ОТ РЕДАКЦИИ

РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ГУМАНИТАРНОМ ПРАВЕ, ПОЛИТИКЕ И ДЕЯТЕЛЬНОСТИ: НАМЕЧАЕМ ПЕРСПЕКТИВЫ

Саман Реджали и Янник Хайнигер*

Почему тема цифровых технологий и войны заслуживает отдельного выпуска «Международного журнала Красного Креста»? Авторы, чьи статьи вошли в этот номер, называют две основные причины.

Во-первых, цифровизация стала приоритетным направлением исследований для таких гуманитарных организаций, как Международный Комитет Красного Креста (МККК)[1], поскольку она стремительно формирует новые методы проведения гуманитарных операций и оказания помощи и влияет на то, как гуманитарный сектор работает с пострадавшими.

В связи с этим одна из групп авторов, чьи статьи опубликованы в этом номере (в разделах «Гуманитарная деятельность в цифровую эпоху» и «Бизнес и цифровые технологии в условиях гуманитарных кризисов»), анализирует, каким образом применение цифровых технологий в целях оказания гуманитарной помощи одновременно создает беспрецедентные возможности и беспрецедентный риск. Ученые подчеркивают, что некоторые цифровые технологии, в том числе те, которые упрощают общение и оказание услуг, являются жизненно важными инструментами работы гуманитарного сектора. Эти технологии помогают гуманитарным организациям находить решения в условиях кризисов и продолжать работу с пострадавшими. Например, подключение к интернету и расширение доступа к цифровым инструментам могут помочь людям, пострадавшим в ходе вооруженных конфликтов и иных ситуаций насилия, связаться с другими людьми через приложения для обмена сообщениями и социальные сети, найти в интернете информацию и заявить о своих потребностях через механизмы оперативной обратной связи, благодаря чему пострадавшие становятся активными участниками деятельности гуманитарных организаций[2]. Кроме того, проведение анализа ситуации, упорядочение сведений о конфликтах и оказание услуг с помощью цифровых средств могут дать гуманитарным организациям возможность более эффективно работать

* Саман Реджали — советник МККК по правовым и политическим вопросам, выступил тематическим редактором данного номера журнала, посвященного цифровым технологиям и войне. Янник Хайнигер — заместитель директора отделения сети Swissnex в Сан-Франциско, ранее занимал пост специалиста по связям с партнерами в аппарате директора Управления по переходу на цифровые технологии и работе с данными МККК.

с пострадавшими, а также прогнозировать гуманитарные кризисы и реагировать на них.

С другой стороны, эти авторы также подчеркивают, что наряду с возможностями, которые открывает использование цифровых технологий в гуманитарной деятельности, возникают определенные опасности и оговорки. Для того чтобы хорошо подготовиться к началу процессов перехода на цифровые технологии, гуманитарным организациям необходимо учитывать эти факторы риска и минимизировать их действие. Одна из основных зон риска — конфиденциальность и защита данных: сбор информации о пострадавших, бесспорно, налагает на гуманитарные организации бремя ответственности за то, чтобы эти данные использовались только по назначению и чтобы вместо достижения благих целей, ради которых эта информация была собрана, людям не был причинен вред. Кроме того, в таких условиях, какие сложились, например, в Мьянме[3], способы распространения данных и информации определяют развертывание конфликтов и других насильственных действий. Среди новых факторов риска, появившихся вместе с расширением доступа к социальным сетям и другим инструментам распространения информации в интернете, можно отметить введение в заблуждение, дезинформацию и риторику ненависти, а также «новые реалии», представленные с помощью синтеза изображения (генерация сфабрикованных видео-, аудиоматериалов и текстов за счет машинного обучения)[4]. Ввиду этого один из разделов данного выпуска посвящен роли коммерческих предприятий — а именно технологических компаний, которые все активнее оказывают поддержку гуманитарным организациям и одновременно с этим косвенно участвуют в ведении военных действий за счет применения разработанных ими же технологий.

Есть и еще одна причина, в силу которой цифровизация имеет большое значение для гуманитарного сектора. Цифровые (или «новые») технологии используются в вооруженных конфликтах в качестве средств и методов ведения войны, регулируемых международным гуманитарным правом (МГП). Применение этих новых технологий имеет гуманитарные последствия, поскольку они способствуют развитию беспрецедентных средств

1 В МККК переход к цифровым технологиям является пятым ключевым пунктом Стратегии развития организации на 2019–2022 гг., доступной по адресу: www.icrc.org/en/publication/4354-icrc-strategy-2019-2022 (все ссылки на интернет-ресурсы приводятся по состоянию на январь 2021 г.).

2 Это явление нашло свое отражение в оформлении обложки данного выпуска журнала: в Сирии, где за годы насильственных действий сложилась чрезвычайная обстановка и сформировались огромные долговременные потребности, отец со смартфоном, на экране которого видна фотография его сына, стоит на фоне разрушений, ставших следствием вооруженного конфликта. См.: "In Eastern Ghouta Rubble, a Father Looks for His Son", *Reuters*, 4 March 2018, доступно по адресу: www.reuters.com/article/usmideast-crisis-syria-ghouta-victims-idUSKBN1GG0EJ.

3 Alexandra Stevenson, "Facebook Admits It Was Used to Incite Violence in Myanmar", *New York Times*, 6 November 2018, доступно по адресу: www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

4 Aengus Collins, *Forged Authenticity: Governing Deepfake Risks*, EPFL International Risk Governance Center, 2019, доступно по адресу: https://infoscience.epfl.ch/record/273296?ln=en.

и методов ведения войны. Например, как отмечают в своей статье, написанной для этого выпуска журнала, Жизель, Роденхойзер и Дёрман, кибероперации, мишенью которых являются линии электропередач, системы здравоохранения, ядерные объекты или иные ключевые объекты инфраструктуры, могут нанести «серьезный ущерб людям» и привести к катастрофическим гуманитарным последствиям[5]. Помимо киберугроз, беспокойство с гуманитарной, правовой и этической точек зрения вызывают автономные системы вооружения, в том числе управляемые с помощью искусственного интеллекта (ИИ), поскольку они выбирают мишени и применяют к ним силу без участия человека, то есть оператор не знает, какие именно цели будут поражены, где и когда[6]. В третьей и четвертой частях этого выпуска, где идет речь об ИИ и автономных системах вооружения и о кибероперациях на войне, авторы высказывают разные точки зрения и делятся различными взглядами на то, как цифровые технологии используются в военных действиях, оценивая перспективы применения МГП в тех случаях, когда цифровые технологии применяются в разрушительных целях.

Тем не менее «новые» технологии продолжают идти в ногу с научно-техническим прогрессом. Подобно тому, как телеграф два столетия назад произвел революцию в области связи[7], а сегодня уже практически ушел в прошлое, некоторые из нынешних «новых» технологий однажды утратят свою актуальность, не говоря уже о «новизне», и не исключено, что опасности и возможности, связанные с защитой данных и применением МГП, станут отвлеченными понятиями. Однако существует ряд тем «на все времена», касающихся цифровых технологий и гуманитарного права, политики и деятельности, которые будут актуальны всегда, — о них и пойдет речь ниже.

Мы[8] полагаем, что статьи, опубликованные в этом номере, объединены темой доверия: систематическая гуманитарная деятельность опирается на доверие, а гуманитарные организации обязаны завоевать доверие пострадавших, которым стремятся оказать помощь[9]. При том что цифровые

5 См.: *Жизель, Лоран, Роденхойзер, Тильман и Дёрман, Кнут*. Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперaций во время вооруженных конфликтов (опубликовано в этом выпуске журнала).

6 См.: Vincent Boulanin, Neil Davison, Netta Goussac and Moa Peldán Carlsson, *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC, June 2020 (обзор данной публикации представлен в разделе «Доклады и документы» этого выпуска журнала, см.: Ограничение автономности систем вооружений: определение практических элементов контроля со стороны человека); *Зауэр, Франк*. В шаге от края пропасти: почему многостороннее регулирование автономности систем вооружения столь сложно, но необходимо и возможно (опубликовано в этом номере журнала).

7 Jimmy Stamp, "How the Telegraph Went from Semaphore to Communication Game Changer", Smithsonian Magazine, 11 October 2013, доступно по адресу: www.smithsonianmag.com/arts-culture/how-thetelegraph-went-from-semaphore-to-communication-game-changer-1403433/.

8 Под словом «мы» в данной статье понимаются исключительно ее авторы, а не МККК или гуманитарный сектор. Взгляды, выраженные в статье, принадлежат исключительно ее авторам, но не МККК и не отделению сети Swissnex в Сан-Франциско.

9 Hugo Slim, "Trust Me — I'm a Humanitarian", Humanitarian Law and Policy Blog, 24 October 2019, доступно по адресу: https://blogs.icrc.org/law-and-policy/2019/10/24/trust-humanitarian/.

технологии открывают беспрецедентные возможности для оказания гуманитарной помощи, их использование должно быть этичным и ответственным, чтобы минимизировать описанные здесь факторы риска. Только так гуманитарные организации могут надеяться заручиться доверием пострадавших, перед которыми они несут ответственность.

