Организация Объединенных Наций A/76/135

Генеральная Ассамблея

Distr.: General
14 July 2021
Russian
Original: English

Семьдесят шестая сессия
Пункт 96 первоначального перечня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить настоящим доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Группа была создана в соответствии с пунктом 3 резолюции 73/266 Генеральной Ассамблеи.

* A/76/50.

Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности*

Резюме

Поскольку зависимость мира от информационно-коммуникационных технологий (ИКТ) продолжает расти, ответственное поведение государств при использовании ИКТ приобретает исключительно важное значение для поддержания международного мира и безопасности.

В соответствии с мандатом, содержащимся в резолюции 73/266 Генеральной Ассамблеи, в 2019–2021 годах Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, стремясь выработать общее понимание и обеспечить эффективное осуществление, продолжила исследование возможных совместных мер по устранению существующих и потенциальных угроз в сфере информационной безопасности.

В настоящем докладе содержатся выводы Группы о существующих и возникающих угрозах; нормах, правилах и принципах ответственного поведения государств; международном праве; мерах по укреплению доверия; и международном сотрудничестве и помощи по линии обеспечения безопасности и наращивания потенциала в области ИКТ. По каждой из этих тем данный доклад добавляет новый уровень понимания к выводам и рекомендациям предыдущих групп правительственных экспертов.

* Публикуется без официального редактирования.

Содержание

Предисловие Генерального секретаря

Информационно-коммуникационные технологии (ИКТ) продолжают быстро трансформировать общество, открывая многочисленные возможности и одновременно создавая значительные риски. Пандемия коронавирусного заболевания (COVID-19) еще больше ускорила переход многих аспектов нашей жизни в цифровое пространство и нашу зависимость от цифровых технологий.

Между тем, системы цифрового наблюдения и манипулирования используются все более широко, а пути развития онлайн-мира не всегда отвечают общественным интересам. Если не принять мер, то это может оказать разрушительное воздействие как на общество, так и на отдельных людей. Необходимость решения этих проблем, использования преимуществ ИКТ и поощрения ответственного поведения государств в контексте международной безопасности сегодня актуальна как никогда.

Выполняя свой мандат, за 18 месяцев Группа правительственных экспертов 2019–2021 годов проделала обстоятельную работу. Эти усилия были также подкреплены неформальными консультациями на региональном уровне и неофициальными встречами, открытыми для всех государств-членов. Доклад данной Группы и деятельность Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, которая приняла консенсусный доклад в марте 2021 года, дополняют друг друга.

В последние годы государства и другие государственные и частные заинтересованные стороны придают все большее значение усилиям Организации Объединенных Наций по содействию мирному использованию ИКТ. В этом контексте данный доклад представляет собой вклад в продвижение открытой, безопасной, стабильной и доступной среды ИКТ. Это также возобновленный призыв к дальнейшему сотрудничеству в целях снижения киберрисков для международного мира и безопасности и обеспечения защиты и продвижения прав человека и основных свобод как в Интернете, так и вне его.

Препроводительное письмо

28 мая 2021 года

Имею честь настоящим препроводить консенсусный доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Группа была создана в 2018 году в соответствии с пунктом 3 постановляющей части резолюции 73/266 Генеральной Ассамблеи.

В этой резолюции Генеральная Ассамблея просила создать в 2019 году группу правительственных экспертов на основе справедливого географического распределения, которая продолжит — основываясь на оценках и рекомендациях, содержащихся в докладах Группы правительственных экспертов за 2010, 2013 и 2015 годы, и стремясь выработать общее понимание и обеспечить эффективное осуществление — исследование возможных совместных мер по устранению существующих и потенциальных угроз в сфере информационной безопасности, в том числе исследование норм, правил и принципов ответственного поведения государств, мер по укреплению доверия и наращивания потенциала, а также того, как международное право применяется к использованию информационно-коммуникационных технологий государствами, и представит Генеральной Ассамблее на ее семьдесят шестой сессии доклад о результатах такого исследования с приложением, содержащим представленные участвующими правительственными экспертами национальные материалы по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами. Генеральный секретарь планирует представить Ассамблее соответствующий доклад на ее семьдесят шестой сессии.

В соответствии с мандатом Группы официальный сборник (A/76/136) предоставленных участвующими правительственными экспертами добровольно представляемых национальных материалов (на том языке, на котором они были представлены, без перевода) по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами, будет опубликован на веб-сайте Управления Организации Объединенных Наций по вопросам разоружения.

В соответствии с положениями резолюции, были назначены эксперты из 25 государств: Австралии, Бразилии, Германии, Индии, Индонезии, Иордании, Казахстана, Кении, Китая, Маврикия, Марокко, Мексики, Нидерландов, Норвегии, Российской Федерации, Румынии, Сингапура, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Уругвая, Франции, Швейцарии, Эстонии, Южной Африки и Японии. Список экспертов прилагается к данному докладу.

Группа провела четыре официальные сессии: первую — с 9 по 13 декабря 2019 года в Центральных учреждениях Организации Объединенных Наций, вторую — с 24 по 28 февраля 2020 года в Женеве, третью, в виртуальном формате, — с 5 по 9 апреля 2021 года и четвертую, в виртуальном формате, — с 24 по 28 мая 2021 года. Третья сессия Группы была отложена в соответствии с решением 75/551 Генеральной Ассамблеи в связи с пандемией COVID-19. Тем не менее, в течение этого времени Группа продолжала свою работу, проведя ряд межсессионных неофициальных консультаций. В соответствии с ее мандатом для участия в интерактивных обсуждениях и обмена мнениями был также проведен ряд консультаций с соответствующими региональными организациями и консультативных встреч открытого состава с государствами-членами.

Группа хотела бы выразить признательность за вклад совместной Группы поддержки Управления Организации Объединенных Наций по вопросам разоружения и Института Организации Объединенных Наций по исследованию проблем разоружения.

Я также пользуюсь этой возможностью, чтобы выразить свою личную благодарность правительству Бразилии за мое назначение и Группе за оказанную мне честь председательства. Я также благодарю остальных экспертов, моих бразильских коллег, членов совместной Группы поддержки и Секретариате Организации Объединенных Наций, в частности Высокого представителя по вопросам разоружения, за их поддержку и за то, что они поделились своим огромным опытом в конструктивном духе взаимодействия.

(*Подпись*) Гильерми **ди Агиар Патриота**
Председатель Группы

I. Введение

1. В настоящем докладе отражены итоги обсуждений, проведенных Группой правительственных экспертов в соответствии с резолюцией 73/266 Генеральной Ассамблеи «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности». Ключевая часть работы Группы пришлась на пандемию коронавирусного заболевания (COVID-19), которая высветила огромный потенциал цифровых технологий и одновременно резко повысила зависимость от них всего мира, тем самым еще больше подчеркивая важность ответственного поведения при использовании ИКТ в контексте международной безопасности.

2. В основу этого доклада легли подтверждаемые в нем оценки и рекомендации, содержащиеся в консенсусных докладах групп правительственных экспертов за 2010, 2013 и 2015 годы, в которых рассматриваются существующие и новые угрозы, нормы, правила и принципы ответственного поведения государств, международное право, укрепление доверия, а также международное сотрудничество и наращивание потенциала, что в совокупности представляет собой кумулятивную и эволюционирующую основу ответственного поведения государств при использовании ими ИКТ. Группа приветствует принятие консенсусного доклада Рабочей группы открытого состава Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, созданной в соответствии с резолюцией 73/27 Генеральной Ассамблеи[1], которая подтверждает и развивает эти рамки.

3. Группа рассмотрела эти вопросы в рамках своего мандата в свете их актуальности для международного мира и безопасности. Кроме того, она стремилась обеспечить дополнительный уровень понимания оценок и рекомендаций, содержащихся в предыдущих докладах групп правительственных экспертов в целях выработки рекомендаций, способствующих их осуществлению. Этот дополнительный уровень понимания подтверждает взаимосвязь различных существенных элементов мандата Группы и важность вовлечения других субъектов, включая, при необходимости, представителей частного сектора, гражданского общества, научных и технических кругов, в работу государств по осуществлению этих рекомендаций.

4. Группа признает важную роль региональных и субрегиональных органов в дальнейшем применении оценок и рекомендаций, которые содержатся в докладах групп правительственных экспертов, а также в разработке региональных механизмов и укреплении усилий по наращиванию потенциала для поддержки их реализации. В соответствии с мандатом Группы, эти и другие соответствующие соображения и опыт были представлены Группе в ходе ее неофициальных консультативных встреч с государствами-членами, состоявшихся в Нью-Йорке, а также в ходе ряда консультаций, проведенных в сотрудничестве с региональными организациями[2].

