Организация Объединенных Наций A/74/130

Генеральная Ассамблея

Distr.: General
30 July 2019
Russian
Original: English

Семьдесят четвертая сессия
Пункт 109 предварительной повестки дня*
Противодействие использованию информационно-коммуникационных технологий в преступных целях

Противодействие использованию информационно-коммуникационных технологий в преступных целях

Доклад Генерального секретаря

Резюме

Настоящий доклад подготовлен в соответствии с резолюцией 73/187 Генеральной Ассамблеи, озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях». В этой резолюции Генеральная Ассамблея просила Генерального секретаря запросить у государств-членов информацию о трудностях, с которыми они сталкиваются в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, и представить Генеральной Ассамблее доклад, подготовленный на основе этой информации, для рассмотрения на ее семьдесят четвертой сессии.

Доклад содержит информацию о мнениях государств-членов, представленных во исполнение вышеупомянутой резолюции.

* A/74/150.

V.19-08184 (R) 030919 030919

Содержание

I. Введение

1. В своей резолюции 73/187, озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях», Генеральная Ассамблея просила Генерального секретаря запросить у государств-членов информацию о трудностях, с которыми они сталкиваются в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, и представить Генеральной Ассамблее доклад, подготовленный на основе этой информации, для рассмотрения на ее семьдесят четвертой сессии.

2. В соответствии с этой просьбой в вербальных нотах CU 2019/55/DTA/OCB/CMLS и CU 2019/90/DTA/OCB/CSS от 13 февраля 2019 года и 19 марта 2019 года соответственно, подготовленных Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН), Секретариат предложил государствам-членам представить информацию о проблемах, с которыми они сталкиваются в борьбе с использованием информационно-коммуникационных технологий в преступных целях. Секретариат проинформировал государства-члены о том, что эта информация будет использоваться для подготовки доклада об осуществлении резолюции 73/187, который должен быть представлен Генеральной Ассамблее для рассмотрения на ее семьдесят четвертой сессии. Секретариат отметил, что объем национальных материалов, предоставляемых для целей настоящего доклада, не должен превышать 1 000 слов, за исключением текста любых законов или законодательных актов, которые государство-член, возможно, пожелает представить. Текст законов и/или законодательных актов, приложенный к представлению, будет размещен на информационно-справочном портале «Распространение электронных ресурсов и законов о борьбе с преступностью» (ШЕРЛОК) в качестве дополнительного источника информации.

3. В ответ на это приглашение свои мнения представили следующие государства-члены: Австралия, Австрия, Аргентина, Армения, Беларусь, Боливия (Многонациональное Государство), Ботсвана, Бразилия, Венгрия, Венесуэла (Боливарианская Республика), Гана, Германия, Грузия, Израиль, Индия, Иордания, Ирак, Иран (Исламская Республика), Ирландия, Испания, Италия, Канада, Катар, Китай, Колумбия, Корейская Народно-Демократическая Республика, Коста-Рика, Ливан, Лихтенштейн, Малайзия, Марокко, Монголия, Мьянма, Нидерланды, Никарагуа, Новая Зеландия, Норвегия, Перу, Португалия, Российская Федерация, Румыния, Сальвадор, Саудовская Аравия, Сербия, Сингапур, Сирийская Арабская Республика, Словакия, Словения, Соединенное Королевство Великобритании и Северной Ирландии, Соединенные Штаты Америки, Таджикистан, Таиланд, Турция, Филиппины, Франция, Чехия, Швейцария, Шри-Ланка, Эстония, Южная Африка и Япония.

4. Эти мнения отражены в подготовленных Секретариатом резюме, которые представлены ниже. Содержащаяся в представлениях информация охватывает проблемы как на национальном, так и на международном уровне, а также меры, принимаемые для их решения на обоих уровнях, в том числе в рамках существующих специальных механизмов. Государства-члены представили информацию о технических и технологических проблемах и поделились своим опытом решения этих проблем. Они также подчеркнули важность международного сотрудничества в рамках противодействия использованию информационно-коммуникационных технологий в преступных целях.

II. Ответы, полученные от правительств

Аргентина

5. Аргентина отметила, что к наиболее серьезным проблемам, с которыми сталкиваются государства в борьбе с использованием информационно-коммуникационных технологий в преступных целях, относятся:

a) сфера охвата международных документов. За исключением Конвенции Совета Европы о киберпреступности, другие международные соглашения по этому вопросу пока не заключены. Аргентина вносит активный вклад в деятельность Комитета Совета Европы по Конвенции о киберпреступности и рекомендует государствам, которые еще не стали участниками этой Конвенции, рассмотреть возможность присоединения к ней, с тем чтобы повысить эффективность ее осуществления и расширить круг ее участников за счет присоединения к ней стран, не являющихся членами Совета Европы. Вместе с тем, принимая во внимание глобальный характер явления киберпреступности и необходимость наличия механизмов, позволяющих принимать глобальные ответные меры, Аргентина поддерживает как процессы, осуществляемые в рамках Конвенции Совета Европы, так и обсуждения, нацеленные на проведение в рамках Организации Объединенных Наций переговоров об универсальной правовой базе по данному вопросу;

b) трудности трансграничного доступа к цифровым доказательствам. Основные трудности, с которыми пришлось столкнуться, в большинстве случаев заключаются в том, что данные, которые представляют собой доказательства, находятся в юрисдикции, отличной от той, в которой осуществляется производство по уголовному делу, и практически во всех случаях находятся в распоряжении частных компаний. До настоящего времени все предложенные решения этих проблем, такие как принятый в Соединенных Штатах Акт, разъясняющий законное использование данных за рубежом (CLOUD) (вступил в силу), и инициатива Европейского союза в отношении электронных доказательств (в процессе подготовки), не в полной мере учитывали потребности третьих стран;

c) недостаточный потенциал в плане оценки результатов обмена информацией и передовым опытом. Во многих случаях трудно оценить результаты обмена передовым опытом и информацией, предусмотренные соглашениями;

d) трудности, возникающие при обновлении нормативно-правовой базы в отношении технического прогресса. Постоянное обновление уголовно-правовой базы с точки зрения как существа, так и процедур сопряжено с многочисленными трудностями, которые носят более серьезный характер в странах с систематизированными правовыми системами;

e) низкий уровень осведомленности населения и организаций. Одним из ключевых аспектов борьбы с преступностью является профилактика. Применительно к киберпреступности профилактика напрямую связана с повышением осведомленности людей и организаций о рисках и угрозах, связанных с использованием информационно-коммуникационных технологий. Необходимо разработать национальные планы информирования, в соответствии с которыми усилия и инициативы, как частные, так и государственные, должны быть сформулированы таким образом, чтобы обеспечить согласованность и оптимизировать использование ресурсов;

f) ответственность частного сектора. Частный сектор играет важнейшую роль в связи с проблемами, которые создает киберпреступность. К сфере ответственности компаний относятся такие аспекты, как контроль и управление факторами уязвимостями данных, возникающими на платформах и в устройствах, и использование социальных сетей в преступных целях. Не ограничиваясь добровольным сотрудничеством частного сектора, необходимо про-

вести анализ потребности в правилах, подлежащих обязательному соблюдению;

g) рост рисков. Массовое использование относительно недорогих «умных» устройств, которые предоставляют доступ в интернет, не обеспечивая минимальный уровень безопасности, расширяет основания для потенциальных атак и масштаб киберпреступности. Для решения этой проблемы необходимы дополняющие друг друга меры государственной политики и стратегии корпоративной ответственности. Источником риска могут стать инициируемые государством проекты, направленные на создание механизмов дешифровки информации, полученной с устройств и/или из приложений, а также механизмов обхода компьютерной защиты. Оценки требуют и предлагаемые различными судебными органами инструменты для взлома и извлечения или мониторинга информации.

6. Аргентина выявила основные проблемы, с которыми она сталкивается в процессе расследования и судебного преследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, а именно:

a) подготовка сотрудников во всех звеньях системы уголовного правосудия;

b) необходимость обеспечить сотрудников судебных и правоохранительных органов соответствующими компьютерными и следственными средствами судебной экспертизы;

c) отсутствие предусмотренных законом определений преступных деяний либо непризнание их уголовными преступлениями;

d) процессуальные нормы, учитывающие специфику цифровых доказательств;

e) укрепление механизмов международного сотрудничества;

f) повышение готовности компаний частного сектора (поставщиков услуг интернета) к сотрудничеству.

7. Аргентина заявила также, что наиболее сложную проблему в деле обеспечения эффективного уголовного преследования представляет собой обучение навыкам борьбы с киберпреступностью и сбора цифровых доказательств. Необходимо сосредоточить усилия на углублении знаний операторов системы и, таким образом, обеспечить более эффективное применение действующих законов и международных документов. Это даст возможность обеспечить не только принятие эффективных мер в отношении этих преступлений, но и уважение основополагающих прав сторон судебного разбирательства.

8. Аргентина высоко оценивает вклад международных и региональных организаций, таких как Организация Объединенных Наций (в лице УНП ООН), Организация американских государств, Европейский союз и Совет Европы, в обмен передовой практикой и опытом. Министерство юстиции в настоящее время занимается разработкой типовых процессуальных правил для получения цифровых доказательств, которые должны стать основой для законодательства на федеральном уровне и на уровне провинций.

9. Аргентина является федеративным государством, что, в свою очередь, означает, что федеральная система правосудия сосуществует с 24 провинциальными судебными системами. Это затрудняет реагирование на сложные и международные явления, такие как киберпреступность и сбор цифровых доказательств. Весьма полезной практикой, которая была реализована, стало создание специализированных налоговых подразделений. Продолжаются усилия, направленные на обеспечение внедрения этой модели в различных юрисдикциях в пределах страны, ускорения расследований и обмена информацией.

10. Аргентина также осветила сопутствующую проблему нехватки финансовых средств для осуществления необходимых преобразований в рамках судебной системы и сил безопасности, включая последовательные усилия на уровне государственной политики.

Армения

11. Армения заявила, что соответствующие государственные органы и правительственные учреждения последовательно принимают меры по противодействию возникающим рискам, связанным с преступным использованием информационно-коммуникационных технологий, и по совершенствованию в этих целях отраслевого законодательства, в том числе посредством постоянного диалога со специализированными структурами Организации Объединенных Наций, Организацией по безопасности и сотрудничеству в Европе, Европейским союзом и Советом Европы, а также посредством укрепления сотрудничества и обмена информацией в рамках Антитеррористического центра государств — участников Содружества Независимых Государств (СНГ), Организации Договора о коллективной безопасности и Международной организации уголовной полиции (Интерпол).

12. Армения сообщила, что на период 2019–2020 годов предусмотрено создание межучрежденческой рабочей группы для разработки концепций, национальных стратегий и планов действий в сфере информации и кибербезопасности. Рабочая группа будет состоять из государственных должностных лиц и экспертов, представителей научных и исследовательских учреждений, фондов и организаций гражданского общества и частного сектора, в зависимости от обстоятельств.

13. Армения сообщила также, что были подготовлены проекты законов о внесении поправок соответственно в Уголовный кодекс и Уголовно-процессуальный кодекс, и ожидается, что они будут приняты в ближайшем будущем. Этот пакет законопроектов предусматривает внесение изменений и дополнений в статьи, касающиеся преступлений, совершенных с использованием компьютерных систем. В процессе разработки проекта Уголовно-процессуального кодекса состоялся ряд встреч с представителями полицейских экспертов Совета Европы.

14. Армения проводит периодические оценки национальных рисков, связанных с отмыванием денег и финансированием терроризма. В 2017 году была проведена последняя оценка за период 2014–2017 годов. В аналитическом обновлении Доклада о национальной оценке рисков, связанных с отмыванием денег и финансированием терроризма, за 2014 год[1] были отмечены определенные риски отмывания денег, связанные с использованием информационно-коммуникационных технологий. Было установлено, что новые продукты и механизмы перевода денежных средств (такие, как онлайновые кассовые терминалы, электронные банковские операции, мобильные банковские услуги и цифровые кошельки) все чаще используются для установления деловых связей или осуществления сложных и необычайно крупных операций.

15. Армения отметила, что продукты и услуги, связанные с использованием кассовых терминалов и электронных банковских систем, имеют недостатки с точки зрения выявления рисков, которые могут возникнуть в рамках деловых отношений. В частности, после установления деловых отношений с клиентом

[1] Национальная оценка рисков, связанных с отмыванием денег и финансированием терроризма, направлена на устранение угроз и факторов уязвимости в тех секторах, где наблюдаются значительные изменения и в отношении которых эксперты предоставили рекомендации в рамках взаимной оценки системы Армении по борьбе с отмыванием денег и финансированием терроризма со стороны Комитета экспертов по оценке мер борьбы с отмыванием денег и финансированием терроризма Совета Европы. Резюме размещено по адресу: www.cba.am/Storage/ EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pdf.

и принятия необходимых мер по начальной надлежащей проверке клиента последующая деловая активность клиента происходит в электронной среде, которая не предполагает личного контакта с соответствующими сотрудниками банка (персоналом по работе с клиентами). Такие взаимоотношения создают меньше возможностей для выявления подозрительной деятельности. Кроме того, для регистрации учетных записей цифровых кошельков, активация которых осуществляется путем ввода ряда действительных идентификационных данных банковской карты (номер, срок действия, код проверки подлинности (CVV) карты), могут использоваться данные, украденные с карт, выпущенных иностранными банками. Таким образом, злоумышленники могут получить доступ к финансовым услугам, минуя обязательные процедуры надлежащей проверки в отношении клиентов. Зарегистрированные цифровые кошельки могут впоследствии использоваться для осуществления многократных денежных переводов в целях сокрытия криминального происхождения доходов с последующим переводом остатка средств на счетах.

16. Принимая во внимание выявленные факторы и причины возникновения риска, Центр финансового мониторинга Центрального банка Армении принимает соответствующие меры для их предотвращения и сдерживания, в том числе направляет соответствующие поручения и указания конкретным финансовым учреждениям.

17. В 2018 году отдел по борьбе с преступлениями в области высоких технологий Главного управления полиции по борьбе с организованной преступностью возбудил 79 уголовных дел; 70 из них были связаны с преступлениями в области высоких технологий, а 9 дел, возбужденных на основании других статей, были тесно связаны с использованием информационно-коммуникационных технологий.

18. Согласно результатам проведенного полицией исследования, возросло количество уголовных дел, возбужденных по статье 181 (Хищение, совершенное с использованием компьютерной техники) и статье 254 (Неправомерное завладение компьютерной информацией) Уголовного кодекса Армении. Исследование показало, что жертвами деяний, предусмотренных статьей 181, становятся как физические, так и юридические лица, тогда как жертвами деяний, предусмотренных статьей 254, являются в основном пользователи социальных сетей или услуг электронной почты. Раскрытие информации о преступлениях преимущественно обусловлено тем, что они совершаются за границей или же следы преступлений скрыты в серверных системах ряда стран. Поэтому в таких случаях проведение расследования осложняют различия в законодательстве разных стран. В результате запрашиваемая информация, как правило, не доходит до направившего запрос правоохранительного органа.

19. Согласно соответствующим положениям Конвенции Совета Европы о киберпреступности, национальный контактный центр полиции принял меры по выявлению и раскрытию пользователей нерусских социальных сетей. Запросы, касающиеся операций или уголовных дел, осуществлялись через сеть круглосуточных контактных центров. Согласно сообщению Армении, специализированное подразделение[2] предоставляет профессиональную помощь и консультации по секторальным вопросам территориальным подразделениям полиции по их запросу (в устной или письменной форме). Кроме того, был организован учебный курс с участием начальников территориальных подразделений полиции, в ходе которого были подробно разъяснены характеристики компьютерных преступлений и процесс сбора доказательств.

20. Представители специализированных полицейских подразделений посещали соответствующие международные организации и принимали участие в специализированных практикумах и семинарах для изучения передовой прак-

[2] Специализированное подразделение осуществляет оперативно-розыскные мероприятия, опираясь на соответствующие законы и руководствуясь задачами, полученными в рамках процесса рассмотрения уголовных дел, а также обрабатывает заявления граждан.

тики в области борьбы с киберпреступностью[3]. В Армении соответствующие организационные механизмы были созданы в рамках операции ПРОКСИ, проходившей под эгидой Организации Договора о коллективной безопасности и направленной на борьбу с использованием информационно-коммуникационных технологий в преступных целях. Полиция проводит мероприятия, направленные на повышение осведомленности о вопросах и проблемах, связанных с информационно-коммуникационными технологиями[4].

21. Специализированное подразделение полиции осуществляет наблюдение за доменной зоной Армении и армянским сегментом популярных социальных сетей в целях выявления преступлений. Мониторинг не ограничивается только выявлением преступлений, для совершения которых необходимо виртуальное пространство (например, деятельность программ-вымогателей), но также охватывает иные киберпреступления (такие, как шантаж, вымогательство и доведение до самоубийства), для которых интернет служит лишь средством совершения преступления, но не является непосредственным инструментом.

22. Армения заявила также, что с точки зрения информационной безопасности подстрекательство к нетерпимости, насилию, ненависти, ксенофобии и экстремистским и террористическим действиям на почве идентичности, а также восхваление лиц, совершающих акты геноцида с использованием интернета, особенно в тех случаях, когда это поощряется и организуется на государственном уровне, вызывают серьезную обеспокоенность и создают риск радикализации общества и появления иностранных боевиков-террористов. В то же время Армения подчеркнула, что права человека и основные свободы, в том числе коллективные права, должны в равной степени и без каких-либо различий обеспечиваться как в интернете, так и за его пределами независимо от границ[5] и правового статуса территорий.

Австралия

23. Австралия отметила, что, по ее мнению, к числу киберпреступлений относятся преступления, целью которых являются компьютеры, а также более традиционные преступления, совершаемые с использованием компьютеров. Австралия также подчеркнула необходимость сосредоточить обсуждение на тех аспектах, по которым имеются специальные экспертные знания. Проблемы киберпреступлений сложны и постоянно изменяются. Решение этих проблем требует постоянного внимания, а также указаний и консультаций со стороны технических экспертов по киберпреступности. В данном контексте Австралия высоко оценивает деятельность Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, учрежденной резолюцией 65/230 Генеральной Ассамблеи. Австралия считает, что Группа экспертов, обладающая соответствующим мандатом Организации Объединенных Наций для обмена информацией о киберпреступности, должна оставаться основным форумом для обсуждения вопросов киберпреступности. В более широком смысле соответствующим мандатом Организации Объединенных Наций на противодействие транснациональной преступности и обороту наркотиков обладает УНП ООН. Поскольку киберпреступность является транснациональным

[3] В частности, в ходе мероприятия, совместно организованного Европейским союзом и Советом Европы, были внедрены передовые методы борьбы с киберпреступностью в рамках второго (укрепление судебной реформы) и третьего (поддержка мер, направленных против серьезных форм киберпреступности) проектов Фонда Восточного партнерства. Кроме того, обсуждался проект уголовно-процессуального кодекса, перспективы реформы законодательства и правовые основания для сотрудничества с частным сектором.

[4] Эти мероприятия включали интервью различным средствам массовой информации, участие в пресс-конференциях, выпуск широкого круга материалов для информирования общественности и участие в телевизионных программах.

[5] Как установлено и подразумевается положениями статьи 19 Международного пакта о гражданских и политических правах.

преступлением, целесообразно продолжать проведение дискуссий по вопросам борьбы с киберпреступностью в Вене под эгидой УНП ООН. Австралия ожидает доклада Группы экспертов в 2021 году, в том числе ее выводов и рекомендаций в отношении национального законодательства, наилучших видов практики, технической помощи и международного сотрудничества.

24. В отношении данных, расположенных в офшорных зонах, Австралия, как и все государства-члены, сообщила, что ее национальные правоохранительные органы сталкиваются с трудностями при получении доступа к данным и непосредственно самих данных для эффективного проведения расследования и судебного преследования киберпреступлений. Ранее в большинстве случаев данные хранились внутри страны, и доступ к ним можно было получить в рамках внутренних следственных полномочий. В настоящее время в связи с распространением глобального сетевого взаимодействия и опорой на облачные вычисления данные распределяются между различными службами, поставщиками, районами и юрисдикциями. Местоположение данных может быть сложно обнаружить, а получить их можно только в результате сложного и медленного процесса международного правового сотрудничества. Расширение масштабов использования услуг связи на основе технологии over-the-top означает, что традиционные правомочия на доступ к сообщениям, хранимым операторами связи и поставщиками услуг доступа к связи, не охватывают всю совокупность данных, необходимых для расследования киберпреступлений.

25. Австралия подчеркнула, что договорные решения, такие как Конвенция Совета Европы о киберпреступности, обеспечивают основу для получения правоохранительными органами разрешения на доступ к данным, находящимся в другом государстве, например, при получении согласия лица, обладающего законными основаниями для разглашения данных, или в тех случаях, когда информация является общедоступной. Ограничения, которые выходят за рамки этих обстоятельств, в том числе требующие согласия государственных органов, создают значительные проблемы для проведения расследования и уголовного преследования киберпреступлений.

26. Традиционным международным механизмам правового сотрудничества, таким как оказание взаимной правовой помощи, непросто удовлетворить спрос, что приводит к задержкам в расследовании киберпреступлений. Целесообразные и оперативные решения могут обеспечить альтернативные варианты международного сотрудничества между компетентными органами государств, правоохранительными органами и, в случае необходимости и в соответствии с внутренним законодательством, поставщиками услуг связи.

27. Австралия сообщила об успешном использовании многосторонних договоров, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Совета Европы о киберпреступности, в качестве основы для международного правового сотрудничества в дополнение к своим двусторонним и внутренним договоренностям. Новые механизмы, подобные предусматриваемым в дополнительном протоколе о трансграничном доступе к данным к Конвенции Совета Европы о киберпреступности (по которому сейчас идут переговоры), отвечают изменяющейся природе киберпреступности и существенно нарастят потенциал правоохранительных органов в части доступа к данным для расследования киберпреступлений. Обеспечивая более эффективный доступ к данным, можно достичь необходимого баланса между потребностями правоохранительных органов и целями защиты данных.

28. Что касается гарантий и полицейских полномочий, то Австралия отметила необходимость надлежащих механизмов надзора для обеспечения баланса между защитой прав человека и основных свобод и законной потребностью правоохранительных структур осуществлять свои следственные полномочия в целях борьбы с киберпреступностью. В Австралии за полномочиями правоохранительных органов ведется тщательный надзор; это, в частности, касается

осуществления более интрузивных полномочий, таких как доступ к хранимому коммуникационному контенту и перехват в режиме реального времени. К этим гарантиям относятся также требования к судебным органам по осуществлению их полномочий, требования относительно отчетности перед парламентом, право обвиняемых на оспаривание допустимости доказательств и право на обжалование, а также надзор за всеми ордерами, касающимися телекоммуникаций, со стороны Уполномоченного по правам человека Австралийского Союза. Обеспечение соответствующего баланса между полномочиями полиции и гарантиями требует постоянной оценки и непрерывного обзора, что может оказаться затруднительным в некоторых юрисдикциях.

29. Касаясь вопроса об адаптивности правовых и оперативных рамок, Австралия подчеркнула свою приверженность поддержанию адаптивности национальной законодательной базы, идущей в ногу с быстрыми темпами технического прогресса и изменениями поведения. Австралия признает сложность разработки законов, которые охватывали бы основные киберпреступления, процессуальные полномочия для расследования киберпреступлений и допустимость электронных доказательств, но в то же время оставались применимыми к изменяющимся технологиям и моделям поведения. Для решения этой задачи Австралия, как внутри страны, так и в рамках своих усилий по укреплению потенциала, содействует принятию технологически нейтрального законодательства, учитывающего будущие технологии и модели поведения в области киберпреступности.

30. Австралия сообщила, что ее нормативно-правовая база разработана по образцу Конвенции Совета Европы о киберпреступности, которая является ведущим международным документом по киберпреступности и обеспечивает прочную правовую и оперативную основу для международного сотрудничества в борьбе с киберпреступностью. Конвенция насчитывает 63 участника, и более половины из них не являются членами Европейского союза. Австралия сообщила, что, как показывает ее опыт, Конвенция является современной, прогрессивной и намеренно технологически нейтральной, благодаря чему она развивается и сохраняет актуальность при появлении новых технологий. Она также служит основой для разработки национальных законодательных подходов в различных регионах мира, в том числе в странах, которые в настоящее время не являются участниками Конвенции.

31. Австралия также считает, что в дополнение к всеобъемлющей рамочной основе для криминализации киберпреступлений необходимо наладить постоянную и непрерывную профессиональную подготовку оперативных сотрудников правоохранительных органов. Подготовка должна касаться преступлений, совершаемых с использованием технологий, а также сбора и использования цифровых доказательств. Австралия считает важным обеспечить и поддерживать обновленную устойчивую систему подготовки сотрудников австралийских правоохранительных органов, а также международных партнеров в рамках программ наращивания потенциала.

32. Борьба с киберпреступностью по своей природе требует тесного сотрудничества с другими государствами. Австралия столкнулась с проблемой, когда государства, с которыми она должна была сотрудничать по вопросам киберпреступности, обладают ограниченным потенциалом или не имеют всеобъемлющих внутренних правовых рамок для борьбы с киберпреступностью. Для решения этой проблемы необходимо, чтобы государства сосредоточили свое внимание на укреплении и наращивании потенциала для борьбы с киберпреступностью, в том числе посредством специальной подготовки по борьбе с киберпреступностью. Австралия подчеркнула, что важное значение имеет также оказание развивающимся странам помощи в проведении законодательной реформы. В целях содействия укреплению технического потенциала государств Австралия оказывает им помощь в наращивании потенциала и техническую помощь. Австралия также поддерживает ценную работу, которая проводится в рамках Глобальной программы УНП ООН по киберпреступности.

Австрия

33. Сообщая о глобальных проблемах в области борьбы с киберпреступностью, Австрия заявила, что киберпреступность представляет собой эволюционирующую проблему, которая затрагивает все страны, что требует эффективного и действенного подхода в целях:

a) максимального увеличения числа стран, располагающих адекватным, совместимым внутренним законодательством, направленным на борьбу с киберпреступностью, которое также поддерживает международное сотрудничество;

b) создания механизмов сотрудничества, укрепления доверия и развития навыков в целях обмена данными для проведения расследований, судебного преследования и сокращения масштабов киберпреступности.

К ним относится, в частности, обеспечение отсутствия у киберпреступников возможности укрыться где бы то ни было и повышение квалификации сотрудников правоохранительных и судебных органов в целях эффективного расследования, уголовного преследования и осуждения киберпреступников.

34. В целях принятия во всех странах Европейского союза всеобъемлющего законодательства, касающегося киберпространства, государства — члены Европейского союза, в том числе Австрия, согласовали ряд документов, содержащих общие определения для уголовных преступлений: директива о нападениях на информационные системы, директива о борьбе с сексуальным насилием и сексуальной эксплуатацией детей и детской порнографией и Рамочное решение от 28 мая 2001 года о борьбе с мошенничеством и подделкой безналичных платежных средств[6]. Кроме того, 17 апреля 2018 года Европейская комиссия представила законодательные предложения по улучшению трансграничного доступа к электронным доказательствам в рамках проведения уголовных расследований.

35. Тем не менее доступ к электронным доказательствам можно рассматривать только как первый шаг, поскольку на европейском уровне отсутствуют общие системы хранения данных, которые обеспечивали бы доступность электронных доказательств. В связи с этим сроки предоставления электронных доказательств и их объем в различных государствах — членах Европейского союза весьма значительно различаются и могут даже зависеть от доброй воли организаций. В этом смысле остается актуальной проблемная ситуация со службой WHOIS, приемлемого разрешения которой до сих пор не найдено. Вопрос необходимости улучшения доступа к электронным доказательствам будет решаться в рамках второго протокола к Конвенции Совета Европы о киберпреступности.

36. Австрия отметила, что в 2013 году Агентство Европейского союза по сотрудничеству в правоохранительной области (Европол) создало Европейский центр по борьбе с киберпреступностью (EC3), который внес значительный вклад в усилия государств — членов Европейского союза по борьбе с киберпреступностью, используя гибкую модель борьбы с преступностью. Австрия заявила о необходимости как можно раньше привлекать работников прокуратуры к рассмотрению дел, связанных с киберпреступностью, и сочла целесообразным создание специализированных сетей, таких как Европейская судебная сеть по борьбе с киберпреступностью.

37. В связи с вариантами ужесточения существующих ответных мер и выработкой предложений в отношении новых национальных и международных пра-

[6] Это Рамочное решение утратило силу; 29 мая 2019 года оно было заменено Директивой (ЕС) 2019/713 Европейского парламента и Совета от 17 апреля 2019 года о борьбе с мошенничеством и подделкой безналичных платежных средств (*Official Journal of the European Union*, L 123, 10 May 2019), pp. 18–29.

вовых или иных мер по противодействию киберпреступности Австрия отметила, что киберпреступления представляют собой глобальную проблему и каждая страна нуждается в помощи других стран для борьбы с ней. Австрия считает, что Конвенция Совета Европы о киберпреступности представляет собой образец для национальных законодательных актов и ценную основу для международного сотрудничества, а также придерживается мнения, что она служит гибким инструментом даже для тех ее участников, которые не являются членами Совета Европы. Поэтому Австрия не поддерживает призывы к разработке нового международного документа о борьбе с киберпреступностью.

38. Австрия заявила, что Группа экспертов для проведения всестороннего исследования проблемы киберпреступности является и должна оставаться основным местом решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций, по крайней мере до 2021 года. Работа Группы экспертов принесла плоды, в том числе в отношении законодательных реформ на основе существующих международных стандартов и, в частности, в плане укрепления потенциала. Следует обновить проект всеобъемлющего исследования по киберпреступности, представленный в 2013 году, для чего потребуется профессиональный опыт Группы экспертов.

39. Австрия предложила УНП ООН и государствам-членам обеспечить достижение этих целей, а государствам-членам — оказать УНП ООН поддержку, с тем чтобы оно уделяло приоритетное внимание следующим конкретным областям, в которых оно могло бы оказать реальное воздействие на угрозу киберпреступности:

a) повышение квалификации сотрудников полиции и правоохранительных органов посредством как общей, так и специальной подготовки;

b) оказание технической помощи развивающимся странам;

c) проведение анализа пробелов в международном сотрудничестве для выявления приоритетных областей;

d) поддержка информационно-просветительских кампаний, направленных на совершенствование работы в области предупреждения преступности и налаживание сотрудничества гражданского общества и бизнеса с правоохранительными органами;

e) укрепление существующих оперативных механизмов, таких как Сеть 24/7;

f) сбор данных об угрозах киберпреступности;

g) выполнение функций центра по обобщению передового опыта и практических примеров борьбы с киберпреступностью.

Беларусь

40. Принимая во внимание модернизацию современной наркопреступности и использование даркнета и криптовалют в целях незаконного оборота наркотиков, Беларусь считает, что одним из приоритетных направлений деятельности государств-членов должна стать организация обмена информацией, касающейся средств совершения преступлений и методов обнаружения преступной деятельности в даркнете, на наднациональном уровне; подборка и изъятие электронных доказательств; а также разработка и использование конкретных методов расследования преступлений, совершенных в виртуальном пространстве. Одним из способов противодействия использованию информационно-коммуникационных технологий в преступных целях может стать разъяснение сотрудникам правоохранительных органов принципов работы даркнета и индустрии криптовалют. Беларусь подчеркнула важность разработки международно-правового механизма (рекомендаций) о порядке изъятия криминальных криптоактивов и их хранения до принятия решения судом.

41. Беларусь отметила, что 18 марта 2019 года была принята Концепция информационной безопасности. В ней перечисляются стратегические задачи и приоритеты в сфере информационной безопасности и борьбы с киберпреступностью. В основу Концепции положены геополитические интересы Беларуси и международные соглашения о сотрудничестве в области обеспечения международной информационной безопасности с учетом основных положений резолюций Генеральной Ассамблеи, а также рекомендаций Организации по безопасности и сотрудничеству в Европе.

42. По мнению Беларуси, разработка и принятие универсального международного документа в рамках Организации Объединенных Наций будет содействовать развитию сотрудничества между компетентными органами государств-членов в борьбе с использованием информационно-коммуникационных технологий в преступных целях.

Боливия (Многонациональное Государство)

43. Многонациональное Государство Боливия отметило, что технический прогресс влияет на все аспекты человеческой деятельности в стране и во всем мире, а также на безопасность, связанную с использованием новых технологий. Развитие информационно-коммуникационных технологий сделало возможным видоизменение и распространение традиционных преступлений за счет использования программного обеспечения, приложений и сетей связи. Зависимость финансовых учреждений от цифровых систем облегчает совершение таких преступлений, как мошенничество. Аналогичным образом, легкий доступ к сотовым телефонам без необходимости предоставления персональных данных позволяет сохранить анонимность при совершении преступлений.

44. Основными приоритетами деятельности полиции Многонационального Государства Боливия являются предупреждение преступности и обеспечение безопасности связи. В рамках Специальных сил по борьбе с преступностью был создан отдел по борьбе с киберпреступностью — специализированное подразделение для выявления преступлений, совершенных с использованием информационно-коммуникационных технологий. В рамках национального правоохранительного ведомства действуют специализированные подразделения по мониторингу прессы и социальных сетей. Мониторинг социальных сетей направлен на предотвращение «информационных пузырей» (ограничение информации в целях негативного влияния на общественное мнение), а также предотвращение вымогательства, угроз, незаконного оборота наркотиков, торговли людьми, мошенничества, кибертравли, дискриминации и других преступлений, угрожающих безопасности государства.

45. Многонациональное Государство Боливия сообщило, что дети, в частности молодые люди в возрасте от 12 до 18 лет, подвержены рискам, связанным с использованием информационно-коммуникационных технологий в преступных целях, поскольку они подвергаются воздействию этих новых технологий с раннего возраста и регулярно используют их для развлечения, общения и получения информации. Однако эти технологии не всегда приносят детям пользу с педагогической или образовательной точки зрения.

46. Многонациональное Государство Боливия представило следующий неисчерпывающий перечень видов неправомерного использования информационно-коммуникационных технологий и компьютерных преступлений.

а) Преследование, оскорбления, клевета и социальная изоляция с использованием социальных сетей, электронных сообщений и даже комментариев в разделах газет для выражения личных мнений. В безобидных, на первый взгляд, условиях, скажем в школах, организуются анонимные кампании против определенных детей с использованием, например, сети Facebook; студенты университетов подвергаются клевете, например обвинениям в проституции; а

также предпринимаются попытки дискредитировать компании на основе ложной информации.

b) Мошенничество и обман, например фишинг, с помощью которого преступные организации получают конфиденциальную информацию, которая позволяет им получать доступ к банковским счетам и опустошать их. Еще одним примером является использование интернет-ресурсов для трудоустройства в качестве прикрытия для сетей, вовлеченных в торговлю людьми и детскую порнографию. В целом мошенничество связано с получением доступа к конфиденциальной информации, а также с возможностью ее изменения.

c) Спам. Не обязательно представляя собой нарушение закона, спам является результатом ненадлежащего использования в коммерческих целях баз данных, которые многие компании используют для охвата потенциальных пользователей своими маркетинговыми кампаниями. Он может содержать рекламу проституции и пропаганду иной незаконной деятельности.

d) Преступные группы используют интернет для продажи материалов, связанных с сексуальными надругательствами над детьми, в форме фотографий и видеозаписей. Это является нарушением Конвенции о правах ребенка и Уголовного кодекса.

e) Интеллектуальная собственность. Права людей и ведущих инновационную деятельность организаций нарушаются различными способами, в том числе путем фотографирования охраняемых текстов (авторское право).

f) Продажи через интернет, в том числе предполагаемыми посредниками — устроителями лотерей и конкурсов.

47. Многонациональное Государство Боливия заявило, что наряду с развитием компьютерных технологий преступники находят инновационные пути для совершения мошенничества и других преступлений быстрее, чем могут реагировать уголовные кодексы. Поскольку мы имеем дело с явлением, масштабы которого возрастают, необходимость профилактики и защиты следует считать обязанностью каждого: государства, компаний, организаций и граждан. В этом смысле технологические новшества ставят перед организациями, отвечающими за их решение, целый ряд сложных проблем, включая:

a) недостаточный уровень осведомленности и информированности общественности относительно использования информационно-коммуникационных технологий. Такое отсутствие знаний делает людей более уязвимыми в отношении различных преступлений. Связанная с этим задача заключается в разработке соответствующих мер политики для повышения осведомленности о надлежащем использовании этих технологий;

b) правовой вакуум вследствие неведения или неприменимости действующего законодательства к новым преступлениям, связанным с информационно-коммуникационными технологиями. Соответственно, необходимо пересмотреть и обновить законодательство;

c) необходимость изменения традиционных стратегий проведения расследований и мер по борьбе с преступностью путем использования новых методов, учитывающих изменение характера преступлений, связанных с информационно-коммуникационными технологиями;

d) необходимость участия в международных соглашениях о сотрудничестве в области научных исследований, обеспечения и получения доказательств в области борьбы с киберпреступностью. Ряд стран Латинской Америки уже являются участниками конвенций и добились более заметного прогресса в развитии своего технического потенциала в области предупреждения и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий.

48. Многонациональное Государство Боливия напомнило, что внедрение новых технологий в государственных учреждениях оказало влияние на организационную культуру путем изменения процедур и включения новых ассимилированных знаний. Многие технологии, разработанные и внедренные в органах безопасности, требуют специальных знаний, что может приводить к предоставлению доступа в эти учреждения лицам или организациям, которые не всегда имеют отношение к сфере безопасности, таким как университеты, технические институты, научно-исследовательские центры и поставщики программного обеспечения. В настоящее время как сотрудники полиции, так и граждане располагают различными технологическими инструментами для решения проблем безопасности и рассмотрения преступных деяний, которые в одних случаях связаны с предупреждением преступлений, а в других — с оказанием помощи при расследовании уголовных дел. Некоторые из этих элементов получили весьма широкое распространение как среди граждан, так и среди сотрудников полиции, в то время как другие являются более дорогостоящими и доступ широкой общественности к ним затруднен.

