Соединенные Штаты Америки

Правительство Соединенных Штатов Америки с удовлетворением принимает поступившее государствам-членам предложение представить свои мнения о сфере охвата, целях и структуре (элементах) новой конвенции в отношении выполнения резолюций 74/247 и 75/282 Генеральной Ассамблеи ООН. Соединенные Штаты рады сотрудничать с другими государствами-членами ООН и заинтересованными сторонами в разработке глобального документа, направленного на улучшение методов расследования и судебного преследования киберпреступлений, в соответствии с существующими правами и обязанностями и исходя из них. Соединенные Штаты подчеркивают важность поддержания открытого, инклюзивного, прозрачного и многостороннего процесса, который позволит всем государствам-членам вести добросовестные переговоры в поиске хорошо информированных, основанных на консенсусе практических решений, которые, по нашему мнению, будут способствовать повсеместному присоединению к новому глобальному документу по борьбе с киберпреступностью.

Предлагаемый срок окончания нашей работы делает наш график крайне сжатым даже в обычных обстоятельствах, но сейчас нам придется работать в условиях глобальной пандемии. Тем более важно сосредоточенно и эффективно трудиться над созданием глобального документа по борьбе с киберпреступностью. К сожалению, пока большинство стран мира ведут борьбу с пандемией COVID-19, киберпреступники извлекают выгоду из возросшей роли и востребованности цифровых технологий. Киберпреступность представляет собой прямую угрозу безопасности и благополучию общества и людей во всем мире. Мы давно сотрудничаем в создании коллективного потенциала по борьбе с этим злом и можем продолжать эту успешную работу,

внимательно рассматривая практические решения. Киберпреступность – это явная и непосредственная угроза, и тем важнее целенаправленно и взвешенно работать над созданием глобального документа по борьбе с ней.

Этот документ по борьбе с киберпреступностью должен быть направлен на расширение международного сотрудничества и создание практических средств для использования национальными правоохранительными органами в борьбе с киберпреступностью, аналогично другим документам ООН по борьбе с другими формами транснациональной преступности, включая коррупцию, незаконный оборот наркотиков, торговлю людьми и контрабанду мигрантов. Кроме того, такой документ должен наделять страны полномочиями для сбора и получения электронных доказательств, относящихся к любому виду преступлений, не только кибер-зависимых, и содействовать международному сотрудничеству в их расследованиях. Как и в случае любого другого документа ООН по борьбе с преступностью, такие средства должны включать в себя соответствующие ограничения и меры предосторожности, применяемые в контексте существующих национальных структур для решения вопросов неприкосновенности частной жизни и гражданских свобод без каких-либо нарушений прав человека. Документ по борьбе с киберпреступностью должен также учитывать растущую потребность в технической помощи и предоставлять государствам-членам возможности для получения такой помощи.

Приступая к разработке этого документа, государства-члены должны понимать, что наша работа ведется не в вакууме. Крайне важно определить, что должен охватывать этот документ, но не менее важно понимать, что не входит в его тематику. В ООН и на других межправительственных и многосторонних форумах ведется ценная работа по решению

других связанных с киберпространством вопросов, выходящих за рамки киберпреступности. Мы не должны дублировать эту работу и мешать ей, как для того, чтобы избежать конфликта обязательств, так и для того, чтобы не отклоняться от нашей цели - создания целевого практического документа по борьбе с киберпреступностью. Попытка решить все вопросы, связанные с киберпространством, в рамках этого документа, предназначенного для отправления уголовного правосудия, может превратить наши переговоры в несфокусированные и отвлеченные дискуссии, которые вряд ли помогут бороться с киберпреступностью и лишь замедлят наше продвижение к созданию полезного документа.

В частности, государства-члены не должны заниматься обсуждением широкого круга вопросов киберуправления или кибербезопасности при работе над документом, посвященном борьбе с киберпреступностью. Хотя борьба с киберпреступностью и кибербезопасность часто рассматриваются как стороны одной медали, ответственность за борьбу с киберпреступностью по сути лежит на правительстве, в то время как обеспечение кибербезопасности является прерогативой целого ряда государственных и частных организаций. Мандат Специального комитета состоит в разработке документа, предназначенного для отправления правосудия при расследовании и рассмотрении уголовных дел, который будет содействовать борьбе с киберпреступностью в международном масштабе, а для этого необходимо дать определение преступной деятельности в киберпространстве и предусмотреть наказание за такую деятельность. Специальный комитет не уполномочен диктовать глобальные нормы некриминальной деятельности в Интернете. Включение концепций киберуправления и кибербезопасности в договор о борьбе с киберпреступностью не отвечает цели создания рационального и

эффективного документа, который должен получить широкую поддержку со стороны государств-членов.

