряженность и подрывая доступность и целостность информации, которая необходима гражданским лицам для их безопасности и выживания во время вооруженного конфликта.

Обоснование: Признание потенциальных человеческих издержек информационных операций.

П 5: В этом пункте преамбулы можно было бы выразить обеспокоенность по поводу гражданских лиц, в частности отдельных лиц, групп и компаний, которые проводят кибер- или информационные операции в связи с вооруженными конфликтами, а также по поводу того, что такие операции подвергают гражданское население вреду и подрывают принцип проведения различия.

Обоснование: Признание рисков, связанных с поощрением или терпимостью к участию гражданских лиц в кибер- и информационных операциях в связи с вооруженными конфликтами.

П 6: В этом пункте преамбулы можно выразить обеспокоенность по поводу того, что военное использование гражданской цифровой инфраструктуры, такой как системы связи или облачной системы, может превратить такую инфраструктуру в военный объект, а также по поводу последствий, которые нападения на такие объекты окажут на гражданское население.

Обоснование: Признание риска использования гражданских объектов в военных целях, что сопряжено с риском превращения их в военные объекты и тем самым нанесения им вреда.

П 7: В этом пункте преамбулы можно было бы выразить обеспокоенность по поводу риска того, что кибероперации, особенно неизбирательные, проводимые в контексте вооруженного конфликта, могут случайно затронуть гражданское население за пределами территории сторон в конфликте из-за глобальной взаимосвязанности киберпространства.

Обоснование: признание риска распространения киберопераций и нанесения вреда гражданскому населению через границы, особенно если такие атаки носят не избирательный характер.

П 8: В этом пункте преамбулы можно было бы напомнить, что технологические компании предоставляют ряд продуктов, услуг и инфраструктуры, от которых зависит гражданское население и правительства, подчеркнуть их ответственность за уважение прав людей, пострадавших в результате вооруженного конфликта, и подчеркнуть важность включения технологических компаний в дискуссиях о защите гражданского населения от цифровых угроз во время вооруженного конфликта.

Обоснование: признание особой роли, которую технологические компании играют в предоставлении цифровых продуктов, услуг и инфраструктуры, в том числе во время вооруженных конфликтов.

П 9: В этом пункте преамбулы можно было бы признать важность цифровых технологий, инфраструктуры (включая подключение к Интернету) и данных для эффективных и действенных гуманитарных операций, а также выразить глубокую обеспокоенность по поводу воздействия киберопераций, включая утечку данных, и информационных операций, направленных на гуманитарную деятельность. Организации рискуют нанести ущерб людям, обслуживаемым этими организациями, самим организациям и их персоналу.

Обоснование: Признание важности цифровых технологий, включая данные, для гуманитарных организаций и вреда, причиняемого их атаками.

П 10: В этом пункте преамбулы можно было бы напомнить о юридической и защитной ценности отличительных эмблем и сигналов, в зависимости от обстоятельств, для идентификации медицинских подразделений и транспортных средств, медицинского и религиозного персонала, а также членов Международного движения Красного Креста и Красного Полумесяца, которые, в силу их включения в четыре Женевские конвенции и непрерывной практики на протяжении более 160 лет, стали общепризнанными символами беспристрастной и нейтральной помощи и защиты жертв вооруженных конфликтов и других чрезвычайных ситуаций, и он мог бы приветствовать проводимые исследования и консультации. МККК в сотрудничестве с академическими учреждениями и другими компонентами Движения о возможности создания «цифровой эмблемы»¹, то есть цифрового средства идентификации цифровой инфраструктуры и данных организаций и субъектов, которые имеют право отображать отличительные эмблемы, признанные международным гуманитарным правом.

Обоснование: Напомним о роли отличительных эмблем согласно международному гуманитарному праву и приветствуем исследования и консультации МККК по поводу возможной «цифровой эмблемы».

