Организация Объединенных Наций E/CN.15/2018/12

Экономический и Социальный Совет

Distr.: General
13 April 2018
Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Двадцать седьмая сессия
Вена, 14–18 мая 2018 года
Пункт 8 предварительной повестки дня*
Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения

Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 3–5 апреля 2018 года

I. Введение

1. В резолюции 65/230 Генеральная Ассамблея просила Комиссию по предупреждению преступности и уголовному правосудию в соответствии с пунктом 42 Салвадорской декларации о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развития в изменяющемся мире — учредить и созвать до двадцатой сессии Комиссии межправительственную группу экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки новых предложений в отношении национальных и международных правовых или иных мер по противодействию киберпреступности.

2. Первое совещание Группы экспертов было проведено в Вене 17–21 января 2011 года. На этом совещании Группа экспертов рассмотрела и утвердила подборку тем для рассмотрения и методологию исследования (E/CN.15/2011/19, приложения I и II).

3. Второе совещание Группы экспертов было проведено 25–28 февраля 2013 года. На этом совещании Группа экспертов приняла к сведению проект всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, подготовленный Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) под руководством Группы экспертов во исполнение

* E/CN.15/2018/1.

мандата, предусмотренного в резолюции 65/230 Генеральной Ассамблеи, и в соответствии с подборкой тем для рассмотрения в рамках всестороннего исследования воздействия киберпреступности и ответных мер и методологии исследования, утвержденными на первом совещании Группы экспертов.

4. В Дохинской декларации о включении вопроса предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности, принятой на тринадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и одобренной Генеральной Ассамблеей в резолюции 70/174, государства-члены отметили деятельность Группы экспертов, международного сообщества и частного сектора и предложили Комиссии рассмотреть вопрос о том, чтобы рекомендовать Группе экспертов на основе проводимой ею работы продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления соответствующих мер и выработки предложений в отношении новых национальных и международных правовых и иных мер по противодействию киберпреступности.

5. Третье совещание Группы экспертов было проведено 10–13 апреля 2017 года. На этом совещании Группа экспертов утвердила подготовленные Докладчиком краткие доклады о работе первого и второго совещаний Группы экспертов, рассмотрела, в частности, проект всестороннего исследования проблемы киберпреступности и замечания к нему, а также вопросы дальнейшей работы над проектом исследования, и обменялась информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве.

6. В своей резолюции 26/4, принятой на двадцать шестой сессии в мае 2017 года, Комиссия по предупреждению преступности и уголовному правосудию просила Группу экспертов продолжать свою работу и при этом проводить периодические совещания и выступать в качестве платформы для дальнейшего обсуждения вопросов существа, касающихся киберпреступности, внимательно следя за новыми тенденциями, в соответствии с Салвадорской декларацией и Дохинской декларацией, и просила Группу экспертов продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мерах по противодействию киберпреступности.

7. Сроки проведения четвертого совещания Группы экспертов были определены решением расширенного бюро 23 января 2018 года при отсутствии возражений и подтверждены на его заседании 26 января 2018 года.

II. Перечень предварительных рекомендаций и выводов

8. В соответствии с планом работы Группы экспертов на период 2018–2021 годов, принятым Группой экспертов на ее 1-м заседании 3 апреля 2018 года, Докладчик подготовит на каждом из совещаний Группы экспертов в 2018, 2019 и 2020 годах, при содействии Секретариата и на основе обсуждений и дискуссий Группы экспертов, перечень предварительных выводов и рекомендаций, предложенных государствами-членами, которые должны быть четкими и ориентированными на укрепление практических мер по противодействию киберпреступности. Как указано в плане работы, этот перечень будет включен в доклад о работе каждого совещания в форме подборки внесенных государствами-членами предложений для дальнейшего обсуждения на обзорном сове-

щании, которое должно состояться не позднее 2021 года. Кроме того, в соответствии с планом работы на этом обзорном совещании Группа экспертов рассмотрит собранные таким образом предварительные выводы и рекомендации для составления сводного всеобъемлющего перечня принятых выводов и рекомендаций для представления Комиссии по предупреждению преступности и уголовному правосудию.