Рука об руку с доверием идут и этические требования: работать так, чтобы отдавать должное людям, которым мы помогаем; заботиться о том, чтобы преимущества применения цифровых технологий перевешивали связанный с ними риск; *взаимодействовать* с пострадавшими, но не принимать за них решения по определяющим для их жизни вопросам. Этические механизмы действуют и в отношении средств и методов ведения войны. Например, говоря о сферах применения ИИ, Пицци, Романофф и Энгельхардт[10], представляющие инициативу Генерального секретаря ООН в области больших данных и ИИ «Глобальный пульс», отмечают, что этические механизмы необходимы для регулирования ИИ, но не всегда достаточны в организационных структурах, где подход, основанный на приоритете этичности, часто не предполагает наличия жестких механизмов подотчетности.

Авторы, чьи статьи опубликованы в этом выпуске, также подчеркивают этические аспекты и возможные препятствия на пути «гуманитарных инноваций», связанные с неравноправием. Гуманитарные инновации способны дать нам новые способы оказания помощи пострадавшим, но если в инновационных проектах не будут предусмотрены меры защиты данных и персональной информации и если они будут создаваться не ради пострадавших и не будут учитывать их интересы, то сопряженные с ними факторы риска могут оказаться более весомыми, чем преимущества[11]. В таких случаях создание «продукта» может опережать проведение всесторонней проверки, необходимой, чтобы удостовериться в том, что польза от применения цифровых технологий будет превышать вред, который может быть причинен пострадавшим. Этому тезису вторят Сандвик и Лоне[12], которые однозначно утверждают: проблема состоит в том, что «пострадавшие часто не участвуют в инновационных процессах — с ними толком не советуются и не приглашают к взаимодействию». Результатом этого могут стать «новые цифровые виды ущерба, будь то за счет обнародования или замалчивания страданий определенных групп или лиц, в связи с нежелательными последствиями или ввиду появления новых факторов риска».

Далее мы рассмотрим, во-первых, как в статьях, опубликованных в этом выпуске, исследуются польза цифровых технологий для гума-

10 См.: *Пицци, Майкл, Романофф, Мила и Энгельхардт, Тим*. ИИ в гуманитарной деятельности: права человека и этика (опубликовано в этом выпуске журнала).

11 См. ICRC, Symposium Report: Digital Risks in Armed Conflicts, Geneva, October 2019 (обзор данной публикации представлен в разделе «Доклады и документы» этого выпуска журнала, см.: Доклад по итогам симпозиума, посвященного цифровым рискам в условиях вооруженных конфликтов).

12 См.: *Сандвик, Кристин Бергтора и Лоне, Кьерсти*. Борьба с сексуальным насилием в условиях конфликта: исследование цифровых аспектов (опубликовано в этом выпуске журнала).

нитарной деятельности и сопряженные с ними опасности, определяются возможности и меры сокращения риска, которые необходимо будет принять в дальнейшем, чтобы начать цифровизацию гуманитарной деятельности с учетом возрастающей роли частного сектора. Затем мы представим обзор возможностей применения цифровых технологий в качестве средства и метода ведения войны в ходе вооруженных конфликтов со ссылками на статьи, в которых раскрывается тема кибероперациий и применения МГП, а также автономных систем вооружения, машинного обучения и ИИ. Этот анализ основан на представлении нас как двух миллениалов, владеющих темой и являющихся соавторами данной редакционной статьи, и завершается перечислением некоторых контекстуальных элементов, повлиявших на публикацию этого выпуска журнала, и размышлениями об общих выводах, сделанных из материалов этого номера.

Взгляд миллениалов на цифровые технологии и войну

Цель данной редакционной статьи состоит в том, чтобы представить беглый обзор разнообразных идей, предложенных в этом номере журнала. Как миллениалы, в течение нескольких лет изучавшие обширную тему технологий в гуманитарной деятельности, мы, наверное, можем считаться представителями первого поколения «цифровых аборигенов»[13]. Предполагается, что мы с легкостью используем цифровые технологии и внедряем их в свою повседневную жизнь. Это действительно так во многих аспектах нашей общественной жизни: Facebook, Twitter, LinkedIn, TikTok и тому подобные платформы занимают значительную часть нашего времени, а взаимодействие в цифровом пространстве для многих становится важным дополнением к общению в физической реальности.

Как говорится в докладе МККК «Миллениалы о войне», составленном в 2020 году[14], миллениалы положительно оценивают потенциал использования цифровых технологий для оказания помощи людям, пострадавшим от войны. Исследуя влияние и последствия применения цифровых технологий в ходе вооруженных конфликтов и иных ситуаций насилия, в этом выпуске мы стремимся выяснить, сможет ли мир, который мы, будучи миллениалами, помогаем создавать, пройти проверку реальностью, и понять, как наши действия в гуманитарной сфере влияют на пострадавших, которым мы хотим помочь. Мы осознаём, что у нас как у миллениалов есть свои предубеждения. «Цифровые аборигены» часто по-своему относятся к принципам, лежащим в основе гуманитарной деятельности, — ней-

13 Berkman Klein Center for Internet and Society at Harvard University (BKC), "Digital Natives", доступно по адресу: https://cyber.harvard.edu/research/youthandmedia/digitalnatives. Согласно определению BKC цифровыми аборигенами считаются представители поколения, «рожденного цифровым», — те, кто вырос в окружении цифровых технологий, для кого жизнь, наполненная цифровыми устройствами, является нормой.

14 *МККК*. Миллениалы о войне. Женева, 2020. Доступно по адресу: https://www.icrc.org/ru/millenialy.

тральности, беспристрастности и независимости[15]. Важную роль в нашем мировосприятии играют цифровые технологии и алгоритмы.

Говоря о принципе гуманности, мы не просто признаём, что «страдание везде одинаково, и на него нужно реагировать»[16], — мы занимаем позицию активистов. С помощью имеющихся у нас социальных сетей и иных каналов мы развиваем бурную деятельность как в виртуальной, так и в физической реальности[17]. Мы пишем как соавторы, выросшие преимущественно в северной части мира, и признаём, что наш опыт не универсален для всех миллениалов, но скорее характерен для подгруппы «граждан мира» в таких центрах, как Женева, Лондон, Нью-Йорк, Торонто, Париж и другие[18]. Наша решимость изменить окружающую действительность и не быть *равнодушными* к чужим страданиям означает, что мы сохранили это намерение на протяжении финансового кризиса (на момент написания этой статьи — уже второго), проходили стажировку за стажировкой, работали по вре́менным контрактам, отказавшись от стабильной жизни, как у наших родителей[19], ради жизни во всем мире, которая у нас сейчас есть[20], чтобы преодолеть все трудности и обрести свое призвание в гуманитарной сфере. Нас не так-то просто остановить, а именно это и нужно миру, поскольку мы боремся с риском, который цифровые технологии могут представлять для гуманитарной деятельности, и с их потенциальным применением в военных целях. Наш мир управляется не только государствами — он многополярен, и в нем все больше и больше негосударственных вооруженных формирований[21], которые используют цифровые технологии для достижения своих целей в вооруженных конфликтах[22]. Кроме того, мы выросли в эпоху

15 Для сравнения: основополагающих принципов Международного движения Красного Креста и Красного Полумесяца (Движения) насчитывается семь: гуманность, беспристрастность, нейтральность, независимость, добровольность, единство и универсальность. *Лаббе, Жереми и Доден, Паскаль*. Применение гуманитарных принципов: размышления об опыте Международного Комитета Красного Креста // Международный журнал Красного Креста. Т. 97, № 897/898, 2016; Office of the UN High Commissioner for Refugees, "Humanitarian Principles", доступно по адресу: https://emergency.unhcr.org/entry/44765/humanitarian-principles; *МККК*. Основополагающие принципы Международного движения Красного Креста и Красного Полумесяца; апрель 2015 г. Доступно по адресу: https://www.redcross.ru/sites/default/files/attachments/4046_fundamental-principles-ru.pdf.

16 *МККК* (примечание 15 выше).

17 Emily Logan, "Millennial Activism: Tapping into a Network of Millennial Donors", доступно по адресу: https://csic.georgetown.edu/magazine/millennial-activism-tapping-network-millennial-donors/.

18 April Rinne, "What Is Global Citizenship?", 9 November 2017, доступно по адресу: www.weforum.org/agenda/2017/11/what-is-global-citizenship/.

19 Janet Adamy, "Millennials Slammed by Second Financial Crisis Fall Even Further Behind", *Wall Street Journal*, 9 August 2020, доступно по адресу: https://www.wsj.com/articles/millennials-covid-financial-crisis-fall-behind-jobless-11596811470.

20 ВКС (примечание 13 выше).

21 Jelena Nikolic, Tristan Ferraro and Thomas de Saint Maurice, "Aggregated Intensity: Classifying Coalitions of Non-State Armed Groups", *Humanitarian Law and Policy Blog*, 7 October 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/10/07/aggregated-intensity-classifying-coalitions-non-state-armed-groups/#.

22 Delphine van Solinge, "Digital Risks for Populations in Armed Conflict: Five Key Gaps the

соцсетей, но и сами все чаще относимся к ним критически[23]. Это особенно верно в отношении глобальных технологических компаний, которые в результате недавнего кризиса, вызванного коронавирусом, еще прочнее завладели ключевыми структурами нашего общества, осложнив повседневную жизнь многих людей, в том числе в гуманитарной сфере.