П 11: Этот пункт преамбулы мог бы напомнить и подтвердить резолюцию 4 «Восстановление семейных связей при соблюдении конфиденциальности, в том числе в том, что касается защиты персональных данных», принятую 33-й Международной конференцией, и подчеркнуть, что вопросы, рассматриваемые в этой резолюции, важны для защиты других гуманитарных данных.

Обоснование: Напоминает и подтверждает соглашение, достигнутое на 33-й Международной конференции о защите данных в работе Движения по восстановлению семейных связей.

П 12: В этом пункте преамбулы можно было бы принять к сведению резолюцию 12 «Защита гуманитарных данных», принятую Советом делегатов 2022 года, и приветствовать обязательства Движения по защите гуманитарных данных.

Обоснование: Признание работы, начатой в Движении по защите гуманитарных данных.

П 13: Этот пункт преамбулы может напоминать об убежденности в том, что ничто в международном гуманитарном праве, в том числе применительно к кибер- или информационным операциям, не может быть истолковано как легитимизирующее или санкционирующее любой акт агрессии или любое другое применение силы, несовместимое с Уставом Организации Объединенных Наций.

Обоснование: Напомним, что государства разделяют убеждения, изложенные в преамбуле Дополнительного протокола I.

1 См. МККК, Оцифровка эмблем Красного Креста, Красного Полумесяца и Красного Кристалла: преимущества, риски и возможные решения, 3 ноября 2022 г.

П 14: В этом пункте преамбулы можно было бы подчеркнуть, что люди, а также медицинские и гуманитарные организации также сталкиваются с цифровыми угрозами в чрезвычайных ситуациях, помимо вооруженных конфликтов, призвать государства опираться на эту резолюцию и принимать эффективные меры для их защиты в соответствии с применимыми правовыми

нормами рамок и опросить Движение всегда принимать соответствующие меры кибербезопасности и защиты данных.

Обоснование: Напомним о значении цифровых угроз за пределами вооруженных конфликтов и о необходимости того, чтобы государства и компоненты Движения принимали защитные меры за пределами вооруженных конфликтов. Опостановляющие пункты

П 1: В постановляющем пункте можно было бы подчеркнуть общую приверженность всех членов Международной конференции защите гражданских лиц, гражданских объектов и других лиц и объектов, специально защищаемых во время вооруженного конфликта, от цифровых угроз.

Обоснование: выражение общей гуманитарной цели по защите гражданского населения и гражданских объектов от цифровых угроз во время вооруженного конфликта.

П 2 постановляющей части мог бы подтвердить основополагающую важность обязательств всех сторон в вооруженных конфликтах согласно международному гуманитарному праву и другим областям международного права, если это применимо, в частности, международному праву человека, по защите гражданских лиц и гражданских объектов и других лиц и объектов, специально защищенных во время вооруженного конфликта от кибер- и информационных операций.

Обоснование: Подтверждение существующей правовой базы, применимой к кибер- и информационным операциям во время вооруженного конфликта.

П 3: Постановляющая часть могла бы призвать все государства и все стороны в вооруженных конфликтах обеспечить, чтобы международное гуманитарное право применялось таким образом, чтобы обеспечить адекватную защиту гражданских лиц, медицинского персонала, военного персонала вне военных действий, гражданской инфраструктуры и данных, а также других лиц: особо охраняемые лица и объекты в обществах, которые становятся все более цифровизированными; требовать соблюдения применимых правил; и настоятельно призывать все государства и других субъектов, которые развивают кибер- или информационный потенциал, принять необходимые законодательные, административные и практические меры внутри страны для выполнения своих юридических обязательств.

Обоснование: Призвать все государства и все стороны в вооруженных конфликтах обеспечить адекватную защиту от цифровых угроз и призвать к выполнению применимых правовых норм.