A. Законодательство и правовая основа

9. В соответствии с планом работы настоящий пункт содержит подборку предложений, внесенных государствами-членами на совещании по пункту 2 повестки дня под названием «Законодательство и правовая основа». Эти предварительные рекомендации и выводы были представлены государствами-членами, и их включение не означает их одобрения Группой экспертов:

a) государствам-членам следует обеспечить, чтобы их законодательные положения отвечали требованиям времени с учетом технического прогресса посредством принятия законодательства, содержащего технически нейтральные формулировки и предусматривающего уголовную ответственность за деятельность, признаваемую незаконной, а не за использование технических средств. Государствам-членам следует также рассмотреть вопрос о разработке согласованной терминологии для описания киберпреступной деятельности и содействия, насколько это возможно, точному толкованию соответствующего законодательства правоохранительными и судебными органами;

b) государства-члены должны уважать суверенные права других государств при разработке политики и законодательства, отвечающих их национальным особенностям и потребностям в области борьбы с киберпреступностью. Для содействия международному сотрудничеству в борьбе с киберпреступностью принцип национального суверенитета не следует ошибочно трактовать как препятствие, а скорее рассматривать его как основополагающий принцип и как исходное положение. Неустойчивый характер передачи и хранения электронных данных, например в так называемых «облаках», может потребовать участия в многосторонних обсуждениях вопроса об оказании государствами новаторской и расширенной взаимной помощи для обеспечения своевременного допуска к электронным данным и доказательствам;

c) для предупреждения возникновения и/или ликвидации «безопасных гаваней» для преступников государствам-членам следует в максимально возможной степени сотрудничать друг с другом в таких областях, как расследование, сбор доказательств, уголовное преследование, вынесение судебного решения и, в необходимых случаях, изъятие незаконного контента из Интернета. Кроме того, государства должны обеспечивать максимально возможную гибкость своего международного сотрудничества для борьбы с киберпреступностью и другими видами преступности, связанными с использованием электронных данных, при ведении расследований или при обмене доказательствами, независимо от того, называются ли по-другому рассматриваемые виды деятельности в соответствующих государствах. При этом государствам-членам следует иметь в виду, что для выдачи обычно требуется соблюдение принципа обоюдного признания соответствующего деяния преступлением, хотя для взаимной правовой помощи соблюдение этого принципа не является обязательным;

d) при разработке политики и законодательства государствам-членам следует учитывать необходимость обеспечения баланса между защитой прав человека, с одной стороны, и соображениями, касающимися национальной безопасности, общественного порядка и законных прав третьих лиц, — с другой. Национальное законодательство, предусматривающее уголовную ответственность за деяния, связанные с киберпреступностью, и предоставление процессуальных полномочий на проведение расследований, возбуждение уголовного пре-

следование и вынесение судебного решения по делам, связанным с киберпреступностью, должны обеспечивать соблюдение надлежащих процессуальных гарантий, принципов неприкосновенности частной жизни, гражданских свобод и прав человека. Национальная политика и национальное законодательство, а также существующие и/или будущие международные документы должны быть основаны на многоаспектном подходе. С одной стороны, они должны включать адекватные меры борьбы с киберпреступностью, основанные на всестороннем понимании более широкого понятие кибербезопасности. С другой стороны, они должны не только охватывать противоправные деяния, но и должны быть направлены на предупреждение преступности и оказание помощи потерпевшим от преступной деятельности и содействия населению в целом. Для создания прочной основы международного сотрудничества в борьбе с киберпреступностью государствам-членам следует прилагать все усилия по формированию и развитию культуры, ориентированной на создание общего будущего для киберпространства;

e) государствам-членам следует осуществлять международное сотрудничество, не требуя при этом полного согласования национального законодательства при условии, что основное деяние является уголовно наказуемым, а законодательство достаточно сопоставимым для упрощения и ускорения осуществления различных форм такого сотрудничества;

f) государствам-членам следует учитывать тот факт, что внутренняя нормативно-правовая база по-прежнему должна играть решающую роль в обеспечении эффективности и общей сбалансированности системы расследований и уголовного преследования, поскольку уголовное законодательство особо восприимчиво к таким вопросам, как соблюдение основных свобод, и поскольку расследования в области компьютерных преступлений в существенной степени затрагивают частные сообщения и данные граждан;

g) для обеспечения возможности уголовного преследования за совершение преступных деяний, государствам-членам следует в законодательном порядке ввести в действие принцип экстратерриториальной юрисдикции в отношении граждан или лиц, обычно проживающих на их территории, независимо от того, совершены ли эти деяния и являются ли они преступлениями в иностранной юрисдикции;

h) государства-члены могут опираться на разные нормативно-правовые базы международного сотрудничества, включая основанные на взаимности двусторонние или многосторонние договоры и другие договоренности. Кроме того, государства-члены, располагающие более широкими возможностями и развитой инфраструктурой в области борьбы с киберпреступностью, должны взять на себя ответственность, соразмерную этим возможностям или инфраструктуре, по оказанию правовой помощи другим государствам;