49. Многонациональное Государство Боливия пришло к выводу, что технические достижения сделали возможным появление новых движущих сил преступности, что заставляет учреждения адаптироваться и внедрять новаторские стратегии, позволяющие им оставаться на шаг впереди лиц, занимающихся преступной деятельностью, защищая общество и сохраняя общественный порядок путем предотвращения и расследования преступлений. Следовательно, невозможно представить, чтобы учреждения, отвечающие за безопасность, рассматривали возможность столкновения с преступным явлением без использования технологических инструментов. Учреждения, отвечающие за безопасность, могут использовать технологические инструменты не только для внутренних целей, но и для привлечения граждан к предупреждению преступности.

Ботсвана

50. Ботсвана отметила следующие проблемы в борьбе с преступностью, в частности с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий:

a) несогласованность законодательства о киберпреступности и защите данных в различных странах и юрисдикциях серьезно затрудняет расследование преступной деятельности в киберпространстве;

b) очевидно, что отсутствие международной рамочной основы для обмена информацией, касающейся кибербезопасности, между различными органами в различных странах создает проблемы для защиты сетей и расследования преступной деятельности, имеющей место в нескольких юрисдикциях;

c) появление таких технологических новшеств, как искусственный интеллект и интернет вещей, которые могут применяться, в числе прочего, в сельском хозяйстве, медицине и анализе климатических данных, однако также потенциально способны служить платформой, с которой или при помощи которой могут осуществляться кибератаки;

d) еще одним препятствием или серьезной проблемой является наращивание потенциала различных субъектов (правоохранительных ведомств, поставщиков услуг, директивных и регуляторных органов) в области решения проблем кибербезопасности;

e) проблемы, связанные с международными компаниями, которые предлагают услуги на рынке страны без соответствующей лицензии, такими как Facebook, WhatsApp, Google, Microsoft и Netflix. Процесс получения сведений или доказательств, касающихся преступлений, совершенных в рамках этих сетей, затруднен;

f) Ботсвана, как и многие другие страны, не является участником существующих конвенций по вопросам информационно-коммуникационных технологий и кибербезопасности (например, Конвенции Африканского союза о кибербезопасности и защите персональных данных и Конвенции Совета Европы о киберпреступности), что затрудняет поиск возможностей для их использования. Конвенция Совета Европы о киберпреступности обеспечивает правовую основу для международного сотрудничества по вопросам киберпреступности и электронных доказательств, и следует поощрять страны присоединяться к ней;

g) для процесса взаимной правовой помощи характерны медлительность и громоздкость, что делает его неэффективным с точки зрения правосудия Ботсваны и других стран;

h) добровольное раскрытие информации о киберпреступности попрежнему является препятствием во многих юрисдикциях. Процесс получения информации является длительным и в некоторых случаях невозможным; отчасти причина заключается в том, что правила получения доступа к сведениям об абонентах не согласованы между государствами. То, что Ботсвана может расценивать в качестве преступления или считать таковым, в другом государстве может им не являться.

51. Ботсвана вынесла следующие рекомендации:

a) налицо необходимость в сотрудничестве и взаимодействии между такими организациями, как УНП ООН, Международный союз электросвязи и Интерпол, для осуществления совместной работы в целях решения проблем, связанных с использованием преступниками сетей информационно-коммуникационных технологий для совершения преступлений. Роли различных учреждений в решении проблем кибербезопасности нуждаются в уточнении;

b) следует разработать международные рамки для обмена информацией о кибербезопасности между государствами — членами Организации Объединенных Наций;

c) необходимо разработать международную политику и нормативно-правовую базу для надлежащего использования новых технологий, в том числе искусственного интеллекта и интернета вещей;

d) следует разработать программы укрепления потенциала государств-членов;

e) следует разработать механизм предоставления международными корпорациями информации и доказательств государствам-членам, а также оказания корпорациями помощи в расследовании преступлений, совершенных в принадлежащих им сетях;

f) следует рекомендовать Организации Объединенных Наций изучить причины, по которым страны, как представляется, пассивно относятся к ратификации региональных конвенций по вопросам информационно-коммуникационных технологий и кибербезопасности;

g) необходимо принять стандарт упрощенной системы взаимной правовой помощи, который будет принят государствами-членами;

h) наконец, существует необходимость разработки международного договора для решения проблем, связанных с преступностью в сети информационно-коммуникационных технологий. Задачей такого договора является согласование и обеспечение краткого руководства в отношении применимого ко всем случаям законодательства, принципов обмена информацией, минимальных стандартов информационной безопасности и помощи в правоохранительной сфере (расследование преступлений, выдача преступников и уголовное преследование).

Бразилия

52. Бразилия сообщила, что ее власти занимаются борьбой с киберпреступностью с момента появления интернета и что эти преступления становятся все более многочисленными и изощренными. Перенос различных преступлений на цифровые платформы потребовал значительных усилий по обновлению соответствующих законодательных и судебных мер реагирования на новые угрозы. Географическая распространенность этих преступлений также бросила вызов традиционным механизмам, с помощью которых Бразилия предоставляет и получает помощь в рамках международного правового сотрудничества. Проблемы колоссальны: поставщики услуг интернета, обладающие информацией, необходимой для расследования киберпреступлений и сбора электронных доказательств, нередко имеют фактическую штаб-квартиру в одной стране, услуги предоставляют на различных континентах, а информацию хранят на серверах в каком-либо еще месте планеты. В таком случае сотрудники правоохранительных органов стремятся выявить и надлежащим образом обратиться к тем, кто обладает юрисдикцией в отношении необходимых данных и имеет прямой доступ к ним. Запросы, касающиеся международного сотрудничества, которые обычно направляются в рамках договоров о взаимной правовой помощи, обрабатываются очень медленно и иногда, учитывая темпы удаления цифровых данных, оказываются неприменимыми.

53. Бразилия сообщила также о том, что при наличии международного компонента в расследованиях и юрисдикции юридическое развитие дела часто замедлялось вследствие расхождений в представлениях о защите неприкосновенности частной жизни, что отражалось в различных национальных требованиях в отношении раскрытия данных. Еще одной проблемой международного сотрудничества в правовой сфере является крайняя нестабильность цифровых доказательств, поскольку огромный объем информации, циркулирующей в мире, и расходы, связанные с хранением данных, вынуждают компании хранить данные не дольше, чем это строго необходимо для их бизнеса.

54. Сотрудники правоохранительных органов Бразилии осуществляют уголовное преследование по делам о многочисленных преступлениях в цифровой среде, среди которых наиболее часто встречается детская порнография. Бразилия вовлечена в решение этой проблемы в максимальной степени, как через Интерпол, так и напрямую (например, из Соединенных Штатов было получено два миллиона сообщений о правонарушениях). К числу постоянно повторяющихся преступлений относятся также вторжение на веб-сайты и фишинг. Оба эти типа преступлений создают условия для банковского мошенничества, которому противодействует, принимая скоординированные упреждающие меры, бразильский финансовый сектор. К тенденциям последнего времени относятся кража биткоинов и криптоджекинг (как, например, в 2017 году с использованием вируса WannaCry), которые к тому же затрудняют классификацию преступлений.

55. Бразилия учитывает особый характер электронных доказательств и киберпреступности. Статья 11 Основ законодательства о защите гражданских прав в интернете предусматривает, что бразильское законодательство должно применяться при сборе, хранении и обработке данных в тех случаях, когда один из компьютерных терминалов расположен на территории Бразилии. В связи с этим иностранные компании, которые имеют филиалы в Бразилии или предоставляют услуги бразильским пользователям и осуществляют сбор, хранение, актуализацию или обработку данных, полученных от пользователей, должны соблюдать законодательство Бразилии. Эта система позволяет властям иметь прямой доступ к электронным доказательствам и данным, полученным в рамках оказания услуг в стране. Бразильская юрисдикция основывается на понятии услуги, предлагаемой или оказываемой на ее национальной территории.

56. Бразилия высказала мнение, что, хотя интернет представляет собой виртуальное пространство без границ, его точка сопряжения с материальным миром находится на существующей и делимитированной территории государства. Шагом вперед в расследовании киберпреступлений является взаимоувязанное международное разграничение юрисдикции. В 2014 году в законодательство Бразилии был включен целевой тест (аналогичный инициативе Европейского союза в области электронных доказательств[7]). Еще до начала переговоров по заключению глобального договора по этому вопросу Бразилия предвосхитила будущую унификацию внутреннего законодательства, использовав правовой механизм целевого теста, который не принимает во внимание местонахождение серверов и национальную принадлежность компании, ответственной за хранение данных.

57. Бразилия заявила о необходимости более широкого и эффективного сотрудничества либо путем разработки усовершенствованной модели осуществления действующих договоров о взаимной правовой помощи, либо на основе дополнительных договоров о киберпреступности, которые будут способствовать активизации международного обмена изначально эфемерными цифровыми доказательствами. Характерное для киберпреступности многообразие платформ, систем и стратегий также требует расширения технического сотрудничества. Соответствующие эксперты, сотрудники полиции, прокуроры и судьи должны иметь больше возможностей для ознакомления с опытом и методами, которые доказали свою эффективность в ходе их использования зарубежными партнерами.

58. Бразилия также заявила о том, что проведение многосторонних переговоров относительно международного документа под эгидой Организации Объединенных Наций может стать способом установления общих минимальных стандартов в отношении обмена информацией и доказательствами для борьбы с киберпреступностью с опорой на уже существующие международные и региональные документы. Такое обсуждение следует организовать в Вене при поддержке УНП ООН, поскольку там уже накоплен опыт борьбы с киберпреступностью, а Группа экспертов для проведения всестороннего исследования проблемы киберпреступности уже обсуждает этот вопрос. Первым шагом на пути создания конвенции о киберпреступности мог бы стать созыв группы экспертов открытого состава для начала разработки проекта документа.

Канада

59. Канада сообщила, что, хотя ее законодательство было недавно обновлено в целях повышения эффективности борьбы с преступностью в XXI веке, проблемы остаются. Канада особо отметила два направления, в рамках которых международное сообщество уже работает над устранением основных причин возникновения этих проблем.

60. Во-первых, с точки зрения осуществления процесса, Канада подчеркнула значимость работы Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Группе поручено провести всестороннее исследование проблемы киберпреступности и действий по ее преодолению в целях изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности. Эта работа продолжается в соответствии с планом, согласно которому Группа должна завершить свою работу в 2021 году. Канада считает работу Группы, которая обеспечивает площадку для обмена экспертными мнениями в рамках обсуждения узкоспеци-

[7] Рамочное решение 2008/978/ПВА Совета Европейского союза от 18 декабря 2008 года о европейском ордере на получение доказательств в целях получения предметов, документов и информации для использования в ходе производства по уголовным делам (*Official Journal of the European Un*ion, L 350, 30 December 2008).

альной темы киберпреступности, включая ее аспекты в области международного сотрудничества и создания потенциала, крайне важной для проведения дальнейших дискуссий в рамках Организации Объединенных Наций в отношении возможных мер по противодействию киберпреступности.

61. Во-вторых, с точки зрения существа, Канада полностью поддерживает Конвенцию Совета Европы о киберпреступности как наиболее эффективный международный инструмент для борьбы с киберпреступностью. Конвенция эффективно решает проблемы, связанные с глобальным характером использования информационно-коммуникационных технологий в преступных целях, обеспечивая международное сотрудничество в борьбе с киберпреступностью при участии ее сторон (в настоящее время их 63, включая значительное и растущее число неевропейских государств). При возникновении новых проблем имеется возможность адаптации Конвенции к ним за счет выпуска руководящих указаний, призванных содействовать сторонам в применении существующих положений к новым явлениям в области киберпреступности, что дополняется работой Сети 24/7 и эффективными программами наращивания потенциала. Стороны Конвенции также работают над совершенствованием механизмов международного сотрудничества, поскольку уголовные расследования все чаще требуют доступа к информации, хранящейся в других юрисдикциях. Канада поддерживает Конвенцию и твердо уверена в том, что она является наилучшим имеющимся вариантом как в качестве юридически обязывающей основы для стран, желающих и способных стать ее участниками, так и в качестве модели для разработки внутреннего законодательства в тех странах, которые к ней не присоединились.

62. Что касается проблем, порождаемых новыми технологическими достижениями, то Канада напомнила о повсеместной распространенности связи: она обеспечивается везде, в любое время, любым поставщиком услуг или посредством любого устройства. Это влияет на деятельность правоохранительных органов. Следователям часто приходится учитывать особенности соглашений о партнерских отношениях, владения активами и местонахождения организаций в глобализированной среде. То, что кажется конечному потребителю единой услугой, почти всегда складывается из ряда услуг, различных технологий, участия нескольких владельцев и распределяется по множеству различных правовых юрисдикций.

63. Кроме того, Канада заявила о том, что преступное поведение, связанное с информационно-коммуникационными технологиями, продолжает меняться и адаптироваться. Оно становится все более ориентированным на получение прибыли, носит транснациональный характер и зачастую является организованным и специализированным. Преступная деятельность разбивается на более мелкие действия, которые часто осуществляют разные преступники, каждый из которых играет свою роль в преступном предприятии. Такая специализация не только повышает уровень сложности преступлений, но может также обеспечивать более высокую степень защиты, поскольку некоторые составляющие элементы могут не являться уголовными преступлениями в отдельных правовых системах. Кроме того, элементы преступления могут быть рассредоточены по нескольким юрисдикциям. Использование преимуществ распределенных сетей кибертехнологий не только эксплуатирует слабость национальных систем правосудия, но также обращает территориальность и суверенитет наций против самих себя.

64. Заостряя внимание на трудностях, связанных с применением национальных законов в тех случаях, когда их применимость ограничена территориально, Канада сообщила, что действие законов, как правило, ограничивается конкретной территорией, что создает серьезную проблему, поскольку в мире, который все больше ориентируется на цифровые технологии, границы нередко становятся неактуальными. Информационно-коммуникационные технологии продолжают развиваться и совершенствоваться головокружительными темпами; соответственно, распространяются и развиваются и киберпреступления

(связанные, в том числе, с неправомерным использованием или эксплуатацией информационно-коммуникационных технологий). Эфемерный и временный характер цифровых доказательств усложняет ситуацию. Их можно быстро удалить или одним нажатием кнопки перенести из одной юрисдикции в другую. Кроме того, трудности возникают в связи с серьезной обеспокоенностью вопросами неприкосновенности частной жизни и прав человека, а также учетом этих вопросов в условиях цифровой среды. Традиционными законами предусмотрены некоторые следственные полномочия, которые остаются полезными в борьбе с киберпреступностью, но необходимы также новые или более сложные правовые инструменты, чтобы потенциал следственных органов соответствовал масштабам использования технологий в преступных целях.

65. Канада отметила, что с практической точки зрения к проблемам, связанным с получением необходимой информации от других государств, относится осведомленность о местонахождении данных, вне зависимости от того, являются ли они доступными и облечены ли они в понятную форму. В некоторой степени это зависит от того, к какому типу компьютерных данных они относятся. Некоторые виды данных могут храниться для поддержания их долгосрочной доступности, в то время как другие виды данных, например информация о трафике, могут носить более кратковременный характер. Телекоммуникационные компании имеют глобальный охват, но, как правило, обязаны соблюдать национальные или региональные законы: способы получения доступа к данным и их хранения в разных странах могут отличаться. Некоторые режимы хранения данных вызывают обеспокоенность Канады, учитывая серьезные последствия для защиты персональных данных и отсутствие поддержки со стороны общества. Канада считает разумной альтернативой режимы сохранения данных исключительно в целях расследования, предусмотренные Конвенцией Совета Европы о киберпреступности. Кроме того, переговоры по второму дополнительному протоколу к Конвенции будут способствовать укреплению международного сотрудничества и обеспечению доступа к доказательствам в облачных хранилищах.

66. В отношении проблем, связанных с нынешними международными механизмами сотрудничества, Канада придерживается мнения, что получение цифровых доказательств как на национальном, так и на международном уровне является фундаментом успешного расследования и судебного преследования киберпреступлений и других видов серьезных преступлений. Однако последствия одностороннего пересечения границ для получения цифровых доказательств, какими бы важными они ни были, могут вызвать напряженность в международных отношениях и поставить под вопрос законность такого поиска.

67. Канада констатировала, что для получения такой информации преимущественно используются договоры о взаимной правовой помощи. Вместе с тем Канада отметила, что существующие процессы не всегда являются достаточно оперативными для проведения расследований, связанных с электронными доказательствами, и не рассчитаны на большой объем запросов, возникающих в связи с самыми разными преступлениями, оставляющими улики в виде цифровых доказательств. По мнению Канады, механизмы взаимной правовой помощи, предусмотренные Конвенцией Совета Европы о киберпреступности, в настоящее время являются наилучшей моделью практического международного сотрудничества между различными государствами-участниками. Кроме того, переговоры по второму дополнительному протоколу к Конвенции будут способствовать дальнейшему укреплению международного сотрудничества и обеспечат основанный на договорных нормах доступ к доказательствам в облачных хранилищах.

Китай

68. Приветствуя принятие Генеральной Ассамблеей резолюции 73/187, озаглавленной «Противодействие использованию информационно-

коммуникационных технологий в преступных целях», Китай отметил, что Генеральная Ассамблея особо подчеркивала необходимость укрепления международного сотрудничества в борьбе с киберпреступностью в нескольких резолюциях, касающихся предупреждения преступности и уголовного правосудия. Китай рекомендовал Генеральной Ассамблее обсуждать тему киберпреступности на каждой ее сессии, включая рассмотрение вопроса о разрешении на создание соответствующих специальных межправительственных механизмов. В то же время Китай поддержал продолжающееся обсуждение вопроса киберпреступности в рамках Комиссии по предупреждению преступности и уголовному правосудию. Он также выразил поддержку работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, направленной на углубленное обсуждение основных вопросов борьбы с киберпреступностью в соответствии с ее планом работы на период 2018–2021 годов и представление рекомендаций и выводов Комиссии по предупреждению преступности и уголовному правосудию. Китай также призвал различные региональные и международные организации к активному обсуждению вопросов киберпреступности и совместной разработке ответных мер.

69. По вопросу о международном законодательстве Китай высказал мнение, что Конвенция против организованной преступности не может эффективно реагировать на новые требования в отношении международного сотрудничества для борьбы с киберпреступностью. Уже существует ряд региональных конвенций в области борьбы с киберпреступностью, таких как конвенции, разработанные Советом Европы, Шанхайской организацией сотрудничества, Лигой арабских государств и Африканским союзом. В связи с различиями в сфере охвата государств-членов и содержании этих конвенций международное законодательство о борьбе с киберпреступностью носит фрагментированный характер. В связи с этим Китай заявил, что международному сообществу настоятельно необходимо создать глобальную правовую основу для борьбы с киберпреступностью и работать сообща для того, чтобы справиться с все более серьезной криминогенной ситуацией, особенно с новыми проблемами, возникающими в результате появления новых технологий, таких как облачные вычисления, искусственный интеллект, интернет вещей и криптовалюты. Китай поддержал точку зрения, согласно которой всем государствам необходимо обсудить и разработать всемирную конвенцию по борьбе с киберпреступностью, открытую для всех стран, под эгидой Организации Объединенных Наций и с опорой на опыт существующих региональных конвенций.

70. По мнению Китая, необходимо, чтобы такая всемирная конвенция обеспечивала эффективную координацию национальных законов и видов практики в борьбе с киберпреступностью, своевременно реагировала на новые проблемы, обусловленные развитием технологий, и предоставляла приемлемые для всех решения в области глобального управления борьбой с киберпреступностью. С точки зрения сферы применения необходимо, чтобы, помимо преступлений против компьютерных систем, эта конвенция также применялась к преступлениям, совершенным преимущественно путем использования интернета и информационных технологий, а также к действиям, способствующим совершению таких преступлений и подготовке к ним. Что касается охраны правопорядка и проведения расследований, то в конвенции следует предусмотреть адресные меры охраны правопорядка и проведения расследований, а также предусмотреть механизмы решения вопросов государственно-частного партнерства, проясняющие обязанности поставщиков сетевых услуг и операторов сотрудничать в вопросах предупреждения киберпреступности и оказывать содействие охране правопорядка и проведению расследований. Что касается международного сотрудничества, то необходимо, чтобы конвенция регулировала практику трансграничного сбора электронных доказательств, создала более эффективный механизм сбора доказательств, основанный на уважении суверенитета государств и защите прав корпораций и отдельных лиц, и предусматривала положения для систем юрисдикции, соответствующие особенностям киберпреступности. Кроме того, в конвенции следует предусмотреть механизмы

наращивания потенциала, оказания технической помощи и предупреждения преступности.

71. Касаясь международного сотрудничества, Китай подчеркнул, что до вступления в силу всемирной конвенции странам рекомендуется осуществлять прагматичное сотрудничество в области борьбы с киберпреступностью на основе взаимного уважения, равенства и взаимной выгоды в соответствии с Конвенцией против организованной преступности, региональными конвенциями и двусторонними договорами. Китай также отметил, что некоторые страны приняли национальные законы в обход каналов правовой помощи и сотрудничества правоохранительных органов и в одностороннем порядке вывели электронные данные за рубеж, что, в свою очередь, негативно сказалось на основных принципах международного права, таких как суверенитет и защита прав личности и корпоративных прав. Китай продолжает искать баланс между уважением национального суверенитета, защитой корпоративных прав и прав личности и оказанием содействия в проведении расследований, а также занимается повышением эффективности сбора доказательств путем оптимизации процедур правовой помощи и сотрудничества правоохранительных органов и внедрения инновационных моделей сотрудничества.

72. В отношении внутренних мер Китай заявил, что для эффективной борьбы с киберпреступностью государствам следует принимать соответствующие меры на национальном уровне, а именно:

a) установить уголовную ответственность за использование интернета в террористических целях, а также за деятельность, направленную на пособничество и подготовку к совершению киберпреступлений;

b) вменить в обязанность поставщикам и операторам услуг интернета сотрудничество в деле предупреждения киберпреступности и оказание содействия охране правопорядка и проведению расследований и в то же время уточнить границы вышеупомянутых обязательств и гарантировать законные права соответствующих предприятий и отдельных лиц;

c) расширить возможности правоохранительных и судебных органов, необходимые для расследования киберпреступлений, особенно для более эффективного решения проблем, возникающих в связи с новыми технологиями;

d) признать доказательную силу электронных данных и уточнить определение понятия электронных доказательств и сферу их применения;

e) уточнить правила сбора электронных доказательств и принятия их судами, а также предусмотреть в рамках внутреннего законодательства такие меры, как конфискация и опечатывание оригинальных носителей информации, сбор доказательств на месте происшествия, проведение дистанционного обследования и наложение ареста;

f) учитывать специфику электронных доказательств при применении традиционных правил доказывания;

g) активизировать наращивание потенциала подразделений, занимающихся сбором электронных доказательств, создать группы специалистов, обладающих как правовой грамотностью, так и техническими возможностями, и разработать технические стандарты сбора электронных доказательств.

Колумбия

73. Колумбия согласились с необходимостью совершенствования координации и сотрудничества между государствами в борьбе с использованием информационно-коммуникационных технологий в преступных целях путем оказания технической помощи развивающимся странам в совершенствовании их национального законодательства и укрепления потенциала их национальных органов в области предупреждения, выявления, расследования и судебного преследова-

ния случаев такой преступной деятельности. Однако Колумбия считает важным провести различие между вопросами, связанными с киберпреступностью, и возможным широким регулированием информационно-коммуникационных технологий, которое выходит за рамки уголовного регулирования незаконных актов. В этой связи крайне важно иметь четкое представление о концепции регулирования использования информационно-коммуникационных технологий в преступных целях, а также безопасности информации и телекоммуникаций в контексте международной безопасности. Колумбия выступает за свободный, открытый и безопасный интернет и считает важным, чтобы страны имели инструменты, позволяющие им сотрудничать в борьбе с киберпреступностью, наращивать собственный национальный потенциал и принимать меры для укрепления взаимного доверия между странами.

74. Колумбия заявила, что в области борьбы с киберпреступностью существуют масштабные проблемы, в частности: цифровая идентификация личности; сотрудничество с поставщиками услуг интернета; вопросы, касающиеся цифровых доказательств, методов их получения и хранения, порядка передачи, сертификации и юридической силы; а также защита данных, неприкосновенность частной жизни и уважение прав и свобод человека. Кроме того, киберпреступность тесно связана с другими преступлениями, которые носят трансграничный характер. Поэтому Колумбия считает, что необходимо более глубокое понимание сути преступлений, способов их осуществления и т.д., в связи с чем важно осуществлять обмен опытом и передовой практикой между странами в целях повышения эффективности национальных и международных мер по борьбе с такими преступлениями. Цифровой разрыв делает некоторые страны более уязвимыми, и сотрудничество не является неэффективным. Международное сотрудничество в судебной области должно быть адаптировано для ускорения работы (например, в отношении взаимной правовой помощи, запросов на оказание взаимной правовой помощи и договоров о взаимной правовой помощи). Для этого Колумбия выступила с предложением о разработке протоколов и шаблонов, которые способствовали бы пониманию со стороны стран и были бы приемлемыми в рамках расследований и судебных процессов.

75. Однако Колумбия также считает, что Комиссии по предупреждению преступности и уголовному правосудию следует продолжать обсуждение связанных с киберпреступностью вопросов с технической и политической точек зрения в рамках Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Она должна быть главным форумом, и не следует создавать новые альтернативные группы, ограничивающие участие стран. Группа экспертов согласовала план работы, результатом которого в 2021 году, как ожидается, станет доклад, содержащий варианты укрепления нынешних ответных мер и предложения в отношении новых юридических и/или иных мер реагирования.

76. Наконец, Колумбия считает, что необходимости в начале переговоров по новому соглашению о киберпреступности с нуля нет. По мнению Колумбии, первоочередное внимание необходимо уделять укреплению потенциала и сотрудничества на основе существующих договоров, таких как Конвенция против организованной преступности и Конвенция Совета Европы о киберпреступности.

Коста-Рика

77. Коста-Рика отметила, что ее история признания, уважения и защиты прав человека уходит корнями в далекое прошлое. Следовательно, международные договоры, которые страна подписала и ратифицировала, не нарушают суверенитет государства.

78. Коста-Рика высказала мнение, что прокуроры и следователи по делам, связанным с киберпреступностью, помогая жертве, должны обеспечивать ба-

ланс между правом на неприкосновенность частной жизни и общественной безопасностью; эти гарантии должны соблюдаться при сборе доказательств и с этой целью судье должно быть подано ходатайство о выдаче распоряжения, помимо прочего, на проведение обыска, отмену банковской тайны или изъятие налоговой информации. Все это необходимо для достижения успеха в проведении расследований и обеспечения допустимости доказательств в суде.

79. Коста-Рика, являясь государством — участником Конвенции Совета Европы о киберпреступности, имела доступ к углубленной подготовке для юристов-практиков, а также доступ к Сети 24/7 и возможность осуществления обмена с другими должностными лицами из других регионов в целях получения информации, имеющей отношение к расследованию, и обмена ею в режиме реального времени, а также для получения цифровых доказательств. Кроме того, поскольку Коста-Рика является государством — участником Конвенции Совета Европы о киберпреступности, она была включена в проект Совета Европы и Европейского союза «Расширенные глобальные действия по борьбе с киберпреступностью» (GLACY+), в рамках которого она принимала участие в следующих мероприятиях:

a) проведение первоначальной оценки проекта GLACY+, состоявшееся в Сан-Хосе 21–24 мая 2018 года;

b) консультативная миссия по вопросам законодательства, касающегося киберпреступности и электронных доказательств, и консультативная миссия по вопросам национальной политики и стратегии в области борьбы с киберпреступностью. Подготовка и пересмотр законодательной базы в области киберпреступности и цифровых доказательств, а также подготовка и пересмотр национальной политики в области борьбы с киберпреступностью, которые состоялись в Сан-Хосе 8–11 октября 2018 года;

c) курс профессиональной подготовки инструкторов в области киберпреступности и электронных доказательств для судей, прокуроров и адвокатов, проведенный в Сан-Хосе 11–15 февраля 2019 года;

d) углубленный курс профессиональной подготовки в области киберпреступности и электронных доказательств для судей, прокуроров и других сотрудников судебных органов (13–16 мая 2019 года) и консультативная миссия по вопросам процессуального законодательства о киберпреступности и электронных доказательствах (16–17 мая 2019 года).

80. Кроме того, в рамках проекта GLACY+ было оказано содействие участию Коста-Рики в следующих мероприятиях, проходивших на территории других государств:

a) международный семинар, посвященный стратегиям профессиональной подготовки судей в области киберпреступности и электронных доказательств, состоявшийся в Себу, Филиппины, 12–14 декабря 2017 года;

b) совместная международная конференция Совета Европы и Евроюста по вопросам судебного сотрудничества в области борьбы с киберпреступностью, состоявшаяся в Гааге, Нидерланды, 7–8 марта 2018 года;

c) четвертое совещание Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, прошедшее в Вене 3–5 апреля 2018 года;

d) двадцать седьмая сессия Комиссии по предупреждению преступности и уголовному правосудию и совещание Руководящего комитета GLACY+, состоявшиеся в Вене 14–18 мая 2018 года;

e) заседание Комитета по Конвенции о киберпреступности (T-CY), 19-е пленарное заседание T-CY, второе пленарное заседание по подготовке проекта протокола, конференция «Спрут» по вопросам сотрудничества в борь-

бе с киберпреступностью и семинар по вопросу о Сети 24/7, состоявшиеся в Страсбурге, Франция, 9–13 июля 2018 года;

f) международный совместный семинар для подразделений, занимающихся расследованием киберпреступлений, и центральных органов, состоявшийся в Сингапуре 27–31 августа 2018 года;

g) четвертое совещание Рабочей группы по борьбе с киберпреступностью для руководителей подразделений, состоявшееся в Рио-де-Жанейро, Бразилия, 4–6 сентября 2018 года;

h) конференция по теневой экономике и киберпреступности, состоявшаяся в Страсбурге, Франция, 4–7 сентября 2018 года;

i) шестая конференция Интерпола и Европола по борьбе с киберпреступностью, состоявшаяся в Сингапуре 18–20 сентября 2018 года;

j) двадцатое пленарное заседание T-CY, третье пленарное заседание по подготовке проекта протокола, заседание Комитета GLACY+, состоявшиеся в Страсбурге, Франция, 27–30 ноября 2018 года;

k) конференция по вопросам уголовного правосудия в киберпространстве, состоявшаяся в Бухаресте 25–27 февраля 2019 года;

l) курс подготовки инструкторов Интерпола, состоявшийся в Боготе 25 февраля — 1 марта 2019 года;

m) пятое совещание Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, состоявшееся в Вене 27–29 марта 2019 года.

81. В настоящее время Конвенция Совета Европы о киберпреступности ратифицирована 63 странами (как на европейском континенте, так и в других регионах), поэтому для Коста-Рики она представляет собой международный документ с зарегистрированными сведениями о его осуществлении.

Чехия

82. Чехия сообщила, что она ратифицировала Конвенцию Совета Европы о киберпреступности в 2013 году. В 2014 году за этим последовала ратификация Дополнительного протокола к Конвенции, касающегося криминализации актов расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, расширяющего сферу действия Конвенции и ее основных, процессуальных положений и положений, касающихся международного сотрудничества. Конвенция и Дополнительный протокол к ней открыты для присоединения всех стран, а не только государств — членов Совета Европы.

83. Чехия твердо убеждена в том, что Конвенция Совета Европы о киберпреступности является наиболее эффективным и современным инструментом для решения всех проблем, возникающих в связи с явлением киберпреступности во всем мире. В связи с этим Чехия приветствует растущее число государств, которые, не являясь членами Совета Европы, за последнее время присоединились к Конвенции или рассматривают вопрос о присоединении к ней, что обусловлено ее межрегиональным характером и всеохватностью и прозрачностью процедур присоединения. Таким образом, вместо разработки нового документа, что будет скорее контрпродуктивным в связи с длительностью процесса принятия и ратификации конвенций Организации Объединенных Наций, следует сосредоточить внимание на эффективном осуществлении существующих правовых документов, примером которых служит Конвенция Совета Европы о киберпреступности, принимая во внимание также ее позитивный вклад в гармонизацию национальных законодательных норм.

84. Чехия поддерживает и высоко оценивает специальные экспертные знания, обеспечиваемые УНП ООН, и их конкретное воплощение, например Practical

Guide for Requesting Electronic Evidence across Borders («Практическое руководство для запроса электронных доказательств через границы»). Следует и далее уделять первоочередное внимание профессиональным аспектам этого вопроса, которые обсуждаются Группой экспертов для проведения всестороннего исследования проблемы киберпреступности, базирующейся в Вене и вносящей уникальный вклад на уровне Организации Объединенных Наций.

85. Чехия заявила, что первостепенное значение имеет укрепление процессуальных норм в целях борьбы с киберпреступлениями; не менее важны также гарантии соблюдения прав человека и верховенства закона, включая защиту персональных данных.

86. Осознавая, что число связанных с киберпреступлениями угроз возрастает и что эти преступления все отчетливее приобретают трансграничный характер, Чехия сообщила, что в центре ее внимания находится повышение осведомленности о киберугрозах и обучение борьбе с ними, включая наращивание потенциала и набор новых сотрудников правоохранительных органов, обладающих необходимыми знаниями и опытом. В этой ситуации весьма позитивно с точки зрения борьбы с киберпреступностью было воспринято создание национальной сети прокуроров, которая действует на региональном уровне и специализируется на борьбе с киберпреступностью, а также специализированных полицейских подразделений по борьбе с киберпреступностью. Кроме того, согласно этому сообщению, особое внимание уделяется электронным доказательствам, объем которых в уголовном судопроизводстве существенно возрастает. С 1 февраля 2019 года в Чехии действует новый правовой акт, установивший четкие правила оперативного обеспечения сохранности накопленной информации в электронной форме в рамках как национальных, так и транснациональных дел.

87. Цифровизация системы правосудия является одной из приоритетных задач Министерства юстиции Чехии. Правительство утвердило Национальную концептуальную стратегию борьбы с киберпреступностью (этот вопрос отражен в разработанной Министерством внутренних дел и регулярно обновляемой Национальной концептуальной стратегии борьбы с организованной преступностью) и установило конкретные задачи и меры, которые необходимо принять в этой области.

88. Что касается взаимной правовой помощи, то Чехия сообщила, что запросы на оказание помощи и связанные с ними операции все чаще обрабатываются в электронном виде. Соответствующие процедуры были упорядочены в целях обеспечения большей эффективности и оперативного сотрудничества, в том числе в области обмена информацией между государствами (например, путем установления неофициальных каналов связи или пунктов связи в рамках Сети 24/7 в соответствии с Конвенцией Совета Европы о киберпреступности).

89. Чехия упомянула те же потенциальные проблемы, что и другие страны: растущая анонимность пользователей (шифрование как стандарт), доступность вредоносных программ и платных незаконных услуг (преступность как услуга) и возможность скрывать доходы от преступлений в виртуальных валютах, а также их анонимность. Наконец, Чехия подчеркнула, что не менее важна проблема недостаточной эффективности вышеупомянутой системы международной взаимной правовой помощи для решения вопросов, связанных с киберпространством, в частности, ввиду ее медлительности. Средний срок обработки запроса об оказании взаимной правовой помощи в связи с вопросами кибербезопасности составил 21 месяц (среди государств — членов Совета Европы). В связи с этим целесообразно начать обсуждение определения юрисдикции в киберпространстве и прямого доступа к электронным доказательствам на серверах, расположенных за рубежом (или в неизвестном месте). Существует возможность обсуждения прямого сотрудничества с иностранными поставщиками услуг. Чехия, являясь государством — членом Европейского союза и Совета Европы, принимает участие в многочисленных дискуссиях в этой области, в

частности в отношении европейских ордеров на предъявление данных и обеспечение их сохранности и второго дополнительного протокола к Конвенции Совета Европы о киберпреступности.

Корейская Народно-Демократическая Республика

90. Правительство Корейской Народно-Демократической Республики считает, что информационно-коммуникационные технологии не должны использоваться в преступной деятельности таким образом, который угрожает политической, экономической и социальной стабильности государств или ущемляет ее. По ее мнению, для предотвращения использования информационно-коммуникационных технологий в преступных целях первостепенное значение имеют межгосударственное сотрудничество и координация.

91. Принимая во внимание, что в мировом масштабе имеет место недостаток правовых инструментов, направленных на предупреждение и пресечение использования информационно-коммуникационных технологий в преступных целях, Корейская Народно-Демократическая Республика считает, что необходимо будет подготовить резолюцию Организации Объединенных Наций о сотрудничестве в вопросах предотвращения использования информационно-коммуникационных технологий в преступных целях в соответствии с интересами государств.

92. Правительство Корейской Народно-Демократической Республики подчеркнуло, что вопрос об использовании информационно-коммуникационных технологий в преступной деятельности следует обсуждать на совещаниях соответствующей группы экспертов открытого состава с участием всех заинтересованных государств.