Мы, миллениалы, выступаем за трактовку принципа беспристрастности как движущей силы, способствующей достижению подлинной всеохватности и многообразия в гуманитарном секторе[24]. При этом мы осознаём, что, хотя цифровые технологии могут упростить связь и взаимодействие с пострадавшими, они также могут привести к цифровому разрыву, который выльется в неравенство между слоями населения с точки зрения доступа к цифровым технологиям и к их преимуществам, в результате чего некоторые группы пострадавших могут оказаться в невыгодном положении[25]. Об этом цифровом разрыве на примере цифровизации денежных расчетов убедительно пишет Джо Бёртон в своей статье для этого выпуска журнала. Она отмечает следующее:

> Распространение цифровых платежей может усугубить цифровой разрыв… Расплачиваться наличными, если они есть и если имеются в наличии товары и услуги, за которые необходимо заплатить, может любой человек. <…> Однако для использования цифровых платежных средств получатель должен обладать определенной цифровой и финансовой грамотностью. По оценкам специалистов, в основных финансовых понятиях ориентируется лишь треть взрослого населения планеты, при этом среди женщин и малоимущих уровень финансовой грамотности ниже[26].

Как показывает анализ, проведенный Бёртон, цифровой разрыв усугубляется неравенством между различными слоями населения, в том числе по имущественному и гендерному признаку. Однако мы убеждены в том,

Humanitarian Sector should Address", *Humanitarian Law and Policy Blog*, 12 June 2019, доступно по адресу: https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/.

23 Nick Statt, "Facebook's US User Base Declined by 15 Million since 2017, According to Survey", *The Verge*, 6 March 2019, доступно по адресу: www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-millionpeople-united-states-privacy-scandals; Jack Nicas, Mike Isaac and Sheera Frenkel, "Millions Flock to Telegram and Signal as Fears Grow over Big Tech", *New York Times*, 13 January 2021, доступно по адресу: www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

24 Saman Rejali, "Race, Equity, and Neo-Colonial Legacies: Identifying Paths Forward for Principled Humanitarian Action", *Humanitarian Law and Policy Blog*, 16 July 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/07/16/race-equity-neo-colonial-legacies-humanitarian/.

25 Barnaby Willitts-King, John Bryant and Kerrie Holloway, *The Humanitarian "Digital Divide"*, Humanitarian Policy Group Working Paper, Overseas Development Institute, London, November 2019, p. 15; Lina Gurung, "The Digital Divide: An Inquiry from Feminist Perspectives", *Dhaulagiri Journal of Sociology and Anthropology*, Vol. 12, 2018.

26 См.: *Бёртон, Джо*. Принцип «не навреди» в цифровую эпоху: как цифровизация денежных расчетов влияет на гуманитарную деятельность (опубликовано в этом выпуске журнала).

что, если мы будем воплощать на практике принцип беспристрастности, нам удастся сократить системное неравенство, мешающее оказывать гуманитарную помощь.

Что касается принципа нейтральности, то мы, как миллениалы, столкнувшись с многочисленными кампаниями, направленными на введение в заблуждение и распространение дезинформации в социальных сетях, на собственном опыте осознали, что, поскольку люди используют цифровые технологии по-разному, такие технологии не всегда являются нейтральными. Это очень хорошо видно на примере применения цифровых технологий в разрушительных целях в ходе вооруженных конфликтов и других ситуаций насилия.

В целом отношение миллениалов к принципам нейтральности, беспристрастности и независимости в гуманитарной деятельности определяет наши взгляды, мышление и работу с цифровыми технологиями в условиях гуманитарных кризисов и с точки зрения оценки возможности применения МГП к средствам и методам ведения войны. Перспективы использования цифровых технологий, изложенные на страницах этого номера журнала, дают нам уникальную возможность (пере)осмыслить цифровые технологии на войне и посмотреть на них шире, а также служат более масштабной цели применения цифровых технологий в гуманитарной деятельности. Надеемся, что это получится у каждого читателя — вне зависимости от того, к какому поколению он принадлежит.

Цифровые технологии и гуманитарная деятельность: виды риска

В нескольких статьях, опубликованных в этом выпуске журнала, рассматривается вопрос о том, как цифровые технологии могут использоваться без полного осознания возможных последствий их использования. Таким образом, цифровые технологии в условиях конфликтов сопряжены с определенным риском — общественным, экономическим, политическим и когнитивным, — который необходимо учитывать при оказании гуманитарной помощи и осуществлении обычной деятельности. Пожалуй, самый проблематичный аспект заключается в том, что оценка соотношения пользы и риска часто проводится исключительно самими гуманитарными организациями *без* участия пострадавших. Кроме того, больше всего от подобных видов риска страдают именно люди и сообщества в условиях кризиса.

В отношении гуманитарной деятельности выявлено три основных вектора риска[27]: 1) цифровая слежка/надзор, наблюдение и вмешательство;

27 Согласно докладу МККК по итогам симпозиума, посвященного цифровому риску в условиях вооруженных конфликтов, цифровые виды риска «включают в себя (часто непреднамеренные) побочные эффекты экспериментов с цифровыми данными, нарушений неприкосновенности частной жизни, а также некорректного обращения с конфиденциальной информацией, сопровождающие попытки гуманитарного сектора применять новые технологии в условиях, которые и так не отличаются стабильностью». ICRC (примечание 11 выше).

2) введение в заблуждение, распространение дезинформации и риторика ненависти; 3) некорректное использование и обработка данных и персональной информации.

Цифровая слежка/надзор, наблюдение и вмешательство

Риск цифровой слежки/надзора, наблюдения и вмешательства может исходить из разных источников, таких как, например, анализ больших данных, модели машинного обучения, некорректное использование данных органами власти, а также присутствие и деятельность людей в виртуальном пространстве. Как отмечают в своей статье, опубликованной в этом номере журнала, Гази и Газис[28], анализ больших данных и открытых данных не только сопряжен с риском вмешательства в частную жизнь, но и может давать необъективные результаты. Последнее утверждение основано на том факте, что большие данные и открытые данные

> часто не содержат демографических характеристик, таких как возраст и половая принадлежность, имеющих ключевое значение для эпидемиологических исследований. [Кроме того], эти данные охватывают лишь часть населения за исключением маргинализированных и недостаточно хорошо представленных групп, таких как младенцы, неграмотные, люди преклонного возраста, коренное население и люди с ограниченными возможностями, и, возможно, не в полной мере охватывают некоторые развивающиеся страны, где отсутствует широкий доступ к цифровым технологиям.

Это составляет особую проблему для деятельности в области предоставления гуманитарной помощи и защиты, поскольку аналитика больших данных и открытых данных может привести к тому, что гуманитарные организации непреднамеренно упустят из виду маргинализированные группы населения, которые находятся в неравном положении сразу по нескольким признакам и которым эти организации стремятся помогать. Это подтверждает в своем анализе Миланиния[29], иллюстрируя, как модели машинного обучения и анализ больших данных «в существенной степени подвержены обычным человеческим предубеждениям» и в силу этого могут «усугубить существующее расовое, политическое или гендерное неравенство» и, возможно, создать «вводящую в заблуждение и искаженную картину положения дел на местах».

28 См.: *Гази, Теодора и Газис, Александрос*. Гуманитарная помощь в эпоху COVID-19: обзор Общего регламента о защите персональных данных и аналитики больших данных в условиях кризиса (опубликовано в данном выпуске журнала).

29 См.: *Миланиния, Нема*. Предубеждения в моделях машинного обучения и аналитике больших данных: последствия для международного уголовного и гуманитарного права (опубликовано в данном выпуске журнала).

Подобным образом, Пицци, Романофф и Энгельхардт[30] показывают, как недостаток качественных данных повышает риск того, что система ИИ выдаст несправедливый результат, поскольку

> системы ИИ могут выявлять конфиденциальные данные о местонахождении людей, их политических воззрениях, сексуальных предпочтениях и так далее на основе сведений, которые люди добровольно размещают в интернете (например, тексты и фотографии в социальных сетях) или время от времени фиксируют на своих цифровых устройствах (например, данные спутниковой геолокации или местоположение относительно вышек сотовой связи).

Собранные сведения будут в значительной степени подвержены риску некорректного использования, если не принять необходимых мер для защиты данных. Опаснее всего то, что своими действиями в интернете пострадавшие могут, сами того не зная, навлечь на себя опасность причинения им вреда в физической реальности, в том числе, помимо всего прочего, оказаться объектом слежки и попасть в разработку в случае кризиса[31], а также столкнуться с угрозой насилия, преступлений на почве ненависти и/или дискриминации[32]. Реальный случай подобного установления слежки описан в докладе МККК по итогам симпозиума, посвященного цифровому риску в условиях вооруженных конфликтов, представленном в разделе «Доклады и документы» в этом номере журнала: в результате вирусной атаки были взломаны мобильные устройства сирийских беженцев. Среди прочих примеров встречаются случаи установления слежки со стороны самих гуманитарных организаций, которые стремятся применять технологии для более эффективного удовлетворения потребностей — например, посредством использования беспилотных летательных аппаратов в целях картирования и оценки рисков[33]. В этом случае вышеупомянутый риск слежки особенно актуален, поскольку дроны могут собирать информацию о среде, в которой живут пострадавшие, без их согласия и/или ведома. Более сложные примеры слежки/надзора, наблюдения и вмешательства описаны, в том числе, в статье Сятицы[34], где такие вопросы обсуждаются в контексте распознавания лиц.