5. Группа подтверждает, что открытая, безопасная, стабильная, доступная и мирная информационно-коммуникационная среда имеет важнейшее значение для всех и требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Поощрение использования ИКТ в мирных целях отвечает всеобщим интересам и необходимо для

[1] A/75/816.

[2] С докладами о различных консультациях можно ознакомиться по следующим адресам: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf и https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

общего блага. В этих усилиях центральное место по-прежнему занимает уважение суверенитета и прав человека и основных свобод, а также устойчивое и цифровое развитие.

II. Существующие и новые угрозы

6. Хотя информационно-коммуникационные технологии и все более цифровой и подключенный мир открывают огромные возможности для обществ во всем мире, Группа подтверждает, что серьезные угрозы в сфере ИКТ, выявленные в предыдущих докладах, все еще существуют. Инциденты, связанные со злонамеренным использованием ИКТ государствами и негосударственными субъектами, приобретают все более масштабный, серьезный и сложный характер. Хотя в разных регионах угрозы ИКТ проявляются по-разному, их последствия могут быть в том числе и глобальными.

7. Группа обращает особое внимание на содержащийся в докладе за 2015 год анализ того, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей; и на тот факт, что использование ИКТ в будущих конфликтах между государствами становится более вероятным.

8. Злонамеренная информационно-коммуникационная деятельность со стороны представляющих постоянную угрозу субъектов, таких как государства или другие субъекты, может создавать значительный риск для международной безопасности и стабильности, экономического и социального развития, а также для безопасности и благополучия отдельных лиц.

9. Кроме того, государства и другие субъекты активно используют более сложные и многогранные возможности ИКТ в политических и других целях. Более того, Группа с тревогой отмечает рост злонамеренного использования государствами тайных информационных кампаний с применением ИКТ для влияния на процессы, системы и общую стабильность другого государства. Такие действия подрывают доверие, могут привести к эскалации ситуации и угрожать международному миру и безопасности. Они также могут наносить прямой и косвенный вред людям.

10. Вредоносная деятельность с применением ИКТ в отношении объектов критически важной инфраструктуры, предоставляющих услуги внутри страны, на региональном или глобальном уровнях, о которой говорилось в предыдущих докладах, становится все более серьезной проблемой. Особую озабоченность вызывают злонамеренная деятельность в сфере ИКТ, затрагивающая критически важную информационную инфраструктуру, инфраструктуру, обеспечивающую основные услуги для населения, техническую инфраструктуру, необходимую для обеспечения общей доступности или целостности интернета и структур сектора здравоохранения. Пандемия коронавирусного заболевания (COVID-19) наглядно показала риски и последствия вредоносной деятельности, направленной на использование факторов уязвимости во времена тяжелых испытаний, выпавших на долю общества.

11. Новые и новейшие технологии расширяют возможности для развития. Однако их постоянно изменяющиеся свойства и характеристики также расширяют диапазон атаки, создавая новые векторы и уязвимые места, которыми можно воспользоваться для нанесения вреда с применением ИКТ. Становится все сложнее обеспечивать защиту от злонамеренного использования уязвимостей в операционной технологии и взаимосвязанных вычислительных устройствах, платформах, машинах или объектах, составляющих интернет вещей.

12. Возможности обеспечения безопасности информационных систем попрежнему различаются во всем мире, равно как и возможности создания потенциала противодействия, защиты критически важной информационной инфраструктуры, выявления угроз и принятия своевременных мер в связи с ними. Эти различия в возможностях, ресурсах, национальных законах, правилах и практике, касающихся использования ИКТ, а также неравная информированность о существующих региональных и глобальных формах сотрудничества, имеющихся для смягчения последствий таких инцидентов, их расследования или восстановления после них, и доступ к ним повышают степень уязвимости и риска для всех государств.

13. Группа подтверждает, что существует все более серьезная опасность использования ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру, а не только для вербовки сторонников, финансирования, обучения и подстрекательства, и если не принять соответствующих мер, то это может поставить под угрозу международный мир и безопасность.

14. Группа подтверждает также, что существующую угрозу усиливают такие факторы как многообразие злоумышленников из числа негосударственных субъектов (включая преступные группировки и террористов), разнообразие их мотивов, скорость осуществления злонамеренных нападений в сфере ИКТ, а также трудности, связанные с возложением ответственности за инцидент в сфере ИКТ.

III. Нормы, правила и принципы ответственного поведения государств

15. Что касается использования ИКТ государствами, то Группа вновь подтверждает, что принятие добровольных и необязательных норм ответственного поведения государств может привести к снижению угрозы международному миру, безопасности и стабильности. Нормы и существующее международное право существуют параллельно. Эти нормы не направлены на ограничение или запрещение действий, согласующихся с международным правом. Они отражают ожидания международного сообщества и определяют стандарты ответственного поведения государств. Такие нормы могут способствовать предупреждению конфликтов в информационно-коммуникационной среде и использованию ИКТ в мирных целях для обеспечения полной реализации выгод от их использования в целях ускорения социального и экономического развития во всем мире.

16. Группа также подчеркивает взаимосвязь между нормами, касающимися мер укрепления доверия, международного сотрудничества и создания потенциала. Группа, учитывая уникальные особенности ИКТ, подтверждает содержащееся в докладе за 2015 год замечание о том, что со временем могут быть разработаны дополнительные нормы и, отдельно, отмечает возможность, при необходимости, разработки в будущем дополнительных твердых обязательств.

17. Помимо работы в системе Организации Объединенных Наций, Группа признает формирующийся ценный опыт в области внедрения норм на региональном уровне, включая нормы, информация о которых была распространена в ходе неофициальных консультаций, проведенных с государствами-членами в Нью-Йорке, и в сотрудничестве с региональными организациями в соответствии со своим мандатом, отмечая, что эти усилия следует учитывать в будущем при проработке темы ИКТ в контексте международной безопасности. Группа принимает к сведению международные правила поведения в области обеспечения

информационной безопасности, предложенные Казахстаном, Китаем, Кыргызстаном, Российской Федерацией, Таджикистаном и Узбекистаном (см. A/69/723).

18. В принятой консенсусом резолюции 70/237 Генеральная Ассамблея призвала государства-члены при использовании информационно-коммуникационных технологий руководствоваться докладом Группы правительственных экспертов 2015 года, в котором содержится 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств. В соответствии со своим мандатом по содействию ответственному поведению, Группа обеспечила дополнительный слой понимания этих норм, подчеркивая их ценность в отношении ожидаемого поведения государств при использовании ИКТ в контексте международного мира и безопасности и приводя примеры категорий институциональных механизмов, которые государства могут создать на национальном и региональном уровнях для поддержки их реализации. Группа напоминает государствам, что такие усилия должны предприниматься в соответствии с их обязательствами, вытекающими из Устава Организации Объединенных Наций и других норм международного права, с целью сохранения открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Государства призваны избегать использования ИКТ, не соответствующего нормам ответственного поведения государства, и воздерживаться от него.

Норма 13 a): в соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности.

19. Поддержание международного мира и безопасности и международное сотрудничество являются одними из основополагающих целей Организации Объединенных Наций. Эта норма служит напоминанием о том, что сотрудничество и совместная работа по содействию использованию ИКТ в мирных целях и предотвращению конфликтов, связанных с их ненадлежащим использованием, является общим стремлением всех государств и отвечает их интересам.

20. В связи с этим и в развитие соблюдения данной нормы Группа призывает государства воздерживаться от использования информационно-коммуникационных технологий и информационно-коммуникационных сетей для осуществления деятельности, которая может угрожать поддержанию международного мира и безопасности.

21. Меры, рекомендованные предыдущими группами правительственных экспертов и рабочими группами открытого состава, закладывают первоначальную основу принципов ответственного поведения государств в области использования ИКТ. В качестве дополнительной поддержки и для облегчения такого сотрудничества Группа рекомендует государствам создать или укрепить существующие механизмы, структуры и процедуры на национальном уровне, такие как соответствующие директивные и законодательные меры и обзорные процессы; механизмы управления кризисными ситуациями и инцидентами; механизмы сотрудничества и партнерства с участием всего правительства; и механизмы сотрудничества и диалога с частным сектором, научными и техническими кругами и гражданским обществом. Государствам также рекомендуется собирать и упорядочивать представляемую ими информацию об осуществлении норм, в том

числе путем проведения добровольного обзора ведущейся на национальном уровне работы и обмена опытом.

Норма 13 b): в случае возникновения инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности в ИКТ-среде, а также характер и масштабы последствий.

22. В этой норме признается, что установление ответственности является сложным делом и что определение источника информационно-коммуникационного инцидента требует рассмотрения широкого круга факторов. В этой связи избежать недопонимания и эскалации напряженности в отношениях между государствами поможет осторожность, рекомендуемая в п. 71 g) данного доклада и в предыдущих докладах групп правительственных экспертов.

