Взлом гуманитарных организаций: определение киберпериметра и разработка стратегии кибербезопасности для международных гуманитарных организаций в период цифровой трансформации

Массимо Марелли*
Массимо Марелли — руководитель отдела защиты данных Международного Комитета Красного Креста.

* Мнения и взгляды, изложенные в настоящей статье, принадлежат самому автору и не обязательно отражают мнение и взгляды МККК. Автор выражает благодарность Брюно Демейеру, Кубо Мачаку, Тильману Роденхойзеру, Андрее Рааб, Эве Ла-Э, Жилю Черутти, Дельфине ван Золинге, Пьеррику Девидалю, Венсану Графу Нарбелю, Фабьену Леймгруберу, Мартину Шюппу, Адриану Перригу, Саи Сатьянараянану Венкатешу и Саману Реджали за ценные комментарии к проекту статьи. Ответственность за все допущенные ошибки несет автор.

Аннотация

Цифровизация и новые технологии играют сегодня все более важную роль в гуманитарной деятельности. Гуманитарные организации все активнее используют новые цифровые технологии и все больше на них полагаются, превращаясь из простых наблюдателей в полноценных участников киберпространства, уязвимых к вредоносным кибероперациям, которые могут повлиять на их способность защищать людей, пострадавших от вооруженных конфликтов и иных ситуаций насилия, и оказывать им помощь.

Ввиду такого перехода гуманитарным организациям необходимо изучить и надлежащим образом очертить свой киберпериметр. Гуманитарные организации могут защитить себя и свою деятельность, разработав соответствующие киберстратегии для своей цифровой среды. Четкое определение цифровых границ, в пределах которых гуманитарная организация ведет свою работу, закладывает основу для выработки стратегии поддержки и защиты гуманитарной деятельности в цифровой среде, направления имеющихся ресурсов туда, где они нужнее всего, и выявления тех областей, в которых необходимо адаптировать операционное взаимодействие и методы работы к существованию в киберпространстве.

Цель настоящей статьи состоит в том, чтобы выявить уникальные проблемы, с которыми сталкиваются международные гуманитарные организации, работающие в киберпространстве, и предложить способы их решения. Так, в статье определены ключевые элементы, которые следует учесть международным гуманитарным организациям при выработке стратегии кибербезопасности. Для иллюстрации выявленных проблем и предлагаемых методов их решения на протяжении всей статьи в качестве примера используется Международный Комитет Красного Креста и специфика его работы.

Ключевые слова: кибернетический, стратегия работы в киберпространстве, кибербезопасность, кибероперации, кибератака, цифровые услуги, международные организации, гуманитарные организации, гуманитарная деятельность, цифровая трансформация.

: : : : : : : :

Некоторые из тем, рассмотренных в настоящей статье, были раскрыты в рамках серии публикаций в блоге МККК «Гуманитарное право и политика». См.: Massimo Marelli, "Hacking Humanitarians: Moving Towards a Human Cybersecurity Strategy", 16 January 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/; Massimo Marelli and Adrian Perrig, "Hacking Humanitarians: Mapping the Cyber Environment and Threat Landscape", 7 May 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/05/07/hacking-humanitarians-mapping-cyber-environment/; Massimo Marelli and Martin Schüepp, "Hacking Humanitarians: Operational Dialogue and Cyberspace", 4 June 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/06/04/hacking-humanitarians-dialogue-cyberspace/.

Введение и «подготовка почвы»

Цифровизация и новые технологии играют сегодня все более важную роль в гуманитарной деятельности[1]. Это происходит по ряду причин и в ответ на ряд новых проблем. Например, вооруженные конфликты становятся все более разрозненными и все менее очевидными, а безопасность и принятие утрачивают свои позиции, затрудняя международным гуманитарным организациям[2] доступ в зоны конфликтов и к пострадавшим.

В таких условиях гуманитарные организации стремятся развиваться и адаптироваться, чтобы иметь возможность более эффективно реагировать на кризисы в гуманитарной сфере. Они начали проявлять интерес к возможности дополнить физическое присутствие цифровым — например, посредством обеспечения своей доступности и ответов на запросы информации и помощи через социальные сети или приложения для обмена сообщениями[3]. Они развивают новые цифровые каналы как для оказания новых гуманитарных услуг, изначально доступных в цифровом формате, так и для предоставления привычных видов помощи пострадавшим, которые, возможно, уже имеют онлайн-доступ к другим государственным и частным услугам и ожидают того же от гуманитарных организаций. Кроме того, организации отмечают положительную роль цифровых платформ в укреплении существующих и создании новых механизмов обеспечения жизнестойкости пострадавших и задаются вопросом о том, как они могут содействовать работе или наращиванию таких механизмов[4].

Следует также отметить, что рост числа вооруженных конфликтов и иных ситуаций насилия наблюдается именно в городской среде, где име-

1 См.: Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector", *Humanitarian Law and Policy Blog*, 5 December 2016, доступно по адресу: https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/ (все ссылки на интернет-ресурсы приводятся по состоянию на январь 2021 г.).

2 Аналитический охват настоящей статьи ограничен международными гуманитарными организациями, то есть организациями, имеющими статус международных или приравненных к ним и мандат на осуществление гуманитарной деятельности. Неправительственные организации к ним не относятся. Для целей настоящей статьи основная разница между международными гуманитарными и неправительственными организациями состоит в том, что международная гуманитарная организация обладает привилегиями и иммунитетами, чтобы выполнять свой мандат совершенно независимо. Существование и функционирование международных гуманитарных организаций занимают центральное место в деятельности международного сообщества: оно ожидает от международных гуманитарных организаций решения задач, с которыми отдельные государства или группы государств не могут справиться поодиночке. Благодаря этому работа международных гуманитарных организаций не теряет своей актуальности, но в то же время они становятся очень уязвимыми к возможным кибератакам. Однако особый статус, привилегии и иммунитеты, которыми они обладают, могут стать важными способами защиты организаций, если надлежащим образом применять их в киберпространстве.

3 См.: International Committee of the Red Cross (ICRC), in collaboration with The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action*, January 2017, доступно по адресу: www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

4 См.: A. Kaspersen and C. Lindsey-Curtet (примечание 1 выше).

ется подключение к интернету[5] и где зачастую разобраться в обстановке мешает не отсутствие данных, а скорее их избыток и сложности, связанные с тем, чтобы вычленить из них смысл. То есть гуманитарные организации рассматривают преимущества использования новых технологий, таких как искусственный интеллект (ИИ), машинное обучение и анализ больших данных, чтобы попытаться разобраться в сложной среде, в которой им приходится работать[6]. Иногда эти технологии встроены в продукты, которые имеются в продаже и которые можно приобрести в готовом виде у компаний, часто заинтересованных в партнерстве с гуманитарными организациями.

Добавим, что вооруженные конфликты стали длиться дольше. Период, в течение которого Международный Комитет Красного Креста (МККК) присутствует в странах, где проводятся десять самых крупных операций, составляет в среднем более сорока лет[7]. В условиях затяжных конфликтов гуманитарным организациям иногда приходится планировать ответные меры на долгий срок, выходя далеко за пределы срочной разовой раздачи продуктов питания и непродовольственных товаров или оказания медицинской помощи пострадавшим в ходе боевых действий и предусматривая повторное распределение помощи в долговременной перспективе. Такие ответные меры также предполагают работу с системами и объектами инфраструктуры, например в области водоснабжения, канализации и энергоснабжения. В таких условиях гуманитарный сектор заинтересован в цифровых технологиях идентификации получателей помощи, в том числе до некоторой степени в технологии биометрии.