30 *Пицци, Романофф и Энгельхардт* (примечание 10 выше).
31 *Бёртон* (примечание 26 выше).
32 ICRC (примечание 11 выше).
33 Faine Greenwood, "Data Colonialism, Surveillance Capitalism and Drones", in Doug Specht (ed.), *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, London, 2020.
34 См.: *Сятица, Илья*. Свобода собраний под угрозой: всеобщий неизбирательный надзор и вмешательство во взаимодействие людей в интернете (опубликовано в этом выпуске журнала).

Введение в заблуждение, распространение дезинформации и риторика ненависти

Рассуждая о введении в заблуждение, распространении дезинформации и риторике ненависти в интервью, подготовленном для этого номера журнала[35], Дельфина ван Золинге говорит о способах манипулирования информацией и ее распространения с помощью цифровых технологий, особенно в условиях пандемии коронавируса, когда люди в большей степени полагаются на информационно-коммуникационные технологии. Примером тактики распространения дезинформации может служить синтез изображения — создание подложного видео- и аудиоконтента с помощью машинного обучения[36]. В условиях кризисов, например в Мьянме, Южном Судане и Эфиопии[37], вводящие в заблуждение сведения, дезинформация и риторика ненависти распространяются через социальные сети, а общественным мнением манипулируют с помощью ложных или неполных данных, усугубляя уже существующие гуманитарные кризисы. Использование технологий широкими массами населения дает разработчикам соцсетей, мессенджеров и поисковых машин все бóльшую власть, в том числе в условиях вооруженных конфликтов и других ситуаций насилия. Недавно мы стали свидетелями того, как крупные технологические компании оказались на слуху у всего мира, поскольку, с одной стороны, они превратились в арбитров в вопросах свободы слова, а с другой стороны — стали инструментами распространения в социальных сетях вредоносной информации (то есть вводящих в заблуждение данных, дезинформации и риторики ненависти). Сейчас, во время пандемии коронавируса, это еще более актуально, поскольку пострадавшие как никогда сильно полагаются на подобные платформы как на источники информации и средства общения друг с другом.

Некорректное использование и обработка данных и персональной информации

В контексте некорректного использования и обработки данных понятие «техноколониализм», введенное в оборот Миркой Мадиану[38], служит отличным примером того, что может произойти даже при самых благих намерениях, если стремиться внедрять цифровые инновации и собирать агрегированные биометрические данные в условиях гуманитарного кризиса без претворения в жизнь необходимых процедур защиты данных и механиз-

35 См.: Интервью: гуманитарные операции, распространение вредоносной информации и защита данных (опубликовано в этом выпуске журнала).

36 Harvard Kennedy School, Belfer Centre for Science and International Affairs, "Tech Factsheets for Policymakers: Deepfakes", Spring 2020, доступно по адресу: www.belfercenter.org/sites/default/files/2020-10/tappfactsheets/Deepfakes.pdf.

37 Интервью (примечание 35 выше).

38 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society*, Vol. 5, No. 3, 2019, доступно по адресу: https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

мов соблюдения конфиденциальности, скорректированных с учетом цифрового характера информации. Технологии на самом деле включают в себя и усиливают систему ценностей, культуру и мировоззрение своих создателей. Бесконтрольные цифровые инновации и работа с данными могут еще сильнее укоренить пережиток колониальных времен — асимметричное распределение власти между гуманитарными организациями и пострадавшими[39].

Это выражается в феномене «капитализма слежки», описанного Зубофф как «использование данных отдельных людей для извлечения прибыли за счет самих этих людей»[40]. В контексте гуманитарных кризисов это означает, что данные пострадавших могут не только собираться, но и использоваться в коммерческих целях. Поскольку такой сбор данных часто происходит без ведома человека, Зубофф проводит параллель с колониальной практикой конфискации без согласия. В этом отношении Сандвик и Лоне отмечают, что в результате такого бесконтрольного сбора данных и фиксации сведений о пострадавших в облачных сервисах могут создаваться «цифровые тела», и это может иметь гендерно обусловленные последствия в контексте борьбы с сексуальным насилием в ситуации конфликта[41].

О последствиях того, что происходит в гуманитарном секторе, когда меры защиты данных не внедрены должным образом, рассказывают Массимо Марелли в интервью для этого выпуска[42] и Джо Бёртон, которая применяет к цифровизации денежных расчетов принцип защиты данных, основанный на недопущении нанесения цифрового вреда. Бёртон отмечает, что метаданные — данные, которые содержат информацию о других данных, — могут становиться источником серьезных проблем в условиях гуманитарных кризисов и использоваться для получения военного преимущества, особенно когда мы слышим, как влиятельные люди уровня генерала Хайдена, бывшего руководителя Агентства национальной безопасности и Центрального разведывательного управления США, говорят: «Мы убиваем людей, опираясь на метаданные» — такую цитату приводит в своей статье Бёртон[43].

Вопрос о том, что происходит с данными пострадавших после их сбора гуманитарными организациями, имеет важнейшее значение. Крупные технологические компании неоднократно предоставляли данные пользователей правительствам стран, что может представлять угрозу для безопасности граждан в условиях вооруженного конфликта и иных

39 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society*, Vol. 5, No. 3, 2019, доступно по адресу: https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

40 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future*, PublicAffairs, New York, 2019.

41 *Сандвик и Лоне* (примечание 12 выше).

42 Интервью (примечание 35 выше).

43 *Бёртон* (примечание 26 выше).

ситуаций насилия[44]. Стоит отметить, что, даже если данные пострадавших никому не предоставляются, место их хранения может быть взломано, а данные украдены, если гуманитарные организации не будут защищать их должным образом[45]. Этот риск, связанный с защитой данных, отмечается и в докладе МККК по итогам симпозиума[46]: «Гуманитарные организации собирают, хранят, предоставляют и анализируют данные, которые представляют интерес для сторон в вооруженном конфликте. <…> В результате гуманитарные организации все чаще подвергаются цифровым атакам и становятся объектами кибершпионажа, превратившись в весьма лакомые мишени».

Цифровые технологии и гуманитарная деятельность: польза и меры уменьшения вреда

Для того чтобы учесть все эти виды риска, связанные с цифровыми технологиями и имеющими общественные, экономические, политические и когнитивные последствия для пострадавших в условиях гуманитарных кризисов, можно принять ряд активных мер, в том числе таких как 1) повышение цифровой грамотности; 2) укрепление мер защиты данных и создание надлежащих механизмов обеспечения безопасности при внедрении цифровых технологий; 3) принятие соответствующей гуманитарной политики, чтобы в центре деятельности гуманитарных организаций по-прежнему оставались люди.

Повышение цифровой грамотности

Цифровая грамотность — не просто «приятное дополнение» к деятельности гуманитарных организаций, а ключевая потребность пострадавших. Это важное наблюдение упоминается на страницах этого выпуска журнала несколько раз. Например, ван Золинге выступает за повышение сопротивляемости людей информации, вводящей в заблуждение, и дезинформации посредством «содействия развитию цифровой грамотности, критического мышления и… гуманитарных ценностей»[47]. Сандвик и Лоне, со своей стороны, подчеркивают, что цифровая грамотность выходит «за рамки технических навыков и включает в себя осознание и восприятие вопросов технологий, юриспруденции, прав и риска»[48]. Эти составляющие имеют ключевое значение и для самих гуманитарных организаций. В каче-

44 Там же; F. Greenwood (примечание 33 выше).
45 Важность принятия мер защиты данных в гуманитарной деятельности подчеркивается в: Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC and Brussels Privacy Hub, Geneva, June 2020 (обзор работы представлен в разделе «Доклады и документы» этого выпуска журнала, см.: Руководство по защите данных в ходе гуманитарной деятельности, второе издание).
46 ICRC (примечание 11 выше).
47 Интервью (примечание 35 выше).
48 *Сандвик и Лоне* (примечание 12 выше).

стве примера реализуемых на данный момент инициатив, направленных на развитие ключевых навыков цифровой грамотности у юристов и у лиц, принимающих решения в гуманитарной сфере, можно привести партнерство МККК с Федеральной политехнической школой в Лозанне (Ecole Polytechnique Fédérale de Lausanne, EPFL) в рамках нескольких совместных инициатив[49], в том числе в целях разработки пятидневного вводного курса по основам информационно-коммуникационных технологий[50]. Действуя в том же направлении, Международная Федерация Обществ Красного Креста и Красного Полумесяца (МФОКК и КП) создала проект инструкции по вопросам, связанным с данными, чтобы «повысить цифровую грамотность в группах, отделах, секретариате МФОКК и КП и национальных обществах»[51]. Несмотря на то что эти конкретные проекты направлены на сами гуманитарные организации, они представляют собой первый шаг в новом для многих гуманитарных организаций направлении и содержат призыв к реализации аналогичных инициатив на местном уровне с акцентом на пострадавших и на повышение их цифровой грамотности.