23. Государствам, которые становятся объектами злонамеренной деятельности в сфере ИКТ, и государствам, на территории которых предположительно осуществляется такая деятельность, рекомендуется проводить консультации с привлечением соответствующих компетентных органов.

24. Государству, ставшему жертвой злонамеренного инцидента с ИКТ, следует учитывать все аспекты такого инцидента при его оценке. Такие аспекты, подкрепленные достоверной информацией, могут включать в себя технические характеристики инцидента; его охват, масштабы и последствия; более широкий контекст, в том числе воздействие этого инцидента на международный мир и безопасность; и результаты консультаций между соответствующими государствами.

25. Ответные действия государства, пострадавшего от злонамеренной деятельности с использованием ИКТ, приписываемой другому государству, должны предприниматься в соответствии с его обязательствами по Уставу Организации Объединенных Наций и другим нормам международного права, в том числе обязательствами, касающимися мирного урегулирования споров и международно-противоправных деяний. Государства могли бы также использовать весь спектр имеющихся у них дипломатических, правовых и других возможностей проведения консультаций, а также добровольные механизмы и другие политические обязательства, которые позволяют урегулировать разногласия и споры с помощью консультаций и других мирных средств.

26. Для введения этой нормы в действие на национальном уровне, содействия расследованию и урегулированию инцидентов в сфере ИКТ с участием других государств государства могут создавать или усиливать соответствующие национальные структуры, информационно-коммуникационные стратегии, процессы, законодательные рамки, координационные механизмы, а также партнерства и другие формы взаимодействия с соответствующими заинтересованными сторонами, с тем чтобы оценить серьезность и воспроизводимость того или иного инцидента в сфере ИКТ.

27. Сотрудничество на региональном и международном уровнях, в том числе между национальными группами реагирования на компьютерные инциденты (ГРКИ) и группами реагирования на инциденты информационной безопасности (ГРИИБ), органами государств, занимающимися вопросами ИКТ, дипломатическим сообществом и сообществом безопасности, может укрепить способность государств выявлять и расследовать злонамеренные инциденты в сфере ИКТ, а также обосновывать свою озабоченность и соответствующие выводы перед завершением обработки инцидента.

28. Государства могут также использовать многосторонние, региональные и двусторонние платформы, а также платформы с участием многих заинтересованных сторон для обмена информацией о национальных подходах к установлению ответственности, в том числе о том, как они различают виды установления ответственности, и об угрозах и инцидентах, связанных с ИКТ, а также соответствующим опытом. Группа также рекомендует рассмотреть в рамках будущей работы способы достижения общего понимания и обмена опытом в том, что касается установления ответственности.

Норма 13 c): государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

29. В этой норме отражено ожидание того, что если государство знает или будет добросовестно уведомлено о том, что международно-противоправное деяние, совершенное с применением ИКТ, исходит с его территории или проходит через нее, оно использует все соответствующие, доступные и возможные — в разумных пределах — шаги для обнаружения, расследования и урегулирования такой ситуации. В ней заложено понимание того, что государство не должно позволять другому государству или негосударственному субъекту использовать ИКТ на своей территории для совершения международно-противоправных деяний.

30. При рассмотрении вопроса о способах достижения целей этой нормы, государствам следует учитывать следующее:

a) в этой норме отражено ожидание того, что государства будут предпринимать разумные и посильные действия, с тем чтобы положить конец деятельности, происходящей на их территории, используя соразмерные, надлежащие и эффективные средства и методы таким образом, чтобы это соответствовало международному праву и внутреннему законодательству. Тем не менее, вряд ли государства могут или должны отслеживать все происходящее в сфере ИКТ на своей территории;

b) государство, которое знает о совершении международно-противоправных деяний с применением ИКТ, расположенных на его территории, но не располагает возможностями для решения этой проблемы, может рассмотреть возможность обращения за помощью к другим государствам или представителям частного сектора в соответствии с положениями международного права и внутреннего законодательства. Поддержку осуществлению этой нормы может оказать создание соответствующих структур и механизмов для формулирования просьб об оказании помощи и реагирования на них. При оказании помощи государствам следует действовать добросовестно, в соответствии с нормами международного права, и не использовать такую возможность для совершения злонамеренных действий против государства, обращающегося за помощью, или против других государств;

c) затронутое государство должно уведомить государство, с территории которого исходит эта деятельность. Уведомляемое государство должно подтвердить получение уведомления для содействия сотрудничеству и прояснению вопроса и приложить все разумные усилия для оказания помощи в установлении факта совершения международно-противоправного деяния. Подтверждение получения данного уведомления не означает согласия с содержащейся в нем информацией;

d) сам по себе инцидент с ИКТ, исходящий с территории третьего государства или осуществляемый с использованием его инфраструктуры, не подразумевает ответственности этого государства за данный инцидент. Уведомление государства о том, что его территория используется для совершения противоправного деяния, само по себе также не подразумевает, что оно несет ответственность за это деяние.

Норма 13 d): государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. При необходимости государствам следует рассмотреть вопрос о разработке новых мер в этой сфере.

31. В этой норме содержится напоминание государствам о важности международного сотрудничества для противодействия трансграничным угрозам, создаваемым преступным и террористическим использованием Интернета и ИКТ, в том числе для целей вербовки, финансирования, обучения и подстрекательства, планирования и координации нападений и пропаганды своих идей и действий, а также для других подобных целей, о которых говорится в настоящем докладе. В этой норме отмечается, что успехи в реагировании на эти и другие подобные угрозы с участием террористических и преступных групп и отдельных лиц с помощью существующих и других мер могут способствовать международному миру и стабильности.

32. Ее соблюдение подразумевает наличие национальной политики, законодательства, структур и механизмов, способствующих трансграничному сотрудничеству по техническим, правоохранительным, правовым и дипломатическим вопросам, имеющим отношение к борьбе с преступным и террористическим использованием ИКТ.

33. Государствам рекомендуется укреплять и далее развивать механизмы, которые могут способствовать обмену информацией и оказанию помощи между соответствующими национальными, региональными и международными организациями для повышения осведомленности государств о безопасности ИКТ и уменьшения оперативной зоны онлайновой террористической и преступной деятельности. Такие механизмы могут укрепить потенциал соответствующих организаций и учреждений при одновременном укреплении доверия между государствами и усилении ответственного поведения государств. Государствам также рекомендуется разработать соответствующие протоколы и процедуры для сбора, обработки и хранения в онлайновом режиме доказательств, имеющих отношение к преступному и террористическому использованию ИКТ, и своевременно оказывать помощь в проведении расследований, обеспечивая принятие таких мер в соответствии с обязательствами государства по международному праву.

34. Ряд специальных форумов, процессов и резолюций в Организации Объединенных Наций посвящен угрозам, связанным с использованием ИКТ в террористических и преступных целях, а также совместным подходам, необходимым для борьбы с такими угрозами. Тематические резолюции Генеральной Ассамблеи включают резолюцию 65/230 о двенадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, на котором была создана межправительственная группа экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности; резолюцию 74/173 о содействии оказанию технической помощи и наращиванию потенциала для усиления национальных мер и укрепления

международного сотрудничества в целях противодействия использованию информационно-коммуникационных технологий в преступных целях, включая обмен информацией; и резолюцию 74/247 о противодействии использованию ИКТ в преступных целях.

35. Кроме того, для содействия обмену информацией и оказанию помощи в борьбе с использованием ИКТ в преступной и террористической деятельности государства могут использовать существующие процессы и инициативы и правовые инструменты, а также рассмотреть возможность использования дополнительных процедур или каналов связи. В этой связи государствам рекомендуется продолжать наращивать усилия, предпринимаемые в Организации Объединенных Наций и на региональном уровне в целях реагирования на использование интернета и ИКТ в преступных и террористических целях, и развивать с этой целью партнерские отношения для сотрудничества с международными организациями, промышленными и научными кругами и гражданским обществом.

Норма 13 e): государства в процессе обеспечения безопасного использования ИКТ должны соблюдать положения резолюций Совета по правам человека 20/8 и 26/13 о поощрении, защите и осуществлении прав человека в Интернете и резолюций Генеральной Ассамблеи 68/167 и 69/166 о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение.

36. В этой норме государствам напоминается о необходимости уважать и защищать права человека и основные свободы как в интернете, так и в реальной жизни, в соответствии с взятыми на себя обязательствами. Особое внимание в этой связи следует уделять праву на свободу выражения мнений, включая право на поиск, получение и распространение информации независимо от государственных границ и с помощью любых средств массовой информации, а также другим соответствующим положениям Международного пакта о гражданских и политических правах, Международного пакта об экономических, социальных и культурных правах и Всеобщей декларации прав человека. Соблюдение этой нормы может также способствовать поощрению недискриминации и сокращению цифрового разрыва, в том числе его гендерной составляющей.