Этот процесс «цифровой трансформации», в рамках которого гуманитарные услуги предлагаются и становятся доступными в цифровом формате, выводит сбор и создание персональных данных на новый уровень. В сочетании с необходимостью привлекать сторонних коммерческих и/или технических специалистов, которая обычно возникает при оказании соответствующих услуг в электронном формате, этот процесс резко меняет динамику предоставления гуманитарной помощи, и организации должны иметь это в виду при двустороннем взаимодействии между гуманитарными организациями и их визави. Это изменение приводит к тому, что в гуманитарной деятельности начинают участвовать поставщики технологий, финансовые учреждения, операторы мобильных сетей и лица, занятые масштабным массовым наблюдением в телекоммуникационных сетях или адресной цифровой слежкой.

Защита персональных данных — необходимый инструмент, позволяющий гуманитарным организациям в полной мере разобрать и про-

5 См.: David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*, Oxford University Press, Oxford, 2015, доступно по адресу: www.kilcullenstrategic.com/out-of-the-mountains/.

6 См.: Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of the Red Cross*, Vol. 99, No. 904, 2017.

7 См.: Ellen Policinski and Jovana Kuzmanovic, "Protracted Conflicts: The Enduring Legacy of Endless War", *International Review of the Red Cross*, Vol. 101, No. 912, 2019, p. 965.

анализировать потоки данных, выявить внешних заинтересованных лиц, вычленить новые виды риска и определить меры по его снижению. Следовательно, важно обеспечить внедрение новых технологий таким образом, чтобы не нарушить права, достоинство и представительство пострадавших, добиться подотчетности гуманитарных организаций и доверия к ним и сохранить ответственность за следование принципу «не навреди» в цифровой среде[8].

В связи с этим принципы этики и защиты данных являются ключевыми показателями того, как организация формирует методы работы в киберпространстве в интересах пострадавших, а значит, и свой киберпериметр. Однако в настоящей статье мы стремимся выйти за пределы формального исследования аспектов цифровой трансформации, связанных с защитой персональных данных, и этики работы с гуманитарными данными. Наша задача — выявить уникальные проблемы, с которыми сталкиваются международные гуманитарные организации, работающие в киберпространстве, и предложить способы их решения. Если говорить конкретнее, автор намерен рассмотреть, как увеличение «цифрового следа» с одной стороны в сочетании с юридическими, техническими и геополитическими последствиями цифровизации в гуманитарном секторе с другой формируют киберпериметр международной гуманитарной организации. Для целей настоящей статьи киберпериметр организации определяется как совокупность элементов, формирующих присутствие и поведение организации в киберпространстве: ее мандата, деятельности в киберпространстве и способов осуществления и защиты такой деятельности, в частности, для предотвращения конкретных угроз и реагирования на них.

Осознание и определение своего киберпериметра необходимо для организаций, работающих в гуманитарной сфере и проходящих процесс цифровизации в вышеуказанном масштабе. По мере активизации деятельности в киберпространстве и роста зависимости от него подобные структуры превращаются из простых наблюдателей в полноценных участников этой среды, которая сама по себе уязвима к вредоносным кибероперациям или может оказаться под «перекрестным огнем», что может повлиять на способность организаций осуществлять гуманитарную деятельность в интересах тех, кто больше всего нуждается в помощи.

8 По вопросу защиты данных в гуманитарной деятельности см.: Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC, Geneva, 2020 (Руководство по защите данных в ходе гуманитарной деятельности. Готовится к публикации на русском языке), доступно по адресу: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-print-en. По вопросу последствий создания метаданных за счет взаимодействия с третьими лицами при осуществлении гуманитарных программ см.: Tina Bouffet and Massimo Marelli, "The Price of Virtual Proximity: How Humanitarian Organizations' Digital Trails can Put People at Risk", *Humanitarian Law and Policy Blog*, 7 December 2018, доступно по адресу: https://blogs.icrc.org/law-and-policy/2018/12/07/price-virtual-proximity-how-humanitarian-organizations-digital-trails-put-people-risk/. По вопросу использования биометрических данных в МККК см.: Ben Hayes and Massimo Marelli, "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy", *Humanitarian Law and Policy Blog*, 18 October 2019, доступно по адресу: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.

Ввиду такого изменения гуманитарным организациям необходимо изучить и надлежащим образом очертить свой киберпериметр, образующийся в ходе подобной деятельности. При должном тщании это позволит им сформировать стратегию поддержки и надлежащей защиты процесса оказания гуманитарной помощи в цифровой среде, направить имеющиеся ресурсы туда, где они нужнее всего, и выявить те области, в которых необходимо адаптировать операционное взаимодействие и методы работы к существованию в киберпространстве.

В этом смысле киберпериметр международной гуманитарной организации можно проанализировать с точки зрения: 1) намерений организации относительно работы в цифровой среде и осуществления гуманитарной деятельности в цифровом формате; 2) характера, мандата и методов работы гуманитарной организации, а также пострадавших, которым она оказывает помощь; 3) киберпространства, в частности применительно к тем трудностям и угрозам, с которыми сталкивается организация в цифровой среде.

В настоящей статье говорится о том, что эти три аспекта и проблемы, возникающие в рамках каждого из них при осуществлении деятельности в киберпространстве, и должны формировать стратегию кибербезопасности организации. Таким образом, подобная стратегия позволит внедрить следующие виды защиты и связей (перечень не исчерпывающий): 1) правовая защита, за которой необходимо обратиться; 2) защита данных и потоков данных с помощью технических средств, которую можно применять или за которой можно обратиться; 3) лица, которых необходимо привлечь, и операционное взаимодействие, которое необходимо выстроить с ними. Каждый из элементов по очереди проанализирован ниже.

Предполагаемая деятельность организации в цифровой среде и оказание гуманитарных услуг в цифровом формате

Первым шагом к точному очерчиванию киберпериметра организации является анализ того, какие именно действия организация намерена совершать в киберпространстве, и систематизация видов гуманитарных услуг, которые оказываются или будут оказываться в цифровом формате. Как мы увидим ниже, это необходимо для определения остальных элементов киберпериметра организации и возможных способов его защиты.

В случае МККК предоставление услуг в цифровом формате напрямую их получателям лежит в основе институциональной стратегии организации на 2019–2022 годы[9]. Эта стратегия обусловлена преимущественно 1) затруднением физического доступа в зоны конфликта и вытекающей из него необходимостью дополнить физическое присутствие цифровым присутствием и доступом; 2) тем фактом, что конфликты все чаще происходят там, где у людей с большей вероятностью есть доступ к интернету

9 См.: ICRC, *ICRC Strategy 2019–2022*, Geneva, September 2018, доступно по адресу: www.icrc.org/en/publication/4354-icrc-strategy-2019-2022.

и привычка пользоваться услугами в формате онлайн, в связи с чем они ожидают, что смогут взаимодействовать с гуманитарными организациями в электронной форме. В таких условиях МККК необходимо пройти значительную цифровую трансформацию для достижения своих целей. Это, в свою очередь, приведет к экспоненциальному росту «цифрового следа» организации — в цифровую эпоху эта тенденция является общей для большинства организаций в гуманитарном секторе и за его пределами. Данная тенденция сопровождается естественным появлением новых видов атак и ростом подверженности таким атакам, а также повышением привлекательности организаций в качестве мишеней вредоносных кибероперация[10].

Важная задача, стоящая перед МККК, связана с использованием данных (как сгенерированных в процессе перехода организации к цифровым технологиям, так и сгенерированных, приобретенных или ставших доступными извне), например за счет применения предиктивной аналитики или анализа больших данных либо за счет разработки или настройки инструментов ИИ и машинного обучения для содействия решению проблем, присущих именно гуманитарной деятельности. Это важно, поскольку позволяет организации принимать решения на основе данных и улучшать понимание оперативной обстановки в ходе вооруженных конфликтов и иных ситуаций насилия — например, благодаря получению сведений для прогнозирования моделей перемещения, выявления лиц, пользующихся авторитетом у сторон в конфликте и способных помочь обеспечить доступ, или совершенствования инструментов управления логистикой и цепочками поставок[11]. Кроме того, использование данных может способствовать поддержке гуманитарной деятельности за счет различных инструментов и методов анализа и обработки данных — от статистики до ИИ (например, для определения местонахождения лиц, пропавших без вести, с помощью технологии распознавания лиц)[12].