Сальвадор

93. Правительство Сальвадора считает, что основной проблемой в борьбе с использованием информационно-коммуникационных технологий в преступных целях является отсутствие законодательства, в связи с чем оно указало на следующие моменты:

a) отсутствие контроля или законодательства, регулирующего распределение мобильных телефонов и использование интернета для всего населения в целом и, в частности, телефонов с предоплатными тарифами, которые можно легко приобрести и использовать в любых целях;

b) отсутствие законодательства, позволяющего получать информацию онлайн в режиме реального времени об использовании протоколов и о назначении государственных и частных IP-адресов различными операторами, работающими в стране;

c) отсутствие правил использования технологических устройств, таких как беспилотные летательные аппараты, блокираторы сигнала, перехватчики, зараженные вирусами устройства и другое оборудование, которое позволяет совершать киберпреступления;

d) отсутствие нормативных актов, обязывающих администраторов сетей государственных, частных и некоммерческих организаций создавать, поддерживать и сохранять журналы соединений их внутренних клиентов. Отсутствие таких нормативных актов может быть использовано для совершения традиционных преступлений и киберпреступлений.

Эстония

94. Эстония заявила, что киберпреступность и использование информационно-коммуникационных технологий в преступных целях — это явления, масштабы которых растут, и это создает проблемы для правоохранительных органов во всем мире.

95. Эстония отметила, что, поскольку большинство киберпреступлений носят трансграничный характер, международное сотрудничество имеет исключительно важное значение. Часто бывает так, что электронные доказательства, связанные с преступлением, хранятся за пределами страны, проводящей уголовное расследование. Однако международное сотрудничество не всегда эффективно, и в странах зачастую отсутствуют необходимые нормы материального и процессуального права или достаточный потенциал правоохранительных и судебных органов.

96. Эстония заявила, что в настоящее время единственным юридически обязательным документом для борьбы с киберпреступностью, оказывающим глобальное воздействие, является Конвенция Совета Европы о киберпреступности. Положения этой Конвенции, касающиеся как материального, так и процессуального права и международного сотрудничества, использовались в качестве примера многими странами мира, которые не присоединились к Конвенции. Поскольку эти стандарты были приняты многими странами и уже достигнут определенный уровень унификации, налицо необходимость и возможность дальнейшего сотрудничества. Конвенция, как уже существующий международный юридически обязательный документ, устанавливает стандарты, которые также должны соблюдаться странами, не обладающими необходимой нормативно-правовой базой.

97. С точки зрения Эстонии, Конвенция Совета Европы о киберпреступности является эффективным инструментом для сбора электронных доказательств и обмена ими. Поскольку положения и меры процессуального права Конвенции могут также использоваться для других уголовных преступлений, связанных с компьютерными данными или электронными доказательствами, она представляет собой нечто большее, чем просто документ о киберпреступности. Кроме того, поскольку положения Конвенции могут использоваться для решения проблем, связанных с электронными доказательствами, которые имеют отношение к любым уголовным преступлениям, она стала еще более важной и ценной для государств. Электронные доказательства и доступ к электронным доказательствам превратились в одну из сложнейших проблем для правоохранительных органов при проведении уголовных расследований. Поскольку электронные доказательства часто хранятся в других странах, необходимо использовать меры и каналы международного сотрудничества. Хотя международное сотрудничество, основанное на Конвенции Совета Европы о киберпреступности и других документах, таких как Конвенция против организованной преступности, приносит плоды, существует необходимость в его активизации и повышении его эффективности.

98. Эстония отметила, что на протяжении нескольких лет обсуждался второй дополнительный протокол к Конвенции Совета Европы о киберпреступности. Недавно начались переговоры по этому вопросу. Дополнительный протокол, который будет открыт для государств — участников Конвенции, обеспечит дополнительные инструменты для сотрудников правоохранительных органов и работников судебных органов в целях укрепления международного сотрудничества и обеспечения более четких правил и гарантий. Поэтому Эстония отметила, что глобальное значение Конвенции и ее охват продолжат расти в будущем и другие страны смогут воспользоваться предоставляемыми ею преимуществами.

99. Эстония особо отметила дискуссии по вопросу о борьбе с киберпреступностью и наращивании потенциала на уровне УНП ООН. С 2011 года Группа

экспертов для проведения всестороннего исследования проблемы киберпреступности обсуждает возможные меры по противодействию киберпреступности, в том числе способы обеспечения более эффективного осуществления действующих международных документов. Группа экспертов стала для государств полезной и эффективной платформой для обсуждения проблем и задач, связанных с киберпреступностью и обменом передовым опытом. Хотя консенсуса по многим вопросам пока достичь не удалось, была выражена решительная поддержка укреплению потенциала. В настоящее время Группа экспертов продолжает свою работу в соответствии с согласованным планом работы, и ожидается, что к 2021 году она представит свои выводы и рекомендации.

100. Эстония считает, что было бы преждевременно начинать параллельное обсуждение и подготовку параллельных докладов на уровне Организации Объединенных Наций. Поскольку ресурсы ограниченны, их следует использовать наиболее эффективным образом; поэтому существующая Группа экспертов должна продолжить и завершить свою работу в рамках своего мандата и плана работы. Вместе с тем, как уже показали нынешние обсуждения, появились новые подразделы и темы, связанные с киберпреступностью, интернет-расследованиями и сбором электронных доказательств, что может привести к продолжению работы Группы экспертов после 2021 года.

Франция

101. Франция сообщила о том, что в контексте Парижского призыва к укреплению доверия и безопасности в киберпространстве она вместе с более чем 60 другими государствами и несколькими сотнями международных организаций, представителей гражданского общества и частного сектора подтвердила свою поддержку открытого, безопасного, стабильного, доступного и мирного киберпространства, в котором действуют нормы международного права, включая права человека. Одним из условий достижения этой цели является борьба с использованием цифровых средств в преступных целях.

102. В этом отношении Франция сообщила, что она располагает надежной национальной системой в области борьбы с киберпреступностью с точки зрения действующего законодательства, а также профилактических мер и целевых ресурсов для следователей и судей в целях эффективной борьбы с этим явлением. Этот механизм отчасти основан на переносе в национальное законодательство положений Конвенции Совета Европы о киберпреступности, которая обеспечивает надлежащие и гибкие международные правовые рамки для борьбы с явлением киберпреступности за счет укрепления национальных законодательных систем, а также создания условий для международного сотрудничества. Эти положения дополняют положения, предусмотренные в отношении всех форм транснациональной организованной преступности в рамках Конвенции об организованной преступности.

103. Франция сообщила, что, несмотря на принятые международные правовые рамки и надежную национальную систему, она по-прежнему сталкивается с определенными трудностями в борьбе с киберпреступностью. Эти проблемы решаются в рамках совещаний Группы экспертов для проведения всестороннего исследования проблемы киберпреступности и заключаются в следующем.

a) Неприспособленность национальных законов и специальных средств ряда стран к борьбе с киберпреступностью, в частности отсутствие в некоторых странах национального законодательства (как материального, так и процессуального права), учитывающего проблемы киберпреступности, а также недостаточность профессиональной подготовки и адаптированных ресурсов для следователей и действующих субъектов системы уголовного правосудия для эффективной борьбы с киберпреступностью. В целях содействия укреплению механизмов в этой области Франция активно участвует в ряде программ по

наращиванию потенциала на двусторонней основе, а также на уровне Европейского союза и Совета Европы.

b) Неготовность частного сектора и некоторых иностранных юрисдикций к сотрудничеству в вопросах передачи данных и даже соблюдения постановлений о замораживании активов в рамках расследований и судебных разбирательств. Сотрудничество со стороны поставщиков услуг на данном этапе по-прежнему носит ограниченный характер (в среднем 60 процентов, однако показатель подвержен значительным колебаниям зависимости от партнеров). Крайне важно, чтобы последние отвечали на запросы, направляемые компетентными органами государств в рамках расследований и уголовного судопроизводства, не ставя эти ответы в зависимость от национальной принадлежности IP-адресов. В целях улучшения доступа к электронным доказательствам Франция активно участвует в переговорах в рамках Европейского союза по двум законодательным предложениям, представленным Европейской комиссией 27 апреля 2018 года, а именно проекту правил, определяющих условия доступа к электронным доказательствам, и проекту директивы, требующей от поставщиков услуг назначения юридического представителя, уполномоченного получать судебные предписания и реагировать на них. Франция участвует также в деятельности Рабочей группы, которой было поручено разработать проект дополнительного протокола к Конвенции Совета Европы о киберпреступности, также направленного на решение этой проблемы.

c) Постоянная проблема адаптации к новым технологиям, в частности криптовалютам, которые регулируются лишь частично, что приводит к возникновению серьезных рисков, связанных с анонимизацией финансовых потоков, даркнетом, шифрованием и интернетом вещей. В рамках Группы экспертов для проведения всестороннего исследования проблемы киберпреступности и, в более широком плане, в рамках УНП ООН проводятся обсуждение и обмен передовым опытом, нацеленные на лучшее понимание этих явлений, и Франция хотела бы подчеркнуть ценность этого обсуждения и обмена для оперативной деятельности.

Грузия

104. Грузия сообщила, что с 2008 года она провела серьезные реформы своего основного и процессуального законодательства и инструментов политики в целях эффективной борьбы с киберпреступностью. Все основные реформы были проведены в соответствии с Конвенцией Совета Европы о киберпреступности, к которой Грузия присоединилась в 2012 году.

105. Грузия считает трудности трансграничного доступа к данным одной из основных проблем в борьбе с киберпреступностью. Традиционные механизмы взаимной правовой помощи в условиях постоянно развивающихся облачных вычислений в значительной степени устарели. Грузия считает, что прекращение регулирования или иное облегчение трансграничного доступа к данным — это реформа, проведение которой неизбежно в целях повышения эффективности расследования киберпреступлений и судебного преследования за их совершение. Однако эти реформы должны осуществляться государствами в рамках многосторонних документов, а межюрисдикционные процессуальные полномочия должны сопровождаться надежными гарантиями. По мнению Грузии, важную возможность в этом отношении представляет собой работа над проектом второго дополнительного протокола к Конвенции Совета Европы о киберпреступности.

106. Грузия сообщила, что в последние годы она принимала участие в различных проектах по наращиванию потенциала, осуществляемых и/или поддерживаемых Советом Европы (проекты Восточного партнерства), Европейским союзом и правительством Соединенных Штатов. В рамках этих проектов прошли подготовку несколько сотен работников правоохранительных и судебных орга-

нов, а правительство приняло ряд стратегических документов, основанных на многонациональном опыте в вопросах киберпреступности, электронных доказательств и кибербезопасности.

107. Касаясь вопросов материального права, Грузия сообщила о криминализации незаконного доступа и перехвата, вмешательства в данные и системы, а также неправомерного использования устройств согласно статьям 284–286 Уголовного кодекса 1999 года и в соответствии с положениями статей 2–6 Конвенции Совета Европы о киберпреступности. Судебное преследование всех киберпреступлений осуществляется по аналогии с обычными преступлениями без каких-либо серьезных проблем. Например, в последнее время растет число таких преступлений, как кибермошенничество, однако грузинские суды без труда применяют к подобным случаям нормы законодательства об обычном мошенничестве.

108. В отношении процессуального права Грузия сообщила, что с 2010 года она включила в свое законодательство все процессуальные полномочия, предусмотренные Конвенцией Совета Европы о киберпреступности, включая распоряжение о предъявлении, сбор данных о трафике и перехват информации в режиме реального времени, в то время как некоторые другие полномочия уже присутствовали в ее законодательстве. В то же время Грузия обеспечила надежные процессуальные гарантии, включая судебное разрешение на все процессуальные полномочия в отношении неприкосновенности частной жизни, требование соразмерности, ограничение использования некоторых процессуальных полномочий (используются только в случаях тяжких преступлений) и требование использовать наиболее щадящий вариант имеющихся процессуальных полномочий.

109. В отношении сотрудничества с иностранными поставщиками интернет-услуг было заявлено, что правоохранительным органам Грузии удалось получить информацию об абонентах от различных глобальных интернет-компаний (Facebook, Apple, Microsoft и т.д.) в связи с предоставляемыми в Грузии услугами. Так, например, Грузия вошла в число десяти стран мира с наивысшим уровнем раскрытия информации, причем уровень раскрытия информации из сети Facebook для процессуальных нужд составил в период 2017–2018 годов 94 процента. В 2018 году Грузия ввела форму международного распоряжения о предъявлении, дающую грузинским судьям возможность выдавать распоряжения о предъявлении физическим или юридическим лицам за пределами территориальной юрисдикции Грузии, если в совокупности соблюдаются следующие условия: согласие лица, которому выдается распоряжение, на добровольное раскрытие электронных данных; и разрешение от страны пребывания иностранной структуры на раскрытие такой информации в соответствии с законами или политикой исполнительной власти. Прокурор обязан получить такое распоряжение у суда, а затем передать его через должностное лицо, уполномоченное генеральным прокурором. Неисполнение таких распоряжений не влечет за собой никакой юридической ответственности. В соответствии со статьей 18 Конвенции Совета Европы о киберпреступности Грузия направляла международные распоряжения о предъявлении в адрес сети Facebook и других международных поставщиков услуг в связи с предоставляемыми в Грузии услугами.

Германия

110. Германия отметила, что развитие технологий ведет к непрерывным изменениям в обществе. Оно создает новые возможности, которые могут принести пользу как каждому человеку, так и обществу в целом. С другой стороны, технический прогресс порождает новые вызовы. Технологические возможности оперативного общения и совершения действий в глобальном масштабе используются и в незаконных целях. Таким образом, по мнению Германии, важно противостоять вызовам и бороться с преступным поведением. Для этого требу-

ется не только достаточно развитая национальная нормативно-правовая база, но и действенное трансграничное сотрудничество.

111. По мнению Германии, любое решение на международном уровне должно специально разрабатываться с учетом конкретных проблем, порождаемых информационно-коммуникационными технологиями, и касаться вопросов конфиденциальности, целостности и доступа к информационным системам (так называемые основные киберпреступления). Не представляется ни возможным, ни желательным пытаться выработать нормы, применимые ко всем преступлениям, совершенным с использованием компьютера или через интернет. Необходимо придать положениям о борьбе с основными киберпреступлениями гибкость, достаточную для того, чтобы они шли в ногу с техническим прогрессом. С другой стороны, для расследования киберпреступлений, их судебного преследования и наказания за их совершение необходимы механизмы трансграничного обмена данными.

112. Германия подчеркнула, что Конвенция Совета Европы о киберпреступности хорошо подходит для эффективного решения существующих проблем в области борьбы с киберпреступностью. В этом контексте Конвенция доказала, что она является подходящим инструментом для борьбы с киберпреступностью, который также открыт для третьих стран. Германия отметила, что Конвенция была широко признана многими государствами в качестве ведущего международного документа по борьбе с киберпреступностью, а также использовалась властями Германии в качестве руководства для разработки внутреннего законодательства. Актуальным остается технологически нейтральное определение преступлений в Конвенции. По мнению Германии, именно тот факт, что основное внимание в Конвенции, в принципе, уделяется преступлениям против конфиденциальности, целостности и доступности информационных систем, способствовал высокому уровню ее глобального признания. Поэтому Германия считает важным сохранить понимание понятий, касающихся свода основных киберпреступлений. В противоположность этому следует проявлять осторожность при расширении понятия киберпреступности на формы поведения, в рамках которых компьютерные устройства используются лишь в качестве средства для совершения обычных преступлений. Почти любое преступление может быть совершено с использованием компьютерных устройств, однако это не делает их «киберпреступлениями».

113. Германия отметила, что адаптацию к событиям последнего времени следует проводить на основании Конвенции Совета Европы о киберпреступности, как это происходит сейчас в процессе переговоров по второму дополнительному протоколу в части обеспечения сохранности электронных доказательств. Второй дополнительный протокол будет направлен на расширение сотрудничества между сторонами в области отслеживания киберпреступлений и в области обеспечения сохранности электронных доказательств. В связи с этим Германия не поддерживает призывы к разработке нового международного документа о борьбе с киберпреступностью.

114. Кроме того, Группа экспертов для проведения всестороннего исследования проблемы киберпреступности проводит всестороннее исследование проблем в области борьбы с киберпреступностью. Предметные дискуссии по проблемам киберпреступности ведутся в рамках этой Группы экспертов с 2011 года. По мнению Германии, Группа экспертов является и должна оставаться основным местом решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций. По возможности следует избегать параллельных процессов, связанных с резолюциями Генеральной Ассамблеи, и потенциального дублирования усилий.

115. Германия подчеркнула, что особое внимание следует уделять осуществлению законодательства о борьбе с киберпреступностью и достижению реального прогресса на местах, в том числе путем оказания технической помощи. Недостатка в надлежащих международных стандартах нет, а государства-члены

также приняли законодательство в области материального уголовного права в отношении киберпреступности для осуществления действующих стандартов. Вопрос, которым следует сейчас заняться Группе экспертов для проведения всестороннего исследования проблемы киберпреступности, состоит в том, как предоставить правоохранительным структурам прочную правовую основу и необходимые ресурсы для обеспечения безопасности электронных доказательств и в то же время установить границы полномочий правоохранительных органов путем определения условий и гарантий, основанных на принципах верховенства права и защиты основных прав и свобод.

Гана

116. Гана сообщила, что в настоящее время в стране действуют два основных законодательных акта о кибер- и электронных доказательствах: Закон об электронных сообщениях от 2008 года (Закон № 775) и Закон об электронных сделках от 2008 года (Закон № 772).

117. Хотя в Гане основным государственным обвинителем по всем уголовным преступлениям является генеральный прокурор, по уполномочию генерального прокурора обвинение по преступлениям поддерживают и другие ведомства, такие как полиция. Однако Генеральная прокуратура осуществляет уголовное преследование по делам, переданным ей полицией. Количество дел, связанных с киберпреступлениями или совершенных с использованием компьютера, которые полиция передает Генеральной прокуратуре, уменьшается, в связи с чем наблюдаются определенные проблемы и неудачи в осуществлении судебного преследования по таким делам.

118. Гана сообщила о том, что полиции, основному следственному органу, не хватает необходимых инструментов, поскольку все инструменты судебной лаборатории по борьбе с киберпреступностью устарели. В связи с этим расследования передаются частным судебным лабораториям с сопутствующими расходами, которые нередко перекладываются на заявителя. Неспособность оплатить стоимость исследования часто негативно сказывается на проведении судебного разбирательства. Если оплата в конечном счете осуществляется, полиции требуется длительное время для сбора соответствующей суммы. Задержка оплаты, как правило, влияет на своевременность представления отчета, что приводит к задержке судебного разбирательства. Специализирующаяся на киберпреступлениях лаборатория является единственной в стране. Однако ей не хватает необходимых компетентных сотрудников. Отсутствие компетентного персонала также серьезно сказывается на результатах ее деятельности.

119. Гана сообщила, что на сегодняшний день в стране имеются два противоречивых решения Высокого суда относительно получения доступа к содержимому электронного устройства. Согласно одному из этих решений, правоохранительным органам не требуется судебного ордера для получения доступа к содержимому подозреваемого устройства; в другом решении особое внимание уделяется получению ордера до получения доступа к данным. Для обеспечения согласованности двух противоположных решений и внесения ясности вопрос был передан для принятия решения в Верховный суд Ганы.

120. В силу своего характера киберпреступления могут происходить на территории нескольких государств. Поэтому важнейшая информация, необходимая для успешного уголовного преследования по делу, может находиться в другой юрисдикции. Гана подчеркнула, что получение доступа к такой информации зачастую может быть невозможным или удручающе медленным. В отсутствие договора о взаимной правовой помощи между сторонами получение информации может оказаться невозможным. Но и при наличии договора о взаимной правовой помощи процесс передачи информации нередко происходит медленно и носит бюрократический характер, что приводит к задержкам в проведении расследования и последующего судебного разбирательства по делу.

Венгрия

121. Венгрия сообщила, что число жертв, пострадавших от неправомерного использования информационно-коммуникационных технологий, выросло как на национальном, так и на международном уровне. В целом преступники в большей степени предпочитают использовать интернет-приложения (например, Viber, Snapchat, Messenger, WhatsApp и iMessage), не требующие никаких специальных знаний, нежели технологии на основе глобальной системы подвижной связи. Венгрия считает это вызовом для полиции и других правоохранительных органов.

122. Венгрия также отметила, что современные информационно-коммуникационные технологии используются в качестве средства для совершения таких преступлений, как интернет-мошенничество, распространение детской порнографии в интернете и незаконный оборот синтетических наркотиков через интернет. Социальные сети также используются для получения легкого доступа к детям и сексуальной эксплуатации в виде фотографий или видеозаписей. Кроме того, даркнет используется для незаконного и анонимного приобретения оружия, наркотиков и поддельных документов. Для осуществления платежей за эти незаконные и опасные предметы используется биткоин. Кроме того, если вести речь о производстве оружия или его компонентов, то новую угрозу в этом смысле потенциально может представлять технология трехмерной печати.

123. Венгрия далее подчеркнула, что большинство преступлений, связанных с информационно-коммуникационными технологиями, носят международный характер и в них часто оказываются вовлечены более двух стран. Это создает трудности для органов власти в тех случаях, когда для обмена информацией между этими государствами требуется судебное поручение. Органы власти могут сталкиваться с трудностями при расследовании соответствующих преступлений, например, в связи с тем, что пользование услугами виртуальных частных сетей затрудняет установление фактических персональных данных пользователей. Следовательно, необходимы дополнительные усилия в сфере профилактики.

124. По мнению Венгрии, национальным поставщикам услуг интернета придется тесно сотрудничать с государственным сектором, в том числе с полицией. В отсутствие каких-либо международных стандартов, регламентирующих обязанности поставщиков услуг интернета, национальным органам следует унифицировать обязательства таких поставщиков в отношении записи, хранения и совместного использования информации (сохранение данных), связанной с коммуникациями, включая вид данных, минимальный и максимальный срок сохранения данных и особенности коммуникаций. Также необходимо установить стандарты в отношении минимальных требований для направления запроса поставщикам услуг интернета со стороны полиции, поскольку для обработки запроса поставщики, как правило, ожидают большего объема информации, нежели имеющийся в распоряжении органов власти.

125. В качестве примера передового опыта Венгрия рекомендовала рассмотреть работу сети круглосуточных контактных центров, учрежденных каждым государством-членом в рамках Конвенции Совета Европы о киберпреступности. Она также предложила использовать для обмена информацией канал связи Интерпола.

126. Венгрия сообщила, что шифрование личных технических средств может оказаться полезным с точки зрения предупреждения киберпреступности, однако преступники используют шифрование для того, чтобы скрывать свою личность и местонахождение. Еще одной проблемой для полиции является раскрытие шифра. Потребуется повышение осведомленности о кибербезопасности как в государственном, так и в частном секторе. Кроме того, для укрепления

потенциала на национальном уровне необходимы модернизация информационно-технической инфраструктуры организаций и подготовка сотрудников государственного и частного секторов.

127. Венгрия подчеркнула, что необходимым условием для успешного завершения расследования дел является тесное сотрудничество между различными государствами. В Европе доминирующую роль в сфере сотрудничества играет Европол. Что касается получения электронных доказательств от поставщиков услуг из других стран, примером надлежащей практики могут служить положения Конвенции Совета Европы о киберпреступности.

128. Поскольку киберпреступность — это эволюционирующая проблема, которая затрагивает все страны, для эффективной борьбы с ней Венгрия считает необходимым выполнение следующих требований:

a) максимально увеличить число стран с адекватным, совместимым внутренним законодательством о борьбе с киберпреступностью, которое содействует международному сотрудничеству;

b) развивать механизмы сотрудничества, укреплять доверие и совершенствовать навыки в целях обмена данными для проведения расследований, судебного преследования и сокращения масштабов киберпреступности;

c) искоренять безопасные убежища для преступников и повышать потенциал правоохранительных и судебных органов, особенно в отношении получения электронных доказательств.

129. Что касается технической помощи, Венгрия напомнила о проекте всестороннего исследования проблемы киберпреступности, отметив, что был достигнут широкий консенсус по вопросу о необходимости усилий по укреплению потенциала в целях борьбы с киберпреступностью. Существует Глобальная программа УНП ООН по киберпреступности, участие в которой всех государств-членов имеет важное значение. Существует также ряд других программ по укреплению потенциала, которые поддерживает Венгрия, например программы, осуществляемые Советом Европы и Европейским союзом. По мнению Венгрии, необходимо обеспечить, чтобы все проекты по наращиванию потенциала носили подлинно адресный характер и эффективно координировались во избежание дублирования усилий, надлежащим образом разрабатывались и выстраивались в целях удовлетворения потребностей международного сотрудничества и обеспечения устойчивых результатов, а также оперативно оценивались в целях анализа их воздействия.

130. Что касается вариантов усиления существующих национальных и международных мер по противодействию киберпреступности и выработки новых мер, Венгрия высказала мнение, что Конвенция Совета Европы о киберпреступности представляет собой эффективную модель национального законодательства и ценную основу для международного сотрудничества. Являясь открытой для присоединения стран, не являющихся государствами — членами Совета Европы, Конвенция представляет собой гибкий инструмент для этого (разработки национальных мер и содействия международному сотрудничеству). В связи с этим Венгрия не поддержала призыв к разработке нового международного документа о борьбе с киберпреступностью.

131. По мнению Венгрии, Группа экспертов для проведения всестороннего исследования проблемы киберпреступности является и должна оставаться основным местом решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций, по крайней мере до 2021 года. Она добилась результатов, в том числе в отношении законодательных реформ, основанных на существующих международных стандартах, а также с точки зрения укрепления потенциала. В течение последних шести лет был отмечен значительный прогресс в плане законодательных реформ, в частности в тех случаях, когда страны использовали существующие международные стандарты. Многие

организации разработали программы укрепления потенциала. Эти усилия необходимо продолжать и расширять в дальнейшем.

132. Венгрия предлагает государствам-членам оказывать УНП ООН поддержку в осуществлении следующих мер по борьбе с угрозой киберпреступности:

a) повышение квалификации сотрудников полиции и правоохранительных органов посредством как общей, так и специальной подготовки;

b) оказание технической помощи развивающимся странам;

c) проведение анализа пробелов в международном сотрудничестве для выявления приоритетных областей;

d) поддержка информационно-просветительских кампаний, направленных на совершенствование работы в области предупреждения преступности и налаживание сотрудничества гражданского общества и бизнеса с правоохранительными органами;

e) укрепление существующих оперативных механизмов, таких как Сеть 24/7;

f) сбор данных об угрозах киберпреступности;

g) выполнение функций центра по обобщению передового опыта и практических примеров борьбы с киберпреступностью.

Индия

133. Индия обратила внимание на неуклонный рост киберпреступности, что создало новые проблемы и сложности для правоохранительных органов. Киберпреступность существенно отличается от традиционных преступлений по характеру, сфере охвата, средствам, уликам и действиям; таким образом, обмен информацией в режиме реального времени или близком к реальному времени имеет существенно важное значение для сбора доказательств в целях привлечения киберпреступников к ответственности. Преступления в киберпространстве являются технически и юридически сложными. Киберпространство и киберпреступность не имеют физических границ, и поэтому международное сотрудничество имеет ключевое значение, среди прочего, для проведения расследований, сбора данных и доказательств и наказания.

134. Индия сообщила, что, согласно данным Национального бюро регистрации преступлений, в 2014 году было зарегистрировано 9 622 киберпреступления, в 2015 году — 11 592, а в 2016 году — 12 317. В течение 2016 года 48,6 процента сообщений в отношении дел о киберпреступности были связаны с незаконным обогащением (5 987 из 12 317 случаев), 8,6 процента, или 1 056 дел, — с местью и 5,6 процента, или 686 дел, — с оскорблением благопристойности женщины.

135. Индия далее сослалась на национальную нормативно-правовую и институциональную базу для борьбы с киберпреступностью, указав, что Закон об информационных технологиях от 2000 года с поправками, внесенными в 2008 году, и Уголовный кодекс Индии обеспечивают нормативно-правовую базу для решения вопросов, связанных с электронной торговлей, кибербезопасностью, киберпреступностью и кибертерроризмом. Национальное законодательство достаточно обширно и охватывает большинство вопросов, связанных с киберпреступностью.

136. Индия также отметила, что различные виды противоправного использования информационно-коммуникационных технологий в форме «основных» киберпреступлений и киберпреступлений, совершаемых с помощью информационно-коммуникационных технологий, создают различные проблемы, которые нуждаются в решении. Противоправное использование информационно-коммуникационных технологий включает вторжение на веб-сайт и искажение

его внешнего вида, распространение вирусов и вредоносных кодов, обычные и распределенные атаки типа «отказ в обслуживании», хакерскую деятельность, фишинг, кибертерроризм, детскую порнографию, «сексуальное вымогательство», хищение личных данных, виртуальное преследование и домогательства, распространение ложных новостей и пропаганды, незаконные азартные игры, продажу поддельных лекарственных средств и наркотиков, кибершпионаж и т.д.

137. Индия отметила, что киберпреступления совершаются с использованием современных информационно-коммуникационных технологий, таких как вредоносные программы (malware), бот-сети, многослойная маршрутизация и даже простые мобильные телефоны, применяемые в целях социальной инженерии.

138. Говоря о проблемах в области борьбы с использованием информационно-коммуникационных технологий в преступных целях, Индия отметила следующее:

a) использование множества видов вредоносных программ и бот-сетей позволяет преступникам избегать средств технического контроля, таких как антивирусное программное обеспечение и фильтрация интернет-контента, а также обнаружения правоохранительными органами;

b) использование таких технологий с применением запутывания, анонимности, вычислительных мощностей и воспрепятствования отслеживанию источника или лица, совершившего преступление;

c) тот факт, что услуги виртуальных частных сетей обеспечивают возможность анонимного обмена сообщениями в интернете;

d) многообразие инструментов, которые позволяют преступникам сохранять сетевую анонимность или не оставлять следов. Из всех этих инструментов наибольшую проблему в силу ряда причин представляют собой бот-сети;

e) тот факт, что борьба с киберпреступностью требует специализированных юридических знаний, навыков проведения расследований, инструментов судебной экспертизы, аналитического склада ума и проницательности;

f) с точки зрения проблем правового характера, обеспокоенность вызывает тот факт, что транснациональный характер киберпреступности приводит к сложностям во взаимодействии юрисдикций, что, в свою очередь, затрудняет проведение расследования и судебного преследования. Несогласованность законодательства разных стран создает трудности для расследования преступлений, связанных с кибертерроризмом, и уголовного преследования за них.

139. Заострив внимание на проблемах международного уровня, которые препятствуют сотрудничеству в борьбе с преступным использованием информационно-коммуникационных технологий, Индия отметила следующее:

a) временной фактор имеет ключевое значение в расследовании киберпреступлений, в связи с чем необходимо определить сроки представления цифровых доказательств в рамках многостороннего сотрудничества между государствами;

b) в договорах о взаимной правовой помощи первоочередное внимание уделяется тому, что происходит после совершения преступления, тогда как принципиальное значение для предупреждения киберпреступности, в отличие от традиционных преступлений, имеет оперативный обмен информацией. Кроме того, необходимо налаживать международное сотрудничество в области предупреждения киберпреступности;

c) в договорах о взаимной правовой помощи отсутствуют нормы об удовлетворении запросов в экстренных ситуациях, что является ключевым

условием для борьбы с киберпреступлениями. Данный вопрос нуждается в обсуждении;

d) международное сотрудничество в сфере обеспечения защиты от киберпреступлений имеет принципиальное значение, учитывая широкое использование средств контроля и командования, бот-сетей и технологий «глубокой сети»;

e) законы о защите частной жизни затрудняют обмен информацией.

Иран (Исламская Республика)

140. Касаясь проблем в области борьбы с использованием информационно-коммуникационных технологий в преступных целях, Исламская Республика Иран сообщила, что основной проблемой она считает неподчинение требованиям со стороны иностранных поставщиков услуг интернета и операторов социальных сетей. Интернет и социальные сети вносят гигантский вклад в улучшение жизни людей. Однако повсеместное распространение и возможность беспрепятственной передачи данных через интернет и социальные сети провоцируют правонарушителей, особенно организованные преступные группы, активнее использовать такие технологии в преступных целях. Поставщики услуг интернета и социальных сетей играют незаменимую роль в предотвращении и противодействии использованию информационно-коммуникационных технологий в преступных целях, в частности в области сбора и хранения электронных доказательств, а также охраны правопорядка.

141. По мнению Исламской Республики Иран, справедливость и устойчивость мер реагирования в значительной степени зависит от регулирования деятельности в социальных сетях. Деятельность в социальных сетях, принадлежащих частному сектору Ирана, эффективно регулируется национальными властями в соответствии с Процессуальным законом о компьютерных преступлениях. Правоохранительные органы могут выявлять преступную деятельность в киберпространстве, заниматься сбором и сохранением электронных доказательств и осуществлять эффективное расследование и уголовное преследование использования информационно-коммуникационных технологий в преступных целях. Вместе с тем, учитывая экстерриториальный характер киберпреступности, власти сталкиваются с серьезными проблемами в расследовании преступлений, совершенных с использованием серверов, расположенных в других странах и принадлежащих иностранному государственному или частному сектору. В большинстве случаев операторы иностранных социальных сетей отказываются от сотрудничества по уголовным делам. Невыполнение такими структурами просьб о сотрудничестве со стороны государств создает проблему для эффективного предотвращения преступлений и борьбы с ними и ставит под угрозу верховенство права на национальном и международном уровнях.

142. Что касается односторонних принудительных мер, Исламская Республика Иран, которая расположена в регионе, страдающем от организованной преступности, сообщила о международных препятствиях для сотрудничества на международном уровне по вопросам уголовного правосудия, особенно по вопросам противодействия использованию информационно-коммуникационных технологий в преступных целях. Односторонние принудительные меры, которые негативно влияют на коллективное реагирование на такие преступления, препятствуют сотрудничеству стран с иранскими правоохранительными органами в расследовании и уголовном преследовании преступлений, в частности, совершаемых с использованием информационно-коммуникационных технологий, а также в передаче технических средств, необходимых для сохранения электронных доказательств и проведения цифровой судебной экспертизы. Односторонние принудительные меры, которые являются вопиющим нарушением основополагающих принципов международного права, сформулированных в Уставе

Организации Объединенных Наций, не только затрудняют эффективное сотрудничество в борьбе с использованием информационно-коммуникационных технологий в преступных целях, но и ведут к ослаблению верховенства права, что поощряет преступников к продолжению их незаконной деятельности. Устранение препятствий международного характера по-прежнему имеет жизненно важное значение не только для эффективной борьбы с использованием информационно-коммуникационных технологий в преступных целях, но и для обеспечения коллективной безопасности государств. Исламская Республика Иран твердо намерена бороться с организованной преступностью. Она выступает в поддержку международного сотрудничества в борьбе с киберпреступностью при содействии УНП ООН и подчеркивает необходимость активизации деятельности по оказанию технической помощи в этой области.

143. В связи с отсутствием всеобъемлющей международной рамочной основы Исламская Республика Иран подчеркнула необходимость создания международно-правовой базы для борьбы с киберпреступностью. В настоящее время отсутствие надежной и всеобъемлющей международной рамочной основы для борьбы с киберпреступностью по-прежнему создает проблемы для противодействия использованию информационно-коммуникационных технологий в преступных целях. Характер киберпреступности обусловливает необходимость конкретных, жизнеспособных и коллективных мер реагирования на основе международного документа, учитывающего потребность идти в ногу с развитием технологий и появлением новых методов деятельности организованных преступных групп. В существующих документах по борьбе с киберпреступностью, разработкой которых занималось ограниченное число государств, отсутствуют элементы, необходимые для таких мер реагирования, что, в свою очередь, приводит к невозможности их применения на международном уровне.

144. Исламская Республика Иран дала высокую оценку и выразила признательность в связи с чрезвычайно значимой обширной работой УНП ООН, в частности Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Она заявила, что по-прежнему поддерживает усилия УНП ООН в этой области и считает, что принятие всеобщей конвенции о киберпреступности под эгидой Организации Объединенных Наций будет отвечать наилучшим интересам государств и позволит смягчить проблемы в борьбе с использованием информационно-коммуникационных технологий в преступных целях.

145. Что касается правовой основы для борьбы с киберпреступностью, в Исламской Республике Иран традиционные преступления, совершенные или ставшие возможными благодаря использованию киберпространства, подлежат наказанию в соответствии с исламским Уголовным кодексом. Однако Исламская консультативная ассамблея (парламент) разработала и утвердила особое законодательство для киберпространства в целях предупреждения и пресечения использования информационно-коммуникационных технологий в преступных целях, в частности для совершения киберпреступлений, на эффективной и устойчивой основе. Это законодательство также охватывает электронные доказательства, учитывая их незаменимую роль в судебном преследовании киберпреступлений.

146. Касаясь материального уголовного законодательства, Исламская Республика Иран упомянула Закон об электронной торговле от 2004 года. В этом законе были установлены меры защиты электронных контрактов и устройств в целях сохранения коммерческой тайны, а также были признаны уголовно наказуемыми деяниями неправомерное использование персональных данных, ущемление прав потребителей и раскрытие секретной коммерческой информации в рамках электронных сделок, равно как и компьютерное мошенничество и подделка документов. Было указано, что Закон о компьютерных преступлениях от 2009 года содержит положения о криминализации и ответственности юридических лиц. В частности, в соответствии с этим законом уголовно наказуемыми деяниями были признаны несанкционированный доступ к данным и

компьютерным системам, распространение материалов непристойного содержания, осуществление действий, направленных против целостности и конфиденциальности данных, а также хищения и мошенничество, связанные с использованием компьютеров. Эти преступления наказываются штрафом и лишением свободы на срок до 15 лет. Статья 26 устанавливает в качестве отягчающих обстоятельств совершение киберпреступлений организованным образом, в крупных масштабах или против государственных компьютерных систем. В настоящее время этот закон анализируется в целях его адаптации к новым способам совершения преступлений и предоставления правоохранительным органам устойчивой правовой базы.