Укрепление мер защиты данных

Наряду с навыками цифровой грамотности необходимы соответствующие меры защиты данных, чтобы предотвратить нежелательный доступ к данным пострадавших посредством слежки, наблюдения или взлома цифровых хранилищ и тем самым способствовать снижению риска, присущего цифровым технологиям. В связи с этим Массимо Марелли, например, подчеркивает, что в МККК

> уже приняли несколько конкретных мер защиты в рамках утвержденных в 2015 году Правил МККК по защите персональных данных; эти меры направлены на снижение риска несанкционированного доступа к персональным данным посредством введения стандартов защиты данных и требований к процедурам обработки данных для всей организации. В тех случаях, когда МККК рассматривает возможность использования новых технологий или более рискованных операций по обработке данных, необходимо провести оценку последствий обработки данных, чтобы определить риск причинения вреда и принять меры для его уменьшения. Кроме того, Правила предписывают МККК придер-

49 EPFL и ETH Zürich объединяются с МККК для изучения инновационных способов урегулирования нынешних гуманитарных кризисов в рамках инициативы «Проблемы гуманитарной деятельности»; см.: EPFL, "Science and Technology for Humanitarian Action Challenges (HAC)", доступно по адресу: http://www.epfl.ch/research/services/fund-research/funding-opportunities/research-funding/science-and-technology-for-humanitarian-action-challenges-hac/. См. также: EPFL, "EPFL, ETH Zürich and the ICRC Team Up to Bolster Humanitarian Aid", 10 December 2020, доступно по адресу: https://actu.epfl.ch/news/epfl-eth-zurich-and-the-icrc-team-up-to-bolster-hu/.

50 EPFL, "Executive Training: Foundations of Information and Communication Technologies", доступно по адресу: www.c4dt.org/event/fict-executive-course/.

51 IFRC, "Discover the Data Playbook Beta Project", 18 October 2018, доступно по адресу: https://media.ifrc.org/ifrc/2018/10/18/discover-data-playbook-beta-project/.

живаться подхода, основанного на «защите данных, обеспечиваемой на конструктивном уровне», чтобы ограничить сбор персональных данных необходимым для работы минимумом и обеспечить соблюдение прав субъектов данных[52].

Гуманитарная политика как стимул для ответственного применения технологий

Среди ресурсов, доступных гуманитарным организациям в процессе балансирования между возможностями и опасностями, политика является уникальным инструментом. В поисках организаций, которые проводят процессы цифровой трансформации и при этом стремятся снизить риск, связанный с цифровыми технологиями, мы обнаружили несколько интересных примеров в дополнение к тем, которые встретятся на страницах этого выпуска журнала. Одной из ключевых резолюций, принятых в ходе XXXIII Международной конференции Красного Креста и Красного Полумесяца (Международная конференция) в 2019 году, стала резолюция № 4 «Восстановление семейных связей с соблюдением требований конфиденциальности, в том числе и в отношении защиты персональных данных»[53]. В этой резолюции содержится призыв к государствам и к Международному движению Красного Креста и Красного Полумесяца (Движение) соблюдать многочисленные положения о защите данных и неприкосновенности частной жизни при обработке сведений о пострадавших. В частности, она призывает государства и Движение к сотрудничеству, с тем чтобы воздерживаться от запроса таких персональных данных и не использовать их в целях, несовместимых с гуманитарным характером деятельности Движения[54]. Положения о защите данных, составляющие основу данной резолюции, воплощены в Кодексе поведения в отношении защиты данных Сети Международного движения Красного Креста и Красного Полумесяца по восстановлению семейных связей[55]. В этом кодексе поведения установлены минимальные принципы, обязательства и процедуры, которые обязаны соблюдать сотрудники МККК, национальных обществ и Международной Федерации при обработке персональных данных в рамках деятельности по восстановлению семейных связей. Благодаря подобным документам можно сформировать у гуманитарных организаций общее понимание существующих видов риска

52 Интервью (примечание 35 выше).

53 ICRC, "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection", 33IC/19/R4, Resolution 4 adopted at the 33rd International Conference of the Red Cross and Red Crescent, Geneva, 9–12 December 2019, доступно по адресу: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

54 Ibid., para. 11.

55 *МККК*. Сеть Международного движения Красного Креста и Красного Полумесяца по восстановлению семейных связей. Кодекс поведения в отношении защиты данных, Женева, ноябрь 2015 г., доступно по адресу: https://www.icrc.org/ru/download/file/54719/ruscodedataprotection.pdf.

и базовых мер, необходимых для функционирования технологий таким образом, чтобы укрепить защиту конфиденциальных данных частных лиц в зонах конфликтов.

На самом деле в рамках Международной конференции 2019 года также было принято цифровое обязательство всех участников Движения «Укрепление национального цифрового потенциала и потенциала данных для гуманитарной деятельности»[56], посредством которого Движение обязалось до конца 2023 года выполнить план действий, предусматривающий 1) укрепление партнерских связей в этом направлении; 2) проведение общей встречи по этим вопросам; 3) развитие навыков цифровой грамотности; 4) содействие всеобщему доступу к цифровым технологиям; 5) обеспечение защиты данных и 6) принятие на себя ответственности за использование цифровых технологий. Этот пример — еще одна иллюстрация того, как важно начать цифровую трансформацию на основе определенных принципов и согласовать позиции по поводу мер, необходимых для уменьшения побочных эффектов применения цифровых технологий. Кроме того, он показывает, как Движение может сыграть ведущую роль и стать примером в вопросах применения основополагающих принципов, распространяющихся на всех участников Движения[57], к использованию таких технологий.

В той же области гуманитарной политики в 2019 году МККК также подготовил программное заявление, посвященное использованию технологий биометрии[58], которые находят применение в судебно-экспертной сфере и в программе восстановления семейных связей. Учитывая, что создание постоянной базы данных людей — вопрос щекотливый, поскольку они могут не желать, чтобы идентифицирующие их сведения хранились в течение неограниченного времени, эта политика способствует ответственному применению данной технологии организацией и определяет связанные с ней сложности в области защиты данных. В целом эти многочисленные инициативы хорошо иллюстрируют ту роль, которую может сыграть гуманитарная политика в создании осуществимого на практике механизма использования новых цифровых технологий на основе определенных принципов.

Преимущества цифровых технологий для гуманитарной деятельности

Несмотря на то что цифровые технологии сопряжены с определенными опасностями, которые описаны выше, они также обеспечивают беспрецедентные преимущества для проведения гуманитарных операций и оказания

56 "Strengthening National Digital and Data Capacities for Humanitarian Action", Digital Pledge, 2019 International Conference, доступно по адресу: https://tinyurl.com/110x3pmp.

57 *МККК* (примечание 15 выше).

58 ICRC, "The ICRC Biometrics Policy", 16 October 2019, доступно по адресу: https://www.icrc.org/en/document/icrc-biometrics-policy.

помощи. Примеры таких преимуществ представлены в этом выпуске журнала в разделе «Взгляд изнутри», где изложены свидетельства очевидцев.

В этом разделе приводятся цитаты из отзывов людей, чья жизнь изменилась к лучшему благодаря провозглашенным МККК инициативам, основанным на цифровых технологиях. В одном из свидетельств идет речь о платформе МККК Trace the Face[59], которая представляет собой «фотогалерею, в которой размещены фотографии людей, ищущих своих пропавших родственников». Именно благодаря этому веб-сайту Матти из Абиджана смогла найти родного дядю, от которого не было никаких вестей с начала кризиса 2010–2011 годов в Кот-д'Ивуаре[60].

Еще одно из приведенных в журнале свидетельств, которое тоже демонстрирует положительный потенциал применения цифровых технологий в условиях гуманитарных кризисов, принадлежит женщине по имени Завади — она рассказывает о том, как ей удалось связаться с семьей мужа благодаря Службе обмена электронными сообщениями Красного Креста — совместному пилотному проекту МККК, Красного Креста в Конго и Красного Креста в Руанде[61]. Реализация этой инициативы была начата в ноябре 2018 года; проект направлен на восстановление связей между разлученными членами семей с помощью сервиса цифровых сообщений Красного Креста. В рамках проекта добровольцы Красного Креста объезжают поселения в восточной части Демократической Республики Конго и Руанды с планшетами, оснащенными доступом в интернет. Проект обладает большим потенциалом, поскольку помогает усовершенствовать одну из самых первых служб МККК — систему обмена сообщениями Красного Креста, — что позволяет содействовать восстановлению семейных связей быстрее и эффективнее, чем раньше. Как показывают отзывы пострадавших, такие инициативы служат примером того, что становится возможным, когда гуманитарные инновации соединяются с цифровыми технологиями, чтобы облегчить страдания людей в условиях вооруженных конфликтов и других ситуаций насилия. Опираясь на эти достижения, МККК реализует пилотную версию цифровой платформы Red Safe[62], с помощью которой пострадавшие могут получить доступ к различным услугам в электронном виде.

В своем интервью для журнала Дельфина ван Золинге также отмечает, что гуманитарные организации «пользуются более совершенными методами оценки ситуации и получения практически значимой информации, которые доступны в цифровую эпоху». К примеру, она отмечает, что правозащитники и гуманитарные организации

59 ICRC, "Trace the Face – Migrants in Europe", доступно по адресу: https://familylinks.icrc.org/europe/en/pages/publish-your-photo.aspx.

60 См.: «Как гуманитарные технологии влияют на жизнь пострадавших» в разделе «Взгляд изнутри» этого выпуска журнала.

61 Там же.

62 См.: ICRC, "ICRC'S Activities in Favour of Migrants in Southern Africa", 2020, p. 5, доступно по адресу: www.icrc.org/en/download/file/147853/icrcs_activities_in_favour_of_migrants_in_southern_africa_newsletter.pdf.