i) для обеспечения должного учета соответствующих вопросов, государствам-членам следует на возможно более раннем этапе консультироваться со всеми соответствующими заинтересованными сторонами, включая межправительственных субъектов, частный сектор и гражданское общество, в тех случаях, когда принимается решение о принятии законодательства о киберпреступности;

j) государствам-членам следует развивать прочное и заслуживающее доверие государственно-частное сотрудничество в области борьбы с киберпреступностью, в том числе сотрудничество между правоохранительными органами и поставщиками коммуникационных услуг. Для укрепления и облегчения сотрудничества требуется также участие в диалоге с частными предприятиями в сочетании, в случае необходимости, с налаживанием государственно-частных партнерских отношений и заключением меморандумов о договоренности;

k) государствам-членам следует оказывать поддержку УНП ООН в разработке образовательного проекта или учебной программы, направленных на

повышение осведомленности сотрудников судебных органов и органов прокуратуры, судебных экспертов по цифровым технологиям государств-членов и сотрудников частных образований о киберпреступности и соответствующих мерах и использовать инструменты наращивания потенциала и платформу управления электронными данными для повышения осведомленности гражданского общества о воздействии киберпреступности;

l) эффективная разработка, принятие и осуществление национального законодательства должны подкрепляться мерами по наращиванию потенциала и программами технической помощи. Государствам-членам следует выделять достаточные ресурсы для наращивания национального потенциала. Надлежащее осуществление законодательства в борьбе с киберпреступностью требует обучения сотрудников полиции и прокуроров, а также проведения информационно-пропагандистских кампаний. Такие ресурсы позволят также развивать международное сотрудничество, поскольку расширению такого сотрудничества способствует внутренняя способность стран проводить расследования киберпреступлений и осуществлять уголовное преследование за их совершение;

m) государствам-членам следует укреплять действующую нормативно-правовую базу и существующие сети для борьбы с киберпреступностью посредством выявления и преодоления недостатков этой нормативно-правовой базы и этих сетей и выделения на эти цели необходимых ресурсов для повышения их эффективности;

n) УНП ООН следует активно участвовать в деятельности по наращиванию потенциала в интересах всех нуждающихся в помощи государств-членов, особенно развивающихся стран. Такая деятельность по наращиванию потенциала должна быть политически нейтральной и свободной от каких-либо условий, а также должна быть результатом тщательных консультаций и добровольного выбора страны получателями помощи. По существу эта деятельность по наращиванию потенциала должна охватывать, по крайней мере, следующие области:

i) обучение судей, прокуроров, следователей и сотрудников правоохранительных органов ведению расследований киберпреступлений, обращению с электронными доказательствами, обеспечению хранения и передачи доказательств и проведению судебной экспертизы;

ii) разработка, изменение и/или осуществление законодательства о киберпреступности и электронных доказательствах;

iii) определение структуры подразделений, занимающихся расследованием киберпреступлений, и предоставление руководящих указаний в отношении соответствующих процедур;

iv) разработка, обновление и осуществление законодательства для борьбы с использованием Интернета в террористических целях;

o) УНП ООН следует добиваться взаимодополняемости и тесно сотрудничать с другими заинтересованными сторонами и организациями, такими как Совет Европы и Организация американских государств (ОАГ), в области разработки и осуществления программ наращивания потенциала в борьбе с киберпреступностью в целях обеспечения того, чтобы мероприятия и инициативы в этой области не носили разрозненного или раздробленного характера;

p) государствам-членам следует и далее использовать Группу экспертов в качестве платформы для обмена информацией и наилучшими видами практики, в том числе о типовых законах или типовых положениях, касающихся таких вопросов, как юрисдикция, специальные методы расследования, электронные доказательства, включая проблемы, создаваемые их изменчивым характером и их допустимостью в судах, и международное сотрудничество;

q) во избежание раздробленности государствам-членам следует изучать повсеместно принятые виды практики и правила посредством проведения многосторонних консультаций под эгидой Организации Объединенных Наций и посредством использования Группы экспертов в качестве платформы;

r) государствам-члена следует проводить оценку возможности и целесообразности поручения Группе экспертов или УНП ООН задачи по проведению и обеспечению наличия на регулярной основе оценки тенденций в области киберпреступности при существенном содействии государств-членов;

s) государствам-членам следует разработать в рамках Организации Объединенных Наций новый международный правовой документ по киберпреступности, в котором будут учтены обеспокоенность и интересы всех государств-членов;

t) государствам-членам следует использовать существующие многосторонние правовые документы по киберпреступности, такие как Конвенция Совета Европы о киберпреступности (Будапештская конвенция), или присоединиться к ним, поскольку они рассматриваются многими государствами как модели наилучшей практики, которыми следует руководствоваться при осуществлении надлежащих внутренних и международных мер по борьбе с киберпреступностью;

u) для укрепления международного сотрудничества как можно большему числу государств следует использовать существующие правовые документы и механизмы, включая Конвенцию Организации Объединенных Наций против транснациональной организованной преступности;

v) под эгидой Группы экспертов государствам-членам следует изучить применимые на международном уровне меры противодействия, которые, в надлежащих случаях, можно отразить в типовых законах и типовых положениях, опираясь при этом на наилучшие виды практики в действующих региональных документах и/или национальном законодательстве.