Как подтверждено в резолюции 75/282 Генеральной Ассамблеи ООН, крайне важно, чтобы переговоры о новом документе по борьбе с киберпреступностью не мешали работе существующих механизмов, включая многонациональные и региональные документы, которые уже содержат ряд средств для эффективной борьбы с киберпреступностью[1]. Лучший способ достичь консенсуса по этому новому документу и избежать обсуждения политических и вызывающих разногласия вопросов — это опираться на существующие и успешно работающие документы. Нам следует ориентироваться на достижения в реализации других договоров ООН, относящихся к уголовному правосудию, таких как UNTOC. UNTOC зарекомендовал себя как чрезвычайно полезный документ, поскольку направлен на борьбу с основными видами организованной преступности и содержит положения о международном сотрудничестве, которые могут широко применяться к любым видам тяжких преступлений, совершаемых с целью получения прибыли тремя или более лицами. Благодаря этому стороны успешно и регулярно пользуются документом UNTOC, в том числе для борьбы с такими преступлениями, при совершении которых используются программы-вымогатели, и сексуальной эксплуатацией детей.

Соединенные Штаты вновь подтверждают важность поддержания открытого, инклюзивного и прозрачного процесса, который позволит всем государствам-членам и заинтересованным сторонам вести добросовестные переговоры в поиске хорошо

[1] Резолюция 75/282, Противодействие использованию информационных и коммуникационных технологий в преступных целях. Принята Генеральной Ассамблеей 26 мая 2021 г. и доступна по адресу https://undocs.org/en/A/RES/75/282.

информированных, основанных на консенсусе практических решений, которые, по нашему мнению, будут способствовать повсеместному присоединению к новому глобальному документу по борьбе с киберпреступностью.

Криминализация основных киберпреступлений

Прежде всего, любой новый документ должен предоставлять странам полномочия для сбора и получения электронных доказательств, относящихся к любому виду преступлений. Такие полномочия необходимы для того, чтобы страны могли эффективно расследовать и преследовать в судебном порядке фактически все виды преступлений, поскольку сегодня очень немногие преступления совершаются полностью за пределами цифровой сферы. Такой документ также должен создавать возможность международного сотрудничества для обмена электронными доказательствами любого вида преступлений с учетом гибкого положения о двойной криминализации, содержащегося в UNTOC и UNCAC[2].

Кроме того, необходимым условием эффективного международного сотрудничества является наличие у государств-членов адекватного внутреннего законодательства, устанавливающего уголовную ответственность за основные киберпреступления. Чтобы не создавать убежища для киберпреступников, государства-члены должны одинаково интерпретировать основные материальные правонарушения и соответствующие процессуальные полномочия. Исследования УНП ООН показывают, что страны в целом одинаково определяют основные виды деятельности, которые должны

[2] Статья 18, пункт 9 UNTOC, статья 46, пункт 9 UNCAC. Хотя положения этих двух конвенций несколько различаются, согласно им обеим принимающие государства-участники наделяются значительной свободой действий при предоставлении помощи, особенно в отношении исправительных мер.

криминализироваться в соответствии с теми или иными законами о киберпреступности, и многие многосторонние соглашения и национальные уголовные законодательства содержат общие положения. Аналогичным образом существует международное понимание законных процессуальных полномочий для обеспечения эффективных расследований киберпреступлений. Благодаря этому у специалистов-практиков накоплен двадцатилетний опыт расследования разнообразных киберпреступлений, который демонстрирует постоянную жизнеспособность общепринятых материальных и процессуальных полномочий для расследования киберпреступлений.

Новый документ по борьбе с киберпреступностью должен содержать определения кибер-зависимых преступлений, т.е. преступлений, в которых какой-либо компьютер или данные являются объектом преступной деятельности, а также определенных видов кибер-поддерживаемых преступлений, т. е. преступлений, для осуществления которых использовался компьютер, и применяться к таким преступлениям.