147. Говоря о процессуальном праве, Исламская Республика Иран упомянула о процессуальном праве в отношении компьютерных преступлений, которое ранее являлось частью Закона о компьютерных преступлениях от 2009 года, а впоследствии было включено в Уголовно-процессуальный закон с незначительными изменениями. Этот законодательный акт охватывает такие вопросы, как юрисдикция, специализированные подразделения для проведения расследования, судебное преследование киберпреступлений, а также условия и процедуры для осуществления поиска и изъятия электронных доказательств, данных и компьютерных систем. Закон гарантирует соблюдение надлежащих правовых процедур и неприкосновенность частной жизни. Согласно статьям 671 и 672, издание судебного ордера на обыск и изъятие данных возможно только при наличии веских и убедительных оснований для таких мероприятий, которые должны проводиться в присутствии законного владельца. Согласно статье 679, запрещается любое изъятие, влекущее за собой причинение ущерба имуществу или ведущее к нарушению процесса оказания общественных услуг.

Ирак

148. Ирак отметил, что использование интернета является одной из особенностей современной цивилизации, а также показателем развития, интеграции в человеческую цивилизацию и взаимодействия с другими странами. Таким образом, произошла революция в методах научного и культурного обмена. Интернет превратился в огромный канал знаний, способствующий связыванию и сплочению обществ и отдельных лиц за пределами географических границ, политических и социальных факторов и интеллектуальных доктрин, сближению цивилизаций и обмену идеями между представителями различных национальностей, языков и религий. Это приводит к рассмотрению вопроса о том, какие ценности и принципы должны регулировать интернет-контент: это по-прежнему является важной и противоречивой темой для обсуждения. Несмотря на то что на долю развивающихся стран приходится небольшая доля пользователей интернета в мире, проблема контента имеет для них большое значение в силу ее воздействия на их общество. Хотя одной из ценностей интернета является равенство и свобода, неприкосновенность частной жизни в обществах развивающихся стран требует, чтобы правительства принимали во внимание эту особенность и старались защитить их от разнообразных установок и культур.

149. Ирак подчеркнул, что это сближение народов также оказало воздействие на глобализацию преступности и преступного поведения, включая преступления, затрагивающие консервативные общества в развивающихся странах. В связи с этим возникла необходимость создания нормативных актов по этике интернета, которые соответствовали бы специфике каждой общины. Следовательно, в ходе разработки нормативных документов будет определен интернет-контент, допустимый для каждой страны или области, с учетом соответствующих этических стандартов, и он не обязательно будет доступен для всех.

150. Ирак особо отметил, что в последние десять лет наблюдался взрывной рост использования онлайновых приложений. Поэтому возникла необходимость их упорядочения и регулирования. Некоторые современные приложения (для развлечений или игр) требуют от подписчиков разрешения на доступ к

определенным персональным данным. Поскольку уровень доступа к имеющейся в сети информации определяет степень неприкосновенности частной жизни пользователей одной и той же сети, Ирак рекомендовал разработчикам приложений и лицам, занимающимся их продвижением, установить стандарты, требующие предоставления доказательства цели, с которой осуществляется доступ к информации или устройству. Другой подход заключается в том, чтобы добровольцы оценивали приложения на основе согласованных стандартов, чтобы упрочить доверие к надлежащим приложениям и уменьшить степень доверия вредоносным программам.

151. Ирак сообщил, что, как известно, новости быстро распространяются в интернете среди широкой аудитории, которая может не иметь возможности или желания для проверки их источника. Следует поощрять компании к точному и объективному обращению с новостями, а не к публикации ложных сведений или видеоматериалов, которые разжигают ненависть между общинами. Также может потребоваться, особенно в настоящее время, сокращение числа источников агрессивных письменных, аудио- и видеоматериалов в средствах массовой информации. Полезно было бы также расширить сотрудничество между авторами новостей и социальных сетей и добровольными группами по оценке, которые анализируют новости и изучают их достоверность.

152. В отношении рисков онлайновой среды для детей Ирак отметил, что информационное общество предлагает мгновенный доступ в цифровой мир одним щелчком мыши. Компьютер или мобильное устройство с доступом в интернет делают доступным беспрецедентный уровень услуг и информации. Препятствия, такие как стоимость устройств и доступа в интернет, быстро уменьшаются. Эти изменения дают детям и молодым людям беспрецедентные возможности стать «цифровыми гражданами» в виртуальном мире, не имеющем ни пределов, ни границ. К онлайновым рискам и факторам уязвимости, связанным с использованием интернета детьми и молодежью, относятся:

a) воздействие незаконного и вредного контента, такого как порнография, азартные игры, сайты, призывающие к причинению себе вреда, сцены насилия, терроризм и иные нежелательные материалы, а также взаимодействие с другими пользователями. В большинстве случаев операторы веб-сайтов, содержащих подобный контент, не принимают эффективных мер по ограничению доступа детей;

b) целенаправленное воздействие путем рассылки спама и рекламы в целях продвижения товаров, ориентированных на определенные возрастные группы и интересы;

c) импульсивное и чрезмерное использование интернета и онлайн-игр;

d) запугивание, преследование, угрозы и вымогательство;

e) воздействие радикализации, расизма и других дискриминационных высказываний и изображений;

f) искажение возраста человека;

g) неправомерное использование персональных данных и раскрытие личной информации, ведущие к риску физического вреда и ущемлению собственных прав или прав иных лиц вследствие плагиата и загрузки контента (особенно в средствах массовой информации) без разрешения, включая неуместные фотографии.

153. Заострив внимание на вопросах государственной безопасности, Ирак подчеркнул, что крупные интернет-компании предлагают широкий спектр услуг и возможностей для социального и экономического развития. Онлайновые платформы подходят для социально-экономического развития лишь в том случае, когда пользователи представляются своими реальными именами. Однако если они действуют анонимно или используют фальшивое имя, что часто встречается в социальных сетях, они могут злоупотреблять этими услугами и

осуществлять такую преступную деятельность, как распространение ненавистнических высказываний и идеологии терроризма, а также рассылка сообщений, содержащих угрозы или шантаж. Это сложная проблема общественной безопасности для правительств развивающихся стран, особенно если они не располагают технологиями высокого уровня и пытаются налаживать сотрудничество с интернет-компаниями. Эти компании могут собирать общие и личные данные своих клиентов в рамках управления их учетными записями, с помощью которых они могут отслеживать их географическое положение, узнавать номера телефонов и другую полезную информацию, а также предотвращать преступления и спасать жизни людей. Это обязывает заинтересованные стороны взять на себя долю ответственности, действуя в тесном сотрудничестве, в целях решения этих проблем и обеспечения безопасных и непрерывных услуг для достижения целей в области устойчивого развития.

154. Ирак также упомянул другие проблемы, с которыми ему пришлось столкнуться в борьбе с использованием информационно-коммуникационных технологий в преступных целях, в том числе: отсутствие глобальной конвенции о киберпреступности; трудность понимания цифровых доказательств или их части и тот факт, что их легко уничтожить или скрыть; тот факт, что киберпреступность выходит за рамки географических границ, а также преодолевает географическое расстояние между преступником и жертвой; отсутствие надлежащей профессиональной подготовки и неудовлетворительное развитие потенциала компетентных органов по борьбе с киберпреступностью; тот факт, что в некоторых случаях опыт и знания в области расследования киберпреступлений, которыми обладают неправительственные организации и другие государственные органы, не используются надлежащим образом; отсутствие необходимой электронной инфраструктуры для борьбы с киберпреступностью; а также трудности в ограничении способов совершения киберпреступлений или воспрепятствовании ему.

155. Ирак пришел к выводу, что существует все возрастающая и настоятельная необходимость более тесного сотрудничества между заинтересованными сторонами в целях обеспечения безопасного цифрового будущего.

Ирландия

156. Ирландия упомянула о проекте всестороннего исследования проблемы киберпреступности, в котором было отмечено, что существует широкий консенсус относительно первостепенной важности усилий по наращиванию потенциала борьбы с киберпреступностью. Более того, на недавнем пятом совещании Группы экспертов для проведения всестороннего исследования проблемы киберпреступности было достигнуто широкое согласие в отношении того, что недостаточность потенциала в настоящее время представляет, возможно, наиболее серьезную проблему для эффективной борьбы с киберпреступностью.

157. Ирландия подчеркнула, что серьезная проблема, связанная с укреплением потенциала, возникает вследствие того, что любое преступление может включать элементы киберпреступности, особенно если речь идет об электронных доказательствах. Поэтому крайне важно, чтобы все следователи, прокуроры и судьи обладали надлежащими знаниями в этой области. Подготовка специалистов-практиков также имеет важное значение в соответствующих случаях. Эта проблема усугубляется тем, что международный характер киберпреступности означает, что отсутствие надлежащего потенциала в одном государстве может негативно сказаться на способности бороться с преступностью не только в этом государстве, но и в любом другом.

158. Ирландия отметила, что для преодоления этих трудностей важно продолжать и расширять программы по укреплению потенциала на национальном и международном уровнях. Эти проекты по укреплению потенциала должны

быть целенаправленными и скоординированными, чтобы избежать дублирования и обеспечить их устойчивость. Кроме того, они должны быть надлежащим образом разработаны с учетом конкретных требований различных правовых систем государств и потребностей международного сотрудничества. Наконец, необходимо провести тщательную оценку таких проектов, с тем чтобы получить информацию для разработки будущих проектов.

159. Ирландия признала ценность площадки, предоставленной Группой экспертов по проведению комплексного исследования проблемы киберпреступности для обмена знаниями и опытом в отношении проблем, связанных с киберпреступностью. В частности, Ирландия отметила, что характер Группы экспертов как экспертного, а не политического форума имел ключевое значение для успеха ее деятельности. В связи с этим Ирландия считает, что Группа экспертов должна оставаться основным местом решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций.

160. Ирландия далее отметила, что основные проблемы, возникающие в связи с киберпреступностью, не связаны с международно-правовой базой в этой области. В этой связи Ирландия подтвердила, что она не поддерживает предложение о разработке нового международного документа о борьбе с киберпреступностью. Являясь первым обязательным международным документом по борьбе с киберпреступностью, Конвенция Совета Европы о киберпреступности доказала свою гибкость в условиях постоянно меняющейся технологической среды и свой глобальный охват. Глобальный характер Конвенции подтверждается участием 63 государств из всех пяти региональных групп Организации Объединенных Наций, а также тем фактом, что значительное число государств, не являющихся участниками Конвенции, приняли законы о киберпреступности, созданные по образцу Конвенции. В этой связи основные положения Конвенции были в значительной степени реализованы в ирландском законодательстве, и Ирландия намерена как можно скорее ратифицировать Конвенцию.

161. Ирландия заявила о своей полной поддержке прилагаемых в настоящее время усилий по согласованию второго дополнительного протокола к Конвенции Совета Европы о киберпреступности, касающегося укрепления международного сотрудничества, который будет способствовать дальнейшему совершенствованию Конвенции и содействовать обеспечению сохранения ею статуса самого важного международного документа по киберпреступности.

Израиль

162. Израиль подчеркнул, что, учитывая тот факт, что находящиеся в частной собственности платформы компаний, занимающихся информационными технологиями, могут также использоваться для преступной деятельности, одной из наиболее важных проблем, с которыми сталкиваются сегодня государства, является взаимодействие между государственными и частными компаниями. В этой связи необходимо рассмотреть вопрос о соответствующей сбалансированной структуре, с тем чтобы, с одной стороны, позволить компаниям предоставлять надежные услуги своим клиентам, при этом сохраняя их конфиденциальность и свободу слова, а также поощряя инновационную деятельность, а с другой стороны — изыскать надлежащие рамки для сотрудничества с правоохранительными органами в случаях преступной деятельности.

Италия

163. Италия сообщила, что за предупреждение киберпреступности и борьбу с ней отвечает итальянская национальная полиция, а именно полицейская служба почтовых и иных сообщений. Круглосуточно работающий Национальный центр по борьбе с преступлениями в сфере информационных технологий и защите важнейших объектов инфраструктуры, созданный в рамках полицейской

службы почтовых и иных сообщений, занимается исключительно предотвращением преступлений в области информационных технологий (общего, организованного или террористического характера), совершаемых против важнейших объектов инфраструктуры, и борьбой с ними. Он успешно выполняет эту задачу путем постоянного мониторинга интернета. Круглосуточно работающий Национальный центр по борьбе с преступлениями в сфере информационных технологий и защите важнейших объектов инфраструктуры предоставляет услуги киберзащиты на основании соглашений, заключенных между Департаментом общественной безопасности и структурами, управляющими важнейшими объектами инфраструктуры (государственно-частное партнерство). В состав Центра входит также итальянский координационный центр для деятельности в технических и оперативных чрезвычайных ситуациях, связанных с транснациональными преступлениями.

164. В отношении кибертерроризма Италия сообщила, что полицейская служба почтовых и иных сообщений отвечает за предотвращение и борьбу с онлайновым подстрекательством к джихадистскому терроризму, в частности, путем мониторинга интернета при поддержке посредников по вопросам языка и культуры и в сотрудничестве с Центральным директоратом превентивной полиции и Отделом общих расследований и специальных операций полиции. Кроме того, несмотря на полномочия национальной полиции, корпуса карабинеров и финансовой гвардии, которые отвечают за мероприятия по расследованию преступлений в области терроризма и подрывной деятельности, полицейская служба почтовых и иных сообщений регулярно обновляет список сайтов, используемых в террористических целях. Кроме того, входящее в состав финансовой гвардии специальное подразделение по борьбе с мошенничеством в сфере высоких технологий занимается выявлением, предупреждением и борьбой с преступлениями, которые совершаются с использованием киберинструментов в таких областях, как уклонение от уплаты налогов, таможенные преступления, мошенничество, связанное с ресурсами Европейского союза, валютные преступления и изготовление контрафактной продукции.

165. На европейском уровне полицейская служба почтовых и иных сообщений выступает в качестве национального контактного центра для Группы по контролю интернет-пространства Европола, отвечающей за получение докладов государств-членов о содержании террористической джихадистской пропаганды в интернете.

166. Что касается банковского сектора, то, в соответствии с распоряжением министра внутренних дел, на полицейскую службу почтовых и иных сообщений была возложена задача предупреждения киберпреступности и борьбы с ней в случаях использования определенных методов фишинга, несанкционированного доступа либо программных средств или оборудования для мошеннического похищения, воспроизведения и использования средств цифровой идентификации личности, кодов для банковского обслуживания через интернет и платежных карт для электронных операций.

167. Что касается криптовалют, Италия указала, что они зачастую используются в качестве платежных средств для приобретения товаров и услуг. Для этих операций характерна анонимность как исполнителей, так и реальных бенефициаров, что способствует их использованию в незаконных целях (например, для фишинга и вымогательства с помощью программ-криптовирусов).

168. Италия заявила, что в рамках полицейской службы почтовых и иных сообщений был создан национальный центр по борьбе с детской порнографией в интернете. Он ведет постоянно обновляемый черный список и знакомит с ним поставщиков услуг интернета, с тем чтобы они могли предостеречь пользователей интернета в Италии от посещения виртуальных пространств, содержащих поступившие из других стран онлайновые материалы о сексуальных надругательствах над детьми. Этот центр также использует возможности сотрудничества со всеми институциональными и социальными субъектами,

участвующими в деятельности, касающейся образования и защиты несовершеннолетних, в целях осуществления общих стратегий по борьбе с этими явлениями и развития исследований и разработки новых методов для содействия проведению расследований. В основе инновационных методов расследований, применяемых полицейской службой почтовых и иных сообщений, лежат самые современные методы скрытых операций, направленные на противодействие системам анонимизации и на идентификацию участников преступной деятельности и несовершеннолетних, в отношении которых было совершено насилие. Расследования также ориентированы на социальные сети, где проявляются новые формы заманивания и случаи кибертравли, а также преступления, связанные с клеветой в интернете (главным образом, в отношении лиц с институциональными обязанностями), преследованием, притеснением, угрозами и подстрекательством к ненависти.

Япония

169. Япония сосредоточивает свои усилия в первую очередь на решении конкретной проблемы, вытекающей из характера киберпреступности. Киберпреступления имеют высокую степень анонимности и практически не оставляют следов. Кроме того, киберпреступность не имеет каких-либо территориальных или временны*х* ограничений и может моментально нанести вред бесчисленному множеству потерпевших. Таким образом, преступники имеют возможность без труда совершать киберпреступления, используя уязвимость тех стран, которые не способны принять эффективные контрмеры, и опираются на такие страны как на фундамент для своей преступной деятельности, жертвы которой есть в каждой стране мира. Таким образом, общая задача международного сообщества состоит в устранении этого пробела в потенциале, с тем чтобы в каждой стране принимались адекватные и надлежащие меры по борьбе с киберпреступностью, что позволило бы лишить преступников пространства для маневра.

170. В Японии эту проблему еще более усугубляют два аспекта: отсутствие нормативно-правовой базы и недостаточные усилия по наращиванию потенциала. Одной из основных проблем является отсутствие прочной нормативно-правовой базы в области как материального, так и процессуального права для борьбы с киберпреступностью в ряде государств-членов. Так, например, есть страны, чьей законодательной базы недостаточно для установления уголовной ответственности за разработку компьютерных вирусов, или страны, не имеющие законодательной базы, позволяющей сохранять интернет-данные, что создает значительные сложности для борьбы с киберпреступностью. Для решения этой проблемы международному сообществу следует оказать государствам-членам помощь в принятии нового законодательства, способного решать проблемы, связанные с новыми и возникающими формами киберпреступности, а также выдержать испытание временем.

171. По мнению Японии, наиболее всеобъемлющим и экономически эффективным способом достижения этой цели является использование существующих международных правовых рамок. Это не только позволит избежать дублирования в работе, но и даст государствам-членам возможность принять законодательство, нормы которого уже получили широкое признание. Это позволит устранить разрыв между государствами-членами, а также будет способствовать международному сотрудничеству (например, государствам-членам, имеющим схожие правовые системы, будет легче соблюдать принцип обоюдного признания соответствующего деяния преступлением). В этой связи Конвенция Совета Европы о киберпреступности получила широкое признание международного общества и служит общей отправной точкой. Принятие законов в соответствии с этой Конвенцией в Японии доказало свою эффективность. Например, положение о признании преступлением «создания электромагнитных записей несанкционированных команд» (статья 168-2 Уголовного кодекса), вступившее в

силу в 2011 году в соответствии с Конвенцией, успешно применяется к новым и возникающим формам киберпреступности, таким как создание программного обеспечения для вирусов-вымогателей, которые не были предусмотрены в момент принятия положения.

172. Япония подчеркнула, что даже при наличии надежной нормативно-правовой базы неспособность правоохранительных и судебных органов ее применять стала бы серьезным препятствием для любых усилий по борьбе с киберпреступностью. В этой связи ключевую роль играет способность правоохранительных органов выявлять и расследовать преступления и собирать электронные доказательства. Судебные органы должны также разбираться в способах совершения киберпреступлений и надлежащим образом оценивать электронные доказательства в целях принятия правильных решений относительно приемлемости и достоверности таких доказательств. По мнению Японии, на уровне международного сообщества по-прежнему наблюдается дефицит усилий по наращиванию потенциала и оказанию технической помощи нуждающимся в этом государствам-членам.

173. Япония сообщила, что она осуществляет программы наращивания потенциала для нуждающихся в этом стран, в частности учебные программы для конкретных стран, в том числе проводимые Японским агентством международного сотрудничества, Азиатским и дальневосточным институтом по предупреждению преступности и обращению с правонарушителями, а также в рамках диалога по вопросам киберпреступности между Японией и Ассоциацией государств Юго-Восточной Азии (АСЕАН). Общей задачей является предоставление странам — получателям помощи возможности самостоятельно и последовательно продолжать свои усилия по укреплению потенциала. В этой связи начиная с 2006 года правительство Японии в сотрудничестве с Глобальным инновационным комплексом Интерпола оказывает странам необходимую помощь для поощрения их собственных усилий по наращиванию потенциала.

174. Япония подчеркнула необходимость продолжения дискуссии экспертов и особо отметила, что наиболее эффективный способ выявления проблем, связанных с законодательством и недостатком потенциала для оказания технической помощи в борьбе с киберпреступностью, заключается в том, чтобы прислушиваться к мнениям и опыту экспертов. Эксперты могут представить актуальное положение дел в области киберпреступности, принимая во внимание ее меняющийся характер, а также новые и возникающие проблемы. Дискуссии между экспертами позволят лучше понять масштабность этой проблемы, с тем чтобы определить, на чем именно международное сообщество должно сосредоточить свои усилия.

175. Япония упомянула Группу экспертов для проведения всестороннего исследования проблемы киберпреступности в Вене, в работе которой принимают участие соответствующие эксперты из разных стран мира и которая является идеальным местом для обсуждения и определения последних тенденций, проблем и дальнейших действий. В настоящее время Группа экспертов обсуждает соответствующие темы на ежегодной основе в соответствии с многолетним планом работы, который был принят на основе консенсуса всех государств-членов. Ожидается, что Группа будет продолжать свою работу и проведет анализ достигнутых результатов в 2021 году. Это мероприятие позволит международному сообществу выявить многочисленные проблемы, а также наметить шаги, которые необходимо предпринять. Любое обсуждение вопроса о киберпреступности должно быть основано на конкретной и обоснованной информации, полученной от экспертов. Таким образом, результаты работы Группы экспертов следует рассматривать в качестве основы для будущих обсуждений. Правительство Японии твердо убеждено в том, что обсуждение киберпреступности должно осуществляться в рамках деятельности Группы экспертов в Вене. Иными словами, любые действия, которые будут препятствовать усилиям Группы экспертов, например перенос обсуждения киберпреступности из Вены в рамки форума, участие в котором принимает ограниченное число экспертов,

серьезно ослабит способность международного сообщества противостоять киберпреступности.

Иордания

176. Иордания перечислила следующие основные проблемы, связанные с борьбой с использованием информационно-коммуникационных технологий в незаконных или преступных целях:

a) наличие бесплатного программного обеспечения и программ, скрывающих личности пользователей и затрудняющих их отслеживание и обнаружение;

b) доступность и простота получения информации и возможность приобретения знаний и опыта в использовании инструментов криминального характера на множестве бесплатных и общедоступных веб-сайтов;

c) даркнет, создающий благодатную почву для незаконной деятельности, включая наем лиц для совершения убийств, незаконный оборот наркотиков, торговлю людьми и эксплуатацию детей, что делает мониторинг и наблюдение за такими веб-сайтами и пользователями сложной задачей ввиду использования шифрования для предотвращения установления личности пользователей;

d) медлительность процедур и обмена информацией в связанных с киберпреступностью делах, имеющих место в нескольких юрисдикциях, особенно с учетом того, что борьба с киберпреступностью требует оперативных процедур и взаимодействия;

e) отсутствие реакции и сотрудничества в отношении обмена информацией с правоохранительными органами со стороны некоторых социальных медиаплатформ;

f) необходимость укрепления потенциала с помощью международных учебных программ и обмена опытом с развитыми странами по вопросам киберпреступности.

Ливан

177. Ливан сообщил, что 2018 год оказался напряженным с точки зрения борьбы с использованием информационных технологий в преступных целях на уровне исполнительной власти, парламента и судебных органов. В Глобальном индексе кибербезопасности Международного союза электросвязи (МСЭ) за 2018 год Ливан занял 124-е место в мире, а показатель пользования интернетом составил 65 (Индекс развития ИКТ МСЭ за 2017 год).

178. Правительство Ливана придает вопросу кибербезопасности большое значение. В заявлении министров прямо упоминалось совершенствование процедур и мер по защите киберпространства и информационной инфраструктуры Ливана и персональных данных физических и юридических лиц, которым правительство намерено заняться в связи с реализацией проекта электронного правительства под названием «Цифровое правительство». В новый состав правительства включено новое министерство (Государственное министерство по вопросам технологий).

179. Кроме того, в конце 2018 года премьер-министр принял решение о формировании национальной группы по вопросам кибербезопасности с участием представителей министерств и соответствующих ведомств. Этой группе было поручено разработать национальную стратегию обеспечения кибербезопасности в Ливане и создать национальный орган для решения этих вопросов. Разрабатываемая национальная стратегия включает пять ключевых аспектов. Ра-

бота над планом началась 15 ноября 2018 года, сразу после подготовительного периода, и должна была завершиться в течение следующих двух месяцев.

180. Ливан также сообщил, что парламентские комитеты, в том числе Комитет по информационным технологиям и Комитет по информации и коммуникации, провели несколько парламентских сессий для оценки нынешней ситуации и вынесения рекомендаций.

181. На законодательном уровне 10 октября 2018 года был издан Закон № 81/2018 об электронных сделках и защите персональных данных, который вступил в силу 17 января 2019 года. Он охватывает многочисленные однородные вопросы, в том числе касающиеся защиты персональных данных и борьбы с преступлениями, связанными с информационными системами и данными. Закон также содержит новую редакцию некоторых положений Уголовного кодекса о киберпреступлениях. Кроме того, закон регулирует вопросы, касающиеся электронных доказательств, и обязывает поставщиков услуг интернета хранить клиентские файлы журналов регистрации в течение трех лет.

182. Ливан сообщил также, что в рамках проекта CyberSouth, который осуществляется совместно с Министерством юстиции и при поддержке Совета Европы и Европейского союза, 20 судей прошли подготовку по работе с электронными доказательствами. На момент представления национального ответа Министерство юстиции готовило нормативные акты для имплементации Закона № 81/2018.

183. Ливан упомянул следующие проблемы, с которыми сталкивается Министерство юстиции в частности и государство в целом:

a) отсутствие нормативных актов, необходимых для введения в действие Закона № 81/2019;

b) двусмысленность или недостаточность некоторых правовых норм, содержащихся в Законе № 81/2018, особенно в части защиты личных данных и учреждения специального судебного органа для ускоренного рассмотрения срочных вопросов, при том что не предусмотрено создание органа для проверки предоставления обязательных данных лицами, занимающимися электронной торговлей (статья 31), или же в отношении защиты от рекламных объявлений (статья 32);

c) отсутствие опыта у всех судей, занимающихся электронными преступлениями или электронными доказательствами, а также необходимость развития потенциала судей и служб безопасности и предоставления им необходимой подготовки и оборудования, позволяющих им конкурировать с возможностями и техническим потенциалом преступников;

d) отсутствие цифровых технологий в судах и необходимость обеспечения их связи со всеми взаимодействующими с ними министерствами и учреждениями;

e) необходимость принятия национальных стратегий и политики в области кибербезопасности на национальном уровне и создания национальных учреждений для осуществления этой политики и стратегий;

f) затруднения с соблюдением процедур Общего регламента Европейского союза по защите данных, не позволяющие сотрудникам судебной полиции получать прямой доступ к IP-адресам, которые ранее были доступны;

g) слабые стороны стандартных систем, используемых поставщиками услуг, таких как сетевая система трансляции сетевых адресов (NAT) для IP-адресов, которую использует Министерство коммуникаций;

h) наличие у преступников возможности скрывать свою личность путем использования специального программного обеспечения (VPN, TOR и т.д.), сложности с определением их фактического местонахождения и использование преступниками методов шифрования для сокрытия своих операций. Все это

мешает компетентным службам безопасности осуществлять расшифровку и раскрытие информации и данных, которые используют преступники для своих фактических и запланированных преступлений;

i) многочисленные устройства, имеющие прямой доступ к информационным технологиям и интернету, где почти любое устройство (холодильник, автомобиль и т.д.) может подключиться к сети на основе технологии интернета вещей, не учитывая вопрос о системах защиты, что требуется до выпуска этих устройств на рынок;

j) отсутствие стратегического плана цифровых преобразований в Ливане и плана его осуществления;

k) отсутствие утвержденных стандартов информационной безопасности и общепризнанной политики в различных департаментах и государственных учреждениях;

l) неспособность обеспечить распространение культуры осведомленности членов общества о кибербезопасности и способах защиты персональной информации и данных, а также о рисках хакерства и хищения и способах внедрения передового опыта и защиты такой информации и данных;

m) существование даркнета — сети, позволяющей преступникам незаконно продавать и покупать товары и вещества и осуществлять тайную преступную деятельность, в частности торговлю наркотиками, продажу оружия и обмен детской порнографией, вредоносными программами и персональными данными отдельных лиц;

n) существование виртуальных и цифровых валют, позволяющих отдельным лицам и террористическим группам покупать и продавать незаконные вещества конфиденциальным образом без возможности отслеживания источников таких средств или предметов, которые были переданы им;

o) отсутствие рамочной структуры международного сотрудничества (конвенция, договор) для обмена информацией между государствами в отношении цифровых доказательств и борьбы с киберпреступностью;

p) необходимость согласованных усилий и обмена информацией между различными службами безопасности и учреждениями государственного и частного секторов;

q) замедленное информационное взаимодействие с местными и международными поставщиками услуг;

r) отсутствие учета части киберпреступлений, особенно вызывающих некоторое смущение, таких как преступления, связанные с сексуальными домогательствами и вымогательством;

s) использование преступниками сложных методов, таких как «распределенные атаки», путем осуществления атак с использованием множества серверов по всему миру либо использование некоторых ранее взломанных «умных» устройств в качестве платформы для совершения нападений на другие цели.

Лихтенштейн

184. Лихтенштейн отметил, что масштабы киберпреступности растут и перед международным сообществом стоит широкий круг различных проблем, в том числе в области расследования случаев такой преступной деятельности и судебного преследования за их совершение. По мнению Лихтенштейна, наиболее серьезными проблемами в настоящее время являются фишинг, «директорское мошенничество», захват почтовых ящиков и незаконный перехват данных. Эти проблемы требуют принятия исполнительной и законодательной властью жестких ответных мер на национальном уровне и расширения сотрудничества

на международном уровне. Однако Лихтенштейн обеспокоен тенденциями регулирования киберпространства, а также криминализации киберпреступлений, их расследования и судебного преследования за их совершение способами, ущемляющими права и основные свободы человека, включая право на неприкосновенность частной жизни. Лихтенштейн отметил, что обязательства государств по международному праву, в частности в области прав человека, должны выполняться при любых обстоятельствах, в том числе при регулировании киберпространства, а также криминализации киберпреступлений, их расследовании и судебном преследовании за их совершение.

185. Лихтенштейн сообщил, что его национальное законодательство о киберпреступности основано на Конвенции Совета Европы о киберпреступности. Во время проведения последних масштабных пересмотров Уголовного кодекса Лихтенштейна в 2009 и 2011 годах Конвенция являлась основным международным стандартом для введения новых положений, касающихся кибербезопасности. Лихтенштейн ратифицировал Конвенцию в 2016 году, и она продолжает служить основой для будущих изменений законодательства.

186. Лихтенштейн выразил поддержку укреплению международного права, направленному на регулирование деятельности в киберпространстве, на основе принципов прозрачности, открытости и сотрудничества и в полном соответствии с существующими нормами в области прав человека. Конвенция Совета Европы о киберпреступности была ратифицирована государствами из всех регионов и в значительной мере способствует сотрудничеству между государствами путем согласования законов, разработки процессуальных норм и создания контактных центров. Лихтенштейн выразил поддержку расширению международного сотрудничества на основе Конвенции и высказался против разработки параллельных или отличающихся нормативных стандартов в области борьбы с киберпреступностью, подтвердив позицию, которую он занял, в том числе в отношении других проблем, проголосовав против резолюции 73/187 Генеральной Ассамблеи.

Малайзия

187. Малайзия отметила, что киберпреступность стала более сложной в результате развития технологий, таких как интернет вещей, облачные вычисления, искусственный интеллект, а также услуг, таких как многослойный маршрутизатор и даркнет. Эти технологии — палка о двух концах: они приносят пользу не только государствам и правительствам, но и лицам, совершающим определенные преступления. В результате у правительств возникает больше проблем в процессе противодействия использованию информационно-коммуникационных технологий в преступных целях.

188. Малайзия отметила, что киберсреда дает определенные преимущества лицам, совершающим преступления, благодаря элементам анонимности и возможности использования псевдонимов и затрудняет для правоохранительных органов процесс выявления преступлений и определения конкретных лиц, виновных в их совершении. Широкое использование шифрования, которое приносит огромную пользу в деле обеспечения конфиденциальности и целостности данных, также создает проблемы для правоохранительных органов с точки зрения сбора доказательств в отношении киберпреступлений. Кроме того, преступники используют преимущества технологий для осуществления своей преступной деятельности. Наконец, в интернете существует множество приложений и инструментов, в том числе предназначенных для защиты от судебной экспертизы, которые можно свободно загрузить и использовать в преступных целях.

189. Кроме того, Малайзия отметила, что в результате появления, например, облачных вычислений преступники получили возможность хранить информацию в облачной среде. Сам характер облачных вычислений создает новые про-

блемы для правоохранительных органов с точки зрения обнаружения и получения цифровых доказательств. Обнаружение и получение цифровых доказательств с удаленных облачных платформ, управляемых поставщиком услуг, существенно отличается от их обнаружения на месте преступления или вблизи него. Таким образом, для получения данных из облачной среды требуются иные инструменты, методы и подходы.

190 По мнению Малайзии, необходимо решать проблемы, с которыми сталкиваются сотрудники, участвующие в обработке цифровых доказательств и занятые обеспечением сохранности доказательств и всеобъемлющих процессов и соответствующей инфраструктуры для повышения уровня приемлемости доказательств в суде. Особую значимость имеет техническая компетентность лиц, участвующих в обработке цифровых доказательств, поскольку это позволяет избежать ущерба и нарушения целостности доказательств. Например, правоохранительные органы и органы прокуратуры сталкиваются с проблемами не только в плане удержания имеющихся экспертов, но и в плане получения новых сил и средств для расследования киберпреступлений. Кроме того, необходимо повышать квалификацию и компетентность судей и прокуроров, а также расширять их знания об основах информационно-коммуникационных технологий и кибербезопасности, включая терминологию, связанную с компьютерными и сетевыми системами. Таким образом, судьям и прокурорам необходима специальная подготовки в области кибербезопасности, киберпреступности и интернет-технологий.

191. По мнению Малайзии, электронные доказательства крайне нестабильны и могут быть легко изменены или удалены. Следовательно, фактор времени играет при сборе доказательств определяющую роль. Малайзия сообщила также, что еще одной проблемой, с которой сталкиваются национальные власти, является кадровый дефицит в правоохранительных ведомствах. В некоторых правоохранительных ведомствах отсутствуют даже специальные подразделения по расследованию киберпреступлений. Электронные доказательства, как правило, находятся на объектах инфраструктуры, принадлежащих частному сектору, а именно телекоммуникационным компаниям и поставщикам услуг интернета, чьи возможности в плане сбора и сохранения цифровых доказательств неодинаковы.

192. Как подчеркнула Малайзия, в ходе расследования киберпреступлений правоохранительным органам необходимо получать цифровые доказательства из-за рубежа по официальному каналу взаимной правовой помощи, чтобы эти доказательства были приемлемыми для судебного разбирательства. Сроки получения ответов в рамках такой помощи могут оказаться очень долгими, что может затянуть судебное разбирательство. Кроме того, запросы о представлении доказательств за пределами юрисдикции по-прежнему обусловлены обоюдным признанием соответствующего деяния преступлением.

193. Малайзия упомянула также о другой проблеме, с которой сталкивается правительство в борьбе с неправомерным использованием преступниками информационно-коммуникационных технологий: необходимо добиться, чтобы закон обеспечивал адекватную реакцию на современные высокотехнологичные методы совершения киберпреступлений. Кроме того, Малайзия подчеркнула, что, согласно ее внутреннему законодательству, разработчики документов обязаны проверять свои источники информации или удостоверять подлинность доказательств в суде. Однако нежелание некоторых свидетелей, таких как глобальные поставщики услуг, предоставить доказательства подлинности документа или сведения об источнике информации для дачи показаний в суде, приводило к прекращению судебного преследования.

Монголия

194. Монголия подчеркнула, что за последнее десятилетие масштабы использования интернета быстро росли благодаря улучшению качества услуг, увеличению скорости и расширению охвата. Как следствие, с каждым днем растет число преступлений и нарушений, связанных с интернетом. Физические лица и коммерческие структуры нередко подвергаются атакам со стороны иностранных преступных групп, использующих интернет-платформы.

195. Монголия указала на три основных элемента в борьбе с киберпреступностью: мониторинг интернета и цифровое отслеживание, аналитическая работа и международное сотрудничество. Необходимо наращивать потенциал борьбы с киберпреступностью и соблюдать международные стандарты борьбы с преступностью такого рода.

196. Монголия заявила о необходимости уделять особое внимание киберпреступности, включающей различные кибератаки, финансовые пирамиды, фишинг, незаконную торговлю через интернет, сетевые угрозы, аферы с картами, мошенничество в интернете, детскую порнографию и совершаемые с использованием интернета преступления против прав интеллектуальной собственности.

197. Как сообщила Монголия, по своей структуре и организации подразделения по борьбе с киберпреступностью других государств делятся на три группы: a) борьба с киберпреступностью, направленная против компьютеров, сетей и систем; b) борьба с киберпреступностью с использованием компьютеров, сетей и систем; c) отслеживание, укрепление и изучение цифровых следов. Однако на национальном уровне в стране не хватает людских ресурсов для борьбы с киберпреступностью, в связи с нежеланием наращивать потенциал и людские ресурсы в этой области. Например, в Российской Федерации существует специальная школа сетевой безопасности, целью которой является подготовка кадров для дальнейшей борьбы с киберпреступностью. Монголия в настоящее время не располагает специализированным учреждением для подготовки будущих кадров для борьбы с киберпреступностью. Монголия подчеркнула, что, таким образом, в будущем для борьбы с такими преступлениями при содействии и сотрудничестве со стороны стран, которые играют ведущую роль в борьбе с киберпреступностью, необходимы будут профессиональная подготовка и наращивание потенциала будущих кадров и, кроме того, регулярное обучение и подготовка действующих сотрудников, чтобы они обладали достаточными возможностями для борьбы с киберпреступностью.