37. Принятие упомянутых в этой норме резолюций, а также других резолюций, которые были приняты впоследствии, является признанием новых трудностей и дилемм, возникших в связи с использованием ИКТ государствами, и соответствующей необходимости их решения. Такая государственная практика, как произвольное или незаконное массовое наблюдение, может иметь особенно негативные последствия для осуществления и реализации прав человека, в частности права на неприкосновенность частной жизни.

38. При осуществлении этой нормы государствам следует учитывать конкретные указания, содержащиеся в цитируемых резолюциях. Они также должны принять к сведению новые резолюции, принятые после доклада Группы правительственных экспертов 2015 года, и внести свой вклад в новые резолюции, которые, возможно, потребуется принять в свете происходящих событий.

39. Усилия государств по поощрению уважения и соблюдения прав человека и обеспечения безопасного использования ИКТ должны носить взаимодополняющий, взаимоукрепляющий и взаимосвязанный характер. Такой подход способствует созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Он может также способствовать достижению целей в области устойчивого развития.

40. Следует признать важность технологических инноваций для всех государств; вместе с тем новые и самые последние технологии могут также оказать серьезное влияние на права человека и безопасность в области ИКТ. Для решения этой проблемы государства, возможно, рассмотрят вопрос об инвестировании в разработку технических и правовых мер, призванных направлять развитие и использование ИКТ в более инклюзивном и доступном ключе, без негативного воздействия на членов отдельных общин или групп, а также об ускорении такой разработки.

41. Группа отмечает наличие в Организации Объединенных Наций ряда специальных форумов, посвященных вопросам прав человека. Кроме того, она признает, что различные заинтересованные стороны по-разному содействуют защите и поощрению прав человека и основных свобод в интернете и в реальной жизни. Привлечение этих сторон к процессам разработки стратегий в области информационно-коммуникационной безопасности может поддержать усилия по поощрению, защите и осуществлению прав человека в интернете и помочь уточнить и свести к минимуму потенциальное негативное воздействие директивных мер на людей, в том числе на тех, кто находится в уязвимом положении.

Норма 13 f): государства не должны заведомо осуществлять и поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

42. Что касается этой нормы, то информационно-коммуникационная деятельность, которая наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры, используемой для обслуживания населения, может вызвать цепную реакцию и иметь внутренние, региональные и глобальные последствия.

43. В этой норме также указывается на основополагающее значение критически важной инфраструктуры как национального достояния, поскольку такие инфраструктуры лежат в основе обеспечения жизненно важных функций, услуг и деятельности общества. Их значительное ослабление или повреждение может привести к серьезным людским потерям, а также оказать заметное воздействие на экономику, развитие, политическое и социальное функционирование и национальную безопасность государства.

44. Как отмечается в норме 13 g), государствам следует принимать надлежащие меры для защиты своей критически важной инфраструктуры. В этой связи каждое государство определяет, какие находящиеся в его юрисдикции объекты инфраструктуры или сектора оно считает критически важными, в соответствии с национальными приоритетами и методами определения объектов критически важной инфраструктуры.

45. Пандемия COVID-19 привела к более глубокому осознанию исключительной важности защиты санитарно-медицинской инфраструктуры и объектов здравоохранения, в том числе посредством реализации норм, касающихся критически важной инфраструктуры (таких как данная норма и нормы g) и h)). Другими примерами секторов критически важной инфраструктуры, предоставляющих базовые услуги населению, могут служить энергетика, производство электроэнергии, водоснабжение и санитария, образование, коммерческие и финансовые услуги, транспорт, телекоммуникации и процесс проведения выборов. К категории критически важных инфраструктур могут также относиться

инфраструктуры, обслуживающие несколько государств, такие как техническая инфраструктура, необходимая для обеспечения общедоступности и надежности интернета. Такие инфраструктуры могут иметь решающее значение для международной торговли, финансовых рынков, глобального транспорта, связи, здравоохранения или гуманитарной деятельности. Использование такой инфраструктуры в качестве примеров ни в коей мере не исключает того, что государства определяют другие инфраструктуры в качестве критически важных, и не означает косвенного попустительства в отношении злонамеренных действий, затрагивающих другие категории инфраструктур, не указанные выше.

46. В целях содействия осуществлению этой нормы, помимо учета вышеизложенных факторов, государствам рекомендуется принять соответствующие директивные и законодательные меры на национальном уровне для обеспечения того, чтобы деятельность в области ИКТ, осуществляемая или поддерживаемая государством, которая может повлиять на критически важную инфраструктуру, используемую для оказания основных услуг населению другого государства, согласовывалась с этой нормой, использовалась в соответствии с его международно-правовыми обязательствами и подлежала всеобъемлющему обзору и надзору.

Норма 13 g): государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи.

47. В этой норме подтверждается приверженность всех государств делу защиты объектов критически важной инфраструктуры, находящихся под их юрисдикцией, от связанных с ИКТ угроз и важность международного сотрудничества в этой связи.

48. Отнесение государством инфраструктур или секторов к категории критически важных является полезным шагом для защиты таких инфраструктур или секторов. Помимо определения того, какие инфраструктуры или сектора инфраструктуры оно считает критически важными, каждое государство определяет структурные, технические, организационные, законодательные и нормативные меры, необходимые для защиты их критически важной инфраструктуры и восстановления функциональности в случае инцидента. В резолюции 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и приложении к ней освещаются меры, которые государства могут в этой связи принимать на национальном уровне[3].

49. В ведении некоторых государств находятся инфраструктуры, поддерживающе оказание услуг на региональном или международном уровне. Информационно-коммуникационные угрозы для таких инфраструктур могут стать дестабилизирующим фактором. Государства, участвующие в таких схемах взаимодействия, могут поощрять трансграничное сотрудничество с соответствующими владельцами и операторами инфраструктуры в целях усиления мер информационно-коммуникационной безопасности, принимаемых в отношении такой инфраструктуры, и укрепления существующих или разработки дополнительных процессов и процедур для выявления инцидентов в области ИКТ, затрагивающих такую инфраструктуру, и смягчения их последствий.

[3] Резолюция 58/199 Генеральной Ассамблеи, которая является частью пакета из трех резолюций, включая резолюции 57/239 и 64/211 Генеральной Ассамблеи.

50. Достижению цели данной нормы также будет способствовать поощрение мер по обеспечению безопасности и защищенности продуктов ИКТ на протяжении всего их жизненного цикла или классификации инцидентов в сфере ИКТ с точки зрения их масштаба и серьезности.

Норма 13 h): государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства также должны удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета.

51. В этой норме государствам напоминается о важнейшей роли международного сотрудничества, диалога и должного уважения суверенитета всех государств в деле реагирования на просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Эта норма особенно важна в тех случаях, когда речь идет о действиях, которые потенциально могут угрожать международному миру и безопасности.

52. При получении просьбы об оказании помощи государствам следует предлагать любую помощь в рамках имеющихся у них возможностей и ресурсов с учетом имеющихся у них разумных возможностей и в соответствии с обстоятельствами. Государство может решить обратиться за помощью на двусторонней основе или в рамках региональных или международных соглашений. Государства могут также обращаться к частному сектору с просьбой оказать им поддержку в реагировании на просьбы об оказании помощи.

53. Эффективность осуществления этой нормы обеспечивается с помощью соответствующих национальных структур и механизмов обнаружения и смягчения последствий инцидентов в сфере ИКТ, потенциально угрожающих международному миру и безопасности. Такие механизмы дополняют существующие механизмы повседневной обработки и урегулирования инцидентов в сфере ИКТ. Так, государству, желающему обратиться за помощью к другому государству, было бы полезно знать, к кому обращаться и какой канал связи следует использовать. Государству, получающему просьбу о помощи, необходимо как можно более транспарентно и своевременно, а также с учетом срочности и деликатности просьбы определить, располагает ли оно возможностями, потенциалом и ресурсами для оказания запрошенной помощи. От государств, к которым обратились за помощью, не требуется обеспечивать конкретный результат или исход.

54. Единые и транспарентные процессы и процедуры обращения за помощью к другому государству и реагирования на просьбы об оказании помощи могут способствовать сотрудничеству, о котором говорится в этой норме. В этой связи типовые формы запроса об оказании помощи и реагирования на такие запросы могут обеспечить предоставление запрашивающим помощь государством как можно более полной и точной информации государству, у которого оно запрашивает помощь, способствуя тем самым сотрудничеству и своевременному реагированию. Такие формы могут быть разработаны на добровольной основе на двустороннем, многостороннем или региональном уровне. Типовая форма ответа на запрос об оказании помощи может включать элементы, подтверждающие получение запроса, и, если помощь возможна, указание сроков, характера, объема и условий оказания такой помощи. В тех случаях, когда злоумышленная

деятельность исходит с территории конкретного государства, его предложение об оказании запрошенной помощи и предоставление такой помощи могут помочь свести к минимуму ущерб, избежать недопонимания, снизить риск эскалации и помочь восстановить доверие.