B. Криминализация

10. В соответствии с планом работы настоящий пункт содержит подборку предложений, внесенных государствами-членами на заседании по пункту 3 повестки дня под названием «Криминализация». Настоящие предварительные рекомендации и выводы были представлены государствами-членами, и их включение не означает их одобрения Группой экспертов:

a) государствам-членам следует учитывать тот факт, что многие основные положения уголовного законодательства, применяемые к офлайновым преступлениям, могут также применяться к преступлениям, совершенным в режиме онлайн. В этой связи государствам-членам с целью укрепления правоохранительной деятельности следует применять, в надлежащих случаях, действующие положения внутреннего законодательства и международного права в отношении преступлений, совершаемых в онлайновой среде;

b) государствам-членам следует применять внутреннее законодательство с целью криминализации киберпреступных деяний и предоставления правоохранительным органам процессуальных полномочий по расследованию предполагаемых преступлений при соблюдении должных процессуальных гарантий, принципов обеспечения неприкосновенности частной жизни, гражданских свобод и прав человека;

c) государствам-членам следует и далее принимать уголовное законодательство, касающееся киберпреступлений, в котором учтены новые преступные деяния, связанные с неправомерным использованием информационно-коммуникационных технологий, не полагаясь при этом на общепринятые положения уголовного законодательства;

d) государствам-членам следует ввести уголовную ответственность за совершение основных киберпреступлений, которые воздействуют на конфиденциальность, целостность и доступность компьютерных сетей и компьютерных данных, с учетом широко признанных международных стандартов;

e) деяния в киберпространстве, которые являются незначительными нарушениями, а не уголовными преступлениями, должны регулироваться не уголовным законодательством, а гражданскими и административными положениями;

f) в той степени, в которой они уже не сделали этого, государствам-членам следует рассмотреть вопрос о криминализации:

i) новых или возникающих форм киберпреступной деятельности, таких как преступное использование криптовалют, преступления, совершаемые в «теневой сети» и Интернете вещей, фишинг и распространение зловредных программ и любого другого программного обеспечения, используемого для совершения преступных деяний;

ii) раскрытия личной информации и «порномести»;

iii) использования Интернета для совершения деяний, связанных с терроризмом;

iv) использования Интернета для подстрекательства к совершению преступлений на почве ревности и воинствующего экстремизма;

v) оказания технической помощи или содействия в совершении киберпреступления;

vi) создания незаконных онлайновых платформ или публикации информации с целью совершения киберпреступлений;

vii) незаконного получения доступа к компьютерным системам или их взлома;

viii) незаконного перехвата или повреждения компьютерных данных и повреждения компьютерных систем;

ix) незаконного вмешательства в компьютерные данные и системы;

x) неправомерного использования устройств;

xi) компьютерного подлога и мошенничества;

xii) сексуального принуждения и сексуальной эксплуатации детей;

xiii) нарушения авторских прав;

xiv) сексуального принуждения и сексуальной эксплуатации детей и подстрекательства несовершеннолетних к совершению самоубийства;

xv) оказания незаконного воздействия на важнейшую информационную инфраструктуру;

g) государствам-членам следует обеспечить, чтобы преступления, связанные с использованием компьютеров, рассматривались в специальных положениях, которые не просто предусматривают распространение применения положений о традиционных преступлениях на цифровую среду, а учитывают особенности цифровой среды и фактическую потребность в криминализации на основе тщательной оценки;

h) государствам-членам следует иметь в виду, что основное внимание при международном согласовании положений, касающихся криминализации киберпреступлений, следует уделять основному своду преступлений против конфиденциальности, целостности и доступности информационных систем, при том что вопросам, связанным с необходимостью согласования порядка крими-