198. Монголия также заявила, что IP-адреса играют решающую роль в расследовании киберпреступлений и кибернарушений. Вместе с тем по соображениям финансового, технологического и программного характера поставщики услуг интернета в Монголии предоставляют один IP-адрес многим пользователям, что затрудняет определение точной даты и времени совершения действий. Таким образом, довольно сложно отследить человека, совершившего киберпреступление или кибернарушение. Чтобы получить соответствующую лицензию от Комиссии по регулированию связи, поставщики услуг интернета обязаны иметь технические возможности, позволяющие обеспечить совместное пользование IP-адресом не более чем для 20 человек. Однако Монголия считает осуществление этого положения неадекватным и неэффективным. Таким образом, быстрое расследование киберпреступлений почти невозможно без решения проблемы, касающейся IP-адресов.

199. Кроме того, Монголия подчеркнула, что необходимо уточнить некоторые понятия, используемые в Уголовном кодексе. Например, дополнительных разъяснений требуют такие понятия, предусмотренные статьей 26 Уголовного кодекса Монголии, как «электронные устройства», «защищенные сети» и «незаконные нападения»; их использование на практике затруднено в связи с отсутствием разъяснения или толкования этих понятий в других законах и законодательных актах. Правила и положения других государств в отношении кибер-

преступности носят весьма всеобъемлющий характер. Элементы такого преступления, предусмотренные Уголовным кодексом, вполне очевидны; таким образом, нет места для недоразумений или неверного толкования соответствующих статей.

200. Граждане Монголии используют главным образом созданные на базе интернета социальные платформы, такие как Facebook, Twitter, Instagram и Yahoo!; все они зарегистрированы в качестве корпораций в соответствии с законами и нормативными актами различных государств. Поэтому национальные власти не могут получить документы, необходимые для расследования киберпреступлений, от структур, зарегистрированных за рубежом. Существует договор о сотрудничестве между органами полиции Монголии и Соединенных Штатов, касающийся запроса о предоставлении документов. Тем не менее, согласно законодательству Соединенных Штатов, для получения соответствующих документов необходимо получить судебный приказ о предоставлении этих документов, что делает сотрудничество невозможным.

201. По мнению Монголии, существует необходимость принятия национальной программы борьбы с киберпреступностью. Приняв такую программу, можно будет поэтапно и устойчиво осуществлять политические меры по борьбе с киберпреступностью. Монголия могла бы улучшить текущее состояние нормативных актов, касающихся киберпреступности, и создать специализированное подразделение по борьбе с такими преступлениями.

202. В нынешнюю эпоху, отличающуюся быстрым развитием информационных технологий, крайне важно повышать национальную кибербезопасность и бороться с киберпреступностью. В Глобальном индексе кибербезопасности МСЭ за 2018 год Монголия занимала 84-е место. По мере развития информационных технологий киберпреступность приобретает более сложный характер, включая появление новых видов преступлений. Полностью ликвидировать киберпреступления, совершаемые в интернете, невозможно. Тем не менее, используя соответствующие законы и нормативные акты, Монголия способна реагировать на них путем как предотвращения, так и пресечения.

203. Кроме того, Монголия заявила, что основными причинами появления жертв киберпреступности являются неосведомленность общественности об опасности, а также отсутствие соответствующих знаний, новостей и предупреждений о киберпреступности. Поэтому Монголия подчеркнула необходимость укрепления потенциала и расширения осведомленности о потенциальных опасностях киберпреступности в интернете. Важно обеспечить строгое соблюдение технических требований, следить за осуществлением соответствующих положений, решать краткосрочные проблемы с IP-адресами и другие проблемы, а также повышать ответственность поставщиков услуг интернета в целях предупреждения, пресечения, выявления киберпреступности и борьбы с ней.

204. Монголия отметила, что нынешняя ситуация явно свидетельствует о том, что для предотвращения таких преступлений и борьбы с ними необходима хорошая подготовка сотрудников правоохранительных органов. Поэтому для борьбы с киберпреступностью крайне важно обеспечить подготовку и обучение сотрудников, а также укрепление потенциала таких учреждений всеми возможными способами. Необходимо также создать лабораторию, ответственную за выявление, укрепление, проведение исследований и анализ цифровых следов, и увеличить количество подразделений по борьбе с киберпреступностью.

205. По мнению Монголии, существует необходимость создания международно-правового инструмента для противодействия преступлениям, связанным с информационно-коммуникационными технологиями, и борьбы с ними.

Марокко

206. Марокко отметило, что современный мир переживает революцию в сфере информационно-коммуникационных технологий, включая высокопроизводительные компьютеры и разработанные крупнейшими компаниями программы обработки информации. Влияние на этот процесс оказали глобализация и простота передачи информации, что привело к сокращению расхождений между правовой и судебной системами. Эти элементы глобализации привели к глобализации преступности, а также способов совершения преступлений. Несмотря на преимущества информационных технологий, они сопровождаются рядом серьезных негативных последствий, возникающих в результате их неправомерного использования и отклонения от намеченных целей, главным образом путем посягательств на фундаментальные ценности и интересы отдельных лиц, учреждений и государств. Возник ряд преступлений, совершаемых с использованием интернета и электронных средств массовой информации, что, в свою очередь, упрощает их совершение и позволяет избежать осуществления правосудия (с точки зрения установления как личности, так и местонахождения преступников).

207. Согласно данным расследований, проведенных децентрализованными службами судебной полиции в этой связи, Марокко сообщило, что проблемы при реагировании на киберпреступность в основном связаны с:

a) анонимностью: использование посредников и даркнета;

b) транснациональным характером: хранение доказательств на серверах, расположенных за пределами национальной территории;

c) частым использованием шифрования данных;

d) использованием криптовалюты в преступных целях;

e) постоянным изменением используемых способов деятельности;

f) трудностями в доступе к данным о передвижении пользователей определенных приложений или сайтов, находящихся за границей;

g) планированием постоянной подготовки в области борьбы с киберпреступностью для персонала, участвующего в расследовании киберпреступлений и сборе цифровых доказательств, чтобы не отставать от стремительного развития технологий;

h) приобретением соответствующих и эффективных специальных аппаратных средств и программного обеспечения для расследования киберпреступлений;

i) необходимостью охвата пользователей информационно-коммуникационных технологий программой повышения осведомленности о рисках несоблюдения мер защиты;

j) введением в действие механизмов защиты от киберугроз и реагирования на них на уровне Содружества Независимых Государств;

k) межгосударственным сотрудничеством и координацией при уточнении правовых вопросов и осуществлении соответствующего законодательства, а также в процессе деятельности следственных органов и эффективного проведения расследования с использованием цифровых доказательств.

208. Марокко напомнило о том, что международное сообщество отреагировало на киберпреступность с помощью нормативных документов, приняв соответствующие конвенции, и организовало многочисленные конференции. В силу своего стратегического положения Марокко пришлось также принять законодательство в отношении такого явления, как информатика, и установить партнерские отношения, прежде всего с Европейским союзом, которые оказались весьма полезными.

209. Законодательный орган Марокко принял уголовное законодательство, учитывающее особенности использования информационно-коммуникационных технологий в преступных целях и соответствующее общим принципам уголовного правосудия. Это законодательство включает Закон № 03.07 о контроле автоматизированных систем обработки данных, принятый в 2003 году в рамках Уголовного кодекса (разделы с 3/607 по 11/607). Этот закон служит основой для борьбы с киберпреступностью в Марокко, и его положения разработаны на основе международных конвенций, в первую очередь Конвенции Совета Европы о киберпреступности и Дополнительного протокола к ней, в соответствии с опубликованным 12 мая 2014 года Королевским указом № 1.14.85 о введении в действие Закона № 136.12 об одобрении Конвенции о киберпреступности. Также он был основан на проекте закона о руководящих указаниях по борьбе с преступлениями в области информационных технологий.

210. Марокко также одобрило Арабскую конвенцию о борьбе с преступлениями в области информационных технологий, подписанную в Каире 21 декабря 2010 года, в соответствии с Указом № 46.13.1 от 13 марта 2013 года о введении в действие Закона № 12.17, опубликованного в «Официальном вестнике» № 6140 от 4 апреля 2013 года.

211. Статья 3 Закона № 108.13 о военной юстиции предусматривает определенные требования, касающиеся преступлений, которые подпадают под юрисдикцию военного суда, что позволяет этому суду также выносить приговоры по делам о киберпреступлениях.

212. Превентивные законы, направленные на защиту персональных данных или электронного обмена данными, такие как Королевский указ № 1.07.129 от 30 ноября 2007 года о введении в действие Закона № 53.05 об электронном обмене правовыми данными и Королевский указ № 1.09.15 от 18 февраля 2009 года о введении в действие Закона № 09.08 о защите персональных данных, делают Марокко привлекательным направлением для инвестиций в сферу информационных технологий и цифровой экономики.

213. Согласно Закону № 96-24 о корреспонденции и сообщениях, введенному в действие Королевским указом № 1.97.162 от 1 августа 1997 года с внесенными в него изменениями и дополнениями, и Указу № 444-08-2 от 21 мая 2009 года был создан национальный совет по медийным технологиям и цифровой экономике, которому была поручена координация национальной политики и оценка ее реализации.

214. В статьях 187, 448/1 и 448/2 проекта закона об организованной информационной преступности также предусмотрено множество инструментов для реагирования на этот вид преступности.

215. На институциональном уровне была создана целевая группа судебной полиции для борьбы с киберпреступностью. В рамках национального аппарата безопасности Марокко были созданы два антитеррористических подразделения для борьбы с преступлениями, связанными с информационными системами, на уровне как расследования, так и розыска преступников через интернет. Министерство национальной обороны создало Управление по вопросам киберпреступности для расследования киберпреступлений, отслеживания их последствий и борьбы с ними во взаимодействии с различными департаментами национальной и международной безопасности.

216. Марокко подчеркнуло, что, несмотря на эти усилия, в борьбе с этим видом преступности все еще существует множество проблем. Законодательству трудно реагировать на быстрое развитие киберпреступности; например, отсутствует правовая база для борьбы с преступлениями, совершаемыми с использованием социальных сетей. Большинство действующих правовых норм касаются пользователей социальных сетей и не содержат каких-либо требований, устанавливающих ответственность поставщиков сетевых услуг и обязывающих их удалять, блокировать, приостанавливать или закрывать доступ к незаконно-

му электронному контенту. Эта ситуация усугубляется тем, что большинство этих поставщиков и управляющих этими платформами находятся за пределами юрисдикции страны.

217. Марокко обратило особое внимание на то, что международное сотрудничество в борьбе с киберпреступностью также представляет собой проблему с точки зрения взаимодействия с поставщиками телекоммуникационных услуг в других юрисдикциях, что требует принятия международного документа, допускающего прямое сотрудничество с поставщиками услуг в других юрисдикциях в целях обеспечения трансграничного взаимодействия для передачи данных.

218. С другой стороны, Марокко подчеркнуло также, что борьба с киберпреступностью ставит еще более масштабную задачу в части укрепления потенциала правоохранительных органов. Масштабное и непрерывное совершенствование методов совершения киберпреступлений, в частности преступлений, связанных с использованием интернета, кибератак, фишинговых атак, электронного фишинга, доступа к интернету, виртуальных валют, облачных вычислений и криптографии, требует от следственных органов изменения их стратегий поиска и расследования уголовных преступлений и предоставления электронного справочника, приемлемого и достоверного с точки зрения судебной системы.

Мьянма

219. Мьянма отметила, что борьба с киберпреступностью имеет жизненно важное значение для национальной кибербезопасности и защиты национальной информационной инфраструктуры. Существует настоятельная необходимость разработки надлежащего национального законодательства, отвечающего международным стандартам, в целях достижения максимальной эффективности в деле борьбы с киберпреступностью. Правоохранительные органы следует обеспечить правовыми документами, техническими средствами и инфраструктурой, а также надлежащими полномочиями, которые необходимы для проведения эффективного расследования и успешного судебного преследования.

220. Кроме того, Мьянма подчеркнула, что поиск стратегий и возможностей устранения угрозы киберпреступности является серьезной проблемой для развивающихся стран. Что касается территориальных различий, владельцы вебсайтов, содержащих незаконный контент, перемещают свою деятельность в страну, где уголовная ответственность за противоправный контент не предусмотрена, с тем чтобы избежать проведения уголовных расследований. Такое перемещение деятельности в зарубежные страны является одной из проблем для правоохранительных органов, поскольку сервер находится за пределами территории страны. Преступники в полной мере пользуются такими территориальными различиями, используя для распространения, распределения, обмена и хранения незаконного контента и непристойных изображений не местные жесткие диски, а внешний сервер, доступ к которому они могут получить через интернет. Таким образом, международное сотрудничество имеет исключительно важное значение для выявления правонарушителей и преодоления трудностей, возникающих в результате территориальных различий. При принятии национальной политики в области кибербезопасности и формировании соответствующей нормативно-правовой базы необходимо принимать во внимание как согласованность с действующими национальными законами, так и степень соответствия международным стандартам.

221. Мьянма сообщила о следующих проблемах, с которыми государство сталкивается при разработке политики в области кибербезопасности и последующих правовых документов.

a) Необходимо принять всеобъемлющую национальную политику и надлежащее законодательство по борьбе с киберпреступностью, совместимые с

международными нормами и процедурами. Государству необходимо привести свои стратегии обеспечения кибербезопасности и борьбы с киберпреступностью в соответствие с международными стандартами.

b) Тщательный анализ действующих национальных законов имеет исключительно важное значение для выявления любых возможных пробелов и совпадений в законодательстве о киберпространстве и других законодательных актах. Подробное изучение соответствующего законодательства требует длительного времени, а также применения высоких профессиональных стандартов и рассмотрения понятий, основанных на международной практике и обмене мнениями.

c) Для согласования интересов национальной безопасности и верховенства права с основополагающими правами граждан необходимо создать правоохранительное ведомство. Одновременно с этим должен быть создан центр правомерного перехвата сообщений для осуществления контроля за коммуникациями путем использования стандартных оперативных процедур правомерного перехвата, основанных на международных принципах и стандартах в области защиты данных и гарантий неприкосновенности частной жизни.

d) Необходимо создать группы реагирования на киберинциденты и кибератаки (т.е. группы реагирования на критические ситуации в компьютерных сетях, группы реагирования на компьютерные сбои, группы реагирования на инциденты, связанные с компьютерной безопасностью), обладающие достаточной квалификацией для урегулирования кибернетических кризисных ситуаций и оценки угроз и факторов уязвимости. Предполагается, что эти группы будут заниматься распространением информации по вопросам безопасности и предоставлением консультаций по безопасности в связи с киберинцидентами, киберрисками и кибератаками и потенциальными рисками таких кибератак для общественности, а также оказанием поддержки правоохранительным органам путем предоставления необходимой технической помощи для эффективного проведения расследований.

e) Государству следует ассигновать средства для осуществления технических мер защиты в целях создания надежного и безопасного интернета, а также для обеспечения сетевой безопасности и гарантий, в том числе путем предоставления инфраструктуры, средств и оборудования, необходимых для осуществления таких мер защиты и деятельности по обеспечению безопасности.

f) В процессе адаптации национальной нормативно-правовой базы по киберпространству в целях регулирования уголовных расследований важно принимать во внимание гарантии защиты прав человека при использовании персональных данных.

g) Представителям частного сектора, участвующим в сборе, хранении или совместном использовании данных пользователей, необходимы четкие и ясные стандарты в области защиты данных и гарантий неприкосновенности частной жизни.

h) Пользователям интернета следует предоставлять четко структурированную информацию о кибербезопасности, характере и видах киберпреступлений и сложной и неоднозначной ситуации кибератак. Кроме того, необходимо поддерживать проведение кампаний, направленных на повышение осведомленности и подготовку пользователей, а также повышать уровень цифровой грамотности, особенно в случаях, когда объединенные в глобальную сеть информационно-коммуникационные технологии подвергаются локализации для национальных пользователей.

222. В Мьянме нередко встречаются случаи мошенничества и клеветы в интернете. Наиболее часто такие правонарушения в интернете связаны с использованием онлайновых коммуникаций и информации для подстрекательства к беспорядкам на расовой и религиозной почве и угроз в адрес государственных

служащих и организаций. Мьянма в основном сталкивается с использованием социальных сетей для организации террористических актов, пропаганды и личных нападок. При проведении уголовных расследований власти не получают конкретной информации или содействия со стороны поставщиков услуг интернета.

223. Кроме того, Мьянма сообщила о том, что в тех случаях, когда возникала необходимость запросить информацию об абоненте у иностранных операторов социальных сетей, эти компании отказывали в удовлетворении запроса на том основании, что эти запросы не охватываются стандартными процедурами. В связи с этим возникают трудности при проведении расследований.

224. Мьянма также упомянула о многочисленных трудностях в проведении расследований в связи с нехваткой ресурсов для технических специалистов, отсутствием знаний у пользователей интернета и слабостью юридически обязывающего воздействия законов и процедур. В связи с развитием технологий и получением возможности доступа к мобильным банковским услугам с мобильного телефона кибератаки в настоящее время в большей степени ориентированы на пользователей мобильной телефонной связи.

225. Мьянма выразила мнение, что существующих правовых механизмов недостаточно для борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. Сообщалось о происходящей в настоящее время разработке киберзаконодательства и соответствующих стратегий в области электронного правительства, электронной торговли и кибербезопасности, которая осуществляется в рамках проекта под руководством Министерства транспорта и связи с учетом рекомендаций независимой консалтинговой фирмы.

226. Мьянма указала, что, учитывая потребность в международном сотрудничестве, решение проблемы может быть достигнуто путем разработки и принятия конвенции Организации Объединенных Наций.

227. Мьянма согласилась с тем, что для реагирования на использование информационно-коммуникационных технологий в преступных целях требуется постоянное и открытое обсуждение с участием всех заинтересованных государств. Платформой для проведения такого обсуждения могла бы стать рабочая группа открытого состава Организации Объединенных Наций, уполномоченная разрабатывать любые соответствующие документы и принимать решения на основе большинства голосов. Мьянма также выразила согласие и дала высокую оценку тому факту, что Группа экспертов для проведения всестороннего исследования проблемы киберпреступности сосредоточила свое внимание, в первую очередь, на вопросах, касающихся противодействия информационным преступлениям.

Нидерланды

228. Нидерланды отметили, что международное сообщество органов правосудия и охраны правопорядка несет общую ответственность за то, чтобы интернет не превратился в безопасное убежище для преступников и чтобы их преступления не сходили им с рук. Исключительно важное значение для борьбы с киберпреступностью имеют эффективные правовые документы, обеспечивающие уважение основных прав человека. Можно выделить различные категории документов: документы национального, регионального и международного уровней. Во-первых, многие страны укрепили свой внутренний потенциал борьбы с киберпреступностью. Вместе с тем на международном уровне существуют различия в уголовном праве, экспертных знаниях и оборудовании, что осложняет принятие мер в отношении явления, носящего такой трансграничный характер, и противодействие ему. Эта проблему можно решить только путем активизации усилий по наращивания потенциала на внутригосударственном и межгосударственном уровнях. Создав широкую международную сеть

эффективных правоохранительных органов, можно нанести серьезный удар по организованной киберпреступности. Второй тип документов — это документы регионального уровня. Региональными они называются потому, что недоступны странам, находящимся за пределами данного региона. Примерами таких инициатив являются инициатива Европейского союза в области электронных доказательств и рамочные программы Шанхайской организации сотрудничества, межправительственных организаций африканских стран и Лиги арабских государств. В-третьих, существуют международные документы, открытые для стран всего мира. Примерами таких документов являются Конвенция Совета Европы о киберпреступности, участниками которой являются 63 страны (и их количество растет) и которая является типовым законодательством еще для почти 70 государств, и Конвенция об организованной преступности и протоколы к ней. Будучи одним из первых государств, подписавших и ратифицировавших Конвенцию Совета Европы, Нидерланды ощутили на себе преимущества Конвенции с точки зрения получения результатов уголовных расследований благодаря адаптации национального законодательства к расширенным возможностям для сотрудничества с другими государствами-участниками. Нидерланды также особо отметили преимущества участия в Конвенции против организованной преступности.

229. Нидерланды заявили, что наиболее актуальными и неотложными практическими потребностями правоохранительных органов в киберпространстве являются, во-первых, трансграничный доступ к электронным доказательствам и, во-вторых, международное сотрудничество в проведении уголовных расследований. Двустороннего сотрудничества и взаимной правовой помощи недостаточно, когда речь идет о трансграничных и быстро меняющихся видах преступлений. В настоящее время потребность в доступе к электронным доказательствам существует для всех видов преступлений, учитывая использование информационно-коммуникационных технологий, особенно значительного количества новых функций, таких как социальные сети и обмен сообщениями через интернет, что привело к беспрецедентному росту объемов цифровых данных. Достичь укрепления международного сотрудничества можно только в том случае, если правоохранительные органы будут обладать потенциалом и возможностями участия, например, в проведении совместного расследования. Инновационные подходы к трансграничному доступу к электронным доказательствам, такие как распоряжение о предъявлении или расширенный поиск по сети, уже находятся в процессе разработки и обсуждения. Текущие переговоры по дополнительному протоколу к Конвенции Совета Европы о киберпреступности подтверждают общую готовность многих государств адаптировать существующую правовую базу к нуждам действенного упрочения системы уголовного правосудия в киберпространстве.

230. Нидерланды заявили, что важной задачей в рамках противодействия использованию информационно-коммуникационных технологий в преступных целях является обеспечение того, чтобы существующие правовые документы в полной мере реализовали свой потенциал и чтобы и без того скудные ресурсы и энергия не перенаправлялись на осуществление долгосрочного процесса разработки новой наднациональной рамочной концепции. Конвенция Совета Европы о киберпреступности уже является ощутимым результатом, который ежедневно доказывает свою дополнительную ценность. Правоохранительные и судебные органы различных стран — от Соединенных Штатов до Шри-Ланки и от Японии до Сенегала — имеют доступ к различным возможностям, которые предоставляет Конвенция, что приводит к достижению конкретных результатов в проведении уголовных расследований. Дополнительный протокол к Конвенции является уже осуществляющимся шагом в рамках все более необходимых усилий по обеспечению соответствия современным требованиям и последним достижениям науки и технологий.

231. За истекший период прилагались значительные усилия по наращиванию потенциала, но многое еще предстоит сделать, и эта деятельность является

второй важной задачей. Ее можно решать как на двусторонней основе, так и совместно с созданным Советом Европы Управлением по программе в области киберпреступности и УНП ООН. Что касается Организации Объединенных Наций, то Группа экспертов для проведения всестороннего исследования проблемы киберпреступности идеально подходит для создания платформы для обмена мнениями и передовым опытом. Нидерланды сообщили, что в ходе углубленных консультаций, проведенных в течение предыдущего и нынешнего года, Группа экспертов значительно улучшила показатели осуществления своего плана работы на 2017 год. Нидерланды рассчитывают, что этот процесс приведет к появлению в 2021 году более своевременного и актуального обзора проблем в области уголовного правосудия в киберпространстве, а также к выработке рекомендаций на будущее.

232. Нидерланды призвали к тому, чтобы улучшения в работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, отмеченные в 2017 году, стали основой для дальнейшего прогресса, и рассчитывают достичь этого главным образом за счет уделения повышенного внимания технической помощи в целях содействия обмену передовым опытом и наращиванию потенциала во всем мире. Они призвали к участию в текущих переговорах, которые уже доказали свою ценность и дали результаты. Они призывают другие государства не растрачивать ресурсы и энергию, отходя от тематики этих переговоров путем введения новых инициатив.

Новая Зеландия

233. Новая Зеландия отметила, что географически изолированное положение страны исторически защищало ее от некоторых видов угроз. Однако трансграничный характер киберпреступности означает, что удаленность не обеспечивает защиты. К наиболее серьезным проблемам, с которыми столкнулась Новая Зеландия в борьбе с использованием информационно-коммуникационных технологий в преступных целях, относятся:

a) неполнота картины киберпреступности в Новой Зеландии и во всем мире;

b) трудность расчета издержек киберпреступности;

c) трудность выявления, расследования и судебного преследования киберпреступлений;

d) вопросы, возникающие в связи с совместной ответственностью правительства, неправительственных организаций, частного сектора и физических лиц.

234. В отношении борьбы с киберпреступностью Новая Зеландия сообщила, что она уделяет первостепенное внимание разработке соответствующего законодательства, использованию совместного подхода, повышению уровня осведомленности и просвещения и международному сотрудничеству. Информация, представленная для целей настоящего доклада, была получена из Национального плана по борьбе с киберпреступностью (2015 год), размещенного в интернете.

235. Полное представление о явлении киберпреступности отсутствует. Киберпреступность можно отличить от «традиционных преступлений» по проблемам, которые возникают у правоохранительных органов вследствие ее глобального характера. Отдельные лица и группы за пределами государства могут действовать везде, где есть возможность выхода в интернет. Подавляющее большинство преступников находится за пределами государства и очень хорошо организованы. О многих случаях совершения киберпреступлений по всему миру не сообщается. В некоторых случаях потерпевшие даже не знают о том, что они пострадали. Другие жертвы стыдятся сообщить о преступлении, не знают, к кому обращаться, или не верят, что правоохранительные органы могут

защитить их права. Жертвы могут не сообщать о преступлении и в том случае, если их права защитил поставщик услуг или финансовое учреждение. Наконец, компании могут неохотно раскрывать информацию о потерях или нарушениях, опасаясь подрыва репутации.

236. Рассчитать издержки от киберпреступности сложно; затруднительно и дать количественную оценку связанных с киберпреступностью косвенных издержек, включая издержки упущенных возможностей. Для многих малых и средних предприятий киберпреступность может стать препятствием к ведению бизнеса: возможно, ничего не украдено, но атака могла ограничить их возможности вести торговлю. Компании и частные лица также сталкиваются с проблемой затрат на защиту от киберпреступности и (при необходимости) на восстановление. Киберпреступность может также способствовать организации и совершению традиционных преступлений, таких как мошенничество, вымогательство, организация беспорядков, сексуальное и иное насилие. Киберпреступность может привести к причинению социального вреда в результате нарушения душевного равновесия и ощущения беспокойства, а в более серьезных случаях — физического или морального вреда. Хотя финансовые потери от киберпреступности в отдельных случаях могут быть небольшими, последствия для общественного доверия могут с течением времени оказаться разрушительными. Киберпреступность приносит высокую прибыль при низких затратах и относительно низком риске для преступника. Тысячи электронных писем, содержащих спам, могут привести к небольшим потерям для каждой жертвы, но гораздо более значительному ущербу для Новой Зеландии в целом.

237. Обнаружение, расследование и судебное преследование киберпреступлений затруднено. Глобальный характер киберпреступности затрудняет поиск преступника и доступ к соответствующим доказательствам. Обмен информацией и сотрудничество между различными странами могут быть неэффективными, а процессы, происходящие в рамках договора о взаимной правовой помощи, могут быть весьма медленными и обременительными даже при наличии прочных отношений сотрудничества. Для проведения расследования отдельных случаев могут потребоваться непропорционально серьезные усилия, что приводит к сокращению ресурсов, доступных для решения других задач. Страна, в которой находится преступник, также может не располагать необходимым потенциалом для проведения расследования или сохранения доказательств.

238. В еще большей степени проведение расследований осложняется возможностью действовать в интернете практически анонимно. Установить виновника киберинцидента очень трудно, особенно в тех случаях, когда атака осуществляется из-за рубежа. Это делает киберпреступность сложной проблемой не только для расследования, но и для судебного преследования. Преступники могут с успехом использовать прокси-серверы и такие каналы, как Tor и одноранговые сети, чтобы попытаться скрыть свою личность под слоями шифрования. Эти сети зачастую используются для содействия преступной деятельности и создают трудности для правоохранительных органов. Кроме того, в таких сетях и на сайтах даркнета организуется торговля киберпреступностью как услугой, например торговля услугами хакеров по найму или просто наборами инструментов. Все это снижает «порог входа» в сферу киберпреступности. Таким образом, даже действия группы неопытных злоумышленников могут привести к достаточно пагубным последствиям. На другом конце спектра по мере расширения масштабов деятельности и усложнения методов размываются границы между преступными и государственными субъектами (часть из которых могут также действовать с преступными намерениями). По мере развития технологий и стратегий расследования изменяется и поведение злоумышленников, и борцам с преступностью непросто не отставать от них. Правонарушители охотно пользуются технологиями анонимизации, в том числе программным обеспечением, например браузером Tor, чтобы попытаться скрыть сайты с материалами, касающимися эксплуатации детей и торговли наркотиками.

239. В Новой Зеландии обязанности по противодействию киберпреступности распределены между правительством, неправительственными организациями, частным сектором и физическими лицами. Ряд государственных учреждений в Новой Зеландии занимается осуществлением стратегических и оперативных мер реагирования в отношении киберпреступности. Распределение этих функций происходило по большей части естественным образом, а не по расчету. Киберпреступность является общей проблемой, и неправительственные организации, гражданское общество и частный сектор должны играть свою роль в области как предотвращения, так и реагирования на нее. Эта коллективная ответственность может приводить к возникновению проблем. Информация о некоторых происшествиях будет поступать сразу в несколько мест, а пострадавших могут перенаправлять из одного учреждения в другое, чтобы найти наиболее подходящее место для решения проблемы. Также в зависимости от учреждения могут различаться и способы реагирования. Новая Зеландия добилась прогресса в этой области с момента создания в 2016 году Новозеландского правительственного учреждения по кибербезопасности (CERT NZ). CERT NZ позволяет получить более четкое представление о том, куда следует сообщать о киберинцидентах, обеспечивает более эффективное распределение киберинцидентов между соответствующими учреждениями и предоставляет более действенные и своевременные рекомендации ведомствам, компаниям и частным лицам. Многие частные компании также осуществляют противодействие киберпреступности в рамках основного обслуживания клиентов. У правительства есть возможность создать более благоприятные условия для жертв киберпреступности, а также добиться лучшего понимания этой проблемы и повышения осведомленности.

Никарагуа

240. По мнению Никарагуа, существующих положений об уголовной ответственности недостаточно для борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. Многие страны стали жертвами таких преступлений. Поэтому Никарагуа убеждена в том, что Организации Объединенных Наций следует рассмотреть эту тему в целях разработки и утверждения международного соглашения о сотрудничестве и регулировании по этому вопросу.

241. Аналогичным образом, Никарагуа считает целесообразным как можно скорее создать рабочую группу открытого состава в целях ускорения разработки международного нормативного документа в отношении преступлений, совершенных с использованием информационно-коммуникационных технологий.

Норвегия

242. Норвегия сослалась на данные по стране, которые были направлены в УНП ООН 4 марта 2019 года и касались мер и инициатив по борьбе с киберпреступностью в связи с работой Группы экспертов для проведения всестороннего исследования проблемы киберпреступности[8].

243. Норвегия ратифицировала Конвенцию Совета Европы о киберпреступности в 2005 году и внимательно следит за процессом разработки второго дополнительного протокола. Норвегия поддерживает статус Группы экспертов для проведения всестороннего исследования проблемы киберпреступности как основного места решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций, по крайней мере до 2021 года.

[8] Доступно по адресу: www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

244. Норвегия отметила, что по мере нарастания угроз в области киберпреступности необходимо расширять масштабы реагирования на эти вызовы, поскольку отсутствие эффективных мер может представлять собой угрозу для верховенства права. Электронные доказательства приобретают все бóльшую актуальность в уголовных делах. Эти данные часто хранятся за границей, что затрудняет их поиск и получение. Сотрудничество играет важную роль как на национальном, так и на международном уровне. Поскольку правоохранительные органы ограничены национальными границами, необходимы более эффективные международные механизмы. В то же время во главу угла в усилиях по разработке новых международных документов надлежит ставить соблюдение основных прав человека и высокую степень осведомленности о гарантиях.

245. Норвегия подтвердила, что она обеспечит достаточный потенциал, компетенции и технические возможности для борьбы с новыми и постоянно меняющимися видами преступлений. Норвегия отметила, что в рамках работы, ведущейся на национальном уровне, первостепенное внимание уделяется необходимости более глубокого понимания угроз, стоящих перед страной в цифровой сфере. Кроме того, важно рассматривать новые проблемы в контексте более традиционных преступлений. Киберпреступность не является отдельным видом преступности: она представляет собой сквозной элемент многих видов преступлений, в том числе транснациональной организованной преступности и терроризма. Одним из важнейших компонентов решения этой проблемы являются согласованные совместные действия правительств и частного сектора.

246. Норвегия далее подчеркнула, что в соответствии с Международной стратегией кибербезопасности Норвегии (2017 год) норвежские власти обеспечат тесную координацию между органами, представляющими Норвегию на аренах, где вырабатывается международная политика в области кибербезопасности и развивается сотрудничество в области противодействия киберпреступности и нейтрализации киберинцидентов. В рамках дальнейших международных усилий по борьбе с киберпреступностью Норвегия будет поддерживать совместные подходы к поиску эффективных решений, поддерживая демократические ценности и защищая универсальные права человека.

Перу

247. Перу сообщило, что в 2016 году Межамериканский банк развития в сотрудничестве с Организацией американских государств подготовил доклад о кибербезопасности в Латинской Америке и Карибском бассейне за 2016 год. После проведения оценки по 49 показателям, касавшимся различных областей (политика и стратегия, культура и общество, образование, нормативно-правовая база и технологии), для Перу были определены следующие четыре основные задачи:

a) укрепление потенциала вооруженных сил в области киберзащиты;

b) укрепление технических возможностей Отдела по расследованию преступлений в области высоких технологий (DIVINDAT) в области обращения с электронными доказательствами;

c) повышение осведомленности общественности о кибербезопасности;

d) наращивание потенциала преподавателей университетов и проведение учебных курсов для сотрудников компаний.

248. Согласно докладу Microsoft Security Intelligence Report (2017), вредоносным программным обеспечением в Перу были заражены 16,9 процента компьютеров, тогда как среднемировой показатель составил 7,8 процента. Аналогичным образом, уровень заражения троянскими программами (8,13 процента), «червями» (5,7 процента) и вирусами (0,92 процента) в Перу также превышает среднемировой показатель.

249. В недавнем исследовании Секретариат цифрового правительства при Председателе Совета министров Перу указал, что 22,6 процента структур государственного управления не имеют возможности внедрить свою общую систему обеспечения цифровой безопасности. Были названы следующие причины:

a) нехватка экономических ресурсов, необходимых для реализации;

b) нехватка персонала (50,9 процента);

c) отсутствие достаточных знаний для начала реализации (22,6 процента);

d) данный вопрос не является приоритетным для их сектора (16 процентов).

250. Негативное воздействие рисков в области информационной безопасности оказывает серьезное влияние на важнейшие ресурсы организации, вследствие чего организации несут экономические и пассивные издержки. В некоторых случаях основные бизнес-процессы прерываются или останавливаются, когда организации оказываются объектом шантажа или вымогательства крупных денежных сумм за восстановление информации.

251. В качестве приоритетных задач правительство Перу отметило необходимость создания специализированной прокуратуры по компьютерным преступлениям, дополнительной подготовки сотрудников налоговых органов по этому вопросу и создания учреждения, отвечающего за предотвращение киберпреступлений, совершаемых гражданами. Существенно возросло число жалоб на совершение компьютерных преступлений, особенно в форме компьютерного мошенничества. Основные проблемы, которые предстоит решать, заключаются в следующем.

a) Компьютерное мошенничество в виде «кардинга», когда преступные организации используют конфиденциальную информацию с банковских карт для совершения покупок в онлайновом режиме в интернет-магазинах через веб-домены и серверы, расположенные за рубежом. Наличие в каждой стране законов, регулирующих объем информации, который обязана предоставлять каждая компания, в значительной степени затрудняет своевременное получение информации.

b) Хищение личных данных в социальных сетях как следствие свободы, с которой пользователи могут создавать аккаунты и управлять ими анонимно, даже создавая различные имена, используемые незаконно.

c) Склонение детей к развратным действиям, когда криминальные организации притворяются детьми, чтобы побудить своих жертв раздеться перед видеокамерой ноутбука или компьютера. В других случаях проводятся личные встречи, в ходе которых приобретаются материалы о сексуальных надругательствах над детьми для последующей продажи и обмена с другими педофилами на национальном и международном уровнях, в том числе с помощью таких приложений, как WhatsApp.

d) Шантаж и вымогательство со стороны бывших партнеров, связанные с фотографиями или видеоматериалами сексуального характера, которые они угрожают опубликовать в интернете. Цели такого поведения могут быть различными, например получение экономической выгоды или возобновление отношений.

e) Атаки со стороны хакеров-активистов в рамках кампаний, целью которых является воздействие на имидж организации, и использование анонимных сетей, таких как Tor, которые позволяют осуществлять атаки, якобы исходящие из азиатских стран, что делает их идентификацию невозможной. Аналогичным образом, происходят посягательства на имеющуюся у организаций коммерческую информацию, целью которых является получение обширной информации от организаций для последующего использования в преступных

целях. Существует также вероятность использования кибератак или кибершпионажа со стороны средств массовой информации в целях получения доступа к ценным с информационной точки зрения материалам.