55. Соблюдению этой нормы может способствовать участие в совместных механизмах, определяющих средства и способы связи в кризисных ситуациях, а также обработки и урегулирования инцидентов.

Норма 13 i): государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

56. В этой норме признается необходимость укрепления доверия конечного пользователя к открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среде. Обеспечение надежности каналов поставки в сфере ИКТ и безопасности информационно-коммуникационных продуктов, а также предупреждение распространения злонамеренных программных и технических средств в сфере ИКТ и использования скрытых вредоносных функций приобретают все большее значение для международной безопасности и экономического развития.

57. Глобальные каналы поставки в сфере ИКТ характеризуются обширностью, все большей сложностью и взаимозависимостью и охватывают множество различных сторон. Разумные меры для поощрения открытости и обеспечения надежности, стабильности и безопасности каналов поставки могут включать:

a) создание на национальном уровне всеобъемлющих, транспарентных, объективных и беспристрастных рамок и механизмов для управления рисками в отношении каналов поставки в соответствии с международными обязательствами государств. Такие рамки могут включать оценки рисков, учитывающие целый ряд факторов, в том числе преимущества и риски, связанные с новыми технологиями;

b) разработка стратегий и программ, направленных на поощрение внедрения поставщиками оборудования и систем ИКТ передовых методов в целях укрепления международного доверия к целостности и безопасности информационно-коммуникационных продуктов и услуг, повышения качества и содействия выбору;

c) уделение повышенного внимания в национальной политике и в диалоге с государствами и соответствующими участниками в Организации Объединенных Наций и на других площадках вопросу о том, как обеспечить всем государствам возможность равноправно конкурировать и внедрять инновации, с тем чтобы создать условия для полной реализации ИКТ в целях ускорения глобального социального и экономического развития и содействия поддержанию международного мира и безопасности при одновременном обеспечении национальной безопасности и учете общественных интересов;

d) совместные меры, такие как обмен передовым опытом на двустороннем, региональном и многостороннем уровнях по управлению рисками в отношении каналов поставки; разработка и внедрение глобально совместимых общих правил и стандартов безопасности каналов поставок; и другие подходы, направленные на снижение уязвимости каналов поставок.

58. Государства могут рассмотреть вопрос о разработке и внедрении на национальном уровне следующих средств борьбы с распространением злонамеренных программных и технических инструментов в сфере ИКТ и использованием скрытых вредоносных функций, включая закладки:

a) меры по повышению целостности каналов поставок, включая требования к поставщикам ИКТ учитывать вопросы безопасности и защиты информационно-коммуникационных продуктов при их проектировании и разработке, а также на протяжении всего их жизненного цикла. С этой целью государства могут также рассмотреть вопрос о создании независимых и беспристрастных процессов сертификации;

b) законодательные и другие гарантии, повышающие уровень защиты данных и конфиденциальности;

c) меры, запрещающие внедрение вредных скрытых функций и использование уязвимостей в продуктах ИКТ, которые могут поставить под угрозу конфиденциальность, целостность и доступность систем и сетей, в том числе в критически важной инфраструктуре.

59. В дополнение к вышеизложенным шагам и мерам государствам следует и далее содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности как самих ИКТ, так и процессов их использования, включая безопасность каналов поставок продуктов ИКТ, способствуя тем самым достижению задач этой нормы.

Норма 13 j): государства должны способствовать ответственному представлению информации и факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

60. В этой норме государствам напоминается о важности обеспечения быстрого устранения уязвимостей ИКТ в целях уменьшения возможности их использования злоумышленниками. Своевременное обнаружение и ответственное раскрытие уязвимостей ИКТ, сопровождающееся соответствующей отчетностью, может предотвратить вредные или угрожающие практики, повысить доверие и укрепить уверенность, а также уменьшить связанные с этим угрозы международной безопасности и стабильности.

61. Стратегии и программы раскрытия информации об уязвимости, а также международное сотрудничество в этой связи направлены на обеспечение надежного и последовательного процесса регулярного раскрытия такой информации. Скоординированный процесс раскрытия информации об уязвимости может свести к минимуму вред, наносимый обществу уязвимыми продуктами, и систематизировать отчетность об уязвимости ИКТ и просьбы об оказании помощи в странах и группах экстренного реагирования. Такие процессы должны осуществляться в соответствии с внутренним законодательством.

62. На национальном, региональном и международном уровнях государства могли бы рассмотреть вопрос о создании беспристрастных правовых рамок, стратегий и программ, которыми можно было бы руководствоваться при принятии решений по устранению факторов уязвимости ИКТ и ограничить их коммерческое распространение, что выступит средством защиты от любого ненадлежащего использования, являющегося потенциальным фактором риска для международного мира и безопасности или прав человека и основных свобод.

Государства могли бы также рассмотреть вопрос о введении правовой защиты для исследователей и специалистов по тестированию на проникновение.

63. Кроме того, в консультации с соответствующими отраслевыми и другими субъектами, занимающимися вопросами безопасности ИКТ, государства могут разработать согласующиеся с соответствующими международными техническими стандартами руководящие принципы и стимулирующие меры, которые касаются ответственной координации работы с уязвимостями и составления соответствующей отчетности, а также соответствующих ролей и обязанностей различных заинтересованных сторон в процессе представления отчетности; типов технической информации, подлежащих раскрытию или публичному распространению, включая обмен технической информацией о серьезных инцидентах в области ИКТ; и способов работы с конфиденциальными данными и обеспечения безопасности и конфиденциальности информации.

64. Рекомендации предыдущих групп правительственных экспертов по укреплению доверия, международному сотрудничеству и наращиванию потенциала могут оказаться особенно полезными для выработки общего понимания механизмов и процессов, которые государства могут создать для ответственного раскрытия информации об уязвимостях. С этой целью государства могут рассмотреть вопрос об использовании существующих многосторонних, региональных и субрегиональных органов и других соответствующих каналов и платформ с участием различных заинтересованных сторон.

Норма 13 k): государства не должны заведомо осуществлять и поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренного реагирования (также именуемым группами реагирования на компьютерные инциденты или группами реагирования на инциденты информационной безопасности) другого государства. Государство не должно использовать уполномоченные группы экстренного реагирования для осуществления злонамеренной международной деятельности.

65. В этой норме отражен тот факт, что ГРКИ/ГРИИБ или другие уполномоченные органы реагирования наделены уникальными обязанностями и функциями по обработке и урегулированию инцидентов в сфере ИКТ и тем самым играют важную роль в содействии поддержанию международного мира и безопасности. Они особенно важны для эффективного обнаружения и смягчения немедленных и долгосрочных негативных последствий инцидентов в сфере ИКТ. Вред, наносимый группам чрезвычайного реагирования, может подорвать доверие и затруднить выполнение ими своих функций и может привести к более широким и зачастую непредвиденным последствиям для различных секторов и, потенциально, для международного мира и безопасности. Группа подчеркивает важность недопущения политизации ГРКИ/ГРИИБ и признания независимого характера их функций.

66. В знак признания важнейшей роли ГРКИ/ГРИИБ в защите населения и предотвращении экономических потерь в результате инцидентов, связанных с ИКТ, многие государства относят их к категории элементов своей критически важной инфраструктуры.

67. При рассмотрении вопроса о том, каким образом их действия в отношении групп чрезвычайного реагирования могут способствовать международному миру и безопасности, государства могли бы публично объявить или принять меры, подтверждающие, что они не будут использовать уполномоченные группы чрезвычайного реагирования для участия в злонамеренной международной деятельности, и признать и уважать сферы деятельности и этические принципы,

которыми руководствуются в своей работе уполномоченные группы чрезвычайного реагирования. Группа принимает к сведению возникающие инициативы в этом отношении.

68. Государства могли бы также рассмотреть вопрос о принятии других мер, таких как создание национальной системы обработки инцидентов в сфере ИКТ с определенными функциями и обязанностями, в том числе для ГРКИ/ГРИИБ для упрощения сотрудничества и координации между такими группами и другими соответствующими органами по вопросам безопасности и техническими органами на национальном, региональном и международном уровнях. Такая система может включать в себя политику, нормативные меры или процедуры, которые более точно определяют статус, полномочия и мандаты ГРКИ/ГРИИБ и отделяют уникальные функции таких групп от других функций управления.