К первой и основной категории преступлений, которые должны быть определены в этом новом документе, относятся такие преступления, которые не могут быть совершены без неправомерного использования компьютеров или сетевых систем и, следовательно, не существовали как преступления до появления компьютерных систем. Кибер-зависимые преступления могут совершаться в полностью цифровой сфере. Для основных видов кибер-поддерживаемых преступлений, таких как атаки типа «отказ в обслуживании» или повреждение компьютеров и данных, необходимы специальные законы о киберпреступности, поскольку в большинстве юрисдикций уголовное законодательство трактуется строго, а традиционные законы, которые оперируют знакомыми понятиями, такими как нарушение права владения или вандализм, часто неадекватны для применения

к киберпреступности. Более того, некоторые положения уголовного кодекса, применимые к преступлениям, совершаемым вне компьютерной сети, нелегко применить к действиям, совершаемым с использованием компьютеров.

С другой стороны, нужно иметь в виду, что нельзя рассматривать традиционные преступления как «киберпреступления» только потому, что они планировались или совершались с использованием компьютера. Некоторые преступные действия могут подпадать под действие общих законов несмотря на неправомерное использование компьютера для совершения преступления, поскольку в таком использовании компьютерной системы нет ничего особенного или уникального. Однако некоторые кибер-зависимые преступления должны быть включены в тематику документа по борьбе с киберпреступностью, например такие, при совершении которых использование компьютера увеличивает:

- масштаб преступления, например, приводит к тысячам жертв или хищению миллионов платежных данных;
- скорость атаки, потому что компьютер экспоненциально увеличивает возможность успешного проведения атаки;
- масштаб ущерба или телесных повреждений, нанесенных потерпевшим; или
- анонимность преступника.

Исходя из этих соображений, некоторые виды традиционных преступлений, такие как мошенничество и эксплуатация детей, также было бы разумно включить в тематику этих переговоров. Однако, чтобы не деформировать устоявшиеся концепции уголовного правосудия, государства-члены должны рационально подойти к определению круга

кибер-поддерживаемых преступлений, которые следует включить в тематику документа. Устоявшееся уголовное законодательство и средства не теряют своей применимости только лишь потому, что то или иное преступление включает в себя некий «кибер» компонент.

Глобальный документ по борьбе с киберпреступностью также должен призвать стороны принять законодательство, криминализирующее основные киберпреступления без привязки к технологиям, но предусматривающее процессуальные ограничения. Криминализация правонарушений без привязки к технологиям (т.е. криминализация *деятельности*, затрагивающей конфиденциальность, целостность и доступность компьютерных данных вместо *криминализации конкретной* используемой *формы* или *метода*, например, фишинга или программ-вымогателей) гарантирует, что материальные положения уголовного законодательства будут применимы не только к сегодняшним технологиям и преступным методам, но и к технологиям и методам будущего. В качестве иллюстрации того, насколько быстро развиваются технологии, даже в Предварительном всестороннем исследовании киберпреступности 2013 года, явно задуманном как *всеобъемлющее,* отсутствовала подробная информация о технологиях или методах, которые не использовались широко или только появлялись на момент исследования, таких как программы-вымогатели, Интернет вещей, криптовалюта, а также о быстром развитии и преобладании мобильных технологий. Ввиду этой проблемы государства-члены в Группе экспертов УНП ООН согласовали следующий вывод и рекомендацию: «Государства-члены должны позаботиться о том, чтобы их законодательные положения выдержали испытание временем в процессе будущего развития технологий, путем принятия законов с технологически нейтральными формулировками, которые

криминализируют деятельность, считающуюся незаконной, а не используемые в такой деятельности методы»[3]. Это особенно важно, поскольку мы пытаемся разработать долговечный документ, который будет адекватно применяться к технологиям завтрашнего дня и удовлетворять потребности сотрудников правоохранительных органов как сейчас, так и в будущем. Исходя из этих принципов, глобальный инструмент борьбы с киберпреступностью должен включать криминализацию

- незаконного доступа, то есть доступа к компьютеру или компьютерной системе без разрешения;
- незаконного перехвата, то есть неправомочного перехвата в реальном времени содержания сообщений или данных трафика, связанных с сообщениями;
- вмешательства в данные или системы, то есть вредоносного ПО, атак типа «отказ в обслуживании», программ-вымогателей, удаления или изменения данных;
- неправомерного использования устройств, то есть продажи или использования данных кредитных карт, паролей и личной информации, предоставляющей доступ к ресурсам;
- правонарушений, связанных с материалами сексуального насилия над детьми;
- правонарушений, связанных с мошенничеством, осуществляемым с помощью компьютера, то есть манипулирования компьютерными

[3] UNODC/CCPCJ/EG.4/2021/2, Отчет о заседании Экспертной группы по проведению комплексного исследования киберпреступности, проходившем в Вене с 6 по 8 апреля 2021 г., доступен по адресу https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf.