Таким образом, МККК намеревается использовать киберпространство для следующих целей: 1) организация цифрового присутствия в дополнение к физическому, оказание гуманитарных услуг и обеспечение доступности в цифровом и дистанционном формате для пострадавших, которые все чаще имеют доступ к интернету; 2) создание и использование новых механизмов обеспечения жизнестойкости пострадавших с помощью цифровых платформ; 3) использование данных для принятия решений на основе информации, что, в свою очередь, влияет на формирование киберпериметра.

10 См.: ICRC, *The Potential Human Cost of Cyber Operations*, Geneva, 29 May 2019, доступно по адресу: www.icrc.org/en/document/potential-human-cost-cyber-operations.

11 См., например: "Big Data, Migration and Human Mobility", *Migration Data Portal*, доступно по адресу: https://migrationdataportal.org/themes/big-data-migration-and-human-mobility.

12 См., например: ICRC, "Rewards and Risks in Humanitarian AI: An Example", *Inspired*, 6 September 2019, доступно по адресу: https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/.

Характер, мандат и методы работы организации

Для определения киберпериметра организации при проведении анализа важно отталкиваться от характера, мандата и принципов ее работы, чтобы выяснить, что́ нуждается в защите и каким образом можно организовать такую защиту в соответствующей области киберпространства. Каждой организации следует начинать анализ с рассмотрения своей специфики.

Возвращаясь к примеру МККК, отметим, что он является нейтральной, беспристрастной, независимой организацией, преследующей исключительно гуманитарные цели, связанные с защитой жизни и достоинства жертв вооруженных конфликтов и иных ситуаций насилия. Работа МККК основана на Женевских конвенциях 1949 года, Дополнительных протоколах к ним, Уставе МККК и Международного движения Красного Креста и Красного Полумесяца (Движение), а также на резолюциях международных конференций Красного Креста и Красного Полумесяца.

МККК имеет особый правовой статус, привилегии и иммунитеты в соответствии с международным правом и внутригосударственным законодательством[13]. Привилегии и иммунитеты предоставляются ему с тем, чтобы он мог эффективно исполнять свой мандат в полном соответствии со своими основополагающими принципами и методами работы[14].

Как будет показано ниже, нейтральность, беспристрастность и независимость МККК, исключительно гуманитарный характер его деятельности, а также привилегии и иммунитеты, которыми он располагает в большинстве стран, позволяют ему исполнять свой мандат и являются неотъемлемыми элементами, формирующими киберпериметр организации и четко отделяющими его от киберпериметров других организаций.

В рамках международного гуманитарного права и Устава Движения[15] государства поручают МККК предоставлять людям помощь и защиту в ходе вооруженных конфликтов и иных ситуаций насилия. Как показано выше, сегодня для осуществления этого мандата организация также должна присутствовать и работать в киберпространстве, например, оказывая услуги в цифровом формате. Обязательство государств по отношению к работе МККК в физической реальности и к методам его деятельности в интересах пострадавших от вооруженных конфликтов и иных ситуаций насилия должно распространяться и на киберпространство (с необходимыми поправками).

При исполнении своего мандата МККК придерживается подхода, основанного на присутствии, за счет привлечения около 20 тысяч сотрудников в 80 странах в целях реагирования на гуманитарные потребности

13 См.: *Дебюф, Эльс*. Инструментарий МККК: правовой статус, привилегии и иммунитеты // Международный журнал Красного Креста. Т. 97, № 897/898, 2016 г., доступно по адресу: https://international-review.icrc.org/ru/articles/tools-do-job-icrcs-legal-status-privileges-and-immunities.

14 См.: ICRC, "Fundamental Principles", доступно по адресу: www.icrc.org/en/fundamental-principles.

15 См.: Устав Международного движения Красного Креста и Красного Полумесяца, принятый XXV Международной конференцией Красного Креста в Женеве в 1986 г. (с поправками, внесенными в 1995 г. и 2006 г.), доступно по адресу: https://www.icrc.org/ru/doc/assets/files/red-cross-crescent-movement/movement_statutes_rus.pdf.

пострадавших и взаимодействия с ключевыми заинтересованными лицами по поводу применения международного гуманитарного права[16]. В отличие от других гуманитарных организаций, которые часто действуют через партнеров-исполнителей, МККК осуществляет такую деятельность, которая требует непосредственной близости к пострадавшим (например, перемещенным лицам, людям, находящимся в местах лишения свободы, раненым и больным, разлученным членам семей, несовершеннолетним, которые остались без присмотра взрослых, и родственникам пропавших без вести), а также физического присутствия в местах нахождения этих пострадавших.

Непременным условием получения доступа является доверие. Это относится к доверию 1) как со стороны пострадавших, 2) так и со стороны участников вооруженных конфликтов и иных ситуаций насилия. Доверие со стороны пострадавших основано на гарантии того, что любое взаимодействие между ними и МККК будет носить исключительно гуманитарный характер. В частности, пострадавшие ожидают, что информация, которую они предоставляют в гуманитарных целях, будет применяться только в этих целях и не будет использоваться или обрабатываться таким образом, который может нанести ущерб их безопасности или гуманитарной деятельности в более общем смысле, например посредством использования полученных сведений участниками, которые не являются гуманитарными организациями, для достижения целей, связанных с конфликтом, борьбы с терроризмом, контроля миграционных потоков или извлечения коммерческой выгоды. Важность обеспечения того, чтобы данные, собранные в гуманитарных целях, не использовались для других целей, признается и в резолюции о неприкосновенности частной жизни и международной гуманитарной деятельности (принятой Международной конференцией комиссаров по вопросам неприкосновенности частной жизни и защиты данных, которая состоялась в 2015 году в Амстердаме)[17], и в резолюции Движения «Восстановление семейных связей с соблюдением требований конфиденциальности, в том числе и в отношении защиты персональных данных», принятой в 2019 году[18].

Для того чтобы заручиться доверием сторон в вооруженном конфликте и участников иных ситуаций насилия, необходимо сообщить им уверенность в нейтральности, беспристрастности, независимости и исключительно гуманитарном характере организации. Это означает, что организация должна принимать меры для минимизации риска получения такими субъектами доступа к собранным данным и обеспечения того, чтобы эти

16 См.: *МККК*. Что делаем. Доступно по адресу: https://www.icrc.org/ru/what-we-do.

17 См.: "Resolution on Privacy and International Humanitarian Action", 37th International Conference of Data Protection and Privacy Commissioners, Amsterdam, 27 October 2015, доступно по адресу: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

18 См.: 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.

данные не использовались для достижения целей, связанных с конфликтом, не передавались правоохранительным органам или службам разведки, не предъявлялись в уголовном разбирательстве в качестве улик и не становились достоянием гласности иным образом. Следовательно, одним из ключевых принципов работы, позволяющим МККК получить доступ в зоны конфликтов и к пострадавшим в ходе конфликта людям, является обеспечение конфиденциальности[19]. В частности, МККК не предоставляет никаким третьим лицам информацию, имеющую отношение к конфиденциальному двустороннему взаимодействию с органами власти и иными субъектами, участвующими в конфликтах и иных ситуациях насилия. Этот принцип работы также подкрепляется правом не раскрывать информацию — особой мерой защиты, предусмотренной обычным международным правом, которой может пользоваться только МККК, — другие организации лишены этой привилегии[20].