IV. Международное право

69. Международное право является основой общей приверженности государств предотвращению конфликтов и поддержанию международного мира и безопасности и ключом к укреплению доверия между государствами. При рассмотрении вопроса о том, как международное право применяется к использованию ИКТ государствами, Группа подтверждает оценки и рекомендации по международному праву, содержащиеся в докладах предыдущих групп правительственных экспертов, касающиеся в том числе применимости норм международного права, в частности положений Устава Организации Объединенных Наций, и их ключевого значения для поддержания мира и стабильности и для создания открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Эти оценки и рекомендации, в сочетании с другими существенными элементами предыдущих докладов, подчеркивают, что важнейшую основу действий государств при использовании ИКТ составляет соблюдение государствами международного права, в частности их обязательств по Уставу.

70. В этой связи Группа подтвердила обязательства государств по соблюдению следующих принципов Устава и других норм международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; обязательство воздерживаться в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, не совместимым с целями Организации Объединенных Наций; уважение прав человека и основных свобод; и невмешательство во внутренние дела других государств.

71. В дополнение к работе предыдущих групп правительственных экспертов и руководствуясь Уставом и мандатом, содержащимся в резолюции 73/266, настоящая Группа предлагает дополнительный уровень понимания оценок и рекомендаций, содержащихся в докладе Группы 2015 года, относительно того, как международное право применяется к использованию ИКТ государствами, а именно:

a) Группа отмечает, что в соответствии со своими обязательствами по пункту 3 статьи 2 и Главе VI Устава Организации Объединенных Наций, государства, участвующие в любом международном споре, включая споры, связанные с использованием ИКТ, продолжение которого могло бы угрожать поддержанию международного мира и безопасности, должны прежде всего стараться разрешить спор с помощью средств, описанных в Статье 33 Устава, то есть переговоров, обследования, посредничества, примирения, арбитража, судебного

разбирательства, обращения к региональным органам или соглашениям или иными мирными средствами по своему выбору. Группа также отмечает важность других положений Устава, относящихся к разрешению споров мирными средствами;

b) Группа подтверждает, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над инфраструктурой ИКТ, расположенной на их территории. К деятельности государств в сфере ИКТ применимы существующие обязательства по международному праву. Государства осуществляют юрисдикцию в отношении инфраструктуры ИКТ на своей территории, *в частности*, принимая директивные и законодательные меры и создавая необходимые механизмы для защиты инфраструктуры ИКТ на своей территории от связанных с ИКТ угроз;

c) в соответствии с принципом невмешательства, государства не должны прямо или косвенно вмешиваться во внутренние дела другого государства, в том числе с помощью ИКТ;

d) при использовании ИКТ и в соответствии с Уставом Организации Объединенных Наций государствам следует воздерживаться в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, не совместимым с целями Организации Объединенных Наций;

e) особо отмечая стремление международного сообщества к мирному использованию ИКТ в интересах всеобщего блага человечества и напоминая, что Устав применяется в полном объеме, Группа вновь отмечает неотъемлемое право государств принимать меры, соответствующие международному праву и признанные в Уставе, а также необходимость продолжения изучения этого вопроса;

f) Группа отмечает, что нормы международного гуманитарного права применимы только в ситуациях вооруженных конфликтов. Она напоминает об установленных международно-правовых принципах, включая, где это применимо, принципы гуманности, необходимости, соразмерности и избирательности, которые были отмечены в докладе 2015 года. Группа признает необходимость дальнейшего изучения вопроса о том, как и когда эти принципы применяются к использованию ИКТ государствами, и подчеркивает, что напоминание об этих принципах ни в коем случае не узаконивает и не поощряет конфликты;

g) Группа вновь подтверждает, что государства должны выполнять свои международные обязательства в отношении международно-противоправных деяний, приписываемых им в соответствии с международным правом. Она также подтверждает, что государства не должны использовать посредников для совершения международно-противоправных деяний с применением ИКТ и должны стремиться обеспечить, чтобы их территория не использовалась для совершения таких деяний негосударственными субъектами. В то же время Группа напоминает, что указания на то, что та или иная деятельность в сфере ИКТ была начата или иным образом происходит с территории или объектов ИКТ-инфраструктуры государства, может быть недостаточно для приписывания этой деятельности указанному государству; и отмечает, что обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. Призвание государства к ответственности за международно-противоправное деяние сопряжено со сложными техническими, юридическими и политическими моментами.

72. Без ущерба для существующего международного права и дальнейшего развития международного права в будущем Группа признает, что продолжение коллективного обсуждения и обмена мнениями между государствами в Организации Объединенных Наций о том, как конкретные нормы и принципы международного права применяются к использованию ИКТ государствами, имеет особое значение для углубления общего понимания во избежание недоразумений и повышения предсказуемости и стабильности. В основу таких обсуждений могут лечь информация и аргументы, выработанные при обменах мнениями между государствами на региональном и двустороннем уровнях.

73. В соответствии с мандатом Группы официальный сборник (A/76/136) предоставленных участвующими правительственными экспертами добровольно представляемых национальных материалов по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами, будет опубликован на веб-сайте Управления Организации Объединенных Наций по вопросам разоружения. Группа призывает все государства продолжать добровольно делиться своими мнениями и оценками национального характера, передавая их через Генерального секретаря Организации Объединенных Наций или по другим каналам, сообразно обстоятельствам.

V. Меры по укреплению доверия

74. Группа отмечает, что, благоприятствуя укреплению доверия, сотрудничества, транспарентности и предсказуемости, меры по укреплению доверия могут способствовать стабильности и помочь снизить риск недопонимания, эскалации и конфликта. Укрепление доверия — это долгосрочная и последовательная работа, требующая постоянного вовлечения государств. Эффективному внедрению и усилению таких мер может способствовать поддержка со стороны Организации Объединенных Наций, региональных и субрегиональных органов и других заинтересованных сторон.

75. Чтобы подкрепить свои усилия по укреплению доверия и обеспечению мирной информационно-коммуникационной среды государствам рекомендуется публично подтвердить свою приверженность принципам ответственного поведения государств, упомянутым в пункте 2, и действовать в соответствии с ними. Государствам также рекомендуется принимать во внимание Руководящие принципы для мер по укреплению доверия, принятые Комиссией по разоружению Организации Объединенных Наций в 1988 году и утвержденные консенсусом Генеральной Ассамблеей в резолюции 43/78 (H), а также опыт в области мер по укреплению доверия и их введения в действие, накапливаемый на региональном и субрегиональном уровнях.

Совместные меры

Координаторы

76. Назначение компетентных координаторов на политическом и техническом уровнях может способствовать обеспечению надежной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере ИКТ и ослабления напряженности в кризисных ситуациях. Коммуникация между координаторами может помочь снизить напряженность и предотвратить недопонимание и неверное толкование, которые могут возникнуть в результате инцидентов в сфере ИКТ, в том числе затрагивающих критически важную инфраструктуру и имеющих национальное, региональное или глобальное значение. Они могут также расширить обмен информацией и помочь

государствам более эффективно обрабатывать и урегулировать инциденты в сфере ИКТ.

77. При определении координаторов или вовлечении в координационную сеть государствам следует рассмотреть следующие шаги:

a) назначение специальных координаторов на стратегическом, дипломатическом и техническом уровнях и выработка рекомендаций по определению конкретных характеристик координаторов, включая ожидаемые роли и обязанности, координационные функции и требования к готовности;

b) создание межправительственных и внутригосударственных процедур для обеспечения эффективной коммуникации между координаторами во время кризисов. В типовых формах могут указываться виды требуемой информации, включая технические данные и характер запроса, но при этом эти формы должны быть достаточно гибкими, чтобы обеспечить возможность коммуникации, даже при нехватке информации по некоторым вопросам;

c) извлечение уроков и передового опыта из деятельности региональных координационных сетей, в том числе в отношении обсуждения, разработки и реализации практических подходов к использованию координационных сетей в национальном, региональном и международном контекстах, включая ранее предупреждение о серьезных инцидентах в сфере ИКТ с целью укрепления координации и обмена информацией между назначенными координаторами.

78. Борьба с глобальными угрозами безопасности ИКТ также требует глобальных ответных мер, носящих как всеохватный, так и универсальный характер. Государства могли бы предложить Генеральному секретарю Организации Объединенных Наций содействовать добровольному обмену опытом между всеми государствами-членами в отношении уроков, передового опыта и руководящих указаний, имеющих отношение к координационным сетям, которые уже существуют на региональном и субрегиональном уровнях. Такая работа может стать вкладом в обсуждение, связанное с созданием на глобальном уровне каталога таких координаторов.

Диалог и консультации

79. Диалог в рамках двусторонних, субрегиональных, региональных и многосторонних консультаций и взаимодействия может способствовать углублению взаимопонимания между государствами, укреплению доверия и содействию более тесному сотрудничеству между государствами в деле смягчения воздействия инцидентов в сфере ИКТ при одновременном снижении рисков недопонимания и эскалации. Другие заинтересованные стороны, такие как частный сектор, научные и технические круги и гражданское общество, могут внести значительный вклад в содействие проведению таких консультаций и налаживанию такого взаимодействия.