нализации общих преступлений, совершаемых с использованием информационно-коммуникационных технологий, следует рассматривать главным образом на специальных форумах, посвященных конкретным областям преступности;

i) государствам-членам следует избегать криминализации широкого круга видов деятельности провайдеров интернет-услуг (ПИУ), особенно в тех случаях, когда такие правила могут ненадлежащим образом ограничивать законную свободу слова и законную свободу выражения идей и убеждений. Вместо этого государствам-членам следует взаимодействовать с ПИУ и частным сектором для расширения сотрудничества с правоохранительными органами с учетом, в частности, того факта, что большинство ПИУ абсолютно заинтересованы в том, чтобы их платформы не использовали преступники;

j) государствам-членам следует принять и использовать на практике внутреннюю нормативно-правовую базу, касающуюся доказательств, которая позволяет считать допустимыми электронные доказательства при проведении уголовных расследований и осуществлении уголовного преследования, включая надлежащий обмен электронными доказательствами с иностранными правоохранительными органами-партнерами;

k) государствам-членам следует использовать Конвенцию об организованной преступности с целью облегчения обмена информацией и доказательствами для проведения уголовных расследований киберпреступлений, принимая во внимание частые случаи участия организованных преступных групп в совершении киберпреступлений;

l) государствам-членам следует изучить пути оказания помощи для своевременного и безопасного обмена информацией между следователями и прокурорами, занимающимися делами, связанными с киберпреступностью, в том числе посредством укрепления сетей национальных учреждений, которые могут работать круглосуточно;

m) при решении вопроса о введении уголовной ответственности в отношении ПИУ за несоблюдение требований правоохранительных органов государствам-членам следует проявлять осторожность и уделять пристальное внимание недопущению пагубных последствий для деятельности частного сектора и соблюдения основных прав человека, в частности свободе слова;

n) для эффективной борьбы с киберпреступностью государствам-членам следует учитывать существующие основы защиты прав человека, в частности касающиеся свободы выражения и права на неприкосновенность частной жизни, и соблюдать принципы законности, необходимости и соразмерности при проведении уголовных разбирательств, касающихся борьбы с киберпреступностью;

o) государствам-членам следует выявлять тенденции в деятельности, лежащей в основе киберпреступности, посредством проведения соответствующих исследований и продолжать работу по оценке возможности и целесообразности поручения Группе экспертов или УНП ООН проведения и опубликования на ежегодной основе оценки тенденций в области киберпреступности при активной поддержке со стороны государств-членов;

p) государствам-членам следует рассмотреть вопрос о принятии всеобъемлющих стратегий борьбы с киберпреступностью, которые включают проведение обзоров виктимизации, а также информирование потенциальных жертв киберпреступности и расширение их прав и возможностей;

q) государствам-членам следует рассмотреть вопрос о принятии дальнейших превентивных мер борьбы с киберпреступностью, включая, в частности, меры по обеспечению ответственного использования Интернета, особенно детьми и молодежью.

III. Резюме обсуждения

A. Утверждение предложения Председателя по плану работы Группы экспертов на период 2018–2021 годов

11. На 1-м заседании 3 апреля 2018 года Группа экспертов рассмотрела пункт 1 (c) повестки дня «Утверждение предложения Председателя по плану работы Группы экспертов на период 2018–2021 годов». Предложение Председателя по плану работы Группы экспертов на период 2018–2021 годов было утверждено.

B. Законодательство и правовая основа

12. На 2, 3 и 4-м заседаниях 3 и 4 апреля 2018 года Группа экспертов рассмотрела пункт 2 повестки дня «Законодательство и правовая основа».

13. В дискуссии по этому пункту участвовали: Лу Чуаньин (Китай), Джордж Мария Тьенвезва (Нигерия), Кристина Шульман (Румыния), Педру Верделью (Португалия), Клаудио Пегеро (Доминиканская Республика), Мария Алехандра Даглио (Аргентина) и Мохамед Мгхари (Марокко).

14. В ходе дальнейших прений многие делегации сообщили о внесении изменений в законодательство и политику своих стран с целью противодействия киберпреступности и решения проблем кибербезопасности. При этом они особо подчеркнули важность программ повышения потенциала и технической помощи для успешного применения национального законодательства и создания национального потенциала в области расследования преступлений, судебного преследования, вынесения судебных решений и международного сотрудничества. Была также отмечена необходимость применения междисциплинарных подходов, предполагающих участие гражданского общества и частного сектора.