Несмотря на то что в поддержку этого тезиса не нашлось никаких научных работ, по опыту автора и других участников гуманитарной деятельности, в реальном мире и для достижения физического присутствия необходимо заручиться доверием за счет ряда факторов, включая уязвимость[21]. Для того чтобы обеспечить и закрепить свое присутствие, МККК обычно не прибегает к помощи вооруженного сопровождения, не использует бронированные машины и не создает физические барьеры; вместо этого организация полагается исключительно на принятие своей гуманитарной деятельности и на доверие к своему нейтральному, беспристрастному и независимому подходу, несмотря на то, что таким образом она оказывается уязвимой. Если кому-либо из заинтересованных сторон это покажется неубедительным, такая сторона может очень легко причинить вред персоналу и имуществу организации. Тот факт, что организация и ее сотрудники действуют открыто и демонстрируют свою уязвимость перед лицом любых злонамеренных третьих лиц, заставляет собеседников принять слова организации на веру и не искать в них скрытых мотивов.

Однако в цифровом мире уязвимость является не сильной, а слабой стороной. Одного лишь понимания того, что системы организации при желании могут быть легко взломаны, достаточно, чтобы подорвать любое доверие к этой организации и отвратить заинтересованных лиц от того, чтобы вступать с ней во взаимодействие. Следовательно, для завоевания доверия и создания цифрового присутствия не в ущерб физическому МККК должен иметь возможность продемонстрировать безопасность и жизнестойкость своей информационной инфраструктуры. Поэтому международная гуманитарная организация должна полностью осознавать ту киберсреду, в которой она действует, а также присущие ей проблемы и угрозы.

19 См.: *МККК*. Конфиденциальность: вопросы и ответы, 15 января 2018 г., доступно по адресу: https://www.icrc.org/ru/document/konfidencialnost-voprosy-i-otvety.

20 См.: *Дебюф, Эльс* (примечание 13 выше).

21 См.: Philippe Dind, "Security in ICRC Field Operations", *Secure 02*, Finnish Red Cross, June 2002, p. 27, доступно по адресу: www.icrc.org/en/doc/assets/files/other/secure02_dind.pdf.

Киберпространство и присущие ему проблемы и угрозы, с которыми сталкиваются организации

Киберпространство, в котором функционирует международная гуманитарная организация, порождает ряд угроз. Их обычно анализируют с позиции триады «конфиденциальность, целостность, доступность»[22]. Как говорится ниже, в случае международной гуманитарной организации «классического» анализа этой триады недостаточно — он нуждается в адаптации с учетом конкретных угроз безопасности, возникающих из соображений, связанных с юрисдикцией, то есть из того факта, что доступ может быть получен органами власти, к юрисдикции которых относятся организации, осуществляющие обработку данных, или их субподрядчики. В отношении безопасности цепочки поставок необходимо выработать дополнительные конкретные соображения. Каждый из этих аспектов по очереди рассматривается ниже.

Конфиденциальность

Гуманитарная организация может оказаться в ситуации, когда лица или группы лиц, поддерживающие одну из сторон в вооруженном конфликте (или участника иных ситуаций насилия), могут попытаться получить доступ к конфиденциальным данным, имеющимся у организации. Это обусловлено тем, что такие данные могут относиться к конкретным важным лицам или группам населения, имеющим общее этническое происхождение или связанным общими этническими корнями либо принадлежащим к национальной или политической группе, которая является противником указанной стороны. Например, информация медицинского характера может дать представление о состоянии здоровья человека, являющегося приоритетной целью[23].

Еще одной важной проблемой в поле конфиденциальности могут стать нападения в целях «кражи больших данных». Они могут быть направлены на сбор как можно большего количества наборов данных, которые затем сопоставляются, анализируются и используются для определения характеристик лиц, представляющих интерес для нападающего[24]. Такими лицами могут быть, в том числе, получатели гуманитарной помощи или другие лица, взаимодействующие с гуманитарной организацией в рамках нейтрального и беспристрастного общения. Затем за людьми, чьи характеристики были определены таким образом, может быть установлена при-

22 См.: Michael Nieles, Kelley Dempsey and Victoria Yan Pilliterri, *An Introduction to Information Security*, NIST Special Publication 800-12, National Institute of Standards and Technology, June 2017, доступно по адресу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

23 См., например: C. Currier, "The NSA Plan to Find Osama Bin Laden by Hiding Tracking Devices in Medical Supplies", *The Intercept*, 21 May 2015, доступно по адресу: https://theintercept.com/2015/05/21/nsa-plan-find-osama-bin-laden-infiltrating-medical-supply-chain/.

24 См., например: Bill Gertz, "Cybercom: Big Data Theft at OPM, Private Networks Is New Trend in Cyber-Attacks", *Washington Free Beacon*, 27 July 2015, доступно по адресу: https://freebeacon.com/nationalsecurity/cybercom-big-data-theft-at-opm-private-networks-is-new-trend-in-cyber-attacks/.

цельная слежка, а сведения о них могут быть использованы для планирования дополнительных действий, направленных на достижение целей, связанных с конфликтом. Это опасение может относиться к большим наборам данных, включая метаданные (то есть данные о данных), хранящимся как в самих гуманитарных организациях, так и у третьих лиц, которые являются их поставщиками (таких как операторы телефонной связи или финансовые учреждения); все они могут генерировать и использовать эти данные в рамках гуманитарных программ, например, связанных с мобильными денежными переводами.

С точки зрения конфиденциальности большое значение имеет и сотрудничество или взаимодействие со сторонними поставщиками технических услуг по поводу прохождения или обработки данных, например на базе некоторых видов облачных решений или в программах, связанных с денежными переводами, в которых участвуют поставщики финансовых услуг и/или операторы сетей мобильной связи. Международные гуманитарные организации могут пользоваться определенными привилегиями и иммунитетами в отношении данных, которые они собирают. В таких случаях органы власти не могут на законных основаниях надлежащим образом истребовать доступ к хранящимся у них данным, что позволяет сохранить конфиденциальность. Важно, чтобы аналогичные защитные меры действовали и в тех случаях, когда данные для организации обрабатывают сторонние подрядчики, хотя определенные трудности, с которыми сопряжена генерация и обработка данных с помощью цифровых инструментов такими третьими лицами, осложняет применение этого принципа.

Для того чтобы понять, в связи с чем сторонние поставщики могут представлять угрозу безопасности данных международной гуманитарной организации, необходимо четко оценить применение принципа суверенитета к киберпространству, в частности посредством анализа того, как государства воспринимают свою юрисдикцию в отношении поставщиков технологий, инфраструктуры для обеспечения потоков данных и самих этих потоков как на территории этих государств, так и за ее пределами. Любой международной гуманитарной организации, особенно такой как МККК, важно иметь гарантию того, что никакие органы власти не могут законным путем истребовать доступ к данным, хранящимся в организации ни напрямую, ни через третьих лиц, выполняющих обработку данных.

Цифровизация такого масштаба и размаха, как описано выше, вероятнее всего, будет невозможной без использования публичных облачных сервисов по крайней мере для части предлагаемых организацией услуг[25]. Технологические компании активно и стремительно перемещают свое программное обеспечение и услуги хранения данных в публичные облачные пространства и уже не поддерживают альтернативные решения, не осно-

25 О том, что такое публичный облачный сервис и почему он может стать важным инструментом, который необходимо использовать, см.: *Майкрософт.* Что такое общедоступные, частные и гибридные облака?, доступно по адресу: https://azure.microsoft.com/ru-ru/overview/what-are-private-public-hybrid-clouds/.

ванные на облачных технологиях, что часто приводит к устареванию таких решений. Кроме того, некоторые инструменты, позволяющие максимизировать объем информации, — например, за счет использования ИИ — можно более эффективно приобрести и развернуть именно в публичном облаке. В связи с этим в среднесрочной перспективе становится все труднее поддерживать модель, не основанную на применении облачных технологий и предполагающую хранение, использование и поддержку решений в помещениях организации, — эту модель традиционно предпочитают организации, проявляющие заботу о безопасности. Даже программное обеспечение, приобретаемое сегодня для использования в помещениях организации, вероятно, будет связано с приложениями, размещенными в публичном облаке, и/или будет обмениваться диагностическими или телеметрическими данными с другими юрисдикциями[26]. Это означает, что данные, собранные и созданные организацией, на каком-то этапе, скорее всего, будут обрабатываться сторонними поставщиками технологий. Такая постановка вопроса создает новые серьезные трудности в обеспечении конфиденциальности.