80. Региональные органы предприняли значительные шаги по разработке и реализации мер по укреплению доверия, которые могут снизить риск недопонимания, эскалации и конфликтов, связанных с инцидентами в области ИКТ. Взаимодействие с такими органами позволяет сосредоточиться на региональных особенностях и проблемах, а межрегиональные обмены способствуют взаимному обучению таких организаций. Государствам рекомендуется продолжать эту работу, а также активно взаимодействовать с теми государствами, которые в настоящее время не являются членами соответствующей региональной или субрегиональной организации.

81. В целях дальнейшего укрепления мер сотрудничества, касающихся национальных групп реагирования на компьютерные инциденты и других уполномоченных органов, государства могли бы поощрять обмен и распространение информации и передового опыта в области создания и обеспечения функционирования национальных ГРКИ/ГРИИБ, а также в области работы с инцидентами через существующие региональные и глобальные организации и сети по реагированию на чрезвычайные ситуации. Такое поощрение и поддержка ГРКИ/ГРИИБ послужили бы также цели повышения осведомленности государств об их обязательствах в отношении таких групп и других соответствующих органов в соответствии с нормой 13 k).

Меры по обеспечению транспарентности

82. Особое значение для укрепления доверия и предсказуемости, сокращения возможностей для неправильного толкования и эскалации и оказания помощи отдельным лицам и организациям в принятии правильных решений в области управления рисками имеет обеспечение транспарентности на добровольной основе путем обмена национальными мнениями и опытом по инцидентам, связанным с безопасностью ИКТ, и другим связанным с ними угрозам, а также путем обнародования связанных с ИКТ советов по обеспечению безопасности, рекомендаций, руководящих указаний, фактологической базы и подтверждающих данных для принятия решений.

83. Для того, чтобы и далее повышать транспарентность и предсказуемость поведения государств, иметь возможность ознакомиться с более широким диапазоном мнений и опыта и повысить готовность и раннюю осведомленность государств в отношении растущих угроз, государства могли бы рассмотреть возможность использования двусторонних, субрегиональных, региональных и многосторонних форумов и неофициальных консультаций для добровольного обмена информацией о передовых методах, уроках или аналитических докладах в отношении существующих и новых угроз и инцидентов, связанных с безопасностью ИКТ; о национальных стратегиях и стандартах анализа уязвимости информационно-коммуникационных продуктов; и о национальных и региональных подходах к управлению рисками и предотвращению конфликтов.

84. Государства также могут воспользоваться этими существующими форумами для уточнения позиций и добровольного обмена информацией о национальных подходах к обеспечению безопасности ИКТ; защите данных; защите объектов критически важной инфраструктуры с использованием ИКТ; и миссиях и функциях структур по обеспечению информационно-коммуникационной безопасности, стратегии в области ИКТ на национальном или организационном уровнях, а также правовых и надзорных режимов, в рамках которых они работают.

85. Рекомендации по мерам по укреплению доверия, содержащиеся в предыдущих докладах групп правительственных экспертов, обеспечивают основу для совместного противодействия растущим угрозам, связанным с проблемами критически важной инфраструктуры, и для реализации соответствующих норм. Государствам рекомендуется продолжать повышать осведомленность о важности защиты объектов критически важной инфраструктуры, поощрять обмен информацией между заинтересованными сторонами, занимающимися объектами критически важной инфраструктуры, и обмениваться передовым опытом и рекомендациями. В соответствующих случаях они могут использовать существующие платформы и механизмы отчетности (см. пункт 86 ниже) для добровольного обмена сформированными на национальном уровне мнениями на темы классификации критически важной национальной инфраструктуры и

критически важной инфраструктуры, обеспечивающей предоставление основных услуг на региональном или международном уровнях, соответствующей национальной политики и законодательства и основы для оценки рисков и для выявления, классификации и урегулирования инцидентов в области ИКТ, затрагивающих критическую инфраструктуру.

86. Государства могли бы также использовать ресурсы Организации Объединенных Наций, такие как механизм добровольных докладов Генеральному секретарю, портал по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), а также ресурсы других соответствующих международных и региональных организаций, для обобщения информации и примеров передового опыта, предоставляемых государствами в отношении национальных стратегий, программ и директивных и законодательных мер, охватывающих вопросы безопасности ИКТ, имеющие отношение к международной безопасности и стабильности.

VI. Международное сообщество и помощь по линии обеспечения безопасности и наращивания потенциала в области ИКТ

87. Группа подчеркивает важность международного сотрудничества и помощи в области информационно-коммуникационной безопасности и создания потенциала, а также их важность для всех элементов мандата Группы. Активизация сотрудничества наряду с более эффективной помощью и наращиванием потенциала в области информационно-коммуникационной безопасности с участием других заинтересованных сторон, таких как частный сектор, научные круги, гражданское общество и технические круги, могут помочь государствам применять принципы ответственного поведения государств при использовании ими ИКТ. Они имеют решающее значение для преодоления существующих разногласий внутри государств и между ними по политическим, правовым и техническим вопросам, касающимся безопасности ИКТ. Они также могут способствовать достижению других целей международного сообщества, таких как цели в области устойчивого развития.

88. Международное сотрудничество и помощь в деле обеспечения безопасности и наращивания потенциала ИКТ могут способствовать укреплению потенциала государств по выявлению угроз, расследованию их обстоятельств и реагированию на них, а также обеспечению того, чтобы все государства имели возможность и потенциал для принятия ответственных мер при использовании ими ИКТ. Они могут также способствовать тому, чтобы все государства достигли необходимых уровней защиты и безопасности критически важных объектов инфраструктуры, располагали необходимыми возможностями для обработки инцидентов, а также могли запрашивать помощь или реагировать на призывы об оказании помощи в случае злоумышленной деятельности в области ИКТ, исходящей с их территории или затрагивающей ее.

89. Группа рекомендует и далее укреплять международное сотрудничество и помощь в области безопасности ИКТ и создания потенциала для помощи государствам в следующих областях:

a) разработка и осуществление национальных директив, стратегий и программ в сфере ИКТ;

b) создание и укрепление потенциала ГРКИ/ГРИИБ и укрепление механизмов сотрудничества между такими группами;

c) повышение безопасности, жизнестойкости и защиты объектов критически важной инфраструктуры;

d) создание или укрепление технического, правового и политического потенциала государств для выявления, расследования и урегулирования инцидентов в сфере ИКТ, в том числе посредством инвестиций в развитие людских ресурсов, институтов, отказоустойчивых технологий и образовательных программ;

e) углубление общего понимания вопросов применимости международного права к использованию ИКТ государствами и содействие обмену мнениями на эту тему между государствами, в том числе в рамках обсуждений в Организации Объединенных Наций;

f) укрепление технического и правового потенциала всех государств в вопросах расследования и урегулирования серьезных инцидентов в сфере ИКТ;

g) соблюдение согласованных добровольных и необязывающих норм ответственного поведения государств;

h) с этой целью и в качестве средства оценки собственных приоритетов, потребностей и ресурсов государствам рекомендуется использовать добровольный Обзор национального осуществления, рекомендованный Рабочей группой открытого состава Организации Объединенных Наций[4].

90. В целях преодоления «цифрового разрыва» и обеспечения получения всеми государствами выгоды от этих и других областей помощи и укрепления потенциала государствам рекомендуется по возможности выделять достаточные финансовые ресурсы, оказывать техническое и политическое консультирование и поддержку странам, запрашивающим помощь в их работе по повышению безопасности ИКТ.

91. Что касается развития международного сотрудничества и оказания помощи по линии обеспечения безопасности и наращивания потенциала в области ИКТ, то Группа подчеркивает добровольный, политически нейтральный, взаимовыгодный и взаимный характер наращивания потенциала. В этой связи Группа приветствует принципы наращивания потенциала, касающиеся процесса, цели, партнерства и людей, рекомендованные Рабочей группой открытого состава, и призывает все государства руководствоваться этими принципами в своих усилиях по развитию сотрудничества и оказанию помощи[5].

92. Содействие взаимопониманию и взаимному обучению может также способствовать укреплению международного сотрудничества и сотрудничества в области безопасности ИКТ и наращивания потенциала. Государствам следует рассмотреть вопрос о междисциплинарности, многосторонности, модульности и измеряемости оказания помощи в обеспечении безопасности ИКТ и создании потенциала. Этого можно добиться путем взаимодействия с Организацией Объединенных Наций и другими глобальными, региональными и субрегиональными структурами вместе с другими соответствующими заинтересованными сторонами в деле содействия эффективной координации и осуществлению программ по наращиванию потенциала, а также поощрения транспарентности и обмена информацией об их эффективности.