15. Ряд выступавших высказали мнение, что в разработке нового глобального всеобъемлющего правового документа по киберпреступности нет необходимости, поскольку для принятия надлежащих мер противодействия киберпреступности на национальном и международном уровнях достаточно уже таких имеющихся международно-правовых документов, как Будапештская конвенция и Конвенция против транснациональной организованной преступности. По мнению этих выступавших, Будапештская конвенция обеспечивает государствам-участникам (в число которых входит ряд государств, не являющихся членами Совета Европы) и государствам, которые используют эту Конвенцию в качестве справочного документа, эффективную правовую и оперативную основу для борьбы с трансграничной киберпреступностью, поскольку, в частности, она облегчает международное сотрудничество и согласование соответствующих положений уголовного и уголовно-процессуального законодательства. Было также упомянуто о работе Комитета участников Конвенции о компьютерных преступлениях и проектах развития потенциала Совета Европы, направленных на содействие осуществлению этой Конвенции, таких как проект «Расширенные глобальные действия по борьбе с киберпреступностью», а также о других внешних проектах технической помощи, в том числе осуществляемых в рамках ОАГ и Экономического сообщества западноафриканских государств. Кроме того, было отмечено, что для согласования нового договора потребуется слишком много времени и ресурсов из-за отсутствия консенсуса по таким ключевым аспектам, как сфера охвата, национальный суверенитет и юрисдикция, что может повлиять на принятие государствами надлежащих стандартов для борьбы с киберпреступностью.

16. Другие выступавшие вновь заявили о необходимости новых мер реагирования, включая принятие нового универсального или глобального правового документа по киберпреступности в рамках Организации Объединенных Наций,

для решения проблем, связанных с быстрым развитием интернет-технологий, которые не охвачены существующими механизмами. Было высказано мнение, что существующие механизмы не должны препятствовать проведению международного обсуждения новых мер реагирования. Некоторые выступавшие высказали мнение, что Будапештская конвенция как региональный правовой документ не учитывает аспекты, вызывающие обеспокоенность всех государств-членов. Ряд выступавших высказали обеспокоенность по поводу закрытого порядка присоединения к Конвенции, присоединиться к которой можно только по приглашению и с согласия остальных государств-участников. Один выступавший высказал мнение, что одной из эффективных возможностей для сотрудничества между государствами, не являющимися участниками Будапештской конвенции, является проект конвенции Организации Объединенных Наций о сотрудничестве в области борьбы с киберпреступностью, который был представлен Генеральному секретарю 11 октября 2017 года (A/C.3/72/12, приложение).

17. Несколько выступавшие напомнили о том, что любой документ должен включать надлежащие нормы и гарантии по защите основных прав человека.

18. Несколько выступавших высказали мнение, что Будапештская конвенция, особенно пункт (b) статьи 32, содержит положения, которые с трудом согласуются с принципами международного права, касающимися, в частности, уважения национального суверенитета. Другие выступавшие отметили, что сфера действия пункта (b) статьи 32 имеет ограниченный характер и что некоторые государства в настоящее время выходят за рамки действия пункта (b) статьи 32 без процедурных мер защиты, которые применяются ко всем статьям Будапештской конвенции.

19. Некоторые выступавшие выразили мнение, что, поскольку киберпреступность приобретает все более выраженный транснациональный характер и часто бывает связана с организованной преступностью, для борьбы с ней подходит Конвенция об организованной преступности.

20. Группа экспертов обсудила также взаимосвязь между кибербезопасностью и киберпреступностью и различия между этими двумя понятиями. Несколько выступавших отметили, что это два разных понятия, относящиеся к широкому кругу проблем, связанных с использованием современных информационно-коммуникационных технологий, и что поэтому их следует обсуждать на разных и более подходящих для этого форумах в рамках Организации Объединенных Наций, таких как Международный союз электросвязи или Группа правительственных экспертов по информационной безопасности. Тем не менее ряд выступавших отметили, что эти темы являются взаимосвязанными, поскольку на практике для эффективной борьбы с киберпреступностью необходимо решать вопросы, связанные с кибербезопасностью. Был также высказан призыв к налаживанию тесного сотрудничества и достижению соглашений с частным сектором.

21. Многие выступавшие с удовлетворением отозвались о работе УНП ООН в рамках Глобальной программы борьбы с киберпреступностью и рассказали о мероприятиях по оказанию технической помощи и развитию потенциала, проведенных в рамках этой программы в их странах и регионах. Несколько выступавших отметили также, что оказанием законодательной и иной помощи в сфере противодействия киберпреступности в их регионах занимаются также другие межправительственные организации, в частности Содружество независимых государств, ОАГ, Африканский союз, Шанхайская организация сотрудничества и Совет Европы.

22. Выступавшие выразили признательность Председателю и членам Бюро Группы экспертов и Секретариату за организацию совещания. Многие выступавшие заявили о поддержке работы Группы экспертов. Несколько выступавших отметили, что она служит ценным форумом для многостороннего обсуждения проблем экспертами из разных правовых систем. По мнению ряда выступавших,

Группа экспертов может сыграть эффективную роль в обсуждении мер реагирования на общие угрозы, создаваемые киберпреступностью, в том числе в удовлетворении потребностей стран в технической помощи и создании потенциала. При этом было с удовлетворением отмечено, что принятие плана работы Группы экспертов на 2018–2021 годы является шагом в правильном направлении.