Поэтому гуманитарным организациям важно тщательно проанализировать эту сферу и найти решения, подходящие для той деликатной работы, которую они выполняют. Такие соображения должны учитывать конкретные архитектурные особенности публичного облака[27] и законодательство, позволяющее органам власти получать доступ к данным, сгенерированным и/или хранящимся за пределами их территории, например акт Конгресса США, разъясняющий законное использование данных за рубежом, и другое подобное законодательство в иных странах. Законы такого типа и последствия их принятия быстро распространяются по всему миру[28] преимущественно в связи с двумя факторами: 1) другие страны воспроизводят содержание указанного акта в своем законодательстве, чтобы обеспечить контроль над данными в рамках своей юрисдикции; 2) США в соответствии с этим актом заключают с третьими странами соглашения, позволяющие обеим сторонам требовать предоставления доступа к данным, относящимся к юрисдикции друг друга.

Целостность

С точки зрения целостности серьезную проблему представляет активизация применения ИИ и машинного обучения для принятия решений и оценки обстановки. С учетом этого создается угроза вмешательства третьих лиц, стремящихся нарушить точность и целостность данных, которые исполь-

26 См., например: Dutch Ministry of Justice, *DPIA Office 365 ProPlus Version 1905: Data Protection Impact Assessment on the Processing of Diagnostic Data*, June 2019, доступно по адресу: www.government.nl/documents/publications/2019/07/22/dpia-office-365-proplus-version-1905.

27 См.: *Майкрософт.* Что такое облачные вычисления? Руководство для начинающих, доступно по адресу: https://azure.microsoft.com/ru-ru/overview/what-is-cloud-computing/.

28 См.: US Department of Justice (DoJ), "CLOUD Act Resources", доступно по адресу: www.justice.gov/dag/cloudact.

зуются для обучения алгоритмов и разработки моделей, а также наборов данных, на основе которых выполняется анализ, чтобы повлиять на результаты анализа и на принимаемые решения[29]. Следовательно, гуманитарные организации могут стать объектом манипуляций и неправильно расставить приоритеты, отдав предпочтение определенным группам пострадавших перед другими или выбрав определенные районы для осуществления своей деятельности в ущерб другим, или иным образом подпасть под влияние третьих лиц, что может пагубно отразиться на пострадавших или нарушить нейтральность, беспристрастность и независимость деятельности гуманитарных организаций.

Доступность

С точки зрения доступности или обеспечения своевременного и надежного доступа к информации и ее использования опасение вызывают ситуации, в которых гуманитарная организация оказывает пострадавшим услуги в цифровом формате. Это может происходить в тех случаях, когда цифровое присутствие успешно создано и дополняет присутствие физическое или когда физический доступ невозможен, и вместо него приходится обеспечивать доступ в цифровой форме. Если от доступности услуг гуманитарной организации в цифровом формате зависит наличие у пострадавших средств к существованию или их гуманитарная защита, любая кибероперация, которая отрицательно скажется на доступности таких услуг, будет иметь гуманитарные последствия. В таких случаях кибероперации, влияющие на доступность гуманитарных услуг (в цифровом формате), например DDoS-атаки (распределенные атаки типа «отказ в обслуживании») или операции с использованием программ-вымогателей, вызывают очень серьезные опасения гуманитарного характера. Гуманитарным организациям следует также рассмотреть влияние подобных операций на свою способность оказывать гуманитарные услуги в цифровом формате и на возможность доступа к ним пострадавших[30]. Кроме того, гуманитарным организациям необходимо учесть в своем киберпериметре вероятность того, что операции с применением киберсредств могут проводиться одной из заинтересованных сторон в отношении ее противников под видом самой организации или под ее именем[31] либо за счет ее репутации, тем самым нанося ущерб доверию, которое могут питать к ней люди, хотя эта проблема и не оказывает непосредственного влияния на системы и инфраструктуру такой организации.

29 См.: C. Kuner and M. Marelli (eds) (примечание 8 выше), Chap. 16.3.5.

30 См.: Berhan Taye and Sage Cheng, "The State of Internet Shutdowns", *Access Now*, 8 July 2019, доступно по адресу: www.accessnow.org/the-state-of-internet-shutdowns-in-2018/.

31 См., например: Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender", *Citizen Lab*, 24 August 2016, доступно по адресу: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Безопасность цепочек поставки

Обеспечение безопасности цепочек поставки сопряжено с особыми проблемами[32]. Это означает, к примеру, что в аппаратных или программных решениях, приобретаемых и используемых гуманитарными организациями для оказания гуманитарных услуг в цифровом формате и/или для управления своими системами, не должно быть вредоносных программ, известных как бэкдоры. Что касается аппаратной части, то, хотя в перспективе организация может произвести вложения в обеспечение безопасности некоторых ключевых компонентов приобретаемых устройств[33], рассчитывать на обеспечение безопасности всех необходимых составляющих не приходится.

Возможно, организации придется разработать комплексную стратегию решения проблем, связанных с безопасностью цепочки поставок. В такой стратегии необходимо предусмотреть ряд элементов, таких как общедоступные компоненты аппаратных решений, закупочный процесс, информирование о правилах пользования и отработка их применения (например, обучение сотрудников, но одновременно с этим и минимизация возможностей аппаратных и программных решений, с тем чтобы они обрабатывали только те данные и выполняли только те операции, которые строго необходимы для целей обработки), а также партнерство с научными кругами в вопросах разработки решений для отслеживания работы устройств в целях обнаружения любых возможных аномалий, связанных с получением несанкционированного доступа к части оборудования[34]. Что касается программного обеспечения, то некоторые разработчики могут предоставить странам и международным организациям исходный код, чтобы они могли провести его аудит и убедиться в отсутствии бэкдоров[35].

Международной организации может потребоваться доступ к таким программам, однако может статься, что подобное решение имеется не у всех поставщиков. Кроме того, даже если организации будет предоставлен доступ к исходному коду, у нее может не быть средств для тщательной проверки всех строк кода предоставленного программного обеспечения и, соответственно, для самозащиты.

32 См., например: ICT Switzerland, “Supply Chain Security”, доступно по адресу: https://ictswitzerland.ch/en/topics/cyber-security/supply-chain/.

33 См.: Fabio Bergamin, “Open-Source Microprocessor”, *ETH Zürich*, 30 March 2016, доступно по адресу: https://ethz.ch/en/news-and-events/eth-news/news/2016/03/open-source-microprocessor.html.

34 См.: Markus Gross, “A Booting Computer Is as Vulnerable as a Newborn Baby”, *ETH Zürich*, 5 November 2019, доступно по адресу: https://ethz.ch/en/news-and-events/eth-news/news/2019/11/project-opentitan.html.

35 См.: Microsoft, “Government Security Program”, доступно по адресу: www.microsoft.com/en-us/securityengineering/gsp.

Средства правовой защиты, к которым должна прибегнуть международная гуманитарная организация

Первыми правовые последствия хостинга данных для другого субъекта публичного международного права стали исследовать правительства Эстонии и Люксембурга после открытия в Люксембурге «виртуального посольства» Эстонии в 2017 году[36]. Трактовка законодательства в этой сфере еще не до конца определена, и в этом разделе статьи поднимается несколько вопросов, не имеющих ответа, а также предлагаются рекомендации по поводу возможных уточнений в отношении привилегий и иммунитетов, которые можно попытаться получить для того, чтобы соглашения о размещении штаб-квартир полностью отражали особые потребности, связанные с хостингом данных и приложений в стратегических точках, где организация размещает основную часть своих данных и приложений.