применяют дистанционные датчики в дополнение к инструментам раннего оповещения о нарушениях прав человека и документирования таких случаев. Они задействуют мобильные решения для отслеживания условий, характеристик и маршрутов транзита мигрантов и беженцев, используют метаданные из расшифровок звонков для исследования распространения инфекционных заболеваний, проводят анализ общественных настроений и сбор слухов в нестабильных районах с помощью социальных сетей и, разумеется, применяют воздушную робототехнику для наблюдения за пораженными объектами и за ключевой инфраструктурой.

В период пандемии COVID-19 цифровые инструменты, искусственный интеллект и «анализ больших данных» используются в различных условиях для поддержки мер реагирования в системе здравоохранения. Они могут помочь собрать, проанализировать и передать ключевую информацию для распределения медицинских ресурсов и сил, ускорения работы медицинских, логистических цепочек и цепочек поставок или обеспечения общественной безопасности и порядка в условиях изоляции.

При том что в своей статье для этого выпуска журнала Гази и Газис[63] анализируют вышеупомянутый риск, связанный с использованием больших данных, они также упоминают и о возможной пользе больших данных для гуманитарной деятельности, отмечая, что при ликвидации последствий чрезвычайных ситуаций большие данные позволяют отреагировать на миграционные кризисы, эпидемии и стихийные бедствия, а также наладить санитарно-эпидемиологический надзор и реагирование. В качестве примера они приводят программное приложение Ushahidi, которое применяется для повышения эффективности гуманитарной помощи. С помощью этой платформы ученые в Кении

проанализировали географию использования мобильных телефонов почти 15 миллионов человек за период с июня 2008 года по июнь 2009 года, чтобы оценить мобильность людей с низким уровнем дохода в Кении и объяснить распространение малярии и инфекционных заболеваний. Кенийская телефонная компания Safaricom предоставила исследователям обезличенные данные, а те выявили на их основе модели перемещений пользователей. Сопоставив сведения о перемещениях с картой распространения малярии, подготовленной официальными органами, ученые оценили вероятность инфицирования местных жителей и приезжих в каждом из районов.

Использование таких данных для отслеживания распространения инфекционных заболеваний имеет огромный потенциал, особенно сейчас, в эпоху COVID-19. Разумеется, как подчеркивают Гази и Газис, любой подобный

63 *Гази и Газис* (примечание 28 выше).

сбор данных сопряжен с «риском обратной идентификации на основе уникальных моделей, на которых строятся действия пользователей. Поэтому при использовании обезличенных персональных данных для целей анализа в процессе анонимизации обычно производится небольшое изменение исходных сведений (в результате чего полезность данных частично утрачивается), чтобы защитить сведения о личности пользователей».

Миланиния[64] также подчеркивает некоторые из преимуществ цифровых технологий для мониторинга соблюдения МГП и для других целей и рассказывает о положительных примерах использования машинного обучения, «в том числе для выявления массовых захоронений в Мексике, поиска подтверждений уничтожения жилых домов и школ в Дарфуре, обнаружения сфабрикованных видеороликов и подложных данных, прогнозирования результатов судебных слушаний в Европейском суде по правам человека и сбора доказательств совершения военных преступлений в Сирии».

Таким образом, в статьях рассматриваются и польза, и риск, связанные с применением цифровых технологий в гуманитарной деятельности и других сферах, и отмечается важность использования цифровых технологий гуманитарными организациями при условии принятия соответствующих мер для снижения риска.

Взаимодействие гуманитарных организаций со сферой технологий

Еще одно интересное направление, вытекающее из перспективы использования цифровых технологий, связано со взаимодействием между гуманитарными организациями и разработчиками таких технологий. Мы упомянули о возможном применении технологий в кибероперациях и об их потенциальных последствиях для людей — подробнее эта тема исследуется в разделе этого выпуска «Кибероперации и война» и в следующей части этой редакционной статьи. Технологии создаются не на пустом месте — они лежат в основе продуктов и решений, которые разрабатываются конкретными компаниями. Как в таких условиях гуманитарным организациям, которые опираются на подтвержденный десятилетиями опыт «гуманитарной дипломатии»[65], лучше взаимодействовать с представителями технологической сферы? На ум приходит несколько примеров, иллюстрирующих и содержательную часть возможного диалога, и формы, которые он способен принять.

Массимо Марелли подчеркивает в этом выпуске, что для полного контроля над конфиденциальной информацией, находящейся в ведении гуманитарной организации, необходимы конкретные решения и объекты инфраструктуры — например, создание гуманитарного цифрового про-

64 *Миланиния* (примечание 29 выше).
65 *МККК*. Гуманитарная дипломатия. Доступно по адресу: https://www.icrc.org/ru/what-we-do/humanitarian-diplomacy-and-communication.

странства по модели «суверенного облака» или «цифрового посольства»[66]. Разработка новых технологий, обеспечивающих постоянный единоличный контроль МККК над собранными им данными, может стать одним из перспективных направлений активного диалога и предметного сотрудничества между гуманитарными организациями, технологическими компаниями, государственными органами и научными кругами[67].

В связи с этим в качестве первого шага к построению стабильного диалога с глобальными технологическими компаниями по поводу влияния цифровых технологий на людей, пострадавших в ходе вооруженных конфликтов и других ситуация насилия, МККК открыл отделение в США в районе Кремниевой долины[68]. Основная идея такого взаимодействия состоит в том, чтобы привнести в диалог, посвященный ответственному применению технологий в гуманитарной деятельности, — которое включает в себя базовые принципы доверия и неприкосновенности частной жизни, — опыт МККК в операционной и юридической сфере и его знание обстановки. Для этого сторонам потребуется учиться друг у друга тому, как технология может, с одной стороны, быть полезна людям, оказавшимся в зонах конфликта, а с другой — создавать различные опасности для этих людей, сообществ и обществ и причинять им вред. На этой основе принимаются меры, направленные на то, чтобы технологии, которые используют МККК и пострадавшие (или которые оказывают на них воздействие), были как можно более эффективными и безопасными. Это может потребовать совместных усилий для создания новых инструментов и сервисов (таких, как те, что упомянуты выше и которые нельзя просто закупить у коммерческих поставщиков), а также работы в сфере гуманитарной дипломатии, чтобы убедить различных заинтересованных лиц поддержать МККК, его подход и рекомендации (юридические, политические и/или этические).

В то же время диалог в узком кругу с технологическим сектором также играет ключевую роль в лучшем понимании его интеллектуальной основы. Технологические компании проявляют все больший интерес к сотрудничеству с гуманитарными организациями, поскольку среди них крепнет убеждение в том, что цифровые технологии не только являются источником благ, но и могут помочь гуманитарным организациям эффективно удовлетворять потребности пострадавших, внося долговременный положительный вклад в их жизнь. Тем не менее это взаимодействие может быть испорчено «технологическим детерминизмом»[69] и «культурой пред-

66 См.: *Мареллли, Массимо*. Взлом гуманитарных организаций: определение киберпериметра и разработка стратегии кибербезопасности для международных гуманитарных организаций в период цифровой трансформации (опубликовано в этом выпуске журнала).

67 EPFL, "EPFL, ETH Zürich and the ICRC Leverage Science and Technology to Address Humanitarian Challenges", 10 December 2020, доступно по адресу: https://essentialtech.center/engineering-humanitarian-aid-awards-six-epfl-ethz-icrc-projects/.

68 Sean Capitain, "The Red Cross Presses Silicon Valley to Fight Cyberwarfare", *Fast Company*, 10 October 2017, доступно по адресу: https://www.fastcompany.com/40476581/red-cross-could-silicon-valley-limit-cyberwarfare-if-governments-wont.

69 John Naughton "Think the Giants of Silicon Valley Have Your Best Interests at Heart? Think Again",

принимательского героизма»[70]. Есть мнение, что эти два понятия неразрывно связаны с Кремниевой долиной США[71], где бытуют два убеждения: технология «несет благо всем» и «необходимо как можно быстрее внедрять новые виды технологий, даже если пока не совсем понятно, как они работают и каким может быть их влияние на общество»[72]. Это один из доводов, которые приводит Джо Бёртон, цитируя Натаниэля Рэймонда и призывая гуманитарные организации воздержаться от «слепого восторга по поводу возможных "перспектив Кремниевой долины"», поскольку ее склонность сводить сложные проблемы к технологическим решениям, очевидно, сослужила бы дурную службу в работе со сложностями, которые встречаются в зонах конфликтов. Такие допущения могут иметь тяжелые последствия для оценки возможности применения технологий в гуманитарной деятельности и свидетельствуют о необходимости критического взаимодействия с технологическим сектором и занятыми в нем предприятиями и работниками повсюду, где разрабатываются технологии.

Пилотный характер проекта МККК в Кремниевой долине иллюстрирует потенциал аналогичного взаимодействия в других центрах разработки цифровых технологий, где могут быть спланированы будущие кибероперации. Недавно МККК активизировал взаимодействие с технологическими компаниями в Японии[73], но очевидно, что возможности для подобного сотрудничества существуют и в других технологических центрах по всему миру.