23. На своем 3-м заседании Группа экспертов продолжила рассмотрение пункта 2 повестки дня. Выступавшие отметили дополнительные моменты, в частности важность обеспечения того, чтобы в законодательстве о борьбе с киберпреступностью и соглашениях и договоренностях о международном сотрудничестве, особенно связанных с использованием электронных доказательств, были предусмотрены гарантии защиты прав человека в соответствии с международным правом и международными стандартами. Был, в частности, обсужден вопрос о важности поиска оптимального соотношения между соблюдением прав на неприкосновенность частной жизни и свободу выражения мнения и необходимостью предупреждения и противодействия киберпреступности. Несколько выступавших отметили, что, по их мнению, наблюдается значительное сходство в подходах к введению уголовной ответственности за преступления в киберпространстве в разных правовых системах, что в свою очередь способствует сокращению разрозненности правовых норм в данной области. В качестве остальных задач были названы дальнейшее укрепление международного сотрудничества на официальной и неофициальной основе, а также решение вопросов юрисдикции, возникающих в связи с облачной обработкой данных.

24. Группа экспертов рассмотрела также вопрос о трансграничном доступе к данным. Было высказано мнение, что обсуждение данного вопроса в Группе экспертов и в рамках других соответствующих межправительственных форумов весьма полезно для выявления наилучших видов практики и расширения сотрудничестве между правовыми системами в сфере расследования киберпреступлений. Вопрос о соблюдении принципа государственного суверенитета требует дальнейшего изучения, поскольку не совсем ясно, как совместить с этим принципом практику доступа к данным, хранящимся на территории другого государства. Было также отмечено, что усилия по противодействию киберпреступности должны соответствовать принципу соразмерности. Многие выступавшие также отметили, что в законодательстве о противодействии киберпреступности следует использовать нейтральные формулировки, не связанные с конкретными технологиями, чтобы оно сохраняло актуальность по мере развития технологий и изменения схем совершения преступлений, но что, вместе с тем, такое законодательство должно быть достаточно детальным, чтобы охватывать все основные виды преступлений. Несколько выступавших отметили необходимость реагирования на учащение случаев использования Интернета для осуществления террористической деятельности, а также разжигания ненависти и распространения дезинформации посредством разработки и обновления национального законодательства. Было высказано мнение, что внедрение любых правовых норм идет успешнее, если оно сопровождается проектами технической помощи и развития потенциала.

C. Криминализация

25. На 4-м и 5-м заседаниях 4 и 5 апреля 2018 года Группа экспертов рассмотрела пункт 3 повестки дня «Криминализация».

26. В дискуссии по этому пункту участвовали: Малини Говендер (Южная Африка), Ли Джиньинг (Китай), Вадим Сушик (Российская Федерация), Эрик ду Валь Ласерда Согосиу (Бразилия), Маруан Хейжужи (Марокко) и Норманд Вонг (Канада).

27. Многие выступавшие представили информацию о путях криминализации киберпреступлений в их странах. К числу наиболее распространенных видов

преступлений, упомянутых выступавшими, относятся конкретные киберпреступления, часто называемые основными киберпреступлениями, такие как преступления, направленные на подрыв конфиденциальности, целостности и доступности компьютерных систем, а также преступления, совершаемые в киберпространстве, включая преступления, связанные с насилием в отношении детей и их эксплуатацией, преступления, связанные с посягательством на неприкосновенность частной жизни, преступления, связанные с использованием личных данных и использованием Интернета в террористических целях. Выступавшие отметили, что в большинстве стран уже принято законодательство, предусматривающее уголовную ответственность за совершение основных киберпреступлений. Выступавшие отметили, что для соблюдения принципа обоюдного признания соответствующего деяния преступлением и ликвидации «безопасных гаваней» для преступников государствам не нужно придерживаться одинаковой типологии преступлений при условии, что соответствующее деяние признается преступлением во всех правовых системах.

28. Выступавшие также подчеркнули, что для эффективной борьбы с киберпреступностью необходимо законодательство, касающееся допустимости электронных доказательств в уголовных расследованиях и судебном преследовании. Введение в действие такого законодательства должно сопровождаться надлежащей профессиональной подготовкой и повышением квалификации сотрудников правоохранительных органов, прокуроров и судей. Была также подчеркнута важность обмена электронными доказательствами между различными правовыми системами.