Независимость, необходимая международной организации для полного и эффективного осуществления своего мандата, обычно обеспечивается с помощью соглашений с принимающим государством о размещении штаб-квартиры или об особом статусе. Они предусматривают ряд привилегий и иммунитетов для организации и ее сотрудников, в том числе защиту организации, ее имущества и персонала от судебных и административных разбирательств, а также неприкосновенность ее помещений, имущества, активов, переписки и архивов. Трактовка этих соглашений и их применение в цифровой среде могут потребовать уточнений.

Важно пояснить, что привилегии и иммунитеты международных организаций должны распространяться и на данные (при передаче, в хранилище и в процессе обработки), которые хранит и обрабатывает не только непосредственно сама гуманитарная организация, но и сторонние поставщики услуг или отдельные организации, в том числе при хостинге или иной обработке данных сторонними поставщиками технических решений от имени организации; кроме того, подобные привилегии и иммунитеты должны распространяться на серверы и сети, используемые организацией, независимо от того, принадлежат ли они этой организации или стороннему поставщику[37]. Как ни странно, насколько известно автору, этот чрезвычайно важный вопрос никак не освещен в научной литературе.

Среди прочих положений, которые обычно предусматриваются в соглашениях о размещении штаб-квартиры, можно отметить гарантии того, что принимающее государство позволит организации свободно пользоваться средствами связи, которые она сочтет наиболее подходящими, для официальных целей и без какого бы то ни было вмешательства. Эти

36 См.: e-Estonia, "Estonia to Open the World's First Data Embassy in Luxembourg", доступно по адресу: https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

37 Отсылку к позиции Государственного департамента США в поддержку такого применения привилегий и иммунитетов государств см.: *Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation*, 2015, p. 14, n. 12, доступно по адресу: https://tinyurl.com/3rucylfy.

гарантии распространяются на потоки данных, необходимые для наладки гуманитарных услуг в цифровом формате и создаваемые в процессе их оказания, в дополнение к прочим положениям об иммунитетах и неприкосновенности. Кроме того, эти соглашения предусматривают право организации на применение специальных технических средств защиты для практического воплощения этих положений. Среди таких мер защиты могут быть сложные алгоритмы шифрования или технологии, содержащие такие алгоритмы, а также технологии, позволяющие предотвратить перехват или создание помех для связи и потоков данных, касающихся организации.

В соглашении между принимающим государством и международной гуманитарной организацией может также потребоваться пояснение о том, что разрешение на свободное использование средств связи и их защита подразумевают, в том числе, к примеру, отказ от намеренного создания помех для доступа в интернет, от прекращения или замедления подключения к интернету для организации или ее стороннего поставщика. Однако, учитывая, что некоторые из подобных мер могут оказаться необходимыми для борьбы с DDoS-атаками и во избежание нежелательных последствий, важно также пояснить, как применяются эти гарантии в ситуации, когда организация подвергается DDoS-атаке. Гарантия беспрепятственной связи может потребовать от государства не блокировать и не сокращать входящий трафик данных организации, однако подобные меры могут потребоваться принимающему государству для защиты средств связи в случае применения DDoS-операций в отношении организации.

В тех случаях, когда организация обрабатывает данные с помощью поставщиков облачных решений, расположенных на территории принимающего государства, может быть необходимо учесть особые соображения. В частности, в дополнение к вышеперечисленным соображениям необходимо пояснить, могут ли иммунитеты, действующие в отношении персонала организации, распространяться на сотрудников сторонних поставщиков технических решений в части, касающейся выполнения ими задач для такой организации, при условии, что они обрабатывают данные организации и имеют доступ к открытым, незашифрованным данным, — и если да, то в какой мере. Эти лица могут получить доступ к конфиденциальной информации, например при оказании технической поддержки или при выполнении технического обслуживания, поэтому им необходимо предоставить некий ограниченный иммунитет в отношении этих функций. Сейчас разрабатываются определенные технические решения, которые могли бы решить этот вопрос[38]; некоторые из них, такие как гомоморфное шифрование[39], представляются перспективными. Однако их функционал, эффективность и масштабируемость еще не испытаны в полном объеме.

38 См.: Microsoft, “Confidential Computing”, доступно по адресу: www.microsoft.com/en-us/research/theme/confidential-computing/.

39 См.: Andy Greenberg, “Hacker Lexicon: What Is Homomorphic Encryption?”, *Wired*, 11 March 2014, доступно по адресу: www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/.

Кроме того, возможно, имеет смысл уделить должное внимание применению соглашений об обмене данными между принимающей страной и третьими странами, а также возможным попыткам третьих стран получить доступ к данным, хранящимся в технологических компаниях, посредством принятия законов, аналогичных акту Конгресса США, разъясняющему законное использование данных за рубежом, а также посредством иных соответствующих государственных правовых актов, имеющих экстерриториальное применение[40].

Наконец, в таких соглашениях следует учесть последствия отключения интернета для деятельности организации в цифровом пространстве и предусмотреть конкретные способы защиты от них. Например, организация должна стремиться получить конкретные гарантии того, что весь ее входящий и исходящий трафик будет защищен от блокировки. Однако этого может быть недостаточно для того, чтобы обеспечить получателям помощи доступ к гуманитарным услугам, предоставляемым с помощью цифровых средств, в случае полного отключения мобильных или телекоммуникационных сетей, запрета на получение пострадавшими сим-карт или ограничения трафика мобильных данных для пострадавших, то есть если проблема связана не с сетевым трафиком, но с доступом к самой сети. Организации потребуется разработать альтернативные стратегии в рамках своей киберстратегии, чтобы решить подобные проблемы.

В тех случаях, когда гуманитарная организация обрабатывает данные через сторонних поставщиков технических решений, например облачные сервисы, ей необходимо позаботиться о том, чтобы любые договоренности по вышеперечисленным вопросам, достигнутые между ней и принимающим государством, были также отражены в договоре с технологической компанией, чтобы она приняла на себя обязательство отстаивать их, а сотрудники компании были готовы воплотить их на практике.

Вышеописанные меры правового характера направлены преимущественно на обеспечение независимости организации. Соблюдение конфиденциальности данных организации за счет ее привилегий и иммунитетов действительно играет важную роль в том, чтобы организация могла эффективно осуществлять свой мандат — а в случае МККК еще и соблюдать Основополагающие принципы Движения. В этом смысле важно подчеркнуть, что решения, которые могут считаться хорошо защищенными и признаваться в этом качестве в отраслях, характеризующихся жестким регулированием, высокой степенью конфиденциальности данных и строгими требованиями к ее соблюдению (таких как банковская отрасль), могут, тем не менее, оказаться совершенно неподходящими для использования в деятельности МККК, поскольку такие «хорошо защищенные» решения могут

40 См.: DoJ (примечание 28 выше).

все равно предусматривать обязательство организации передавать данные государствам, юридические требования, связанные с возможностью дешифровки, и так далее[41].

Правовой защиты недостаточно: технические средства защиты, которые гуманитарная организация имеет право или может применять для защиты своих данных и потоков данных

Впрочем, одних лишь средств правовой защиты, перечисленных выше, недостаточно для того, чтобы никакие органы власти не могли законным путем получить доступ к данным международных гуманитарных организаций. В этом смысле особое беспокойство вызывают три аспекта: 1) при установлении слежки не всегда соблюдаются привилегии и иммунитеты; 2) трафик данных тоже может быть перехвачен в рамках массового/тотального сбора данных; 3) хостинг и обработка данных организации могут осуществляться через коммерческих поставщиков технических решений.