Многосторонний подход и развитие международного права

Частный сектор пользуется все бóльшим влиянием, и это отражается на многостороннем подходе и развитии права — эта тема подробнее рассматривается в данном выпуске журнала. Учитывая быстрый рост технологического сектора и широкое распространение цифровых технологий, посол Индии Амандип С. Гилл в своей статье «Изменение роли многосторонних форумов в урегулировании вооруженных конфликтов в цифровую эпоху»[74] выявляет структурные проблемы, которые осложняют обсуждение быстро меняющихся цифровых технологий на уровне многосторонних

The Guardian, 21 October 2018, доступно по адресу: https://www.theguardian.com/commentisfree/2018/oct/21/think-the-giants-of-silicon-valley-have-your-best-interestsat-heart-think-again.

70 Daniela Papi-Thornton, "Tackling Heropreneurship", *Stanford Social Innovation Review*, 23 February 2016, доступно по адресу: https://ssir.org/articles/entry/tackling_heropreneurship#.

71 Jasmine Sun, "Silicon Valley's Saviorism Problem", *The Stanford Daily*, 16 February 2018, доступно по адресу: www.stanforddaily.com/2018/02/16/silicon-valleys-saviorism-problem/.

72 J. Naughton (примечание 69 выше).

73 NEC, "NEC and ICRC: A Blueprint for Ethical Technology Partnerships between the Private and Humanitarian Sectors", 11 November 2020, доступно по адресу: www.nec.com/en/global/sdgs/innovators/project/article02.html.

74 См.: *Гилл, Амандип С.* Изменение роли многосторонних форумов в урегулировании вооруженных конфликтов в цифровую эпоху (опубликовано в этом выпуске журнала).

форумов и своевременное реагирование в формате подготовки требуемых норм и политических мер. По мнению Гилла,

> хотя частные компании и представители гражданского общества сыграли важную роль в определении повестки дня и формировании мнения по итогам некоторых дискуссий, они уступают первое место более могущественным государственным и внутригосударственным деятелям. Это асимметричное распределение сил плохо вяжется с цифровой действительностью. Например, у таких цифровых платформ, как Facebook, Alipay и WhatsApp, бывает больше пользователей («виртуальных граждан»), чем жителей в большинстве стран; они эксплуатируют практически глобальную инфраструктуру, выступают в качестве трансграничных «блюстителей контента» и далеко опережают другие отрасли по объему рыночной капитализации, по сравнению с которой ВВП большинства государств кажется ничтожно малым.

В своей статье Гилл подчеркивает: «Для того чтобы нормы, связанные с цифровыми технологиями, могли на что-то влиять, представители цифровой индустрии должны участвовать в обсуждении ответных политических мер и сотрудничать с государством в целях их реализации».

То же верно и для гуманитарного сектора, особенно когда речь идет об МГП и его развитии. Учитывая, какими сложными бывают технологии, как быстро они развиваются и как плохо пока изучены их возможности, международное сообщество и гуманитарные организации должны найти новые способы добиться того, чтобы применение новых технологий в качестве средств и методов ведения войны отвечало нормам МГП.

Цифровые технологии и средства и методы ведения войны

Во второй части этого номера журнала акцент смещается с перспектив использования цифровых технологий в целях оказания гуманитарной помощи и оценки их пользы и сопутствующих опасностей в сторону способов применения новых технологий в разрушительных целях в ходе вооруженных конфликтов.

Так, в статье Франка Зауэра[75] речь идет о последствиях отказа от регулирования автономных систем вооружения, в том числе работающих с помощью ИИ. Раскрывая издержки отсутствия такого регулирования, Зауэр убедительно поясняет, почему регулировать автономные системы вооружения так сложно, но при этом совершенно необходимо по этическим, юридическим и политическим причинам. Как утверждает Зауэр, автономность систем вооружения должна регулироваться «посредством кодификации юридически закрепленного обязательства в значительной мере сохранять контроль человека над применением силы».

75 *Зауэр* (примечание 6 выше).

Новые способы применения датчиков и программного обеспечения, особенно ИИ и систем машинного обучения, также имеют дополнительные последствия для принятия решений в ходе вооруженных конфликтов. Пицци, Романофф и Энгельхардт убеждены в том, что системы ИИ и машинного обучения «могут быть очень мощными, а по своим аналитическим и предиктивным возможностям они все сильнее опережают человека. Поэтому их обязательно будут использовать для принятия решений вместо людей, особенно в тех случаях, когда надо провести быстрый или масштабный анализ, а оператор-человек часто не замечает риска и потенциала нанесения серьезного ущерба отдельным лицам или группам лиц, которые уже находятся в уязвимом положении»[76]. Изложение позиции МККК «Искусственный интеллект и машинное обучение в вооруженных конфликтах: ключевая роль должна принадлежать человеку», актуализированное для этого номера журнала и опубликованное в разделе «Доклады и документы», сформулировано более осторожно: «Системы ИИ и машинного обучения остаются инструментами, которые служат человеку, они должны помогать ему в процессе принятия решений, но не заменять его». В работе приведены доводы в пользу подхода, который ставит на первое место юридические и этические обязательства человека, чтобы «сохранить контроль со стороны человека и верховенство суждения человека, когда системы ИИ и машинного обучения используются для выполнения задач и принятия решений, могущих иметь серьезные последствия для жизни людей, особенно когда такие задачи или решения подвергают людей смертельному риску и когда они подпадают под действие конкретных норм международного гуманитарного права»[77]. В обоих материалах подчеркиваются технические ограничения ИИ, которые вызывают вопросы юридического характера; Пицци, Романофф и Энгельхардт отмечают, что ИИ

> осложняет обеспечение прозрачности и надзор, поскольку разработчики и операторы часто не могут «заглянуть внутрь» систем ИИ и понять, как и почему те принимают то или иное решение. Эта так называемая проблема черного ящика может стать препятствием для эффективной подотчетности в случаях, когда такие системы наносят вред, например когда система ИИ принимает или поддерживает решение, имеющее дискриминационные последствия[78].

Новые цифровые технологи также неизбежно повлияют на кибероперации и кибервойны. Использование сторонами в вооруженных конфликтах новых цифровых технологий напрямую воздействует на сами средства и методы ведения войны, а следовательно, и на применение и трактовку МГП

76 *Пицци, Романофф и Энгельхардт* (примечание 10 выше).
77 См.: *МККК*. Искусственный интеллект и машинное обучение в вооруженных конфликтах: ключевая роль должна принадлежать человеку (опубликовано в этом выпуске журнала).
78 *Пицци, Романофф и Энгельхардт* (примечание 10 выше).

в этом случае. В своей статье для данного номера журнала Лоран Жизель, Тильман Роденхойзер и Кнут Дёрман отмечают следующее[79]:

> …использование кибероперaций во время вооруженных конфликтов стало реальностью вооруженных конфликтов и, по всей вероятности, в дальнейшем таких операций будет еще больше. Такое положение вызывает определенные опасения в сегодняшних все более киберзависимых обществах, где злонамеренные кибероперации могут стать причиной серьезных повреждений и причинить ущерб людям. <…> Международное сообщество, отдельные страны и граждане всё сильнее зависят от цифровых инструментов. Эта тенденция, которая может стать еще более заметной в результате пандемии COVID-19, распространяющейся в момент написания настоящей статьи, увеличивает нашу зависимость от беспрепятственного функционирования этих технологий, что делает нас только более уязвимыми перед кибероперациями.

Последний тезис подтверждается результатами недавних исследований Freedom House[80], которые показывают, как государства по всему миру использовали ситуацию с пандемией, чтобы нарастить свои внутренние возможности слежки/надзора, например с помощью приложений для отслеживания контактов, которые собирают личную информацию. Институт кибермира[81] тоже выразил беспокойство в связи с ростом числа кибератак. Это явление приобретает особую форму, когда речь заходит об инфраструктуре системы здравоохранения, поскольку, как отмечают Жизель, Роденхойзер и Дёрман, «сектор здравоохранения, по-видимому, особенно уязвим для кибератак. Он развивается в сторону все большей цифровизации и взаимосвязанности, что увеличивает его зависимость от цифровых технологий и возможные масштабы поражения в случае нападения»[82]. Об этих тенденциях говорится и в статье, которую представили Чжисюн Хуан и Яохой Ин[83]. Авторы убедительно излагают иной взгляд на применение принципа проведения различия к информационным технологиям, привнося в обсуждение этого вопроса позицию китайских властей и доводы китайских ученых. Они подчеркивают, что некоторые элементы проведе-

79 *Жизель, Роденхойзер и Дёрман* (примечание 5 выше).

80 Adrian Shahbaz and Allie Funk, "The Pandemic's Digital Shadow", Freedom House, 2020, доступно по адресу: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

81 CyberPeace Institute, "A Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector", 26 May 2020, доступно по адресу: https://cyberpeaceinstitute.org/call-for-government/.

82 В свете этой тревожной тенденции МККК вместе с мировыми лидерами призвал прекратить атаки, направленные на инфраструктуру системы здравоохранения, особенно учитывая, что они могут поставить под угрозу жизнь уязвимых граждан. См.: "Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 May 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/.

83 См.: *Хуан, Чжисюн и Ин, Яохой*. Применение принципа проведения различия к информационным технологиям: опыт Китая (опубликовано в этом номере журнала).

ния различия — такие как униформа и знаки отличия — в сфере информационных технологий становятся неудобными или неприменимыми. Хотя сам принцип проведения различия остается актуальным, авторы полагают, что его следует трактовать в соответствии с реалиями кибермира.