П 4: Постановляющая часть могла бы призвать все государства и стороны в вооруженных конфликтах уважать, в частности, кардинальный принцип различия согласно международному гуманитарному праву для защиты гражданского населения от Опасности военных действий, в том числе при проведении кибер- и информационных Операций; подчеркнуть, в частности, что кибервозможности, которые квалифицируются как оружие и носят не избирательный характер, запрещены; и подчеркнуть запрет прямых нападений на гражданских лиц и гражданские объекты, действий или угроз насилия, основная цель которых состоит в том, чтобы посеять террор среди гражданского населения, нападений, которые носят неизбирательный и непропорциональный характер, нападений, уничтожения, удаления или приведения в негодность предметы, необходимые для выживания населения, а также вероломства, а также неправомерного использования особо охраняемых эмблем, сигналов, флагов, униформы и знаков различия, в том числе при использовании цифровых средств и способов ведения войны; и напомнить об обязательствах проявлять постоянную заботу о сохранении гражданского населения и гражданских объектов и принимать все возможные меры предосторожности, чтобы избежать или, по крайней мере, свести к минимуму случайный гражданский ущерб и защитить гражданское население и гражданские объекты, находящиеся под их контролем, от последствий нападений, включая при использовании цифровых средств и методов ведения войны.

Обоснование: подтверждение некоторых основных правил МГП, защищающих гражданское население от цифровых угроз во время вооруженных конфликтов.

П 5: Этот пункт постановляющей части мог бы также призвать государства и стороны в вооруженных конфликтах соблюдать обязательства по международному гуманитарному праву уважать и защищать медицинский персонал, подразделения и транспортные средства при любых обстоятельствах, в том числе от кибер- и информационных операций.

Обоснование: Подтверждение конкретной международно-правовой защиты медицинских подразделений, транспортных средств и персонала от цифровых угроз во время вооруженного конфликта.

П 6: Постановляющая часть могла бы также призвать государства и стороны в вооруженных конфликтах уважать обязательства по международному гуманитарному праву разрешать и облегчать беспристрастную гуманитарную деятельность во время вооруженного конфликта, в том числе осуществляемую с помощью цифровых средств, а также уважать и защищать гуманитарную деятельность, и персонал, в том числе против кибер- и информационных операций.

Обоснование: Подтверждение особой международно-правовой защиты беспристрастных гуманитарных организаций от цифровых угроз во время вооруженного конфликта.

П 7: В постановляющей части можно было бы напомнить, что, когда стороны в вооруженном конфликте поощряют участие гражданского населения в вооруженном конфликте, в том числе с помощью цифровых средств, гражданские лица рискуют потерять свою юридическую защиту от нападения или могут быть восприняты как потерявшие свою защиту, и призвать стороны помнить об этом и принимать все возможные меры предосторожности, чтобы избежать нанесения вреда гражданским лицам.

Обоснование: признание рисков, связанных с поощрением гражданского населения к участию в боевых действиях, и призыв принять все возможные меры предосторожности для защиты гражданского населения.

П 8: В постановляющей части можно было бы подчеркнуть, что негосударственные субъекты, в том числе гражданские лица и негосударственные вооруженные группы, которые проводят кибероперации в связи с вооруженным конфликтом, должны, независимо от своего статуса, соблюдать международное гуманитарное право, подтвердить обязательство государств принимать меры по обеспечению того, чтобы негосударственные субъекты, действующие по указанию, указанию или контролю государства или с его территории, не проводили операции, нарушающие международное гуманитарное право, и пресечению возможных нарушений этого права, а также поощрять МККК и Национальный Красный Крест и Красный Крест Общества Полумесяца возобновить свои усилия по распространению знаний о международном гуманитарном праве.

Обоснование: Подтверждение первоочередной роли государств в обеспечении уважения международного гуманитарного права негосударственными субъектами и признание уставной роли Движения в повышении осведомленности о МГП.

П 9: В этом постановляющем параграфе можно напомнить, что технологические компании, которые работают или предоставляют услуги в условиях, затронутых вооруженными конфликтами, должны понимать и учитывать последствия своей деятельности в соответствии с международным гуманитарным правом, обеспечивать соблюдение своими сотрудниками соответствующих обязательств и принять соответствующие меры для защиты от возможного вреда своему персоналу и любым гражданским лицам, которые полагаются на их продукцию и услуги.