Ввиду таких проблем организации необходимо действовать на двух разных уровнях. Первый из них — правовой уровень, на котором необходимо стремиться к тому, чтобы никакая третья сторона не могла получить доступ к данным законным путем; второй — технический и организационный уровень, на котором следует принимать конкретные меры с целью обеспечить безопасность потоков данных, хостинга и обработки. Как подчеркивается выше, на данный момент для некоторых видов облачной архитектуры таких решений может не быть на рынке, поэтому может потребоваться создание партнерств в целях НИОКР с научными и иными учреждениями для разработки таких решений и последующего обеспечения их стабильной работы. С учетом затрат и имеющихся ресурсов международным гуманитарным организациям, возможно, имеет смысл объединить усилия с другими организациями, имеющими аналогичный мандат и статус, особенно на этапе доработки технических аспектов новых решений до этапа стабильного функционирования.

Операционное взаимодействие организации

Как подробно описано выше, такая организация, как МККК, стремится наладить свое присутствие и работу на основе концепции принятия, которая, в свою очередь, опирается на доверие, обусловленное нейтральностью, беспристрастностью и независимостью МККК, а также тем фактом, что он преследует исключительно гуманитарные цели и заботится о соблюдении конфиденциальности. В этом смысле способность выстроить двустороннее

41 См., например: Julia Carrie Wong, "US, UK and Australia Urge Facebook to Create Backdoor Access to Encrypted Messages", *The Guardian*, 4 October 2019, доступно по адресу: www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption.

конфиденциальное взаимодействие со всеми заинтересованными сторонами, будь то государства или негосударственные субъекты, независимо от того, могут ли они считаться легитимными объединениями, является необходимой предпосылкой к исполнению мандата.

Ниже перечислены характеристики, определяющие формат диалога, который организация — в данном случае МККК — должна вести и в киберпространстве.

Диалог с «принимающими государствами в киберпространстве»

Как уже было упомянуто выше, проработка и внедрение гуманитарных услуг в цифровом формате потребуют от организации выявления одной или нескольких ключевых юрисдикций, где можно безопасно разместить инфраструктуру для оказания таких услуг и получить все необходимое для дальнейшего масштабирования на весь мир. Такие «принимающие государства в киберпространстве», вероятнее всего, будут выбираться из числа стабильных стран, на территории которых не наблюдается активных конфликтов или иных ситуаций насилия, и, следовательно, маловероятно, чтобы гуманитарная организация проводила там какие-либо гуманитарные программы. Скорее всего, такое государство найдется среди технически продвинутых стран с развитой индустрией информационных технологий, потенциалом, научным сообществом и инфраструктурой. Одним из примеров может служить недавно перезаключенное соглашение между МККК и Швейцарской Конфедерацией[42].

Операционное взаимодействие с принимающими государствами в киберпространстве прежде всего регламентируется в самом соглашении, а также в последующих меморандумах о взаимопонимании, документах или сложившейся практике. Это взаимодействие должно строиться таким образом, чтобы охватывать как минимум нижеперечисленные аспекты.

Во-первых, взаимодействие должно касаться возможного сотрудничества в области предупреждения и обнаружения кибероперaций, а также определения их источника (это важная предпосылка к двустороннему конфиденциальному взаимодействию) и соответствующих ответных мер. Поскольку принимающее государство в киберпространстве контролирует сеть, расположенную на своей территории, и проходящие через нее потоки данных, имеющиеся ресурсы и источники знаний, а также сотрудничество с международными объединениями, в которые оно, скорее всего, входит, такое государство располагает гораздо большими средствами для предотвращения и обнаружения кибероперaций, определения их источника и принятия ответных мер, чем организация сама по себе. Определение периметра такого диалога является деликатной задачей и имеет большое значение, с одной стороны, для обеспечения эффективного взаимодействия, а с дру-

42 ICRC and Swiss Federal Council, "Accord entre le Conseil fédéral suisse et le Comité international de la Croix-Rouge en vue de déterminer le statut juridique du Comité en Suisse", 19 March 1993, доступно по адресу: www.fedlex.admin.ch/eli/cc/1993/1504_1504_1504/fr#sidebarLink.

гой — для предотвращения слишком сильной зависимости организации от сотрудничества с таким принимающим государством в киберпространстве, что создало бы риск нарушения нейтральности, беспристрастности и независимости организации.

Во-вторых, необходимо уделить должное внимание вопросу дальнейшей судьбы «киберпреступников» в тех случаях, когда выясняется, что операцию против организации провели преступные группировки, а не государство и не субъекты, действующие при поддержке государства. В какой степени организация может или должна полагаться на защиту своей деятельности со стороны правоохранительных органов принимающего государства и какого рода сотрудничество для этого необходимо? Как организациям и принимающему государству решать вопросы, связанные с трансграничным и международным характером киберпреступности, ввиду которого киберпреступники могут находиться вне юрисдикции принимающего государства, а последствия их действий могут проявляться в третьих странах, где организация осуществляет гуманитарную деятельность? В какого рода механизмах международного сотрудничества участвует принимающее государство и соответствуют ли они характеру, мандату и принципам работы организации?

В-третьих, в ходе взаимодействия следует также выяснить, как следует поступать с вредоносными кибероперациями, в качестве источника которых определяются третьи страны, в том числе субъекты, действующие при поддержке государства. Это тоже щекотливый вопрос, который, возможно, нуждается в отдельном обсуждении и согласовании между организацией и принимающим государством, поскольку он может вызвать проблемы деликатного свойства, связанные с международным публичным правом и международными отношениями. Эти проблемы могут касаться нарушения суверенитета принимающего государства, контрмер, которые оно может принять, и соблюдения обязательства проявлять должную осмотрительность в отношении третьих стран в соответствии с международным правом, чтобы способствовать прекращению вредоносной операции с одной стороны и сохранить нейтральность, беспристрастность и независимость организации — с другой.

Хотя некоторые из этих вопросов, в частности, связанные с неспособностью принимающего государства оказать помощь международной организации и с возможностью принятия контрмер, уже были тщательно проанализированы[43], остается много других вопросов. В частности, хотя вопросы, связанные с суверенитетом, контрмерами и должной осмотрительностью обсуждались в рамках различных форумов[44] и раскрыты

43 См.: "Scenario 04: A State's Failure to Assist an International Organization", цит. по: Kubo Mačák, Tomáš Minárik and Taťána Jančárková (eds), *Cyber Law Toolkit*, доступно по адресу: https://tinyurl.com/3m4nm6nv.

44 См., например: Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017, доступно по адресу: https://ccdcoe.org/research/tallinn-manual/.

в политике и/или заявлениях некоторых государств в области кибербезопасности[45], до сих пор они рассматривались скорее с точки зрения последствий операций, которые влияют на территорию пострадавшего государства, для его суверенитета, а не с точки зрения отношений между принимающим государством и международной организацией (за одним примечательным исключением, упомянутым выше). В этой сфере различные государства могут придерживаться разных и противоречащих друг другу взглядов на то, как следует трактовать эти понятия, и у некоторых из них может не быть четкой публичной позиции по поводу трактовки этой области права. Поэтому в диалоге организации с принимающим государством важно прояснять вопросы, которые могут повлиять на возможность осуществлять свою деятельность.

Иными словами, будет ли принимающее государство в киберпространстве расценивать операцию против организации, размещенной на его территории, как посягательство на свой суверенитет? Если да, то на каких условиях? Может ли в таком случае принимающее государство в киберпространстве принять какие-либо меры в отношении виновных? Если да, то какие? Если операция осуществляется с помощью инфраструктуры, расположенной на территории третьего государства, будет ли принимающее государство в киберпространстве стремиться к сотрудничеству с этим третьим государством, чтобы прекратить осуществление этой операции? Будет ли принимающее государство в киберпространстве ссылаться на обязательство этого третьего государства проявлять должную осмотрительность, чтобы прекратить осуществление этой операции? Будет ли что-либо из вышеперечисленного представлять проблему для организации в связи с тем, что вмешательство принимающего государства в киберпространстве может отрицательно повлиять на ее нейтральность, беспристрастность и независимость и даже подорвать их?