Филиппины

252. Филиппины охарактеризовали киберпреступность как серьезную социальную проблему и отметили, что киберпространство считается новым измерением (в дополнение к земле, воздуху и воде), регулированием которого необходимо заниматься правительству, а правоохранительным органам следует расширять свои мандаты для решения возникающих в киберпространстве проблем. В целях обеспечения безопасности и защиты населения правительство признало необходимость предоставления правоохранительным ведомствам соответствующих полномочий на основании следующих законодательных актов: Закона о предупреждении киберпреступности от 2012 года (Закон Республики № 10175), Закона об электронной торговле от 2000 года (Закон Республики № 8792), Закона о запрете вуайеризма и фотографирования от 2009 года (Закон Республики № 9995), Закона о борьбе с детской порнографией от 2009 года (Закон Республики № 9725), Закона о борьбе с торговлей людьми от 2003 года (Закон Республики № 9208), Закона о регулировании использования средств доступа от 1998 года (Закон Республики № 8484) и Закона о конфиденциальности данных от 2012 года (Закон Республики № 10173).

253. Филиппины присоединились к Конвенции Совета Европы о киберпреступности 20 февраля 2018 года и уже удовлетворили международные запросы о сохранении данных, предоставлении абонентской информации о пользователях, сборе компьютерных и коммерческих данных и конфискации доменных имен.

254. В этой связи национальное законодательство рассматривает специализацию в качестве ключа к успешному проведению расследования и судебному преследованию киберпреступников. В соответствии с Законом о предупреждении киберпреступности от 2012 года для борьбы с киберпреступностью и решения связанных с этим вопросов были созданы следующие специализированные органы:

a) Управление по борьбе с киберпреступностью Министерства юстиции: в качестве центрального органа в соответствии с Законом о предупреждении киберпреступности в целях обеспечения осуществления Конвенции Совета Европы о киберпреступности, включая вопросы международной взаимной помощи и экстрадиции;

b) Центр расследования киберпреступлений и координации: межведомственный орган под административным надзором Министерства информационно-коммуникационных технологий в соответствии с Законом Республики № 10844 от 2015 года; отвечает за координацию политики между соответствующими ведомствами, а также за разработку и обеспечение реализации национального плана кибербезопасности;

c) Отдел по борьбе с киберпреступностью Национального бюро расследований: был реорганизован в целях существенного повышения эффективности его усилий по противодействию киберпреступности и наращивания его потенциала в области цифровой криминалистики и кибербезопасности в соответствии с Законом о киберпреступности. Были созданы три региональных центра по борьбе с киберпреступностью, приобретены новые и обновленные инструменты судебной экспертизы и программное обеспечение, а также проведено соответствующее обучение для экспертов в области цифровых технологий;

d) Национальная группа по борьбе с киберпреступностью: создана вместе с девятью региональными отделениями по борьбе с киберпреступно-

стью по всей стране. Были разработаны четыре специализированных курса по противодействию киберпреступности, предназначенные для сотрудников полиции, специализирующихся на борьбе с киберпреступностью.

255. Вооруженные силы Филиппин под руководством заместителя начальника штаба по связи, электронике и информационным системам разрабатывают стратегический план для киберпространства — дорожную карту создания организации, способной полноценно работать в киберпространстве, к 2022 году.

256. Совет по борьбе с отмыванием денег является органом финансовой разведки страны: ему поручено осуществление Закона о борьбе с отмыванием денег с поправками, внесенными в него Законами Республики № 9194, 10167 и 10365, а также Закона Республики № 10168, известного также как Закон о предотвращении и пресечении финансирования терроризма от 2012 года.

257. В январе 2017 года судебная власть также внесла вклад в усилия по борьбе с киберпреступностью, назначив суды по киберпреступности для рассмотрения дел, охватываемых Законом о предупреждении киберпреступности от 2012 года в дополнение к их работе в качестве арбитражных судов.

258. Филиппины сообщили также, что на национальном уровне были созданы следующие межучрежденческие механизмы сотрудничества:

a) Подкомитет по киберпреступности Национального координационного комитета правоохранительных органов, который способствует укреплению межведомственной координации в целях борьбы с киберпреступностью и осуществлению других видов деятельности, связанных с киберпреступностью, за счет оказания помощи в проведении кампаний по борьбе с киберпреступностью в других государствах, например, путем содействия обмену информацией и аресту лиц, участвующих в совершении киберпреступлений;

b) Межведомственный совет по борьбе с торговлей людьми, который устанавливает правила и положения для эффективного осуществления Закона Республики № 9208, также известного как Закон о борьбе с торговлей людьми от 2003 года, с поправками, внесенными в него Законом Республики № 10364, или Расширенным законом о борьбе с торговлей людьми от 2012 года. Его возглавляет министр юстиции, что, в свою очередь, обеспечивает более оперативную координацию программ и проектов в целях эффективного решения вопросов, связанных с торговлей людьми. Он рекомендует меры по расширению взаимной помощи между зарубежными странами в рамках двусторонних и/или многосторонних договоренностей в целях предотвращения и пресечения международной торговли людьми;

c) Межведомственный совет по борьбе с детской порнографией, состоящий из ряда соответствующих государственных ведомств и неправительственных организаций и возглавляемый министром общественного благосостояния и развития, формулирует всеобъемлющие и комплексные планы и программы по предотвращению и пресечению любых видов детской порнографии и возбуждает дела против отдельных лиц, ведомств, организаций или учреждений, которые нарушают положения Закона о борьбе с детской порнографией от 2009 года (Закон Республики № 9775).

259. Что касается передового опыта охраны правопорядка и проведения расследований, Филиппины признали важность использования специализированных ведомств для охраны правопорядка и проведения расследований. По мнению Филиппин, межведомственное сотрудничество имеет решающее значение для эффективного обеспечения соблюдения законов и расследования, при этом руководящая роль отводится Подкомитету по киберпреступности Национального координационного комитета правоохранительных органов, Межведомственному совету по борьбе с торговлей людьми и Межведомственному совету по борьбе с детской порнографией.

260. Было также отмечено, что еще одним механизмом, который используется правоохранительными органами, является Интерпол, причем Национальное центральное бюро Интерпола в Маниле функционирует в качестве главного органа по координации сотрудничества органов полиции на внутреннем и международном уровнях в борьбе с транснациональной преступностью. Тесное сотрудничество с правоохранительными органами, другими государственными учреждениями и иностранными правоохранительными органами имеет крайне важное значение для расследования, отслеживания и уголовного преследования лиц, совершивших киберпреступления.

261. Филиппинский центр по транснациональной преступности, который является секретариатом Национального центрального бюро Интерпола в Маниле, и Совет по борьбе с отмыванием денег совместно провели оперативное совещание Интерпола, посвященное хищению денежных средств из Банка Бангладеш — одному из самых крупных дел, связанных с отмыванием денег.

262. Что касается передового опыта в области электронных доказательств и криминальной практики, Филиппины сообщили, что специализированные ведомства используют цифровую криминалистическую экспертизу для отслеживания, расследования и уголовного преследования лиц, совершивших киберпреступления. Закон о предупреждении киберпреступности от 2012 года был утвержден 12 сентября 2012 года и вступил в силу 18 февраля 2014 года. В сочетании с использованием правил об электронных доказательствах, изданных Верховным судом, уголовное преследование киберпреступлений в судах по киберпреступности стало более эффективным.

263. Центр координации и расследования киберпреступлений 2 мая 2017 года официально представил Национальный план обеспечения кибербезопасности на период до 2022 года, в котором была отмечена безотлагательная необходимость защиты каждого пользователя интернета на Филиппинах, важнейшей национальной информационной инфраструктуры, государственных сетей, малых и средних предприятий и других организаций и корпораций.

264. Несмотря на прилагаемые правительством совместно со специализированными ведомствами усилия, направленные на борьбу с киберпреступностью, принятие законов по противодействию киберпреступности, создание судов по борьбе с киберпреступностью и использование правил в отношении электронных доказательств, по-прежнему существует необходимость в организации обучения специалистов и экспертов использованию этих инструментов. Необходимо использовать возможности для непрерывного укрепления потенциала, особенно спонсорскую поддержку, как местную, так и иностранную. Кроме того, необходимо периодически проводить анализ и оценку киберпреступности и кибербезопасности, чтобы оценить, в каком направлении движутся Филиппины благодаря прилагаемым усилиям.

Португалия

265. Португалия заявила, что развитие информационно-коммуникационных технологий создает новые возможности для преступников и ведет к росту числа и разнообразия преступлений, совершенных с использованием цифрового мира и внутри него. Такие преступления оказывают все более сильное воздействие на стабильность критически важной инфраструктуры государств и предприятий, а также на благополучие отдельных лиц, учитывая их последствия для полного осуществления прав человека и гражданских свобод. Примерами ситуаций, вызывающих обеспокоенность государств в эпоху цифровых технологий, являются использование технологий и интернета для распространения материалов террористического содержания, для пропаганды ненависти, экстремизма и радикализма, а также для совершения других тяжких преступлений, таких как сексуальное надругательство над детьми, торговля людьми и отмывание денег.

266. Португалия отметила, что государства сталкиваются с трудностями при проведении уголовных расследований вследствие использования технологий шифрования, трудностей в получении и сохранении электронных доказательств, осуществления юрисдикции в киберпространстве и отсутствия международного сотрудничества в этой области. Использование шифрования удовлетворяет законное право на неприкосновенность частной жизни и осуществление основных прав человека, а также отвечает потребностям бизнеса и органов государственной власти; компании осуществляют инвестиции в разработку инструментов, обеспечивающих более эффективную защиту конфиденциальности своих клиентов, заявляя, что меры, направленные на ослабление шифрования, могут раскрыть информацию личного характера людям, могущим использовать ее ненадлежащим образом. Безопасная обработка является важным элементом защиты персональных данных, а постановление 2016/679 Европейского парламента и Совета Европейского союза признает шифрование мерой безопасности. Однако, сохраняя безопасность данных или информации, технологии шифрования открывают широкие возможности для преступников.

267. Еще одна сложность при проведении расследования и судебного преследования связана с получением электронных доказательств, хранящихся в компьютерных системах, и обеспечением их безопасности с учетом их масштаба и сложности. Сетевые услуги могут быть предоставлены в любом месте и не требуют обязательного наличия материальных объектов, сооружений или персонала в соответствующем государстве. Таким образом, соответствующие доказательства зачастую хранятся на серверах за пределами проводящего расследование государства в одной или нескольких иностранных юрисдикциях или даже в неизвестной юрисдикции и могут быть связаны с деятельностью международных поставщиков услуг.

268. Из-за отсутствия связи между следственными органами в различных юрисдикциях просьбы об оказании правовой помощи в большинстве случаев требуют трансграничного доступа к электронным доказательствам и часто адресованы государствам, в которых размещается большое число поставщиков услуг, но которые при этом не связаны конкретным образом с этими процедурами. Получение доказательств в рамках сотрудничества судебных органов может занимать длительное время, в течение которого эти доказательства могут стать недоступными. Еще одна проблема заключается в отсутствии четкого механизма сотрудничества с частными поставщиками услуг, а национальные подходы к такому сотрудничеству разнятся.

269. Португалия упомянула также, что к другим проблемам, стоящим перед государствами на международном уровне, относятся предотвращение и пресечение подстрекательства к терроризму и распространения террористических материалов, а также пропаганды радикализма и экстремизма через интернет и с помощью других информационно-коммуникационных технологий.

270. Борьба с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, и с киберпреступностью является для Португалии стратегически важным вопросом, и она твердо привержена этой борьбе. Закон о компьютерных преступлениях (Закон № 109/1991) был принят в 1991 году и пересмотрен в 2009 году (Закон № 109/2009 (Закон о киберпреступности)). Национальная стратегия в области безопасности в киберпространстве (2015 год) в настоящее время пересматривается, и ожидается, что новая Национальная стратегия будет опубликована в течение ближайших месяцев. Использование информационно-коммуникационных технологий и киберпреступность упоминаются в качестве наиболее важных вопросов и в старой, и в новой версии стратегии.

271. Португалия также сообщила, что был принят закон о хранении данных, сгенерированных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования. Это имеет

особое значение в случае уголовного расследования таких серьезных преступлений, как терроризм и организованная преступность.

272. По мнению Португалии, решающее значение для борьбы с киберпреступностью имеет наличие надлежащей и современной внутренней правовой базы, предоставляющей необходимые процессуальные инструменты и полномочия, что позволяет правоохранительным органам и органам прокуратуры вести расследование и осуществлять сбор цифровых данных с соблюдением прав и гарантий как подозреваемых, так и потерпевших.

273. Португалия создала специализированные подразделения в структуре своих правоохранительных и судебных органов: в 2011 году в структуре Генеральной прокуратуры было создано Бюро по борьбе с киберпреступностью, а в составе Уголовной полиции была создана Национальная группа по борьбе с киберпреступностью и преступлениями, связанными с технологиями, которая осуществляет свою деятельность и координирует усилия на национальном уровне. Государственная прокуратура несет ответственность за проведение уголовных расследований, а Уголовная полиция является правоохранительным органом с исключительными полномочиями в области расследования киберпреступлений и преступлений, совершаемых с применением информационно-коммуникационных технологий, и действует под руководством прокурора в соответствии с Законом об организации уголовных расследований (Закон 49/2008). Такая специализация повышает эффективность расследований и обеспечивает последовательность мер и международную координацию. Важное значение имеет международное сотрудничество в целях получения доказательств из другой страны, и необходимо приложить усилия, особенно на уровне Организации Объединенных Наций, направленные на укрепление потенциала и расширение сотрудничества.

274. Что касается дополнительных проблем, Португалия отметила, что киберпреступность и использование информационно-коммуникационных технологий для совершения преступлений не привязаны к конкретной территории; такие преступления происходят во всем мире. Глобальные услуги (например, услуги электронной почты и социальных сетей, облачные услуги) используются повсеместно и могут быть также использованы в преступных целях с ориентацией на жертв из самых разных государств. В то время как некоторые государства признают необходимость оперативности в делах, связанных с цифровыми доказательствами, другие настаивают на использовании традиционных инструментов, таких как просьбы об оказании взаимной правовой помощи, которые не позволяют своевременно реагировать на текущие потребности или проблемы. Всеобъемлющих международных нормативных положений не существует, а национальные рамки предусматривают различные решения, в связи с чем необходим новый подход.

275. Португалия упомянула также о том, что участники Конвенции Совета Европы о киберпреступности готовят дополнительный протокол к Конвенции. Такой протокол, как ожидается, обеспечит четкое руководство для работников правоохранительных органов и судебной системы в отношении трансграничного доступа к данным и повышения эффективности неофициального взаимодействия, обмена информацией и функционирования системы взаимной правовой помощи для получения данных, хранящихся в других юрисдикциях, при полном соблюдении основополагающих прав и свобод.

276. На уровне Европейского союза ведутся переговоры о разработке регламента и директивы об электронных доказательствах, что позволит обеспечить безопасность и сбор электронных доказательств, а также повысить эффективность сотрудничества в этой области.

Катар

277. Катар отметил, что масштабы неправомерного использования информационных ресурсов и технологий, в том числе в целях совершения киберпреступлений и электронного пиратства, возрастают, и это отрицательно сказывается на безопасности и стабильности стран. Негативные последствия использования информационных ресурсов или технологий для развития, мира, стабильности и прав человека подробно рассматриваются в различных резолюциях структур Организации Объединенных Наций. Преступления, совершаемые в цифровом мире, их растущее многообразие, а также использование таких технологий и средств в целях, несовместимых с задачей поддержания международной стабильности и безопасности, оказывают негативное влияние на целостность инфраструктуры государств и наносят ущерб их безопасности на местах.

278. Необходимо усилить правовые меры на национальном и международном уровнях в целях борьбы с киберпреступностью и предложить новые меры для пресечения, выявления и расследования и судебного преследования киберпреступлений. Необходимо активизировать международные усилия, направленные на предотвращение использования криминальных ресурсов или информационных технологий в преступных и террористических целях. В целях поддержания мира и стабильности и создания открытой, безопасной, стабильной и мирной информационно-коммуникационной среды Катар вновь заявил о поддержке Группы экспертов для проведения всестороннего исследования проблемы киберпреступности и призвал к продолжению ее деятельности.

279. Катар сообщил, что он стремится к повышению безопасности информации в рамках государства и поощрению международного сотрудничества в борьбе с киберпреступностью, особенно с учетом того, что он стал жертвой электронного пиратства, которое послужило прикрытием для создания искусственного регионального кризиса, нанесшего серьезный ущерб региональной и международной безопасности и стабильности. Катар уделяет особое внимание разработке своего законодательства и поощрению совместных международных действий по предупреждению цифровых преступлений, а также обнаружению виновных в их совершении и осуществлении в их отношении судебного преследования.

280. В 2014 году в Катаре был принят Закон № 14 о борьбе с киберпреступностью, представляющий собой важный шаг по укреплению национального законодательства и процедур по борьбе с киберпреступностью. В закон включены разделы, где дано определение киберпреступлений, таких как нарушения информационных систем, программ и сетей, электронное мошенничество и подделка денежных знаков и преступления, связанные с нарушением прав интеллектуальной собственности. Закон содержит положения о процедурах расследования, сборе доказательств, обязательствах поставщиков услуг, обязательствах государственных органов и международном сотрудничестве, включая взаимную правовую помощь и выдачу преступников.

281. В заключение Катар указал, что киберпреступность как новая форма транснациональной организованной преступности представляет собой растущую и меняющуюся проблему. Для ее решения требуются скоординированные и расширенные коллективные меры реагирования, в основе которых лежит принцип общих интересов и совместной ответственности. В этом контексте Катар стремится к укреплению сотрудничества с УНП ООН в целях укрепления национального потенциала, усиления безопасности компьютерных сетей и поощрения регионального и международного сотрудничества в целях создания безопасного и надежного киберпространства.

Румыния

282. Румыния заявила, что, развиваясь, технологии играют важную роль в широком спектре преступной деятельности, оказывая серьезное воздействие и влияние на онлайновую среду. Термин «киберпреступность» включает широкий спектр угроз криминального характера, таких как распространение вирусов-вымогателей и других вредоносных программ, мошенничество с использованием безналичных платежей и онлайновая торговля материалами, связанными с сексуальной эксплуатацией детей.

283. Румыния описала «киберзависимые преступления» как любые преступления, которые могут совершаться только с использованием компьютеров, компьютерных сетей и других видов информационно-коммуникационных технологий. Преступления, совершаемые с использованием киберпространства, могут осуществляться как в интернете, так и вне его. Роль интернета заключается в увеличении масштаба, географического охвата и скорости совершения этих преступлений. Наихудшим вариантом преступлений, совершаемых с использованием киберпространства, является сексуальная эксплуатация детей в интернете. Кроме того, в даркнете появляется все больше форумов, посвященных производству и распространению материалов, связанных с сексуальной эксплуатацией детей, а также обмену ими. В дополнение к этому интернет дает возможность использования широкого круга приложений, таких как пиринговый файлообмен и безопасное хранение данных, которые способствуют совершению этих преступлений.

284. По мнению Румынии, мошенничество с использованием безналичных платежей является еще одной высокоорганизованной, узкоспециализированной и постоянно развивающейся угрозой, которая легко адаптируется к принимаемым против нее мерам и новым технологиям. Эта угроза включает два отдельных вида преступлений: мошенничество без использования платежных карт, которое совершается преимущественно в онлайновом режиме, и мошенничество с использованием платежных карт, которое осуществляется, как правило, в торговых точках и банкоматах. Преступники также захватывают операционные системы банкоматов для облегчения доступа к наличным средствам.

285. Была представлена информация о том, что онлайновые коммерческие платформы могут также использоваться для торговли запрещенными товарами и услугами. На незаконных онлайновых рынках, находящихся как в видимом интернете, так и в даркнете, представлены средства, которые могут использоваться для совершения других видов преступлений, например набор программ для совершения киберпреступлений или фальшивые документы.

286. В качестве еще одного товара, который обычно продается в интернете и может использоваться впоследствии для осуществления мошенничества, были упомянуты данные, целостность которых была нарушена. Как правило, речь идет о финансовых данных, таких как данные платежных карт или учетные данные личного кабинета для управления банковским счетом, целостность которых была нарушена. К ним могут также относиться иные категории данных — от перечней полных персональных данных и отсканированных документов до перечней адресов электронной почты и учетных записей для входа в личный кабинет.

287. Румыния заявила, что преступники используют все имеющиеся каналы связи, причем не только для внутренней коммуникации, но и для установления контакта с потенциальными жертвами, например, путем рассылки фишинговых писем по электронной почте или через социальные сети. Преступники также используют защищенные приложения и подобные им службы для сокрытия своей преступной деятельности. Рост масштабов использования услуг шифрования преступниками и другими злоумышленниками создает серьезные препятствия для выявления, расследования и судебного преследования всех видов преступной деятельности, включая терроризм.

288. Новые формы платежей, такие как криптовалюты и платформы для осуществления банковских операций и расчетов в режиме реального времени, открыли перед преступниками новые пути финансирования и расширения своего преступного бизнеса. Быстрая обработка операций в рамках нескольких юрисдикций и широкое распространение средств шифрования и обеспечения анонимности — вот некоторые из наиболее существенных препятствий, возникающих в ходе финансовых расследований. Наиболее широко используемой валютой для осуществления связанных с киберпреступностью расчетов между преступниками является биткоин. Он принимается на большинстве рынков даркнета и в магазинах с автоматизированной оплатой картами, но все шире используется при совершении преступлений за пределами киберпространства, например при уплате выкупа за похищенных людей.

289. Румыния подчеркнула, что киберпреступность в стране развивалась аналогично другим явлениям глобальной преступности, как описано в докладах Европола за 2014–2017 годы. Преступные группы из Румынии проявляли весьма заметную активность в области киберпреступности. Со временем Румыния также стала объектом таких преступлений. Они представляют угрозу для национальной безопасности в широком смысле, в том числе и для финансовой системы.

290. Румыния сообщила, что она приложила серьезные усилия для принятия всеобъемлющего процессуального законодательства, охватывающего различные аспекты уголовного судопроизводства по сбору электронных доказательств в соответствии с принципом верховенства права, гарантиями и средствами правовой защиты, основанными на Конвенции Совета Европы о киберпреступности. Румыния ратифицировала Конвенцию в 2003 году. Национальное законодательство, предусматривающее уголовную ответственность за незаконную деятельность, как это предусмотрено в статьях 2–9 этой Конвенции, охватывает широкий круг неправомерных действий, позволяя специализированным подразделениям осуществлять расследование соответствующих дел. Эти положения все еще — спустя 15 лет после их принятия — применимы к новым формам киберпреступности. Дополнительные указания в отношении элементов состава преступления представлены в руководящих указаниях, принятых Комитетом по Конвенции о киберпреступности.

291. Сообщалось, что в 2004 году в структуре прокуратуры Румынии было создано Управление по расследованию дел, связанных с организованной преступностью и терроризмом. Кроме того, в рамках полиции было создано Управление по борьбе с организованной преступностью в качестве специализированной структуры для поддержки деятельности Управления по расследованию дел, связанных с организованной преступностью и терроризмом. За последние пять лет расследование было проведено в отношении свыше 28 800 дел, связанных с преступлениями, совершенными в информационной среде или с помощью компьютерных технологий.

292. В качестве примера таких преступлений Румыния упомянула «скимминг», используемый для незаконного завладения данными банковских карт; участие в этой деятельности принимают преступные группы во множестве различных юрисдикций (изготовление составных частей, их сборка и фактическое мошенничество). Эта деятельность подпадает под действие статьи 365 Уголовного кодекса. Что касается методов преступной деятельности, то чаще всего по-прежнему используются социальная инженерия, адресный фишинг, многоуровневые командные серверы и сканирование на уязвимости. Серьезной проблемой для правоохранительных органов является рост использования широким кругом субъектов инструментов с открытым исходным кодом, что затрудняет вменение незаконной деятельности в вину конкретным лицам или группам. Национальное законодательство предусматривает санкции за атаки с использованием вредоносного программного обеспечения в статьях 207 (шантаж), 362 и 363 Уголовного кодекса.

293. Наиболее распространенными формами киберпреступности в Румынии являются методы социальной инженерии, применяемые для совершения мошеннических действий (фишинг, адресный фишинг, «вишинг», «смишинг»), а также такие методы, как «человек посередине» и «человек в браузере», используемые преимущественно для кражи денежных переводов. Они являются уголовно наказуемыми деяниями в соответствии со статьями 325 и 249 Уголовного кодекса (в зависимости от конкретного случая также могут быть предъявлены дополнительные обвинения, например, в неправомерном использовании устройств или нарушении целостности данных). Использование платформы Cobalt Strike для проведения атак на банковскую систему расследуется в соответствии с положениями статей 360, 362, 363, 366 и 249 Уголовного кодекса.

294. Майнинг криптовалют и большинство видов деятельности, связанной со взломом шифрования, расследуются в соответствии со статьями 360 и 366 Уголовного кодекса. Применение скиммеров-накладок также расследуется в соответствии со статьями 360 и 366 Уголовного кодекса.

295. В заключение Румыния отметила, что создание всеобъемлющей правовой базы, основанной на Конвенции Совета Европы о киберпреступности, и специализированных учреждений помогло в решении постоянно меняющихся проблем, связанных с киберпреступностью и электронными доказательствами. На данном этапе требуется больший объем ресурсов, а также дальнейшая подготовка и наращивание потенциала. Обсуждение новых международных договоров в этой области не принесет пользы и может привести к ослаблению усилий.

Российская Федерация

296. Российская Федерация отметила, что проблема противодействия использованию информационно-коммуникационных технологий в преступных целях с точки зрения масштаба и распространенности уже давно стала глобальной угрозой, затрагивающей все страны мира без исключения. В настоящее время мировое сообщество не имеет единого подхода к решению этого вопроса. На международном уровне ситуация усугубляется отсутствием всеобъемлющей международно-правовой основы для сотрудничества и даже общей терминологической базы. На региональном уровне соответствующие документы были разработаны и приняты рядом организаций, но их способность эффективно бороться с такими преступлениями остается недостаточной.

297. Российская Федерация заявила, что ряд государств предлагали в качестве возможного решения Конвенцию Совета Европы о киберпреступности. Однако этого документа недостаточно для устранения существующих угроз. Эта Конвенция была разработана в конце 1990-х годов, и поэтому она не регулирует многие современные «изобретения» преступников. Она также допускает возможность нарушения принципов государственного суверенитета и невмешательства во внутренние дела других государств. Таким образом, по-прежнему существует угроза легитимизации доступа специальных служб ограниченной группы стран к бесконтрольному сбору персональных данных пользователей со всего мира, а также сохраняется установленная рядом государств тенденция консолидации их технических достижений в информационном пространстве и сохранения цифрового разрыва между развитыми и развивающимися странами.

298. Российская Федерация подчеркнула, что она поощряет разработку универсальных принципов и норм, которыми будут пользоваться все заинтересованные стороны и которые заложат основу для эффективного международного сотрудничества в борьбе с киберпреступностью. Таким документом могла бы стать конвенция по борьбе с преступлениями в сфере использования информационно-коммуникационных технологий под эгидой Организации Объединенных Наций, которая будет учитывать нынешние реалии и принципы суверенного равенства и невмешательства во внутренние дела государств. Основой для

такой работы может служить российский проект конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности, который был распространен в качестве официального документа (A/C.3/72/12). Российская Федерация полагает, что этот проект даст «пищу для размышлений», инициирует обсуждение этой темы в рамках ключевых международных форумов, в первую очередь в Организации Объединенных Наций, и позволит объединить и сосредоточить усилия международного сообщества по разработке практических решений в этой области.

299. По мнению Российской Федерации, учитывая глобальный характер явления информационной преступности, недостаточно лишь обсуждать вопросы в рамках Венского форума Организации Объединенных Наций — Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Мандат Группы экспертов ограничивается обсуждением по большей части технических аспектов этого вопроса. В нынешнем контексте основной задачей считаются поиск политического решения и достижение консенсуса.

300. В связи с этим Российская Федерация подчеркнула, что следует строго выполнять положения резолюции 73/187 Генеральной Ассамблеи о противодействии использованию информационно-коммуникационных технологий в преступных целях. Другое решение заключается в создании в рамках Генеральной Ассамблеи постоянного форума для обсуждения на основе комплексного и сбалансированного подхода всех аспектов международного сотрудничества в борьбе с киберпреступностью, которое будет направлено на поиск политического решения и достижение консенсуса с учетом насущных потребностей государств в этой области, а также на содействие обмену передовым опытом в этой области. Одним из вариантов такого форума является создание в рамках Организации Объединенных Наций рабочей группы открытого состава по киберпреступности, которой государства-члены поручат разработать и имплементировать любые соответствующие документы.

Саудовская Аравия

301. Саудовская Аравия указала на следующие препятствия на пути борьбы с использованием информационно-коммуникационных технологий в преступных целях:

a) неэффективное сотрудничество компаний, которые организуют свою деятельность на базе цифровых платформ, с юридическими и правоохранительными органами по всему миру;

b) отсутствие в виртуальном мире цифровой идентификации личности и использование программ-идентификаторов и фиктивных данных, а также выдача себя за другое лицо в интернете, особенно в социальных сетях;

c) различия в законодательстве государств-членов, в том числе уголовном;

d) отсутствие координации, сотрудничества и взаимопомощи между странами в борьбе с киберпреступностью;

e) отсутствие надлежащих механизмов контроля за предоставлением электронных услуг (сетей, ресурсов, облачных сред, услуг и т.д.) во многих странах;

f) отсутствие во многих странах передовых информационных систем, позволяющих отслеживать подозрительные операции и выявлять их источники и тех, кто стоит за ними;

g) низкий кадровый и технический потенциал государственных и частных учреждений и отдельных лиц в области кибербезопасности;

h) отсутствие международного законодательства, касающегося криминализации и отслеживания использования информационно-коммуникационных технологий в преступных целях, которое могло бы внести свой вклад в международные усилия по борьбе с этим явлением;

i) необходимость повышения квалификации людей в области информационной безопасности с помощью специальных программ обучения;

j) многочисленность и разнообразие законодательства и законов в различных странах, которые предусматривают наказание за преступное поведение в области информационных технологий;

k) цель онлайновых торговых платформ заключается исключительно в получении прибыли. Кроме того, подобные платформы обеспечивают благодатную почву для программного обеспечения и приложений, использующих технологии для сокрытия пользователей и совершения киберпреступлений;

l) масштабы преступлений, совершаемых с использованием информационных технологий, и их трансграничный потенциал, что приводит к низкому уровню взаимодействия и коммуникации между государствами в рамках борьбы с такими преступлениями;

m) благодаря замещению традиционных валют цифровыми преступным группам становится проще скрывать многие финансовые операции, проводимые ими в интернете;

n) низкий уровень осведомленности о безопасном и оптимальном использовании информационных технологий и интернета;

o) необходимость присоединения Саудовской Аравии к международному законодательству по борьбе с неправомерным использованием технологий;

p) необходимость активизации профилактических мер путем повышения осведомленности общин о методах, используемых преступными бандами, действующими в интернете.

Сербия

302. Сербия сообщила, что структура и сфера полномочий Специальной прокуратуры Сербии по преступности в области высоких технологий определены в Законе об организации и полномочиях государственных органов в области борьбы с киберпреступностью, вступившем в силу 25 июля 2005 года, и Законе о внесении поправок в Закон об организации и полномочиях государственных органов в области борьбы с киберпреступностью, вступившем в силу 1 января 2010 года. Таким образом, Специальная прокуратура обладает полномочиями для рассмотрения дел, связанных с вышеупомянутыми преступлениями, на территории Сербии.

303. Сербия сослалась на свою законодательную базу и стратегические рамки, включающие:

a) Закон об организации и полномочиях государственных органов в области борьбы с киберпреступностью;

b) Закон о ратификации Конвенции Совета Европы о киберпреступности;

c) Закон о ратификации Дополнительного протокола к Конвенции Совета Европы о киберпреступности, касающегося криминализации актов расистского и ксенофобского характера, совершаемых при помощи компьютерных систем;

d) Закон о ратификации Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия;

e) Уголовный кодекс;

f) Уголовно-процессуальный кодекс;

g) Закон об электронных сообщениях;

h) Закон об информационной безопасности;

i) Стратегию борьбы с преступностью в области высоких технологий на период 2019–2023 годов;

j) Стратегию развития информационного общества в Сербии до 2020 года;

k) стратегическую оценку общественной безопасности Республики Сербия.

304. Недавно проведенные реформы внутреннего законодательства подчеркивают важность Конвенции Совета Европы о киберпреступности и Дополнительного протокола к ней.

305. В сентябре 2018 года правительство одобрило Национальную стратегию по борьбе с киберпреступностью и соответствующий План действий. Кроме того, Министерство юстиции сформировало рабочие группы для внесения поправок в Уголовный кодекс и Уголовно-процессуальный кодекс. В связи с этим представители Государственной прокуратуры и Специальной прокуратуры по преступности в области высоких технологий организовали в марте 2019 года миссию экспертов в рамках совместного проекта Европейского союза и Совета Европы iPROCEEDS. Их задача заключалась в проведении углубленного правового анализа пробелов в национальном законодательстве и оценке его соответствия Конвенции Совета Европы о киберпреступности, Директиве 2013/40/EU о нападениях на информационные системы, заменяющей Рамочное решение Совета 2005/22, а также другим международным стандартам и стандартам Европейского союза. По итогам этого анализа будут выдвинуты предложения по внесению поправок в законы в целях достижения полной гармонизации.

306. Сербия отметила, что опыт последних 15 лет свидетельствует о том, что укрепление потенциала и специализация на национальном уровне, основанные на существующих международных соглашениях, оправдывают себя на практике и позволяют добиваться положительных сдвигов. Сомнительно, что обсуждение новых международных договоров в этой области окажется полезным.

307. Что касается институциональной базы и административного потенциала, Сербия перечислила следующие учреждения, которые уполномочены действовать в области борьбы с киберпреступностью:

a) Специальная прокуратура по преступности в области высоких технологий;

b) Высокий суд Белграда;

c) Департамент Министерства внутренних дел по борьбе с преступностью в сфере высоких технологий и ее пресечению;

d) другие компетентные государственные органы.

308. В отношении статистики и анализа Сербия сообщила, что общее число дел, зарегистрированных в реестре Специальной прокуратуры по преступности в области высоких технологий, в 2018 году составило 3 022, из которых 322 дела были зарегистрированы в реестре известных взрослых преступников, 1 306 дел — в реестре неизвестных преступников, а 1 394 дела — в реестре других уголовных преступлений, что на 27,46 процента больше, чем в 2017 году.

309. Соответственно, как Сербия сообщила далее, значительные позитивные сдвиги были отмечены также в применении различных процессуальных дей-

ствий на различных этапах уголовного судопроизводства: так, количество возбужденных уголовных дел против известных преступников увеличилось на 28,57 процента и достигло 324 случаев; применение отсрочки уголовного преследования увеличилось на 85,71 процента, а использование соглашения о признании вины увеличилось на 105 процентов. Такой значительный рост является следствием увеличения количества зарегистрированных лиц и случаев, увеличения численности сотрудников Специальной прокуратуры и укрепления потенциала компетентных органов.

310. Что касается передовой практики, Сербия привела следующие примеры международных дел, в которых участвовали специализированные органы по борьбе с киберпреступностью Сербии и которые были успешными благодаря осуществлению Конвенции Совета Европы о киберпреступности и положений о международном сотрудничестве, предусмотренных законодательством Сербии:

a) операция «Теневая паутина», февраль 2018 года. Захват одного из крупнейших уголовных форумов, In Fraud, посвященного похищенным данным о кредитных картах. Один сербский гражданин был арестован, и было возбуждено уголовное дело;

b) операция «Выключение питания», апрель 2018 года. Захват крупнейшего в мире криминального сервера для распределенных атак типа «отказ в обслуживании» — Webstresser. Два сербских гражданина были арестованы, и было возбуждено уголовное дело. В операции принимали участие компетентные органы Австрии, Германии, Испании, Италии, Канады, Нидерландов, Сербии, Соединенного Королевства, Соединенных Штатов и Хорватии, а также Гонконга (Китай). Специальная прокуратура по преступности в области высоких технологий начала расследование в отношении двух подозреваемых, и у одного из них была впервые изъята криптовалюта;

c) операция «Темный оверлорд», май 2018 года. Была связана с преступной группировкой, занимавшейся хищением персональных данных и шантажом их владельцев.

311. Сербия сообщила, что в 2018 году международное сотрудничество, осуществляемое Специальной прокуратурой, оказалось особенно успешным. Прокуратура участвовала в работе Группы по трансграничной преступности Конвенции Совета Европы о киберпреступности и в деятельности, связанной с подготовкой дальнейших рекомендаций и руководящих принципов для применения Конвенции. Прокуратура также принимала участие в работе Группы по разработке второго дополнительного протокола к Конвенции. Кроме того, Прокуратура была включена в состав участников совместного проекта Совета Европы и Европейского союза GLACY+, а также других международных мероприятий. В 2018 году представители Специальной прокуратуры приняли участие в проекте EAP III Совета Европы, ориентированном на так называемых соседей Европейского союза, а также в проекте Cyber@South, ориентированном на страны Северной и Западной Африки и Азии в Средиземноморском регионе, и в проекте iPROCEEDS@IPA, участие в котором принимали страны Юго-Восточной Европы и Турция. Европейская судебная сеть по борьбе с киберпреступностью предложила Специальной прокуратуре принять участие в ее заседаниях в Гааге. Представители Специальной прокуратуры также приняли участие в работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности.

Сингапур

312. Сингапур отметил, что проблемы, с которыми он сталкивается, распространены и в других юрисдикциях. К ним относится все большая изощренность преступников, которые стремятся использовать для достижения преступных целей расширение доступа в результате глобализации, а также появление и повсеместное распространение технологий.