системами или данными в мошеннических целях, таких как фишинг, взлом деловой электронной почты и мошенничество на аукционах;

- правонарушений, связанных с нарушением авторских и аналогичных прав; а также
- положения о покушении, пособничестве и подстрекательстве и заговоре.

Более того, следует криминализовать и отмывание доходов от киберпреступности. И наконец, если в киберпреступлениях, запрещенных настоящим документом, участвуют юридические лица, в их отношении должны вводиться уголовные или гражданские и административные санкции.

Процессуальные полномочия для сбора и обмена электронными доказательствами

Помимо криминализации основных правонарушений, глобальный документ по борьбе с киберпреступностью должен предусматривать необходимость национальных юридических полномочий для хранения и сбора электронных доказательств и обмена ими в соответствии с надлежащей правовой процедурой и без нарушений прав человека и основных свобод. Некоторые государства-члены отметили, что в соответствии с их внутренним законодательством традиционные процессуальные полномочия могут быть неприменимы к нематериальным данным или не давать разрешения на достаточно быстрый сбор недолговечных электронных доказательств. Устаревшие законы, как всегда, окажутся недостаточными для решения многих задач расследования электронных преступлений, включая работу с новыми технологиями, такими как широко распространенное шифрование и услуги облачной обработки данных вычислений. Поэтому необходимы специализированные процессуальные полномочия для сбора

электронных доказательств. Эти законы следует разрабатывать с учетом применимых технических концепций, а также практических потребностей следователей по уголовным делам. В частности, эти процессуальные полномочия должны разрешать

- ускоренную консервацию сохраненных компьютерных данных;
- производственные заказы на компьютерные данные;
- поиск и изъятие сохраненных компьютерных данных;
- сбор данных компьютерного трафика в реальном времени; а также
- сбор данных контента в реальном времени в случаях серьезных преступлений.

Кроме того, новый документ должен предусматривать сотрудничество в сборе и получении электронных доказательств любого типа преступлений, а не только киберпреступлений. Почти все серьезные уголовные преступления оставляют электронные улики, будь то данные мобильного телефона, электронная переписка, данные о транзакциях или другие данные, имеющие отношение к расследованию преступлений и судебному преследованию преступников. Внутреннее законодательство государств-членов должно предусматривать наличие современной правовой базы доказательств, позволяющей использовать электронные доказательства в уголовных расследованиях и приобщать их к делу в судах, а также обмен электронными доказательствами с правоохранительными органами других стран.

Международное сотрудничество

Помимо внутреннего законодательства, эффективное международное сотрудничество в борьбе с киберпреступностью предполагает как формальное

сотрудничество на основе договоров, такое как взаимная правовая помощь, так и другие механизмы, такие как традиционное санкционированное сотрудничество полицейских органов. Новый документ по борьбе с киберпреступностью должен использовать эффективные инструменты расширения международного сотрудничества, предусмотренные существующими договорами, не создавая помех работе существующих механизмов и текущему международному сотрудничеству в глобальной борьбе с киберпреступностью. Положения документа о борьбе с киберпреступностью, касающиеся международного сотрудничества, включая взаимную правовую помощь (ВПП), экстрадицию, передачу судебного преследования, конфискацию доходов, в частности виртуальной валюты, и возвращение конфискованных активов потерпевшим, двойную криминализацию, а также сотрудничество между правоохранительными органами должны строго соответствовать положениям UNTOC и UNCAC, включая предусмотренные ими ограничительные и защитные меры, которые успешно применяются подавляющим большинством государств-членов ООН. Кроме того, положение о ВПП должно предусматривать всестороннюю помощь в получении электронных доказательств, касающихся уголовного преступления, независимо от того, было ли оно совершено с использованием компьютерной системы.

Техническая помощь и наращивание потенциала

Согласно исследованиям УНП ООН, в правоохранительных организациях более чем 75 процентов стран имеются специальные подразделения для работы с киберпреступностью, а около 15 процентов стран создали у себя специализированные агентства по борьбе с киберпреступностью. Это подчеркивает специализированный характер расследований киберпреступлений, включая необходимость специальной

подготовки. Более того, сложность киберпреступлений и электронных или цифровых элементов традиционных преступлений значительно возросла, что предъявляет дополнительные требования к обучению и содержанию штата высококвалифицированных следователей и технических экспертов.