Диалог с государством/правительством, на территории которого организация намерена оказывать/предлагать услуги в цифровом формате

Для такой организации, как МККК, работающей в зонах вооруженных конфликтов и в иных ситуациях насилия, диалог с государством, в котором она намерена осуществлять свою деятельность, является непременным шагом для принятия ее действий по налаживанию оказания гуманитарных услуг в цифровом формате.

Это не голословное утверждение, особенно с учетом того, что, как указано выше, подобные услуги должны носить исключительно гуманитарный характер и предоставляться с соблюдением нейтральности, беспристрастности и независимости. В связи с этим пострадавшие ожидают,

45 См.: French Ministry of Defence, *International Law Applied to Operations in Cyberspace*, 2019, доступно по адресу: www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

что содержание любых переговоров с гуманитарной организацией и предоставленные ей данные не будут разглашаться и не будут использоваться третьими лицами для целей, не носящих гуманитарного характера. Аналогично, соответствующее государство должно согласиться с тем, что это гуманитарное цифровое пространство является защищенным, и не вмешиваться в него равно как и не мешать гуманитарным организациям принимать технические меры для его защиты[46].

Кроме того, одной из целей такого диалога должно быть обеспечение защиты входящих «потоков гуманитарных данных» организации от последствий отключения интернета и гарантия максимально возможного доступа пострадавших к сетям связи.

Диалог с нападающим государством и субъектами, действующими при его поддержке

Обеспечение безопасности киберпериметра организации с учетом технических возможностей хакеров, действующих по поручению или при поддержке государства, а в некоторых случаях и определенных групп, связанных с негосударственными вооруженными формированиями, представляет серьезную проблему. Гуманитарная организация, вероятнее всего, никогда не будет обладать достаточными ресурсами для защиты от нападения со стороны подобных противников. С точки зрения такой организации, как МККК, безопасность которой основана на принятии ее гуманитарного мандата и на уважении к нему, ее первоочередная цель будет состоять в том, чтобы обеспечить принятие защищенного гуманитарного цифрового пространства.

Как и в реальном мире, организации необходимо изучить, каким образом обеспечить защиту конфиденциальности двустороннего взаимодействия с государствами и группировками, действующими при поддержке государств или связанными с негосударственными вооруженными формированиями, обладающими большими техническими возможностями, в том числе, возможно, с группами хакеров, чтобы рассказать о своей деятельности, о своем мандате и принципах работы, чтобы вызвать уважение к своему гуманитарному цифровому пространству, чтобы предотвратить вредоносные операции и таким образом обсудить и получить «цифровой доступ». В связи с этим возникнут ключевые вопросы о том, как технически

46 См.: Group of Friends of the Protection of Civilians in Armed Conflict, statement submitted to the UN Security Council Arria-Formula Meeting on Cyber-Attacks against Critical Infrastructure, New York, 26 August 2020, доступно по адресу: www.eda.admin.ch/dam/mission-new-york/en/speeches-to-the-un/2020/20200826-new-york-POC-GoF%20PoC%20statement_E.pdf. «Доверие людей, которым служат гуманитарные организации, — это их валюта. Такое доверие является непременным условием осуществления гуманитарной деятельности. Поэтому мы, как государства-члены, должны создавать соответствующую среду, в том числе безопасную информационную инфраструктуру, которая позволит гуманитарным организациям успешно исполнять свой мандат. Резолюция о восстановлении семейных связей, принятая XXXIII Международной конференцией Красного Креста и Красного Полумесяца в 2019 году, представляет собой важный шаг в этом направлении».

организация может выстроить на практике двусторонний конфиденциальный диалог с этими субъектами, и в частности с группами хакеров, действующими при поддержке государств (и как убедиться в том, что гуманитарная организация ведет диалог именно с ними). Для того чтобы сохранить доверие всех заинтересованных сторон в международном сообществе, также важно, чтобы организация открыто сообщала о ведении такого диалога, о его причинах и целях. Как поясняется на веб-сайте МККК в разделе, посвященном тому, с кем и почему взаимодействует МККК:

> Именно те, кто носит оружие, могут убивать — и быть убиты. Они же могут помогать или мешать гуманитарной деятельности. Поэтому МККК поддерживает диалог со всеми, кто носит оружие, — представляют они государства или иные образования — в рамках своего мандата по предоставлению защиты и помощи людям, пострадавшим от войн и других ситуаций насилия[47].

Этот принцип действует и в реальном мире, и в киберпространстве.

Этот конфиденциальный диалог должен дополняться современными способами обеспечения безопасности[48], а по возможности — и еще более совершенными результатами НИОКР, созданными в партнерстве с научными кругами. Скорее всего, обеспечить в любых обстоятельствах безопасность на уровне, достаточном для противостояния субъектам, действующим при поддержке государства, будет очень сложно, но при определении уровня, который будет внедрен в итоге, необходимо руководствоваться: 1) принципом должной осмотрительности, то есть применять тот уровень безопасности, которого можно ожидать от организации, имеющей дело со строго конфиденциальными данными, учитывая стоимость технологий, конфиденциальность информации и уровень развития науки и техники; 2) стремлением повысить стоимость атаки (с точки зрения финансовых ресурсов, времени и персонала, необходимых для проведения вредоносных операций, а также последствий для репутации), которая способна навредить организации, до того уровня, на котором операция не стоит затраченных на нее ресурсов. Предполагаем, что для обеспечения надлежащей защиты необходимо сочетать эти два элемента.

Заключение

Международная гуманитарная организация, которая находится в процессе цифровой трансформации и стремится предлагать услуги в цифровом формате напрямую их получателям, сталкивается с целым рядом совершенно

47 См.: *МККК*. Диалог с силовыми структурами и вооруженными группами. Доступно по адресу: https://www.icrc.org/ru/what-we-do/building-respect-ihl/dialogue-weapon-bearers.

48 См.: ENISA, “What Is ‘State of the Art’ in IT Security?”, 7 February 2019, доступно по адресу: www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.

новых вопросов — от юридических и организационных до технических и рабочих, — связанных со сквозными и в значительной мере пересекающимися проблемами. При этом ни на один из них сейчас нельзя дать четкого и однозначного ответа.

В связи с этим любой организации, которая становится участником киберпространства, важно провести глубокий анализ вопросов, поднятых в настоящей статье, и найти ответы, подходящие для организации в зависимости от ее статуса, мандата и принципов работы. Далее на основе этих ответов необходимо сформулировать четкую стратегию кибербезопасности, которая будет определять положение организации в киберпространстве, а также ее решения по выявлению приоритетных областей для инвестиций и по распределению ее ресурсов.

В дополнение к стратегии работы в киберпространстве, разработанной на этой основе, международным гуманитарным организациям необходимо рассмотреть уникальные и конкретные технические решения, соответствующие их специфике, такие как создание «гуманитарного цифрового пространства» по модели «суверенного облака» или «цифрового посольства». Сейчас такие решения отсутствуют в коммерческом доступе — в первую очередь потому, что коммерческие решения разрабатываются в ответ на запрос большинства клиентов, которые, в отличие от международных гуманитарных организаций, не имеют привилегий и иммунитетов и контролируются как минимум одним государством в рамках его юрисдикции.

Партнерства с представителями науки и отрасли составляют важную часть этой работы, но их одних недостаточно — важно обеспечить 1) как политическую волю со стороны внешних заинтересованных лиц для гарантии защиты гуманитарного цифрового пространства, 2) так и осведомленность, знания, сосредоточенность и решимость внутренних заинтересованных лиц на деле сохранять независимость, беспристрастность и нейтральность международных гуманитарных организаций в киберпространстве. Без этого международные гуманитарные организации неизбежно будут вынуждены принимать решения, не подходящие для работы, которую они должны выполнять в рамках своего мандата.