313. Сингапур сообщил, что за последнее десятилетие масштабы использования киберпространства значительно возросли. Это связано с появлением более дешевых и доступных технологий, что, в свою очередь, привело к росту числа случаев киберпреступности (преступления согласно Закону страны о неправомерном использовании компьютеров, а также традиционные преступления, совершенные с использованием вычислительных устройств или сетей в качестве орудия). В этой связи полиция Сингапура отметила увеличение числа случаев онлайн-мошенничества и количества жертв, пострадавших от новых методов международных мошенников, которые используют информационно-коммуникационные технологии — от наиболее современных методов, таких как хакерство, до таких технологий, как телефонный фишинг. В связи с широтой охвата и распространенностью киберпреступности в различных юрисдикциях этот вид преступности может укорениться в любом месте, что затрудняет его выявление, искоренение и уничтожение. Для решения этой сложной задачи Сингапур принял меры на национальном, региональном и международном уровнях, о чем более подробно говорится ниже.

314. Касаясь национальных усилий, Сингапур сообщил, что 20 июля 2016 года на Конференции RSA Азиатско-Тихоокеанского региона и Японии министр внутренних дел и юстиции официально представил Национальный план действий Сингапура по борьбе с киберпреступностью. Концепция национального Плана действий по борьбе с киберпреступностью заключается в создании в Сингапуре безопасной и надежной сетевой среды, поскольку масштабы, разнообразие и серьезность деятельности киберпреступников во всем мире продолжают расти. В Плане подробно изложена комплексная стратегия правительства по борьбе с киберпреступностью по следующим направлениям:

a) просвещение и расширение прав и возможностей населения для обеспечения безопасности в киберпространстве;

b) наращивание потенциала и расширение возможностей борьбы с киберпреступностью;

c) повышение эффективности законодательства и системы уголовного правосудия;

d) укрепление партнерских отношений и международного сотрудничества.

315. Что касается мер на региональном и международном уровнях, Сингапур отметил полезную роль, которую международные и региональные организации и партнерства с участием многих заинтересованных сторон играют в укреплении потенциала, распространении информации, обмене сведениями о последних тенденциях и событиях и передовым опытом, а также в международном сотрудничестве в борьбе с трансграничной киберпреступностью.

316. К основным региональным платформам относятся Совещание министров стран — членов АСЕАН по вопросам транснациональной преступности и Совещание старших должностных лиц по вопросам транснациональной преступности. Исполняя функции добровольного ведущего координатора АСЕАН по вопросам киберпреступности, Сингапур выступил с новыми инициативами, направленными на укрепление потенциала реагирования государств — членов АСЕАН в отношении киберпреступности, такими как проведение в июле 2018 года конференции по вопросам киберпреступности в формате «АСЕАН плюс три» и пятого совещания за круглым столом старших должностных лиц АСЕАН по борьбе с киберпреступностью. АСЕАН также сосредоточила усилия на повышении уровня знаний и укреплении потенциала сотрудников прокуратуры в области уголовного преследования киберпреступлений, и в сентябре 2018 года в Сингапуре состоялось заседание за круглым столом прокуроров стран АСЕАН по вопросам киберпреступности. Это ежегодные мероприятия, которые будут организованы и в 2019 году.

317. Сингапур сообщил, что он тесно сотрудничает с Интерполом в целях развития регионального и международного сотрудничества для борьбы с кибер-

преступностью. Сингапур был назначен заместителем Председателя Евразийской рабочей группы Интерпола по киберпреступности на период с 2017 по 2019 год. Кроме того, Сингапур при поддержке бюро Интерпола инициировал создание Отдела АСЕАН по вопросам киберпреступности, который начал свою работу в июле 2018 года в расположенном в Сингапуре Глобальном инновационном комплексе Интерпола. Этот отдел АСЕАН получает доступ к ресурсам Интерпола и использует их для проведения ориентированных на АСЕАН совместных операций по борьбе с киберпреступностью. В феврале 2017 года Сингапур также принимал участие в операции АСЕАН Cyber Surge под руководством Глобального инновационного комплекса Интерпола. В ходе весьма успешной операции, участниками которой являлись семь стран АСЕАН и семь компаний частного сектора, было обнаружено около 9 000 взломанных серверов и сотни веб-сайтов, зараженных вредоносным программным обеспечением.

318. Кроме того, Сингапур является вспомогательным партнером INTERPOL World, международной конференции, которая проводится в Сингапуре раз в два года и в рамках которой представители государственного и частного секторов собираются, чтобы принять участие в диалоге и создании коллективных возможностей для противодействия будущим вызовам в области безопасности и поддержания правопорядка. Это уникальное мероприятие предоставляет соответствующим заинтересованным сторонам ценную платформу для обсуждения глобальных проблем в области киберпреступности и получения от экспертов обновленной информации о последних угрозах, тенденциях и решениях.

319. Сингапур также принимал активное участие в межюрисдикционных международных правоохранительных операциях по борьбе с киберпреступностью. В 2016, а затем и в 2017 году Сингапур участвовал в операции «Лавина», ведущую роль в которой играли Федеральное бюро расследований Соединенных Штатов, Европол и Федеральное управление уголовной полиции Германии (BKA). Целью операции было уничтожение глобальной бот-сети, используемой преступной сетью для кражи информации о банковских счетах и персональных данных и для отмывания денег, а также уничтожение «Андромеды», одной из самых старых существующих систем вредоносного программного обеспечения. Сингапур также активно участвует в деятельности международных форумов, целью которых является расширение глобального сотрудничества и обмен передовым опытом в правоохранительной сфере. К этим форумам относятся первая национальная дискуссия УНП ООН за круглым столом, посвященная вопросам киберпреступности, которая состоялась в Индонезии 2–3 июля 2018 года, семинар экспертов УНП ООН по криптовалютам, состоявшийся в Сингапуре 12–14 марта 2019 года, глобальное совещание Группы экспертов Интерпола в области киберпреступности и конференция Интерпола и Европола по борьбе с киберпреступностью.

320. В заключение Сингапур отметил, что проблемы, с которыми сталкиваются государства-члены в борьбе с использованием информационно-коммуникационных технологий в преступных целях, носят многосторонний характер. Киберпреступность, несомненно, является проблемой, решению которой будут способствовать дальнейшее обсуждение и укрепление международного сотрудничества и взаимодействия на региональном и международном уровнях между государствами-членами и соответствующими заинтересованными сторонами, в том числе в Организации Объединенных Наций. Сингапур привержен международному и региональному сотрудничеству в борьбе с киберпреступностью и надеется на участие, когда это возможно, в усилиях по наращиванию потенциала. Кроме того, Сингапур продолжит поддерживать сотрудничество и обмен информацией в целях борьбы с этими проблемами.

Словакия

321. Словакия сообщила, что она уделяет большое внимание борьбе с киберпреступностью и считает эту борьбу важной задачей. Для эффективного реше-

ния проблемы киберпреступности необходимо соблюдение двух основных аспектов: правового и технического. Во-первых, необходимо иметь адекватное внутреннее законодательство. Положения материального уголовного права должны дополняться соответствующими процессуальными положениями. Словакия считает важным обеспечить расширение традиционных процессуальных положений, таких как проведение обысков в жилище и передача, изъятие или конфискация предметов, чтобы распространить их действие и на данные с изъятых носителей. Таким образом, что касается поиска компьютерных данных, необходимы дополнительные процессуальные положения, чтобы гарантировать, что компьютерные данные могут быть получены законным образом, который столь же эффективен, как и обыск и изъятие материальных носителей данных. Исходя из этого, национальные законы обязательно должны содержать положения, позволяющие государственным органам осуществлять поиск и изъятие сохраненных компьютерных данных. Необходимо обеспечить наличие соответствующих положений у всех государств, с тем чтобы лица, виновные в совершении преступлений, не могли скрыться от правосудия.

322. Для Словакии наилучшим примером модели, содержащей широкий спектр процессуальных полномочий, является Конвенция Совета Европы о киберпреступности, которая предусматривает, в частности, положения, касающиеся обыска и изъятия, распоряжения о предъявлении компьютерных данных и об обеспечении сохранности данных. Словакия ратифицировала эту Конвенцию в 2008 году и считает ее наилучшим международным стандартом, содержащим соответствующие материально-правовые и процессуальные положения и обеспечивающим эффективное международное сотрудничество. В свете вышеизложенного, по мнению Словакии, успешное осуществление процессуальных полномочий, содержащихся в Конвенции Совета Европы о киберпреступности, а также четкая политическая воля являются ключевыми факторами, необходимыми для создания надежной основы для получения доказательств.

323. Кроме того, Словакия считает, что важность пункта 1 (a) статьи 18 Конвенции Совета Европы о киберпреступности, предусматривающего выдачу распоряжений о предъявлении, заключается в том, что он действительно выдержал испытание временем. Ключевым элементом является не местонахождение данных, а присутствие лица, контролирующего данные или владеющего ими, на конкретной территории. Такой подход обеспечивает необходимые решения в большинстве случаев, даже в эпоху облачных вычислений. С учетом вышеизложенного Словакия не видит необходимости в разработке нового международного документа о борьбе с киберпреступностью, и призывает страны, которые не являются участниками Конвенции Совета Европы о киберпреступности, присоединиться к ней.

324. Словакия далее отметила, что электронные доказательства могут возникать в результате практически каждого уголовного преступления. Конвенция Совета Европы о киберпреступности позволяет собирать электронные доказательства по всем видам преступлений, что придает этому документу еще более важное значение. Из этого следует, что каждому судье или прокурору следует знать, каким образом использовать имеющиеся средства обеспечения сохранности электронных доказательств. В этой связи особенно важными считаются образовательные мероприятия и программы по укреплению потенциала на национальном и международном уровнях. По мнению Словакии, программы по укреплению потенциала должны быть целевыми и необходимо по возможности избегать их дублирования.

325. В дополнение к аспектам правового характера Словакия напомнила также о технических аспектах. Государствам следует учитывать, что ключевыми факторами успешного расследования киберпреступлений и преступлений, совершаемых с помощью компьютерных сетей, являются различные виды специализации (местные сети прокуроров, судьи по киберпреступности, специализированные судебные органы по борьбе с киберпреступностью и т.д.), а также регулярная профессиональная подготовка сотрудников правоохранительных и су-

дебных органов для обеспечения правильного применения процессуальных полномочий и корректной реакции на происходящие изменения. Сетевое взаимодействие и обмен передовым опытом необходимы как внутри государств, так и на международном уровне.

326. Чтобы обеспечить специализацию и постоянное обновление знаний, в структуре Главного полицейского управления Словакии был создан специальный Департамент компьютерных преступлений. Этот Департамент способствует более эффективной борьбе с компьютерными преступлениями и преступлениями, совершаемыми через интернет. В настоящее время Департамент занимается преимущественно вопросами, связанными с кибератаками на информационные системы, сексуальной эксплуатацией детей в интернете, мошенничеством в сфере безналичных расчетов и незаконным сетевым контентом (включая материалы террористической направленности). В его задачи входит поиск и мониторинг киберпреступлений (включая секретные операции в интернете). Он также обеспечивает сотрудничество с прокурорами в тех случаях, когда требуется техническая помощь. Сотрудничество работает очень эффективно. Департамент также проводит диалог с международным полицейским сообществом по борьбе с киберпреступностью, а также с частным сектором, особенно с поставщиками услуг интернета, как в Словакии, так и за рубежом, поскольку данные пользователей зачастую находятся в распоряжении или под контролем частных субъектов, в результате чего возникает необходимость обсудить сложности и проблемы, связанные с сотрудничеством.

327. Кроме того, в 2017 году была создана Национальная сеть прокуроров по борьбе с киберпреступностью. Ее основные задачи заключаются в предоставлении практической информации и обмене опытом между членами сети и другими прокурорами по вопросам киберпреступности в отношении как национальных дел, так и дел, связанных с международным сотрудничеством.

328. На национальном уровне была создана межведомственная группа экспертов по киберпреступности. Она объединила экспертов из всех важных государственных органов и частного сектора. В рамках группы, в частности, ведется обсуждение возможности изменить законы, касающиеся раскрытия данных по уголовным делам, таким образом, чтобы для этого не требовался судебный ордер (в Словакии судебный ордер требуется для определения пользователя телефонного номера или IP-адреса). Таким образом, Словакия считает полезным создание специализированных сетей, объединяющих специалистов-практиков по вопросам киберпреступности на национальном и международном уровнях.

329. Словакия подчеркнула свою приверженность делу борьбы с киберпреступностью. В связи с глобальным характером киберпреступности Словакия подтвердила, что она высоко ценит возможность участия в работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Обмен передовым опытом и мнениями с экспертами со всего мира в рамках этой Группы экспертов весьма полезен, и Группа экспертов должна оставаться основным местом решения связанных с киберпреступностью вопросов на уровне Организации Объединенных Наций, по крайней мере до 2021 года.

Словения

330. Словения признала, что в связи с быстрым развитием информационных технологий на рынок выходят не только новые услуги, оборудование и устройства, но также и новые методы деятельности преступников. В связи с этим требуется быстрая и адекватная адаптация со стороны правоохранительных органов, что может быть обеспечено только при условии эффективного и тесного сотрудничества с частным сектором и научно-исследовательскими организациями. Такое сотрудничество требует надежного и быстрого обмена информацией, знаниями и умениями, методами и способами ведения расследований, а также не-

прерывной подготовки персонала. С учетом этих тенденций следует ожидать роста числа уголовных преступлений, совершенных с использованием современных цифровых и виртуальных информационных или иных технологий.

331. Полиция Словении отметила, что лица, совершающие уголовные преступления в киберпространстве, становятся все более технологически квалифицированными и хорошо организованными; они осуществляют свою деятельность на международном уровне и оставляют меньше следов и доказательств, которые могли бы упростить их идентификацию. Все это происходит очень быстро, число жертв растет, а восстановление нормального функционирования занимает гораздо больше времени. Оставленные следы существуют преимущественно только в цифровой форме и часто рассредоточены по нескольким странам или континентам, что отрицательно сказывается на продолжительности и успешности уголовных расследований. Еще одна проблема, о которой сообщила Словения, заключается в постоянном росте объема данных для изучения и анализа в рамках каждого расследования, а также в том, что большинство производителей электронных устройств по умолчанию используют криптостойкое шифрование данных. Это предоставляет преступникам высокий уровень свободы действий и значительно затрудняет их обнаружение и предотвращение преступлений.

332. Вследствие технического прогресса и использования его достижений международное сообщество сталкивается с проблемами, преодолеть которые можно лишь путем расширения сотрудничества и взаимодействия при разработке новых методов предупреждения и снижения рисков, разработки новых подходов, инструментов и механизмов, а также на основе встречных действий и солидарности в области предотвращения на оперативном уровне. Рассредоточение улик и преступных действий по разным странам потребует внедрения новых форм проведения расследований, совершенствования законодательства и повышения квалификации и уровня оснащенности.

Южная Африка

333. Касаясь проблем, связанных с существующими законодательными и уголовно-правовыми инструментами, регулирующими использование информационно-коммуникационных технологий, Южная Африка сообщила, что в стране действует законодательство о борьбе с киберпреступностью, включающее Законопроект о киберпреступности (который вскоре приобретет статус утвержденного парламентом закона), Закон об уголовном судопроизводстве, Закон об электронных коммуникациях и сделках, Закон о международном сотрудничестве по уголовным делам и Закон о защите личной информации. Кроме того, Южная Африка заявила, что отсутствие международного консенсуса по ключевым вопросам и концепциям, включая характер и масштаб киберугроз, справедливость процедур и результаты официальных механизмов, а также криминализацию конкретных деяний и признание их киберпреступлениями, создает проблемы в борьбе с использованием информационно-коммуникационных технологий в преступных целях. Эти проблемы выходят за рамки элементов определения, которые существенно различаются.

334. Южная Африка напомнила также о координации и сотрудничестве между государствами в борьбе с использованием информационно-коммуникационных технологий в преступных целях. Несмотря на наличие ряда существующих механизмов поощрения координации и сотрудничества, таких как взаимная правовая помощь, специализированные контактные центры, обязательства в отношении поставщиков услуг электронной связи и финансовых учреждений, а также оперативное раскрытие данных о трафике различными поставщиками услуг, в деле борьбы с киберпреступностью по-прежнему сохраняются проблемы. В качестве особо значимых проблем были названы следующие: длительность процесса взаимной правовой помощи; несходство мандатов различных учреждений, затрудняющее осуществление централизованной координа-

ции; а также неполная поддержка различными заинтересованными сторонами механизма координации и осуществления предлагаемых мер. В то время как существующие региональные документы могут содействовать борьбе с киберугрозами, обеспечивая сотрудничество между участниками конвенций, самая большая проблема заключается в том, что они, возможно, не способны эффективно бороться с киберпреступностью в глобальном масштабе, поскольку государства, не являющиеся участниками Конвенции, могут отказываться от сотрудничества. Отсутствие общепризнанного определения киберпреступности создает проблему, в результате чего каждая страна разработала свое собственное определение, что приводит к возникновению проблем, когда речь идет о взаимной правовой помощи или международном сотрудничестве, включая выдачу электронных доказательств и обмен ими. Для обеспечения эффективного осуществления законов о киберпреступности, в частности, в тех случаях, когда существует необходимость в сотрудничестве с другими государствами, важно обеспечить определенную степень согласования законодательства, что потребует достижения согласия в отношении определения киберпреступности. Существуют различные обязательные или необязательные региональные документы, направленные на противодействие киберпреступности, однако многие страны могут отказаться ратифицировать какие-либо существующие региональные документы ввиду особенностей расстановки политических сил, международных планов и социально-экономических условий.

335. Что касается технической помощи, Южная Африка отметила, что, несмотря на существование двусторонних и многосторонних соглашений (например, положения Конвенции об организованной преступности, касающиеся взаимной правовой помощи, выдачи и передачи осужденных лиц и конфискации активов), региональные и континентальные соглашения, как представляется, заменяют их с точки зрения функциональности. Международное сотрудничество в области борьбы с киберпреступностью в большинстве случаев является ограниченным и не включает в себя процедуры, необходимые, в том числе, для хранения доказательств, предоставления данных о трафике в ускоренном порядке или обеспечения доступности доказательств.

336. К другим нерешенным, по мнению Южной Африки, проблемам относятся различия в национальном законодательстве стран, включая различные описания киберпреступности, различные процедуры, касающиеся международного сотрудничества, официальные межгосударственные процедуры, которые необходимо соблюдать, чтобы доказательства были приняты судами, законы о неприкосновенности частной жизни и т.д.

337. По мнению Южной Африки, отсутствие в различных странах национальных структур, обладающих полномочиями координировать запросы об оказании взаимной помощи, снижает эффективность взаимной правовой помощи. Различные региональные документы, направленные на борьбу с киберпреступностью, ведут к фрагментации и изолированности взаимодействия между странами и не позволяют обеспечить надлежащее международное сотрудничество. Отсутствие общепризнанного инструмента на уровне Организации Объединенных Наций в отношении международного сотрудничества по вопросам киберпреступности является существенным фактором, обусловливающим неэффективность международного сотрудничества в этой области.

338. Южная Африка убеждена в том, что роль УНП ООН и, в частности, Комиссии по предупреждению преступности и уголовному правосудию в обеспечении укрепления потенциала следует повысить. Проблема заключается в том, что различным национальным органам не хватает средств для проведения специализированной подготовки, которая позволила бы им эффективно расследовать сложные дела о киберпреступности. Кроме того, удержание опытных и подготовленных сотрудников также вызывает трудности ввиду спроса на них в частном секторе. Отмечается повсеместное отсутствие учебных программ базового и среднего уровня в учебных заведениях по подготовке сотрудников правоохранительных органов, а опытным следователям в связи с загруженно-

стью работой нечасто предоставляется возможность посещать курсы повышения квалификации или семинары-практикумы. Даже при наличии наилучших намерений и предлагаемых мер ограниченность бюджета и возможностей затрудняют осуществление предлагаемых мер, а существующие возможности и ресурсы часто ограничены мандатом организации и не могут в обязательном порядке использоваться для оказания помощи другим учреждениям. Кроме того, не существует официальных механизмов или руководящих указаний по сотрудничеству между соответствующими заинтересованными сторонами в области борьбы с киберпреступностью.

Испания

339. Испания сообщила, что киберпреступность, возникшая в результате все более широкого использования информационно-коммуникационных технологий, является одной из главных угроз и одной из наиболее важных проблем, с которыми сталкиваются все государства, в том числе в связи с многообразием преступных методологий, используемых транснациональными организованными группами. Преступники используют коммуникационные платформы и новые информационно-коммуникационные технологии для создания новых незаконных бизнес-моделей, таких как использование даркнета для совершения других преступлений (например, незаконный оборот огнестрельного оружия и фальшивых денег), использование сложных вредоносных программ (например, вирусов-вымогателей) и привлечение лиц, контролирующих банковскую инфраструктуру и так называемых криминальных индивидуальных предпринимателей, предлагающих незаконные услуги. Все вышеперечисленное создает проблемы как для сотрудников служб безопасности, так и для общества в целом.

340. Широко распространенный и быстрый рост доступа в интернет, а также увеличение количества устройств, обеспечивающих связь, приведет к увеличению числа потенциальных жертв киберпреступности. Аналогичным образом, учитывая темпы роста населения в развивающихся странах (главным образом, в Африке) и прогнозы в отношении роста числа пользователей интернета в этих странах, легко предвидеть значительное расширение масштабов использования интернета для совершения преступлений, в особенности экономических преступлений. Однако точно так же, как преступники учатся использовать новые технологии для создания новых методов деятельности, полицейские власти могли бы использовать технологические инновации и разрабатывать новые меры для расследования и пресечения угрозы, исходящей от организованной преступности и тяжких преступлений.

341. Включение в национальное законодательство требований в отношении негласных расследований в интернете было признано Испанией одним из ключевых инструментов в борьбе с организованной преступностью и тяжкими преступлениями, которые совершаются с использованием информационно-коммуникационных технологий. Это также относится к все более широкому использованию новых технологий, таких как беспилотные летательные аппараты, специальное программное обеспечение, облачные услуги и быстрый доступ к социальным сетям.

342. Меры противодействия преступлениям, планируемым и осуществляемым через интернет и в целом с использованием информационно-коммуникационных технологий, являются важной составной частью Стратегии национальной безопасности Испании, опубликованной в декабре 2013 года и обновляемой в настоящее время. В результате борьба с киберпреступностью считается частью более широкой задачи по обеспечению безопасного использования киберпространства на основе комплексной модели. Она включает координацию и сотрудничество между органами государственной власти, частным сектором и населением, а также интеграцию международных инициатив во внутренний и международный правовой режим. Применение этого подхода осуществлялось различными способами.

343. Во-первых, в контексте законодательных реформ, принятие в 2015 году Органических законов № 1/2015 и № 2/2015 позволило провести важную реформу Уголовного кодекса Испании в духе европейских нормативных актов (директива 2013/40 и директива 2011/93, DM 2008/919/JAI и т.д.) а также Конвенции Совета Европы о киберпреступности и Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия. Эти документы содержат определения новых преступлений, которые послужили основанием для широкомасштабной реформы соответствующих положений Уголовного кодекса, касающихся, например, компьютерных атак, сексуальных домогательств в отношении несовершеннолетних, детской порнографии, интеллектуальной собственности, преступлений на почве ненависти, компьютерного мошенничества и преступлений, связанных с терроризмом. Кроме того, в 2015 году путем принятия Органического закона № 13/2015 была проведена значимая реформа уголовно-процессуального законодательства, основанная на Конвенции Совета Европы о киберпреступности. В ее рамках были регламентированы важные технические меры, касающиеся регистрации, накопления и сохранения данных. Для облегчения толкования этих законодательных изменений Генеральная прокуратура опубликовала соответствующие циркуляры.

344. Во-вторых, что касается организационных мер, в структуре всех органов национальной полиции Испании и полиции ее автономных провинций уже свыше 20 лет существуют специальные подразделения, состоящие из сотрудников, обладающих высокой квалификацией в области технологических исследований, а также знаниями и опытом в области эффективного противодействия использованию информационно-коммуникационных технологий в преступных целях. Этот опыт позволяет органам полиции использовать новые технологии, например большие данные, а также сетевые устройства, которые могут быть встроены в такие предметы, как одежда, ювелирные изделия и обувь, в целях расследования преступлений и выявления подозреваемых.

345. В прокуратуре Испании также был создан специализированный отдел в области борьбы с киберпреступностью. С 2011 года в рамках национальной сети прокуроров, созданной специально для осуществления преследования киберпреступлений, работает около 150 прокуроров на всей территории страны, в столицах 50 провинций и в ряде отдельных городов. Специализированные подразделения прокуратуры и полиции поддерживают постоянные контакты с другими органами, отвечающими за обеспечение кибербезопасности, в целях обеспечения надлежащей координации и безопасного использования киберпространства для всех. К их числу относятся Испанское агентство по защите данных, Национальный центр по защите важнейших объектов инфраструктуры, Национальный институт по вопросам кибербезопасности, Национальный криптологический центр и Объединенное командование по кибербезопасности, а также организации частного сектора и такие структуры, как банковские учреждения или учреждения, отвечающие за телекоммуникации и предоставление других основных услуг.

346. Испания сочла важным продолжать поддержку подготовки сотрудников специализированных подразделений по борьбе с киберпреступностью, а также наращивать их людские и материальные ресурсы. В последние годы также уделялось внимание подготовке исследователей и должностных лиц системы правосудия, преимущественно судей и прокуроров, которая осуществлялась на двух уровнях:

a) общая подготовка в области базовых и основных знаний, предназначенная для всех специалистов, участвующих в борьбе с преступностью;

b) специализированная подготовка сотрудников подразделений или групп, которые конкретно занимаются борьбой с киберпреступностью.

347. Испания заявила, что международное сотрудничество играет важную роль в решении общей для всех государств проблемы киберпреступности. К некоторым примерам участия страны в совместных международных усилиях относят-

ся активное участие в работе Сети 24/7, созданной в соответствии со статьей 35 Конвенции Совета Европы о киберпреступности; Европейской судебной сети по борьбе с киберпреступностью; а также Европейской сети специальных прокуроров по защите интеллектуальной собственности. Кроме того, Государственная прокуратура Испании поддерживает работу Иберо-американской сети специальных прокуроров (CibeRed) и участвует в ней.

348. Испания сообщила, что она является активным членом Комитета Совета Европы по Конвенции о киберпреступности и рабочих групп по подготовке второго дополнительного протокола к ней, направленного на укрепление международного сотрудничества и взаимодействие с операторами, поставщиками и организациями частного сектора. Испания участвует в проведении многочисленных транснациональных расследований совместно со странами Европы и Латинской Америки, используя современные методы сотрудничества, такие как создание совместных следственных групп. Кроме того, она участвует в проведении обучения в других странах, в том числе предоставляя инструкторов.

Шри-Ланка

349. Шри-Ланка подчеркнула, что она принимала активное участие в работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, которая недавно провела обзор глав 5 и 6 проекта всестороннего исследования проблемы киберпреступности, представленного в феврале 2013 года. На своем следующем совещании Группа экспертов сосредоточится на двух заключительных главах 7 и 8 («Международное сотрудничество» и «Предупреждение»).

350. Шри-Ланка хотела бы прояснить вопрос о наличии связи между информацией, запрашиваемой в соответствии с резолюцией 73/187 Генеральной Ассамблеи, и текущей работой УНП ООН над проектом всестороннего исследования проблемы киберпреступности, а также вопрос о том, дублируется ли работа Группы экспертов для проведения всестороннего исследования проблемы киберпреступности.

351. По вопросу о внутреннем законодательстве о киберпреступности Шри-Ланка сообщила, что ее основным законодательным инструментом в борьбе с киберпреступностью является Закон № 24 о компьютерных преступлениях от 2007 года. Кроме того, существует Закон № 30 о мошенничестве с платежными инструментами от 2006 года, непосредственно касающийся владения несанкционированными или поддельными платежными инструментами или их использования.

352. Шри-Ланка стала государством — участником Конвенции Совета Европы о киберпреступности в 2015 году. В этой связи она продемонстрировала твердую приверженность гармонизации и совершенствованию национального законодательства в соответствии с наилучшими имеющимися международными стандартами, регулирующими борьбу с киберпреступностью. Шри-Ланка также привержена делу совершенствования методов расследования и расширения возможностей сотрудников системы уголовного правосудия в использовании более эффективных методов правоприменения.

353. Положения материального права, содержащиеся в разделах 3–10 Закона о компьютерных преступлениях, основаны на статьях 2–8 Конвенции Совета Европы о киберпреступности, в то время как статья 9 Конвенции частично отражена в статье 286A Закона № 22 о внесении поправок в Уголовный кодекс от 1995 года. Закон № 36 об интеллектуальной собственности от 2003 года касается преступлений, охватываемых статьей 10 Конвенции Совета Европы о киберпреступности.

354. В целях решения возникающих проблем киберпреступности Шри-Ланка приступила к проведению обзора национальных мер в области уголовного пра-

восудия в области обеспечения безопасности детей в интернете. В связи с этим Шри-Ланка недавно утвердила поправку к Постановлению о непристойных публикациях в целях всестороннего противодействия правонарушениям, связанным с детской порнографией. В соответствии с данной поправкой в Постановление будет включена новая глава «Детская порнография посредством использования компьютерных систем».

355. Что касается правоприменительных мер в отношении киберпреступности и электронных доказательств, то процессуальные положения, содержащиеся в части II Закона о компьютерных преступлениях, предусматривают перехват и сбор основной информации об абонентах и данных о трафике в режиме реального времени и направление просьб об обеспечении сохранности данных. На эти положения распространяются гарантии в соответствии со статьей 15 Конвенции Совета Европы о киберпреступности[9].

356. Согласно статье 18 этого закона, для получения правоохранительными органами основной информации об абонентах, находящейся в распоряжении поставщиков услуг, требуется судебное предписание. Аналогичное требование должно быть соблюдено и в отношении перехвата сообщений. В соответствии со статьей 19 закона при выполнении распоряжений об обеспечении сохранности данных лицо, ответственное за компьютер или информационную систему, обязано обеспечивать сохранность данных по запросу правоохранительных органов. Однако продолжительность периода хранения данных не должна превышать семи дней. Продление срока хранения данных возможно только при наличии соответствующего судебного ордера.

357. Судебный надзор за выполнением данных процессуальных мер служит поставщикам услуг защитой от ненужных и произвольных запросов со стороны правоохранительных органов, а также гарантирует, что поставщики услуг будут оказывать помощь сотрудникам правоохранительных органов в целях эффективной борьбы с преступностью. Данные гарантии, предусмотренные в национальном законодательстве, не оказывают негативного влияния на эффективность и действенность уголовных расследований. С другой стороны, эти гарантии способствуют повышению уровня доверия потерпевших и предприятий (особенно банков и финансовых организаций), побуждая их сообщать о случаях совершения киберпреступлений, а также укрепляют доверие поставщиков телекоммуникационных услуг в вопросах сотрудничества с правоохранительными органами. Они могут послужить примером передовой практики для развивающихся стран.

358. В структуре полиции было создано специальное подразделение по расследованию киберпреступлений с двумя отделами в провинциях. Оно выполняет функции круглосуточного контактного центра, предусмотренного Конвенцией Совета Европы о киберпреступности. Недавно это подразделение прошло модернизацию; оно осуществило успешное расследование более 750 дел благодаря опыту, накопленному национальными сотрудниками в рамках принятия мер по укреплению потенциала, о которых говорится ниже.

359. Шри-Ланка подчеркнула, что получение электронных доказательств от иностранных поставщиков услуг имеет существенное значение для проведения расследований и уголовного преследования киберпреступлений. Поскольку эти доказательства находятся в разных юрисдикциях, первостепенное значение

[9] В соответствии с Законом о компьютерных преступлениях жесткие следственные меры, такие как обыск и конфискация компьютеров или перехват сообщений, должны быть санкционированы судьей (раздел 18). В главе III Конституции Шри-Ланки закреплен и гарантирован ряд основных прав. Шри-Ланка также является государством — участником ряда международных договоров по правам человека, в том числе Международного пакта об экономических, социальных и культурных правах, Международного пакта о гражданских и политических правах, Конвенции о правах ребенка и Конвенции против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания.

приобретает вопрос обеспечения применения более эффективных методов расследования в сочетании с эффективным международным сотрудничеством. Вопросы международного сотрудничества в области уголовного правосудия рассматриваются в соответствии с Законом № 25 о взаимной правовой помощи по уголовным делам от 2002 года. Положения этого закона были включены путем отсылки в Закон о компьютерных преступлениях; в 2018 году Законом № 24 от 2018 года в Закон № 25 от 2002 года были внесены поправки с учетом положений Конвенции Совета Европы о киберпреступности.

360. Что касается мер по укреплению потенциала, то Шри-Ланка разработала для судебной системы, Генеральной прокуратуры и полицейских подразделений ряд программ по киберпреступности и электронным доказательствам, посвященных вопросам совершенствования методов правоприменения и расследования. Эти программы реализуются в рамках проекта, осуществляемого при поддержке Европейского союза и Совета Европы. Благодаря принятию этих мер по наращиванию потенциала сотрудники национальных правоохранительных органов научились использовать более эффективные стандартные оперативные процедуры, основанные на передовой практике и опыте, а также на уроках, извлеченных из опыта других государств — участников Конвенции Совета Европы о киберпреступности.

361. Шри-Ланка сообщила, что в октябре 2018 года ее правительство приняло всестороннюю стратегию обеспечения кибербезопасности. В связи с этим Шри-Ланка в настоящее время разрабатывает законопроекты о кибербезопасности и защите данных. Эти инициативы осуществляются под руководством Министерства цифровой инфраструктуры и информационных технологий при поддержке групп реагирования на критические ситуации в компьютерных сетях, Агентства информационно-коммуникационных технологий, Центрального банка Шри-Ланки и других ключевых заинтересованных сторон. Министерство привлекло частный сектор к участию в этой деятельности, а правительство будет придерживаться инклюзивного подхода, консультируясь с основными заинтересованными сторонами при рассмотрении новых законопроектов.

Швейцария

362. Швейцария отметила, что развитие информационно-коммуникационных технологий создает не только беспрецедентные возможности для частных лиц, корпораций, предприятий и торговли, но и проблемы, особенно в области уголовного правосудия, а следовательно, и в области верховенства права. Киберпреступность в строгом смысле этого слова, т.е. правонарушения, совершаемые через компьютерные системы, включая правонарушения, оставляющие электронные улики в компьютерных системах, переживает непрерывное развитие, а доказательства этих правонарушений все чаще хранятся на серверах, расположенных в иностранных юрисдикциях, причем эти серверы могут быть многочисленными, могут меняться, могут быть неизвестными, как, например, облачные хранилища, тогда как правоохранительные органы ограничены территориальными границами и должны уважать суверенитет государств.

363. Швейцария с обеспокоенностью отметила ограниченную эффективность взаимной правовой помощи в обеспечении сбора нестабильных электронных доказательств, случаи утраты местонахождения данных (информации об их местонахождении), а также тот факт, что в отсутствие международных норм государства все чаще полагаются на принцип использования одностороннего трансграничного доступа к данным.

364. Как государство — участник Конвенции Совета Европы о киберпреступности Швейцария подчеркнула важность данной Конвенции. По мнению Швейцарии, Конвенция способствует значительному упрощению сотрудничества благодаря унификации законов, установлению процедур и созданию кон-

тактных центров. Опираясь на эту Конвенцию, необходимо содействовать установлению и расширению международного сотрудничества.

365. В ближайшие годы решающее значение будет иметь вопрос о том, в достаточной ли мере поставщик услуг представлен на территории государства-участника или предлагает услуги на этой территории, подпадая, тем самым, под юрисдикцию данного государства. Этот вопрос будет важен с точки зрения не только уголовного права, но и, например, налогового и авторского права.

366. Швейцария подчеркнула, что государства обязаны соблюдать на постоянной основе свои обязательства по международному праву, в частности по праву прав человека, в том числе при регулировании киберпространства и при обеспечении криминализации киберпреступлений, их расследовании и судебном преследовании за их совершение. Необходимо учитывать и соблюдать принципы защиты данных и другие гарантии верховенства права, в частности, при рассмотрении и обсуждении новых способов международного сотрудничества и проведения транснациональных расследований.

Сирийская Арабская Республика

367. Сирийская Арабская Республика подчеркнула, что угроза киберпреступности растет с каждым днем по мере расширения масштабов использования информационно-коммуникационных технологий преступными сетями и террористическими группами для достижения своих преступных и террористических целей. Эта угроза подрывает стабильность стран, их инфраструктуру и институты, особенно социальную и культурную структуру, а также экономическое развитие и прогресс в области развития. Расширение цифрового разрыва между государствами неизбежно влияет на возможности многих государств в области предотвращения таких преступлений, осуществления судебного преследования за их совершение и борьбы с ними.

368. По мнению Сирийской Арабской Республики, нет никаких сомнений в том, что высокий уровень преступности и увеличение числа преступлений, совершаемых в цифровом мире, оказали значительное влияние на распространение террористических преступлений по всему миру, особенно преступлений, совершаемых террористическими организациями в Ираке и Сирийской Арабской Республике. Действуя в неконтролируемом и неотслеживаемом цифровом пространстве, террористы получают возможность совершать все виды преступлений — от убийств, торговли людьми, незаконного оборота культурных ценностей и разграбления религиозных памятников и объектов до использования интернета для надругательств над детьми, похищений и вербовки детей для участия в военных действиях и террористических актах, совершения актов расизма и подстрекательства к ненависти и межконфессиональной, этнической или доктринальной розни, а также других тяжких нарушений соответствующих международных законов, конвенций и резолюций, что требует принятия серьезных международных мер реагирования.