Недостаточный внутренний потенциал является наиболее частой причиной того, что страны не могут эффективно сотрудничать на международном уровне. Для большинства стран международное сотрудничество буксует не из-за нежелания сотрудничать, а из-за ограничений либо во внутреннем законодательстве, либо в квалификации правоохранительных органов. Многие государства-члены не обладают достаточными правоохранительными ресурсами для борьбы с киберпреступностью или работы с электронными доказательствами. Например, в свете существующих национальных приоритетов некоторые государства-члены сталкиваются с проблемами в плане обучения и удержания подготовленных следователей и судебно-медицинских экспертов, а также с нехваткой компьютерного оборудования и программного обеспечения. Соответственно, существует широкий международный консенсус в отношении того, что техническая помощь и наращивание потенциала правоохранительных органов, включая следователей, прокуроров и судей, остаются наиболее приоритетными условиями эффективности международных мер борьбы с киберпреступностью. Более того, поскольку электронный след теперь оставляют после себя почти все типы преступлений, даже «неспециализированным» сотрудникам правоохранительных органов требуется определенное базовое понимание техники расследований преступной деятельности с использованием компьютеров.

Положения документа о борьбе с киберпреступностью, касающиеся технической помощи и потенциала, должны предусматривать:

- Меры государств-членов по инициированию, развитию или совершенствованию программ обучения своего персонала, ответственного за предотвращение киберпреступности и борьбу с ней.
- Готовность государств-членов в зависимости от их возможностей предоставлять друг другу всестороннюю техническую помощь в их соответствующих планах и программах по борьбе с киберпреступностью, особенно с учетом потребностей развивающихся стран и тех стран, которые могут сталкиваться с угрозами киберпреступности непропорционального масштаба.
- Создание механизмов, с помощью которых добровольные финансовые взносы государств-членов будут поддерживать исполнение положений документа по борьбе с киберпреступностью.
- Готовность государств-членов добровольно участвовать в финансировании Глобальной программы по борьбе с киберпреступностью Управления Организации Объединенных Наций по наркотикам и преступности и связанных с ней усилий по наращиванию потенциала в области уголовного правосудия.

Участие общественности, юридических лиц и организаций

Противодействие киберпреступности не может быть изолированным усилием ввиду сложности и многогранности этой проблемы. Документ по борьбе с киберпреступностью должен отражать важность активного участия в предотвращении киберпреступности отдельных лиц и групп граждан с соблюдением принципа гендерного

паритета, в частности, неправительственных и общественных организаций, академических учреждений и предприятий частного сектора. Такое участие способствует повышению осведомленности общественности об угрозах киберпреступности, обеспечению прозрачности работы государств-членов и решению существенных вопросов, связанных с неприкосновенностью частной жизни, гражданскими свободами и правами человека. Кроме того, эффективность документа зависит от вклада физических и юридических лиц, обладающих опытом в области киберпреступности. Для исполнения положений практического и эффективного документа по борьбе с киберпреступностью необходимо активное участие экспертов в этой области.

Механизмы реализации

На данном этапе слишком рано решать, нужен ли отдельный механизм для проверки того, как будут исполняться положения нового документа, и, если такой механизм нужен, какую форму он должен принять. Существуют различные успешные образцы таких механизмов. Учитывая нехватку доступных для технической помощи ресурсов, следует выбирать экономичные механизмы, чтобы максимально увеличить донорские взносы на техническую помощь. Одна из таких возможностей – это уполномочить Комиссию по предупреждению преступности и уголовному правосудию, учрежденную резолюцией 1992/1 Экономического и Социального Совета, рассматривать все вопросы, относящиеся к целям документа о борьбе с киберпреступностью. Имеется успешный прецедент такого надзора в отношении Комиссии по наркотическим средствам, которая курирует исполнение трех международных договоров о контроле за наркотиками. Как отмечено в разделе «Участие общественности, юридических лиц и организаций», необходимо учитывать активное участие общественности, юридических лиц и

организаций в реализации любых мер, предусмотренных документом. Однако обсуждение механизмов реализации следует отложить до дальнейшего определения сферы охвата данного документа.