29. Выступавшие обменялись опытом своих стран в области разработки законодательства и законов, направленных на криминализацию преступной деятельности в киберпространстве. Эксперты рассказали о том, в каких случаях необходимо создавать новое конкретное законодательство для криминализации определенных деяний и в каких случаях действующее законодательство и квалификация общих преступлений являются адекватными и достаточными для борьбы с новыми и возникающими формами киберпреступности. Многие выступавшие сочли весьма полезным наличие технически нейтрального законодательства, которое можно по-прежнему применять к новым формам информационно-коммуникационных технологий и киберпреступности. Каждая страна имеет собственные потребности и вправе решать по своему усмотрению, когда ей необходимо квалифицировать новые преступления в зависимости от тех тенденций, с которыми она сталкивается в области преступности. Выступавшие отметили также необходимость наличия надлежащего законодательства для криминализации новых и возникающих форм преступности, появлению которых способствует преступное использование, в частности, криптовалют, Интернета-вещей и «теневой сети».

30. Группа экспертов обсудила вопросы, касающиеся санкций в отношении ПИУ, которые отказываются сотрудничать с правоохранительными органами или соблюдать законодательные требования, направленные на предупреждение киберпреступности. Группа экспертов обсудила также порядок сотрудничества частного сектора с правоохранительными органами на основе выявленных наилучших видов практики, касающихся правовой ответственности и подотчетности ПИУ. Многие выступавшие отметили, что в то же время важно учитывать гарантии защиты прав человека в тех случаях, когда от ПИУ требуется соблюдение установленных правил. Был затронут вопрос о том, должна ли ответственность ПИУ подпадать под действие мер о криминализации.

31. В связи с вопросом о предупреждении киберпреступности несколько выступавших подчеркнули важность проведения информационно-пропагандистских кампаний для широкой общественности, а также разработки целевых учебных программ для детей с целью их ознакомления с опасностью киберпреступности и повышения онлайновой защищенности и кибербезопасности в стране в целом. Кроме того, для повышения потенциала правоохранительных органов в

области предупреждения киберпреступности необходимы специальные учебные курсы и выделение соответствующих ресурсов.

IV. Организация работы совещания

A. Открытие совещания

32. Совещание открыл заместитель председателя Группы экспертов Андре Рипл (Бразилия), исполняющий функции Председателя четвертого совещания Группы экспертов.

B. Заявления

33. С заявлениями выступили эксперты из следующих государств: Албании, Австралии, Алжира, Аргентины, Беларуси, Болгарии, Боснии и Герцеговины, Бразилии, бывшей югославской Республики Македония, Вьетнама, Ганы, Гватемалы, Германии, Грузии, Доминиканской Республики, Египта, Индии, Индонезии, Иордании, Ирана (Исламской Республики), Италии, Казахстана, Канады, Китая, Колумбии, Коста-Рики, Кувейта, Лихтенштейна, Маврикия, Малайзии, Мексики, Нигерии, Нидерландов, Норвегии, Парагвая, Португалии, Республики Молдова, Российской Федерации, Румынии, Сальвадора, Сербии, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Таиланда, Туниса, Турции, Украины, Филиппин, Черногории, Чехии, Чили, Шри-Ланки, Эквадора, Эстонии, Южной Африки и Японии.

34. С заявлениями выступили также представители следующих межправительственных организаций: Европейского союза, Совета Европы и Шанхайской организации сотрудничества.

C. Утверждение повестки дня и другие организационные вопросы

35. На своем 1-м заседании 3 апреля 2018 года Группа экспертов утвердила следующую предварительную повестку дня:

1. Организационные вопросы:
   a) открытие совещания;
   b) утверждение повестки дня;
   c) утверждение предложения Председателя по плану работы Группы экспертов на период 2018–2021 годов
2. Законодательство и правовая основа
3. Криминализация
4. Прочие вопросы
5. Утверждение доклада.

D. Участники

36. В работе совещания приняли участие представители 98 государств-членов, одного государства-наблюдателя, подразделения Секретариата Организации Объединенных Наций, четырех межправительственных организаций и девяти учреждений научного сообщества и частного сектора.

37. На совещании был распространен предварительный список участников (UNODC/CCPCJ/EG.4/2018/INF/1).

E. Документация

38. Помимо проекта всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов на рассмотрение Группе экспертов были представлены следующие документы:

a) предварительная повестка дня (UNODC/CCPCJ/EG.4/2018/1);

b) Chair's Proposal for the 2018–2021 workplan of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4 (UNODC/CCPCJ/EG.4/2018/CRP.1).

V. Утверждение доклада

39. На своем 6-м заседании 5 апреля 2018 года Группа экспертов утвердила свой доклад (UNODC/CCPCJ/EG.4/2018/L.1).