369. Сирийская Арабская Республика приняла многочисленные меры по противодействию угрозе киберпреступности и использованию цифрового пространства террористическими группами для совершения наиболее гнусных форм транснациональных террористических преступлений, в том числе меры по укреплению своей нормативно-правовой базы. В этой связи правительство издало Законодательный указ № 17 от 2012 года о борьбе с киберпреступностью и введении в действие Цифрового уголовного кодекса в целях повышения эффективности борьбы с традиционными преступлениями, связанными с использованием информационно-коммуникационных технологий. В целях повышения осведомленности о серьезности этого преступления, укрепления потенциала и обеспечения защиты потерпевших в стране был принят Закон № 9 от 2018 года, предусматривающий создание государственной прокуратуры и специализированных судов по преступлениям в сфере информации и средств связи.

370. При применении законодательства на практике компетентные органы сталкивались с многочисленными проблемами и задачами, связанными с тем, что данный вид преступлений не имеет ограничений по своему характеру и, таким образом, усложняет проведение уголовных расследований для правоохранительных органов. К числу этих проблем относится наличие монополии развитых стран на глобальный интернет, а также политизация работы и отсутствие сотрудничества с властями Сирийской Арабской Республики в вопросах предоставления доказательств и информации о лицах, совершающих преступные деяния через интернет. Кроме того, Сирийская Арабская Республика сообщила, что блокада и односторонние и незаконные принудительные меры, введенные против нее Соединенными Штатами и другими странами и Европейским союзом, которые обладают монополией на коммуникационные технологии, ограничивают доступ соответствующих властей страны к технологиям и инструментам, необходимым для борьбы с этими преступными деяниями.

371. По мнению Сирийской Арабской Республики, уголовно-правовые документы, используемые в настоящее время на международном и региональном уровнях, не обладают достаточной эффективностью для противодействия незаконному использованию информационно-коммуникационных технологий в преступных и террористических операциях. В настоящее время в этой области не существует ни одной международной конвенции, за исключением Конвенции Совета Европы о киберпреступности, которая, в свою очередь, не охватывает вопросы использования информационных технологий в террористических актах.

372. В свете вышеизложенного и в целях активизации борьбы с использованием информационно-коммуникационных технологий в преступных целях Сирийская Арабская Республика рекомендовала принять следующие меры:

a) государствам следует строго соблюдать свои международные обязательства и выполнять соответствующие резолюции Совета Безопасности по борьбе с терроризмом;

b) содействовать эффективному региональному и международному сотрудничеству, в том числе посредством обмена информацией, и разработать согласованный гибкий механизм обмена информацией и цифровыми доказательствами;

c) достичь предварительной договоренности между государствами-членами о путях поиска решений в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, с тем чтобы создать в Нью-Йорке рабочую группу открытого состава Организации Объединенных Наций для обеспечения участия всех заинтересованных государств в обсуждении этого вопроса;

d) разработать имеющий обязательную юридическую силу международно-правовой документ о международном сотрудничестве в этой области, отвечающий интересам государств-членов, принимая во внимание тот факт, что существующие правовые документы в области уголовного права являются недостаточно эффективными для борьбы с преступностью в сфере информационно-коммуникационных технологий;

e) преодолеть цифровой разрыв за счет отказа государств от их монополии на электронные технологии и инструменты, так как эта монополия оказалась не в состоянии обеспечить полную защиту от последствий неправомерного использования информационно-коммуникационных технологий, путем снятия ограничений на передачу технологий и инструментов всем странам без какой-либо дискриминации;

f) повысить эффективность мер предотвращения и защиты при активном сотрудничестве и участии всех государств;

g) ускорить выполнение просьб о международном сотрудничестве, особенно касающихся сбора и обеспечения сохранности цифровых доказательств, и установить сроки выполнения этих просьб;

h) рассмотреть вопрос о создании интерактивной глобальной онлайновой платформы, объединяющей соответствующие национальные органы власти каждого государства-члена. Эта платформа позволит упростить процедуру обмена информацией по делам о транснациональной киберпреступности; кроме того, на этой платформе будут представлены руководящие принципы безопасного использования онлайновых баз данных, а также специализированные программы содействия предупреждению киберпреступности и участия в ней и другие руководящие принципы, способствующие принятию мер оперативного реагирования, которые соответствуют сложности технологий, используемых в таких преступлениях;

i) укреплять национальный потенциал и наращивать техническую помощь в целях повышения квалификации компетентных органов для эффективного решения проблем киберпреступности и проблем, связанных с цифровыми доказательствами, в том числе путем содействия национальным усилиям по развитию и развертыванию инфраструктуры интернета в целях расширения возможностей борьбы с киберпреступностью, а также содействия профессиональной подготовке кадров и повышению осведомленности по техническим вопросам и вопросам перевода отчетности в цифровой формат;

j) обеспечить наличие необходимого оборудования для сбора цифровых доказательств и способствовать обучению достаточного числа квалифицированных и подготовленных следователей в области цифровых технологий методам контроля киберпреступлений и сбора соответствующих цифровых доказательств;

k) разработать имеющие обязательную юридическую силу нормативные стандарты использования цифрового пространства, принимая во внимание необходимость соблюдения равновесия между свободой интернета, неприкосновенностью частной жизни и безопасностью государств, а также разработать рамки противодействия злоупотреблению цифровым пространством. Например, следует установить наблюдение за веб-сайтами, осуществляющими обмен криптовалюты биткоин, которая может использоваться для отмывания денег и финансирования терроризма, а также за платформами социальных сетей, используемыми для подстрекательства к совершению преступлений;

l) укрепить партнерские связи между соответствующими государственными учреждениями и компаниями частного сектора, такими как поставщики услуг интернета, сети сотовой связи и другие, в целях получения хранящейся информации по запросу, в соответствии с требованиями правового и судебного контроля, для завершения расследования информационных преступлений и получения доказательств.

Таджикистан

373. Таджикистан отметил, что распространение информационно-коммуникационных технологий и развитие информационной инфраструктуры способствовали созданию информационного общества. Как показывает мировой опыт, информационная эра способствовала развитию механизмов политического насилия, прибавив к физическим методам убеждения методы манипулирования сознанием и другие информационные способы воздействия на общественное сознание.

374. Таджикистан сформулировал следующие рекомендации:

a) правительствам следует обеспечивать надлежащую информационную и профессиональную подготовку сотрудников своих правоохранительных органов и снабжать их достаточными ресурсами для эффективного расследова-

ния преступлений, связанных с использованием интернета и других информационно-коммуникационных технологий;

b) правительствам следует рекомендовать своим правоохранительным органам овладеть специальными навыками, помогающими в расследовании киберпреступлений и позволяющими успешно осуществлять уголовное преследование;

c) правительства должны предпринимать совместные действия для обеспечения эффективного межведомственного и межрегионального обмена информацией, устранения препятствий, возникающих при проведении расследований киберпреступлений в нескольких странах, и внесения необходимых изменений в законодательство, практику и процедуры в целях ускорения обмена информацией, обработки запросов, поступающих из различных информационных ресурсов, и передачи цифровых доказательств;

d) необходимо регулярно организовывать специальные курсы и обеспечивать надлежащую профессиональную подготовку сотрудников правоохранительных органов по вопросам борьбы с киберпреступностью и использования интернета и других информационно-коммуникационных технологий;

e) необходимо разработать и принять универсальную, отвечающую интересам всех государств-членов конвенцию Организации Объединенных Наций по вопросам сотрудничества в борьбе с преступлениями, связанными с использованием информационно-коммуникационных технологий.

Таиланд

375. Таиланд сообщил, что типичные киберпреступления, совершаемые в стране, включают хакерскую деятельность, мошенничество в интернете, вторжение на веб-сайты, виртуальное преследование, хищение личных данных в интернете, надругательства над детьми в интернете, распространение оскорбительного контента и вредоносных кодов, а также атаки с использованием программ-вымогателей. Преступники всегда стремятся найти пробелы в технологиях в целях сокрытия своей личности, в том числе применяя инновационные подходы, например используя валюту дешифрования (криптовалюту) в системе блокчейн для отмывания денег.

376. Таиланд также сообщил о возникающих трудностях со сбором цифровых доказательств при расследовании большинства киберпреступлений. Это связано с тем, что важными доказательствами в рамках уголовного преследования за киберпреступления являются данные о компьютерном трафике, хранящиеся у поставщиков услуг интернета и социальных сетей, таких как Facebook, Line, Instagram, WeChat и WhatsApp, которые зачастую зарегистрированы в иностранных государствах и не обязаны оказывать помощь и сотрудничать в соответствии с Законом Таиланда о компьютерной преступности. Таким образом, правоохранительные органы вынуждены запрашивать эти доказательства по официальным каналам договоров об оказании взаимной правовой помощи. Осуществление этого процесса, отнимающее много времени, может оказаться затруднительной задачей. Информация, полученная по неофициальным каналам сотрудничества, может оказаться неприемлемой в качестве доказательства в суде, несмотря на свою ценность.

377. Кроме того, некоторые новые технологии, такие как шифрование, препятствуют получению доступа к данным. Некоторые «умные» мобильные телефоны не могут быть разблокированы без согласия владельцев устройств; это обстоятельство препятствует получению доступа к их операционным системам. Кроме того, специалисты, проводящие компьютерно-техническую экспертизу, повсеместно сталкиваются с проблемой отсутствия цифровых инструментов и программного обеспечения для проведения судебной экспертизы ввиду их высокой стоимости, а бесплатные инструменты и программное обеспечение с от-

крытым исходным кодом имеют ограниченные возможности в области проведения компьютерно-технической экспертизы.

378. Таиланд также сообщил, что правоохранительные органы могут недостаточно хорошо разбираться в цифровых доказательствах и современных финансовых банковских технологиях. Многие сотрудники могут не иметь опыта изучения финансовой отчетности или поиска косвенных доказательств, в том числе при помощи современных методов проведения киберрасследований. В этой связи необходимо организовать подготовку по вопросам киберпреступности для прокуроров и других сотрудников правоохранительных органов, а также создать платформу для обмена знаниями и передовым опытом.

379. Хотя поставщики услуг обязаны обеспечивать сохранность данных о трафике и предоставлять запрашиваемую информацию компетентным органам в соответствии с Законом о компьютерной преступности, некоторые поставщики услуг не всегда полностью соблюдают этот закон. Некоторым поставщикам требуется время для предоставления запрашиваемых данных из-за большого количества поступающих запросов. Некоторые поставщики услуг неохотно раскрывают данные, испытывая опасения в отношении защиты неприкосновенности частной жизни своих клиентов.

380. Таиланд подчеркнул, что важнейшая инфраструктура государств и предприятий оказывается под угрозой ввиду возрастающего использования информационно-коммуникационных технологий и увеличения числа устройств, получающих доступ к интернет-услугам. Техническая целостность и безопасность этих устройств может быть нарушена, однако информационная система должна оставаться стабильной и полностью защищенной. Для защиты системы необходимо сотрудничество между всеми компетентными учреждениями и всеми заинтересованными сторонами. Кроме того, трудно четко определить точную цель запросов, направляемых поставщикам услуг.

381. В Таиланде основным законом в сфере уголовного преследования за киберпреступность является Закон о компьютерной преступности B.E.2550 (2007). Он используется в сочетании с другими законами, предусматривающими уголовную ответственность за киберпреступность, такими как Уголовный кодекс, Закон о борьбе с торговлей людьми, Закон о наркотиках, Закон об авторском праве и Закон о предупреждении и пресечении участия в деятельности транснациональных преступных организаций. Обнародование соответствующих законов должно сопровождаться разработкой программ повышения квалификации сотрудников на рабочем уровне, в том числе сотрудников правоохранительных органов, а также созданием эффективных координационных механизмов. Кроме того, необходимо повышать уровень цифровой грамотности, осведомленности и понимания заинтересованных сторон, а также готовить их к осуществлению таких законов.

382. По вопросам защиты прав отдельных лиц, в том числе детей, Таиланд сообщил, что лица, причастные к торговле людьми, кибертравле и мошенничеству в интернете, включая аферы, используют новые технологии для прямого общения с отдельными лицами и завоевания их доверия в преступных целях. Наряду с этим происходит все более активное распространение экстремистских и негативных идеологий через интернет. К основным задачам относятся следующие:

a) эффективное применение действующих законов и нормативных актов;

b) обеспечение координации между соответствующими учреждениями, такими как правоохранительные органы, финансовые операторы и заинтересованные стороны;

c) привлечение многих заинтересованных сторон к участию в процессе поощрения и защиты прав человека.

383. По мнению Таиланда, при расследовании соответствующих преступлений необходимо принимать во внимание чувства и обстоятельства потерпевших и, следовательно, применять подход, основанный на учете конкретных условий и прав человека. Среди лиц, находящихся в уязвимом положении, особое место занимают дети, становящиеся потерпевшими в делах, связанных с кибертравлей, киберпреследованиями, играми в интернете, рассылкой сообщений сексуального характера, распространением материалов о сексуальном насилии над детьми, привлечением к развратным действиям в интернете (груминг) и сексуальными вымогательствами. Следует обращать особое внимание на социальные сети, такие как Facebook, Instagram и Twitter.

384. Таиланд пришел к выводу, что ни одна страна не может в одиночку предупреждать и пресекать киберпреступность. Поэтому международное сотрудничество и диалог между государствами-членами имеют очень большое значение. Таиланд принимает участие в работе Группы экспертов для проведения всестороннего исследования проблемы киберпреступности — единственной платформы, действующей в этой области. Таиланд надеется, что мандат и деятельность Группы экспертов будут продлены на период после 2021 года.

Турция

385. Турция подчеркнула, что информационно-коммуникационные технологии используются в рамках широкой сети, охватывающей государственный и частный секторы, важнейшую инфраструктуру и отдельных лиц, и получают широкое распространение как на национальном, так и на международном уровне. В результате информационно-коммуникационные технологии играют важную роль с точки зрения устойчивого роста и развития. Однако чем активнее общество использует эти технологии, тем сильнее зависит от них и в большей степени оказывается подверженным рискам, которые сопряжены с их использованием. Отдельные лица, компании, критически важные объекты инфраструктуры и государства сталкиваются с серьезными проблемами, вызванными киберпроисшествиями. Недостатки в обеспечении безопасности информационно-коммуникационных систем могут привести к выходу из строя таких систем, их эксплуатации злоумышленниками или возможной гибели людей, крупномасштабным экономическим потерям, нарушению общественного порядка и/или угрозам национальной безопасности. С другой стороны, преимущества киберпространства позволяют сохранять анонимность и отрицать свою причастность к атакам на информационно-коммуникационные технологии. Трудно обнаружить лиц, предоставляющих финансовую поддержку и организующих постоянные и усовершенствованные кибератаки на информационные системы. В подобной ситуации борьба с угрозами и злоумышленниками становится затруднительной.

386. В этих условиях важнейшую роль играет не только сотрудничество на национальном уровне, в том числе с участием таких заинтересованных сторон, как государственный и частный секторы, университеты, неправительственные организации и отдельные лица, но и международное сотрудничество и обмен информацией. Одной из основных стратегических целей Национальной стратегии и Плана действий в области кибербезопасности является борьба с киберпреступностью. В этой связи Турция поддерживает деятельность на международном уровне в рамках концепции борьбы с киберпреступностью и вносит вклад в эту деятельность.

387. Турция подписала Конвенцию Совета Европы о киберпреступности в 2010 году. Затем Конвенция была включена во внутреннее законодательство посредством принятия в 2014 году Закона об утверждении ратификации Конвенции о киберпреступности. Кроме того, вопросы, связанные с кибербезопасностью, регулируются Уголовным кодексом Турции.

388. Турция отметила, что в условиях все более широкого использования интернета и постоянно развивающихся информационно-коммуникационных технологий киберпространство превратилось в центр всего сущего, привлекая разнообразных лиц, преследующих враждебные цели. Выявление киберпреступников становится все более затруднительным из-за многоуровневой структуры интернета и используемых для доступа к нему прокси-серверов. Злоумышленное использование таких технологий приводит к появлению инструментов, необходимых для совершения киберпреступлений, и удобных средств связи, используемых террористическими группами. Незаконные организации используют информационно-коммуникационные технологии для продвижения и распространения пропагандистских материалов, сбора информации, привлечения средств, вербовки новых членов, управления организованной деятельностью, обмена информацией и планирования или координации террористических актов. Террористические группы, как правило, используют приложения и инструменты с зашифрованными каналами связи для планирования или координации своих враждебных действий. В такой ситуации правоохранительные органы сталкиваются с затруднениями при выявлении личностей и действий террористов.

389. По мнению Турции, укрепление информационной безопасности на глобальном уровне и формирование культуры безопасности в рамках международного сообщества является исключительно важным вопросом для всех заинтересованных сторон. Большое значение имеет также укрепление международно-правовых актов и расширение двусторонних или многосторонних международных соглашений. В этой связи Турция считает, что разработка мер, которые будут способствовать предупреждению использования информационно-коммуникационных технологий в преступных целях и укреплению механизмов международного сотрудничества в этой области, внесет важный вклад в дело выявления террористов и пресечения их деятельности.

390. С другой стороны, публикацию в интернете незаконного контента также можно рассматривать как серьезную проблему, препятствующую обеспечению кибербезопасности. Злоумышленные атаки террористических организаций на общие гуманитарные ценности и право на жизнь во всем мире, а также распространение контента через интернет в качестве инструмента пропаганды свидетельствуют о важности предотвращения использования интернета в незаконных целях. В этой связи борьба с незаконным контентом в интернете должна быть вменена в обязанность не только государствам, но и глобальным интернет-компаниям, которые являются крупнейшими структурами, работающими в сфере интернета. Поэтому структурам, работающим в сфере интернета, следует сотрудничать с соответствующими государствами в целях тщательного предупреждения преступной деятельности всех преступных организаций, действующих на их платформах.

391. По мнению Турции, с учетом того факта, что все террористические группы используют киберпространство для преступной деятельности с различными мотивами, настоятельно необходимо добиться того, чтобы глобальные интернет-посредники как можно быстрее и деликатнее реагировали на просьбы об удалении незаконного контента, связанного с этими террористическими группами. Крайне важно обеспечить энергичное и постоянное выполнение решений об удалении контента; в противном случае злоумышленное использование интернета террористическими группами может нанести непоправимый ущерб. В этой связи сотрудничество со стороны соответствующих поставщиков контента и хостинговых компаний имеет решающее значение для обеспечения полноценного взаимодействия. Глобальные поставщики услуг, выполняющие запросы на удаление контента в соответствии с национальным и международным законодательством и судебными приказами, внесут значительный вклад в борьбу с незаконным контентом на онлайновых платформах.

Соединенное Королевство Великобритании и Северной Ирландии

392. Соединенное Королевство заявило, что при подготовке своего ответа толковало понятие «использование информационно-коммуникационных технологий в преступных целях» как не требующее разъяснений (и более широкое по охвату, чем киберпреступность), хотя обобщенная формулировка этого вопроса не дает возможности сформулировать прямой ответ. Вопросы борьбы с использованием информационно-коммуникационных технологий для совершения преступлений носят чрезвычайно многогранный и сложный характер в зависимости от различных факторов. К этим факторам относятся мотивы преступников, соответствующий профиль и/или уязвимые места потерпевших, методы и технические средства, применяемые преступниками, в том числе конкретные методы маскировки их деятельности, и, отражая все вышеизложенное, наличие факта вторжения в сеть или систему либо связи с преступным контентом (например, материалами, касающимися сексуальной эксплуатации детей) в ходе преступления.

393. С учетом этих вариантов и доминирования информационно-коммуникационных технологий во всех современных видах преступности, как в тех случаях, когда информационно-коммуникационные технологии фигурируют в форме цифровых доказательств, так и в тех случаях, когда элемент информационно-коммуникационных технологий сам по себе является преступлением, понятие «использование информационно-коммуникационных технологий в преступных целях» имеет ограниченную диагностическую ценность. Соединенное Королевство отметило, что «цифровой фактор» преступности является реальностью уже на протяжении некоторого времени, свидетельствуя о том, что преступники всесторонне используют информационно-коммуникационные технологии для расширения масштабов и возможностей совершения правонарушений, а также о том, что общество все шире использует интернет и все сильнее зависит от его использования. Таким образом, правоохранительные структуры сталкиваются с проблемами, которые, по-видимому, неотделимы от некоторых обширных и многочисленных проблем, возникающих перед обществом в процессе борьбы со многими современными преступлениями в целом.

394. Невзирая на эти вопросы, связанные с определениями, Соединенное Королевство упомянуло ряд проблем стратегического характера, повсеместно влияющих на способность государств-членов к проведению конкретных расследований и раскрытию преступлений, включающих элемент информационно-коммуникационных технологий, в том числе следующие проблемы:

a) недостаточный технический потенциал или недостаточный потенциал для проведения расследований с использованием цифровых технологий, включая нехватку сотрудников, обладающих достаточными навыками в области информационно-коммуникационных технологий, или наличие проблем с удержанием таких сотрудников на службе, особенно в национальных правоохранительных органах;

b) отсутствие в ряде стран внутреннего материально-правового законодательства, предусматривающего уголовную ответственность за правонарушения, связанные с информационно-коммуникационными технологиями, и служащего основой для международного сотрудничества посредством взаимного признания таких правонарушений (обоюдное признание соответствующего деяния преступлением);

c) отсутствие внутреннего процессуального законодательства, предусматривающего соблюдение надлежащих гарантий прав человека и режимов надзора, которое допускает проведение расследований правонарушений, связанных с информационно-коммуникационными технологиями, и обеспечивает приемлемость цифровых доказательств в суде;

d) трудности в оценке масштабов и косвенного воздействия правонарушений, связанных с информационно-коммуникационными технологиями, и сопутствующие трудности в повышении осведомленности общества о причиняемом ему вреде и поощрении сообщений о таких правонарушениях;

e) проблемы, связанные с повышением осведомленности общества о необходимости соблюдения правил кибербезопасности и/или о преступлениях, связанных с информационно-коммуникационными технологиями, в целях уменьшения уязвимости в отношении этих преступлений и/или осознания факта совершения преступного деяния для последующего сообщения о нем;

f) проблемы общего характера, возникающие в странах со слабыми правовыми институтами или в государствах, отказывающихся сотрудничать и укрывающих киберпреступников, свидетельствующие о трансграничном характере таких преступлений и о том, что для совершения таких преступлений не требуется физического присутствия преступника в пострадавших странах;

g) как было отмечено в подготовленной Национальным агентством по борьбе с преступностью Национальной стратегической оценке 2018 года, к проблемам, возникающим в связи с использованием преступниками технических средств для более эффективного сокрытия своей деятельности, относятся использование таких технологий, как даркнет, шифрование, виртуальные частные сети и виртуальные валюты.

395. Соединенное Королевство изложило информацию о ряде наиболее актуальных для него вышеупомянутых проблем в письменном представлении пятому совещанию Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, посвященному вопросам правоохранительной деятельности и расследований, а также электронных доказательств и уголовного правосудия[10].

396. Кроме того, помимо этих двух проблем существует серьезная проблема, связанная с неполным предоставлением сообщений о киберпреступности. Соединенное Королевство выявило известный разрыв между опытом общества в области киберпреступности и представлением информации о ней путем сопоставления публичных обследований и официальной статистики отчетности о преступности.

397. Соединенное Королевство также сталкивается с проблемами, вызванными отказом некоторых государств от сотрудничества. В Национальной стратегической оценке 2018 года Национальное агентство по борьбе с преступностью отметило, что «группы киберпреступности, многие из которых действуют на международном уровне и являются русскоговорящими, по-прежнему представляют угрозу для интересов Соединенного Королевства». Во многих случаях такие группы физически базируются в государствах, которые не разрешают выдачу граждан за такие преступления или с которыми не всегда налажено сотрудничество в борьбе против таких групп.

398. Соединенное Королевство считает, что Группа экспертов для проведения всестороннего исследования проблемы киберпреступности предоставляет уникальную возможность дальнейшего изучения основанных на консенсусе решений по борьбе с киберпреступностью среди государств-членов. В частности, статус Группы как платформы для экспертов, уполномоченной систематически рассматривать обширный круг тем, идеально подходит для обеспечения учета широчайшего спектра точек зрения и возможных решений при обсуждении мер реагирования на киберпреступность. Таким образом, Соединенное Королевство считает важным обеспечить признание Группы экспертов в качестве основной платформы для обсуждения киберпреступности под эгидой Комиссии по предупреждению преступности и уголовному правосудию, в соответствии с

[10] Доступно по адресу: www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

мандатом Комиссии на рассмотрение других связанных с преступностью вопросов. Кроме того, Соединенное Королевство призывает УНП ООН и государства-члены в полной мере использовать Группу экспертов в качестве платформы для технических дискуссий экспертов в целях определения принципов работы программы УНП ООН по оказанию технической помощи в борьбе с киберпреступностью.

399. По мнению Соединенного Королевства, Конвенция Совета Европы о киберпреступности является наиболее эффективной рамочной основой для достижения дальнейшего международного консенсуса и согласования подходов к борьбе с киберпреступностью. Конвенция, насчитывающая 63 государства-участника, достигла широкого консенсуса во многих регионах и доказала свою совместимость с различными правовыми и институциональными структурами. Благодаря деятельности Комитета Конвенции о киберпреступности, который содействует диалогу между участниками Конвенции, Конвенция также располагает надежными механизмами, позволяющими учитывать изменения в киберпреступности и идти в ногу с новыми проблемами и технологиями. В связи с этим Соединенное Королевство рекомендует тем государствам-членам, которые еще не являются участниками Конвенции, обратиться с заявкой о присоединении к ней, при условии соблюдения надлежащих гарантий в области прав человека и национального процессуального законодательства. Совет Европы осуществляет программы по наращиванию потенциала для присоединения к Конвенции в странах, еще не обеспечивших соблюдение этих условий; поэтому Соединенное Королевство считает, что государствам-членам следует взаимодействовать с Советом Европы в интересах получения доступа к этим программам технической помощи, когда это необходимо.

Соединенные Штаты Америки

400. Соединенные Штаты сообщили, что сталкиваются с четырьмя основными проблемами, первая из которых связана с давлением в целях ограничения вклада экспертов в международную политику. Хотя традиционные методы правоприменения можно адаптировать к киберпреступности, создаваемые ею проблемы носят сложный и эволюционирующий характер. Таким образом, необходимо, чтобы любые политические дискуссии по вопросам киберпреступности, ведущиеся в Организации Объединенных Наций, опирались на непосредственный вклад и рекомендации технических экспертов. Давление, оказываемое некоторыми правительствами в целях инициирования политических дискуссий по вопросам заключения новых глобальных договоров, несмотря на отсутствие консенсусной поддержки такого подхода, приводит к расходованию ценных ресурсов и подрывает способность экспертов предоставлять содержательные рекомендации относительно путей преодоления основных проблем, с которыми сталкиваются государства-члены при расследовании киберпреступлений и уголовном преследовании за их совершение. Оценка экспертов крайне необходима для понимания таких сложных вопросов, как:

a) защита свободы выражения мнения;

b) надлежащие пределы государственной власти;

c) эффективное осуществление существующих рамок и механизмов;

d) своевременное предоставление развивающимся странам услуг в области профессиональной подготовки и технической помощи.

401. Эта проблема наглядно проявилась в ходе принятия резолюции 73/187 Генеральной Ассамблеи, когда голоса разделились, и это повлекло за собой новые политические прения в Генеральной Ассамблее, подрывающие способность выполнения своего мандата Группой экспертов для проведения всестороннего исследования проблемы киберпреступности, учрежденной резолюцией 65/230 Генеральной Ассамблеи. Резолюция 73/187 препятствует деятельно-

сти Группы экспертов, так как предусматривает подготовку еще одного доклада до того, как Группа завершит разработку своего собственного плана работы, причем этот доклад касается вопросов, в обсуждении которых обычно не участвуют эксперты из правоохранительных органов. Государствам-членам следует способствовать расширению вклада и участия экспертов из правоохранительных органов и системы уголовного правосудия, частного сектора и гражданского общества в процессах разработки политики Организации Объединенных Наций. Государствам-членам следует также обеспечить проведение политических дискуссий на основе рекомендаций национальных экспертов, которые находятся на переднем крае борьбы с киберпреступностью.

402. Вторая проблема связана с эволюцией киберпреступности и транснациональных преступных организаций. Транснациональные преступные организации расширили масштабы угроз киберпреступности, используя информационно-коммуникационные технологии, в том числе даркнет, не только для облегчения атак, но и для создания онлайновых рынков похищенных данных. Государства-члены принимают ответные меры, в том числе за счет увеличения числа государств, присоединившихся к Конвенции Совета Европы о киберпреступности. Используя эту Конвенцию, страны из всех регионов (включая как развивающиеся, так и развитые страны) укрепили свое национальное законодательство и расширили свои возможности в области сотрудничества с другими странами, ограничив тем самым возможности транснациональных преступных организаций использовать национальную инфраструктуру информационно-коммуникационных технологий в преступных целях.

403. Третья проблема касается ограниченности национального потенциала и устаревшей национальной нормативно-правовой базы. Соединенные Штаты сталкиваются с проблемами в работе с партнерами по уголовному преследованию киберпреступности в тех случаях, когда эти страны обладают ограниченным потенциалом и/или не обновили свою внутреннюю нормативно-правовую базу, а также не подготовили свои следственные органы к борьбе с киберпреступностью. В то время как некоторые страны полагаются на уголовные законы общего характера, наиболее эффективными являются особые законы о киберпреступности. Несмотря на отсутствие согласованного определения киберпреступности, существует общее согласие в отношении определения преступного поведения, предусматривающего установление основного перечня правонарушений. Международное сообщество имеет более чем десятилетний опыт разработки эффективных, современных и всесторонних законов о киберпреступности, накопленный в различных правовых системах. Такие законы могут разрабатываться с соблюдением технологического нейтралитета, что позволяет избежать необходимости частого внесения поправок. Конвенция Совета Европы о киберпреступности послужила основным источником для других документов и является образцом для внутреннего законодательства стран с различными культурными и правовыми традициями, включая некоторые государства-члены, которые не рассматривают вопрос о присоединении к Конвенции. Деятельность Соединенных Штатов по уголовному преследованию киберпреступности, осуществляемая совместно с другими странами, оказывается более эффективной при работе со страной, использующей законы, непосредственно касающиеся киберпреступности.

404. Соединенные Штаты также сталкиваются с трудностями при работе со странами, которые успешно приняли законы, непосредственно касающиеся киберпреступности, но которые, однако, либо имеют ограниченные возможности для осуществления своей нормативно-правовой базы, либо не принимают меры по их практическому осуществлению. Кроме того, Соединенные Штаты по-прежнему сталкиваются с серьезными проблемами при получении помощи от некоторых государств-членов, предусматривающей выявление, задержание и судебное преследование правонарушителей в их юрисдикциях и предоставление их компетентным органам полномочий на международное сотрудничество при расследовании дел о киберпреступности. Например, существует настоя-

тельная необходимость в проведении специализированной подготовки сотрудников органов уголовного правосудия по вопросам использования электронных доказательств. Именно поэтому Соединенные Штаты являются донором Глобальной программы УНП ООН по киберпреступности, а также учебных программ, осуществляемых под эгидой Организации американских государств, Совета Европы, АСЕАН и Африканского экономического сообщества. Соединенные Штаты рекомендуют государствам-членам, особенно развивающимся странам, обратить более пристальное внимание на подобные программы. Государствам-членам следует уделять приоритетное внимание вопросам содействия проведению законодательных реформ и наращивания потенциала, с тем чтобы обеспечить претворение новых законов в жизнь.

405. Четвертая проблема связана с трудностями при получении электронных доказательств. Соединенные Штаты, как и другие государства-члены, сталкиваются с трудностями при получении у иностранных государств доступа к электронным доказательствам, все шире используемым правоохранительными органами в ходе расследований в рамках борьбы с киберпреступностью. В частности, Соединенные Штаты сталкиваются с трудностями при получении помощи от государств-членов, не имеющих юридических полномочий или возможностей для эффективного реагирования на просьбы о предоставлении электронных доказательств.

406. Действуя на своей территории, Соединенные Штаты сталкиваются с проблемами, стремясь удовлетворить тысячи просьб других стран об электронных доказательствах; зачастую эти проблемы возникают из-за того, что страны не понимают требований Соединенных Штатов или не предоставляют достаточной информации для соблюдения правовых стандартов Соединенных Штатов. Ввиду недостаточности информации, содержащейся в просьбах об оказании взаимной правовой помощи, власти Соединенных Штатов вынуждены запрашивать разъяснения и дополнительную информацию у зарубежных партнеров, что приводит к задержкам в выполнении этих просьб. Государствам-членам следует принять меры для ликвидации этих пробелов, предоставив центральным и компетентным органам надлежащие ресурсы и необходимую подготовку в соответствии с их обязательствами по таким документам, как Конвенция против организованной преступности. Кроме того, УНП ООН занимается разработкой новых инструментов для центральных и компетентных органов. Соединенные Штаты далее рекомендуют государствам-членам наращивать потенциал в области выполнения требований и процедур взаимной правовой помощи, в том числе при помощи обучения составлению надлежащих просьб о представлении электронных доказательств.

407. Наконец, государства-члены используют для получения электронных доказательств двусторонние договоры о взаимной правовой помощи, а также многосторонние конвенции, такие как Конвенция Совета Европы о киберпреступности и Конвенция об организованной преступности, в качестве правовой основы для сотрудничества. Более 80 стран также принимают активное участие в круглосуточной работе контактных пунктов сети по борьбе с преступлениями в области высоких технологий Группы семи, содействуя обеспечению сохранности данных и удовлетворению других запросов. Соединенные Штаты рекомендуют государствам-членам рассмотреть вопрос о присоединении к таким договорам и сетям и об их использовании в борьбе с киберпреступностью.

Венесуэла (Боливарианская Республика)

408. Правительство Боливарианской Республики Венесуэла признало факт расширения использования информационно-коммуникационных технологий, а также тот факт, что роль международного сообщества в использовании этих технологий может способствовать достижению согласованных на международном уровне целей в области развития, в том числе сформулированных в По-

вестке дня в области устойчивого развития на период до 2030 года, а также решению новых задач.

409. Боливарианская Республика Венесуэла подчеркнула важность устранения препятствий на пути к сокращению цифрового разрыва, в частности таких препятствий, которые мешают всестороннему экономическому, социальному и культурному развитию стран и обеспечению благополучия их народов, особенно в развивающихся странах. Она подчеркнула, что следует прекратить использование тех информационно-коммуникационных технологий, в том числе социальных сетей, которые нарушают международное право и наносят ущерб интересам государств-членов.

410. Боливарианская Республика Венесуэла призвала международное сообщество к совместной работе по обеспечению доступа к информационному обществу, а также к уважению гендерного равенства и расширению прав и возможностей женщин, уважению культурной самобытности, культурного, этнического и языкового разнообразия, традиций и религий и этических ценностей.

411. Боливарианская Республика Венесуэла сообщила, что она стремится обеспечить ответственное использование информации средствами массовой информации и обращение с ней в соответствии с кодексами поведения и профессиональной этики. Средства массовой информации во всех своих формах играют важную роль в информационном обществе, и информационно-коммуникационные технологии должны играть вспомогательную роль в этом отношении. Боливарианская Республика Венесуэла вновь подтвердила необходимость сокращения международных дисбалансов, характерных для средств массовой информации, особенно в области инфраструктуры, технических ресурсов и уровня профессиональной подготовки кадров.

412. Боливарианская Республика Венесуэла заявила о своей обеспокоенности в связи с использованием средств массовой информации в качестве инструмента враждебной пропаганды против развивающихся стран в целях подрыва деятельности их правительств. В этой связи Боливарианская Республика Венесуэла подчеркнула необходимость содействия использованию свободных, плюралистических и ответственных альтернативных средств коммуникации и источников информации, отражающих реалии и интересы стран и народов развивающегося мира.

413. В этой связи Боливарианская Республика Венесуэла, сознавая, что в настоящее время международные уголовно-правовые документы являются недостаточно эффективными для борьбы с преступлениями, связанными с информационно-коммуникационными технологиями, считает необходимым разработать конвенцию Организации Объединенных Наций о сотрудничестве в этой области, которая была бы одобрена международным сообществом и основана на его безоговорочной поддержке и в которой всем государствам-членам было бы рекомендовано создать ответственное информационное общество и содействовать принятию мер, с тем чтобы не допускать осуществления любых односторонних действий, противоречащих международному праву и Уставу Организации Объединенных Наций и препятствующих всестороннему социально-экономическому развитию затронутых стран, а также подрывающих их благополучие.

414. Боливарианская Республика Венесуэла считает, что ввиду этой обеспокоенности по поводу возможного использования информационно-коммуникационных технологий в международных конфликтах, тайных и незаконных операциях и нападениях на третьи страны со стороны частных лиц, организаций и государств с использованием компьютерных систем других стран необходимо принять в рамках Организации Объединенных Наций меры для достижения прогресса в реализации документа, который поможет регулировать использование информационно-коммуникационных технологий и сотрудничество в этой области.

415. С учетом обеспокоенности, вызванной тем, что некоторые правительства способны реагировать на подобные атаки, используя обычное оружие, Боливарианская Республика Венесуэла вновь заявила, что наиболее эффективным способом предупреждения и устранения новых угроз является совместное сотрудничество всех государств, позволяющее избежать превращения киберпространства в театр военных действий. Боливарианская Республика Венесуэла заявила, что считает своим приоритетом содействие диалогу и текущим дискуссиям между государствами-членами в целях обмена передовым опытом, а также национальным или региональным опытом, с уделением особого внимания развивающимся странам. Боливарианская Республика Венесуэла также поддержала предложение о создании межправительственной рабочей группы под эгидой Организации Объединенных Наций, основанной на принципе равенства государств и занимающейся поиском решений и урегулированием разногласий.

416. Боливарианская Республика Венесуэла также признала, что незаконное использование информационно-коммуникационных технологий может иметь пагубные последствия для инфраструктуры, национальной безопасности и экономического развития государств-членов, и поэтому подчеркнула необходимость активизации международных усилий по решению этой проблемы.