[4] Заключительный основной доклад Рабочей группы открытого состава, п. 65.

[5] Заключительный основной доклад Рабочей группы открытого состава, п. 56.

VII. Выводы и рекомендации в отношении дальнейшей работы

93. В свете того, что государства становятся все более зависимыми от ИКТ, необходимы общие рамки ответственного поведения государств при использовании ИКТ в контексте международной безопасности, с тем чтобы все государства могли пользоваться преимуществами этих технологий, а также могли защищаться от их ненадлежащего использования и реагировать на него.

94. Группа сосредоточила свои усилия на содействии общему пониманию и эффективному осуществлению и, опираясь на рекомендации предыдущих докладов, выявила и детально определила те подходы и рекомендации, которые государства могут использовать для обеспечения эффективности совместных мер по борьбе с существующими и потенциальными угрозами в сфере информационно-коммуникационной безопасности. Эти подходы четко изложены в разделах доклада, посвященных нормам, правилам и принципам ответственного поведения государств; международному праву; укреплению доверия; и международному сотрудничеству и укреплению потенциала, в каждом из которых подробно рассказывается об основных элементах ответственного поведения государств, описанных в предыдущих докладах групп правительственных экспертов.

95. Группа также определила потенциальные области для будущей работы, которые, в частности, включают:

a) расширение сотрудничества на двустороннем, региональном и многостороннем уровнях в целях содействия выработке единого понимания потенциальных угроз международному миру и безопасности, проистекающих от злонамеренного использования ИКТ, а также единого понимания безопасности инфраструктуры, зависящей от ИКТ;

b) дальнейший обмен информацией и мнениями о нормах, правилах и принципах ответственного поведения государств, а также о национальной и региональной практике применения норм и мер по укреплению доверия и о применимости международного права к использованию ИКТ государствами, в том числе путем определения конкретных тем международного права для дальнейшего углубленного обсуждения;

c) дальнейшее укрепление международного сотрудничества и наращивание потенциала с использованием оценок и рекомендаций, содержащихся в настоящем докладе, с тем чтобы все государства могли вносить свой вклад в поддержание международного мира и безопасности, принимая во внимание пункт 90 выше;

d) определение механизмов, которые способствуют вовлечению других основных заинтересованных сторон, включая представителей частного сектора, научных и технических кругов и гражданского общества, в работу по внедрению, при возможности, принципов ответственного поведения;

e) обращение с просьбой к ЮНИДИР, который оказывает услуги всем государствам-членам, провести соответствующие исследования по темам, обсуждаемым в данном докладе, а также поощрение проведения таких исследований другими соответствующими аналитическими центрами и исследовательскими институтами.

96. Группа призывает продолжать всеохватный и транспарентный процесс переговоров по ИКТ в контексте международной безопасности под эгидой Организации Объединенных Наций при участи и признании вклада Рабочей группы

открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий 2021–2025 годов, учрежденной в соответствии с резолюцией 75/240 Генеральной Ассамблеи. Группа рекомендует, чтобы будущая работа основывалась на совокупной работе групп правительственных экспертов и рабочих групп открытого состава.

97. Группа призывает государства продолжать работу по развитию принципов ответственного поведения государств, используя Организацию Объединенных Наций и другие региональные и многосторонние форумы для ведения регулярного диалога, проведения консультаций и наращивания потенциала в инклюзивном, транспарентном, консенсусном и практическом ключе. В этой связи и в соответствии с итогами Рабочей группы открытого состава, Группа отмечает целый ряд предложений по содействию ответственному поведению государств в сфере ИКТ, которые, в частности, будут способствовать укреплению потенциала государств в выполнении обязательств по использованию ими ИКТ, в частности Программы действий. При рассмотрении таких предложений следует учитывать обеспокоенность и интересы всех государств путем обеспечения равноправного участия государств в деятельности Организации Объединенных Наций. В этой связи Программу действий следует доработать, в том числе в рамках процесса Рабочей группы открытого состава, учрежденной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

98. Группа рекомендует государствам-членам руководствоваться оценками и рекомендациями настоящего доклада и докладов предыдущих групп правительственных экспертов, а также выводами и рекомендациями заключительного доклада Рабочей группы открытого состава (A/75/816) , а также проанализировать возможные способы доработки и осуществления этих рекомендаций.

Приложение

Список членов Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности

Австралия
Джоанна Уивер
Специальный советник посла Австралии по вопросам киберпространства, Министерство иностранных дел и торговли

Бразилия
Гильерми ди Агиар Патриота
Посол, Генеральный консул Бразилии в Мумбаи

Китай
Ван Лэй
Координатор по вопросам киберпространства, Министерство иностранных дел

Эстония
Хели Тиирмаа-Клаар
Посол по особым поручениям по кибердипломатии, генеральный директор Департамента кибердипломатии, Министерство иностранных дел

Франция
Анри Вердье
Посол по цифровым технологиям, Министерство по делам Европы и иностранных дел

Германия
Регина Гринбергер (третья и четвертая сессии)
Посол по кибернетической внешней политике, Федеральное министерство иностранных дел

Вольфрам фон Хейниц (первая и вторая сессии)
Руководитель Службы координаторов международной киберполитики, Федеральное министерство иностранных дел

Индия
С. Джанакираман
Совместный секретарь и руководитель Отдела электронного управления и информационных технологий и Отдела кибердипломатии, Министерство иностранных дел

Индонезия
Роллианшах Сумират (третья и четвертая сессии)
Директор Управления международной безопасности и разоружения, Министерство иностранных дел

Хардитья Сурьяванто (вторая сессия)
Советник по вопросам коммуникационных технологий и киберпространства, Управление международной безопасности и разоружения, Министерство иностранных дел

Грата Эндах Варданингтяс (первая сессия)
Директор по международной безопасности и разоружению, Министерство иностранных дел

Япония
Такеси Акахори
Посол по делам Организации Объединенных Наций и киберполитике, Министерство иностранных дел

Иордания
Ферас Мохаммад Абдаллах аз-Зуби Руководитель отделения Национальной программы кибербезопасности, Вооруженные силы Иордании

Казахстан
Асет Нусупов
Заведующий сектором, Администрация Президента Республики Казахстан

Кения
Кэтрин Гетао
Главный административный сотрудник, Управление ИКТ

Маврикий
Калим Ахмед Усмани
Руководитель Группы реагирования на связанные с компьютерами чрезвычайные ситуации Маврикия

Мексика
Херардо Исаак Моралес Тенорио
Координатор по вопросам многомерной безопасности, Министерство иностранных дел

Марокко
Абдаллах Бутриг
Старший полковник, директор по содействию, обучению, контролю и экспертизе, Главное управление безопасности информационных систем, Управление национальной обороны

Нидерланды
Кармен Гонсалвес
Руководитель службы международной киберполитики, Министерство иностранных дел

Норвегия
Симен Экблом (третья и четвертая сессии)
Координатор по вопросам киберполитики, Министерство иностранных дел

Анникен Крутнес (первая и вторая сессии)
Заместитель Генерального директора, Департамент политики безопасности и крайнего севера, Министерство иностранных дел

Румыния
Михаэла-Йонелия Попеску
Координатор по вопросам киберполитики, Министерство иностранных дел

Российская Федерация
Андрей Крутских
Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директор Департамента международной информационной безопасности, Министерство иностранных дел

Владимир Шин (третья и четвертая сессии)
Заместитель директора Департамента международной информационной безопасности, Министерство иностранных дел

Сингапур
Дэвид Кох
Главный административный сотрудник Агентства кибербезопасности Сингапура и комиссар по кибербезопасности

Южная Африка
Док Машабане
Генеральный директор, Департамент юстиции и конституционного развития

Молиехи Макумане (третья и четвертая сессии)
Специальный советник представителя Группы правительственных экспертов от Южной Африки

Швейцария
Надин Оливьери Лозано
Посол, руководитель Отдела международной безопасности, Федеральный департамент иностранных дел

Соединенное Королевство
Кэтрин Джонс
Руководитель Отдела международного киберуправления, Управление национальной безопасности, Министерство иностранных дел, по делам Содружества и развития

Александр Эванс (первая сессия)
Бывший директор по вопросам киберпространства, Министерство иностранных дел, по делам Содружества и развития

Соединенные Штаты
Мишель Маркофф
Исполняющий обязанности координатора по вопросам киберпространства, Государственный департамент США

Уругвай

Ноэлия Мартинес Франки (третья и четвертая сессии)
Директор по многосторонним вопросам, Министерство иностранных дел

Алехандра Эррамуспе (первая и вторая сессии)
Старший сотрудник, Управление электронного правительства и информационного общества, Канцелярия Президента