Обоснование: Призвать технологические компании инвестировать в понимание последствий их операций во время вооруженного конфликта и принять меры для защиты гражданского населения.

П 10: Постановляющая часть могла бы побудить государства сегментировать, то есть физически или технически отделять, насколько это возможно, цифровую инфраструктуру, используемую в военных целях, от гражданской инфраструктуры, признавая, что использование гражданской инфраструктуры в военных целях рискует превратить ее в военный объект, что может оказать вредное воздействие на гражданских лиц, которые также используют эту инфраструктуру.

Обоснование: Поощрение государств отделять, насколько это возможно, цифровую инфраструктуру, используемую в военных целях, от инфраструктуры, используемой в гражданских целях.

П 11: Этот постановляющий параграф мог бы побудить всех членов Движения в рамках своей работы учитывать цифровые угрозы и связанный с ними вред, призвать всех членов улучшить свою готовность и способность реагировать на цифровые угрозы против гражданского населения, например, путем наращивание потенциала для обнаружения угроз и проведения мероприятий по защите гражданского населения, а также приглашаем государства поддержать Движение в этих начинаниях.

Обоснование: Поощрять Движение укреплять свой потенциал реагирования на цифровые угрозы и предлагать государствам поддерживать необходимые инвестиции и наращивание потенциала.

П 12: В постановляющей части можно было бы приветствовать результаты продолжающихся исследований и испытаний цифровой эмблемы и призвать МККК, в консультации с государствами и компонентами Движения, предложить техническое, комплексное и долгосрочное решение, а также

предложить варианты включения государств в международное гуманитарное право.

Обоснование: предложить МККК продолжить работу над цифровой эмблемой в тесном сотрудничестве с государствами и Движением.

П 13: Этот пункт постановляющей части мог бы обязать компоненты Движения предпринять соответствующие шаги в рамках своих соответствующих мандатов, возможностей и оперативных потребностей, чтобы повысить свою способность обеспечивать соответствующие уровни кибербезопасности и защиты данных; применять передовой опыт управления данными для всех гуманитарных данных; внедрять соответствующие стандарты и передовую практику обработки персональных данных с учетом Руководства по защите данных при гуманитарной деятельности; и соблюдать действующее законодательство и механизмы защиты персональных данных, а также выражать поддержку государств этим мерам.

Обоснование: Обязательство Движения принять соответствующие меры кибербезопасности и защиты данных для защиты населения, которому оно служит.

П 14: В этом постановляющем параграфе можно было бы напомнить, что обработка персональных данных необходима компонентам Движения для выполнения своих мандатов, особенно в соответствии с международным гуманитарным правом, где это применимо, и в соответствии с Уставом Движения, что такая обработка служит содействию и является необходимой по важным соображениям общественного интереса и жизненно важных интересов людей, и могла бы призвать государства и Движение к сотрудничеству, чтобы гарантировать, что персональные данные не запрашиваются и не используются в целях, несовместимых с гуманитарным характером работы Движения, и в соответствии со статьей 2, включая ее параграф 5, Устава Движения, или таким образом, который мог бы подорвать доверие людей, которым оно служит, или независимость, беспристрастность и нейтральность деятельности Движения.

Обоснование: Напоминание о важности обработки данных в гуманитарной деятельности Движения и для сотрудничества государств при выполнении соответствующих мандатов членов Движения.

П 15: Этот параграф постановляющей части мог бы предложить МККК продолжить оценку цифровых угроз во время вооруженных конфликтов и защиты гражданского населения от них, в том числе в соответствии с

международным гуманитарным правом, и представить доклад по данному вопросу 35-й Международной конференции.

Обоснование: Предложить МККК представить на следующей Международной конференции доклад по теме этой резолюции.