В совокупности эти статьи отражают не только разнообразный опыт авторов, но и итоги многоплановых междисциплинарных исследований, благодаря которым в этом выпуске журнала глубоко рассмотрен вопрос о том, как такие цифровые технологии регулируются МГП в условиях вооруженного конфликта.

Тематический охват выпуска, посвященного цифровым технологиям и войне

Как указано выше, содержание этого выпуска журнала посвящено двойному назначению цифровых технологий: 1) для гуманитарной деятельности и оказания помощи, чтобы с учетом факторов риска и пользы поддержать и защитить пострадавших в ходе вооруженных конфликтов и других ситуаций насилия; 2) для ведения военных действий в ходе вооруженных конфликтов. В статьях, подготовленных для этого выпуска, также отмечается растущая роль частного сектора — особенно крупных технологических компаний — в предоставлении платформ, используемых для распространения вводящих в заблуждение сведений, дезинформации и риторики ненависти и формирующих способы обмена информацией в условиях кризиса.

При подготовке этого выпуска редакционный совет понимал, что мы только начинаем разбираться в закономерностях и тенденциях влияния цифровых технологий на наш мир. Поэтому данный номер, посвященный цифровым технологиям и войне, лишь приоткрывает завесу тайны над тем, как цифровые технологии влияют на вооруженные конфликты и другие ситуации насилия и как сами поддаются их влиянию, но не дает исчерпывающего представления об этом явлении. Иными словами, наше понимание существующих и зарождающихся технологий пока не может считаться полным, и мы постоянно узнаем о новых проблемах и возможностях, связанных с цифровыми технологиями, которые мы внедряем и используем и которых иногда боимся.

Гендерная проблематика, вопросы многообразия и всеохватности в журнале

Важными параметрами при подготовке этого номера журнала были гендерный паритет и отражение различных взглядов и различного опыта. Гендерный разрыв в технологическом секторе — известная проблема;

на женщин там приходится менее 35% всех сотрудников[84]. Что касается многообразия, то в крупнейших технологических компаниях[85] работают почти исключительно молодые белые мужчины[86] — выпускники престижных американских университетов[87], не получившие практически или вовсе никакого образования в сфере гуманитарных наук, этики или международных отношений[88]. Кроме того, высказывается мнение о том, что дискриминация по половому и расовому признакам присуща и самим цифровым технологиям[89], а также цифровым данным, в которых имеются структурные предубеждения, поскольку они отражают и усугубляют существующую в обществе дискриминацию и соотношение сил. Коллектив журнала поставил перед собой цель по крайней мере прервать эту тенденцию с точки зрения состава авторов, представленных в этом выпуске. В то же время мы столкнулись с определенными препятствиями в решении этой задачи; в конце зимы 2019 года, когда мы начинали готовить этот тематический выпуск, на мир обрушилась пандемия коронавируса, превосходящая по своим масштабам все пандемии прошлого века[90].

Для журнала кризис вылился в изменение гендерного состава авторов. Многие женщины, которых мы активно привлекали к работе, прекратили писать для журнала. Такая тенденция наблюдается во всем сегменте научных публикаций: женщины-ученые в большей степени, чем их коллеги-мужчины, столкнулись с двойной нагрузкой, вызванной необходимостью совмещать профессиональную занятость с работой по дому. Поскольку сразу несколько женщин-авторов отменили свои публикации, а наше приглашение присылать статьи женщины отклоняли существенно чаще, чем мужчины, мы продлили сроки публикации, чтобы в итоге в выпуске не было выраженного преобладания одной демографической группы. Как видно по итоговой версии журнала, к сожалению, нам не удалось достичь идеаль-

84 Sam Daley, "Women In Tech Statistics for 2020 (and How We Can Do Better)", *Built In*, 13 March 2020, доступно по адресу: https://builtin.com/women-tech/women-in-tech-workplace-statistics.

85 Jonathan Ponciano, "The Largest Technology Companies in 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive", *Forbes*, 15 May 2019, доступно по адресу: www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/.

86 Shelly Banjo and Dina Bass, "On Diversity, Silicon Valley Failed to Think Different", *Bloomberg Businessweek*, 3 August 2020, доступно по адресу: https://www.bloomberg.com/news/articles/2020-08-03/silicon-valley-didn-t-inherit-discrimination-but-replicated-it-anyway.

87 Avery Hartmans, "These 25 Universities Produce the Most Tech Employees", *Business Insider*, 2 May 2017, доступно по адресу: www.businessinsider.com/top-colleges-for-working-in-silicon-valley-2017-5.

88 Victor Lukerson, "The Ethical Dilemma Facing Silicon Valley's Next Generation", *The Ringer*, 6 February 2019, доступно по адресу: https://www.theringer.com/tech/2019/2/6/18212421/stanford-students-tech-backlash-silicon-valley-next-generation.

89 См., например: Karen Hao, "An AI Saw a Cropped Photo of AOC. It Autocompleted Her Wearing a Bikini", *MIT Technology Review*, 29 January 2021, доступно по адресу: www.technologyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/; Ryan Steed and Aylin Caliskan, "Image Representations Learned with Unsupervised Pre-Training Contain Human-Like Biases", Carnegie Mellon University, 2021, доступно по адресу: https://arxiv.org/pdf/2010.15052.pdf.

90 Eskild Petersen et al., "Comparing SARS-CoV-2 with SARS-CoV and Influenza Pandemics", *The Lancet Infectious Diseases*, 3 July 2020, доступно по адресу: www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30484-9/fulltext.

ного гендерного баланса в составе авторов, гендерный разрыв составляет 0,82 (число женщин-авторов по отношению к мужчинам-авторам), однако коллектив журнала твердо намерен изменить это соотношение в будущих выпусках[91]. Кроме того, мы продолжаем добиваться максимального многообразия — например, совсем недавно был сформирован новый состав редакционного совета журнала на период 2021–2026 годов, в который входят 19 самых разных экспертов со всего мира[92].

Разнообразие в журнале достигается не только за счет разного опыта авторов, но и за счет междисциплинарного и многодисциплинарного подхода к написанию статей. Такой междисциплинарный подход становится все более важным для понимания того, как различные практикующие специалисты, организации и страны учитывают и уменьшают побочное действие цифровых технологий в условиях гуманитарных кризисов и справляются с доселе неизвестными способами применения цифровых технологий в качестве средств и методов ведения войны.

Перспективы

Ключевой вывод из многочисленных статей, опубликованных в этом выпуске журнала, состоит в том, что в процессе цифровизации необходимо оценивать и снижать риск, сопряженный с внедрением новых цифровых технологий в гуманитарную деятельность. Эти инструменты приносят определенную пользу, но они также представляют риск непоправимого ущерба, и в применении цифровых технологий в условиях гуманитарных кризисов есть своя «темная сторона». Существует и еще один аспект: на фоне развития цифровых технологий и их применения в вооруженных конфликтах и других ситуациях насилия сохраняется потребность обеспечить соблюдение МГП. Но возникает вопрос: с чего нам, гуманитарным организациям, начать принимать меры в области цифровых технологий и войны?

Директор Управления МККК по переходу на цифровые технологии и работе с данными Бальтазар Штеелин прекрасно сформулировал вопрос по поводу будущего цифровых технологий на войне: «Данные — это “новая нефть” или новый асбест? Будем ли мы жить в мире Глобальной сети или в мире защитной сетки?»[93]. Однако, как отмечает Б. Штеелин, каким бы ни был ответ на этот вопрос, в ближайшие годы и десятилетия «МККК будет делать все возможное, чтобы адаптироваться к последствиям ускоряющейся цифровизации вместе с теми, кому он помогает в зонах конфликтов и по всему миру, и ради них. Их неизменное доверие к МККК покажет, удалось ли нам ответственно использовать колоссальный потенциал развивающихся цифровых технологий им во благо».

91 В качестве подтверждения см. новый состав редакционного совета журнала по адресу: https://international-review.icrc.org/ru/o-nas/redakcionnyy-sovet.
92 Там же.
93 Цитата предоставлена Бальтазаром Штеелином.

В соответствии с этим ключевым тезисом, который выдвинул Б. Штеелин, большинство разнообразных вопросов, рассмотренных в этом номере журнала, сводится к одному из ключевых условий гуманитарной деятельности — доверию. Через весь этот выпуск красной нитью проходит понимание того, что доверие действительно является основой цифровой трансформации в гуманитарной системе, однако оно не выстраивается быстро. Гуманитарные организации постепенно расширяют охват своей деятельности, опираясь на доверие местных сообществ и органов власти, которое они завоевывают каждый день. Руководствуясь той же логикой, мы можем сказать, что всем заинтересованным лицам, стремящимся к применению «технологии во благо», следует рассматривать влияние цифровых технологий на узы доверия с особым вниманием и тщательностью.

В дальнейшем цифровизация должна предполагать не только внедрение новых технологий, но и заботу о том, чтобы эти технологии укрепляли узы доверия, которые мы как гуманитарные организации формируем с пострадавшими, предлагая им новые возможности для удовлетворения их потребностей. Поэтому мы надеемся на то, что этот выпуск журнала послужит источником вдохновения для разработки стратегий цифровой трансформации, построенной вокруг людей, которым они призваны служить, и вместе с ними.