Организация Объединенных Наций A/70/174

Генеральная Ассамблея

Distr.: General
22 July 2015
Russian
Original: English

Семидесятая сессия
Пункт 93 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта группа была созвана в соответствии с пунктом 4 резолюции 68/243 Генеральной Ассамблеи.

* A/70/150.

15-12404 (R) 180815 200815

Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Резюме

Информационно-коммуникационные технологии (ИКТ) открывают широчайшие возможности и приобретают все большее значение для международного сообщества. Вместе с тем, наметились тревожные тенденции, которые создают угрозу международному миру и безопасности. Существенно важное значение для борьбы с этой угрозой имеет эффективное сотрудничество между государствами.

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, созванная в 2015 году, изучила существующие и потенциальные угрозы, порожденные использованием ИКТ государствами, и проанализировала меры для борьбы с ними, в том числе разработку норм, правил, принципов и мер укрепления доверия. Кроме того, Группа рассмотрела вопрос о применимости норм международного права к использованию ИКТ государствами. Основываясь на работе предыдущих групп, Группа нынешнего созыва добилась существенных успехов в этих сферах.

В настоящем докладе предпринято значительно более широкое обсуждение норм. Группа рекомендовала государствам сотрудничать в деле предупреждения злонамеренного использования ИКТ и не допускать заведомо использования их территории для совершения международно противоправных деяний с использованием ИКТ. Она призвала расширить обмен информацией и оказание взаимопомощи в целях преследования террористов и пресечения случаев преступного использования ИКТ. Группа подчеркнула, что при этом государства должны обеспечивать всестороннее соблюдение прав человека, в том числе права на невмешательство в личную жизнь и свободу выражения мнений.

Одна из важных рекомендаций заключается в том, что государства не должны осуществлять или заведомо поддерживать деятельность в сфере ИКТ, направленную на нанесение преднамеренного ущерба критически важной инфраструктуре или создание иных препятствий в ее использовании или функционировании. Кроме того, государства должны принимать надлежащие меры для защиты их критически важной инфраструктуры от угроз в сфере ИКТ. Государства не должны наносить ущерб информационным системам групп экстренной готовности к компьютерным инцидентам других государств или же использовать такие группы для участия в злонамеренной международной деятельности. Государства должны поддерживать ответственное представление информации о факторах уязвимости в сфере ИКТ, принимать разумные меры для обеспечения неприкосновенности каналов поставок и предупреждать распространение злонамеренных программных средств в сфере ИКТ, технических средств или пагубных скрытых функций.

Меры укрепления доверия способствуют расширению сотрудничества и повышению уровня транспарентности, а также снижают опасность возникновения конфликта. Группа определила ряд добровольных мер укрепления доверия в целях повышения степени транспарентности и предложила государствам рассмотреть дополнительные меры такого рода в целях укрепления сотрудничества. Группа призвала наладить регулярный диалог с большим количеством участников под эгидой Организации Объединенных Наций, а также в рамках двусторонних, региональных и многосторонних форумов. Государства несут основную ответственность за обеспечение безопасности и мирного характера ИКТ-среды, однако надлежащее участие частного сектора, научных кругов и гражданского общества способствовало бы повышению эффективности международного сотрудничества.

Наращивание потенциала имеет существенно важное значение для сотрудничества и укрепления доверия. В докладе Группы за 2013 год (см. A/68/98) к международному сообществу был обращен призыв оказать помощь в укреплении безопасности критически важной инфраструктуры ИКТ, развитии технических навыков и разработке соответствующего законодательства, стратегий и нормативно-правовой базы. Группа нынешнего созыва подтвердила эти выводы и особо отметила, что все государства могут обмениваться информацией об угрозах и эффективных способах реагирования на них.

Группа подчеркнула важность международного права, Устава Организации Объединенных Наций и принципа суверенитета в качестве основы для повышения безопасности в сфере использования ИКТ государствами. Указав не необходимость дальнейшего изучения этого вопроса, Группа отметила, что государства обладают неотъемлемым правом принимать те меры, которые соответствуют нормам международного права и признаны в Уставе. Группа также отметила существующие международно-правовые принципы, в том числе, в соответствующих случаях, принципы гуманности, необходимости, пропорциональности и индивидуализации.

Планируя свою работу на будущее, Группа предложила Генеральной Ассамблее рассмотреть вопрос о созыве Группы правительственных экспертов нового состава в 2016 году.

Группа просит государства-члены внимательно изучить предлагаемые рекомендации и проанализировать возможные пути их доработки и осуществления.

Содержание

Предисловие Генерального секретаря

Информационно-коммуникационные технологии (ИКТ) играют беспрецедентно важную роль в деле преобразования экономики стран, общественных структур и международных отношений. Киберпространство является непременным атрибутом нашей повседневной жизни. ИКТ приносят колоссальную пользу, однако порождают и определенные риски. Обеспечение стабильности и безопасности в киберпространстве может быть достигнуто лишь по линии международного сотрудничества, причем основой такого сотрудничества должны являться нормы международного права и принципы, провозглашенные в Уставе Организации Объединенных Наций.

В настоящем докладе содержатся разработанные Группой правительственных экспертов из 20 государств рекомендации по устранению существующих и потенциальных угроз международному миру и безопасности, проистекающих из использования ИКТ государствами и негосударственными субъектами. Эксперты дополнили утвержденные путем консенсуса доклады за 2010 и 2013 годы и предложили идеи в отношении разработки норм, укрепления доверия, наращивания потенциала и применения норм международного права.

В числе новых сложных вопросов можно назвать все более широкое злонамеренное применение ИКТ экстремистами, террористами и организованными преступными группировками. В настоящем докладе содержатся предложения, которые могут способствовать пресечению этой тревожной тенденции и лечь в основу моего будущего плана действий по предупреждению воинствующего экстремизма.

Все государства должны принимать участие в деятельности по повышению безопасности киберпространства. Наши усилия в этой сфере должны быть направлены на сохранение глобального обязательства по содействию созданию открытого, безопасного и мирного Интернета. В этой связи я передаю настоящий доклад на рассмотрение Генеральной Ассамблеи и международного сообщества в целом, считая, что он является важным вкладом в принятие жизненно необходимых мер для обеспечения безопасности ИКТ-среды.

Препроводительное письмо

26 июня 2015 года

Имею честь препроводить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта группа была созвана в 2014 году в соответствии с пунктом 4 резолюции 68/243 Генеральной Ассамблеи о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. В качестве Председателя Группы я с удовлетворением сообщаю вам, что по этому докладу был достигнут консенсус.

В указанной резолюции Генеральная Ассамблея просила создать в 2014 году на основе справедливого географического распределения группу правительственных экспертов, с тем чтобы продолжить в целях содействия выработке общего понимания исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия, вопросов использования информационно-коммуникационных технологий в конфликтах и того, как международное право применяется к использованию информационно-коммуникационных технологий государствами, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Группе было также предложено принять во внимание оценки и рекомендации, содержащиеся в докладе предыдущей группы (см. A/68/98). К Генеральному секретарю была обращена просьба представить Ассамблее на ее семидесятой сессии доклад о результатах этого исследования.

В соответствии с положениями указанной резолюции были назначены эксперты из 20 государств: Беларуси, Бразилии, Ганы, Германии, Египта, Израиля, Испании, Кении, Китая, Колумбии, Малайзии, Мексики, Пакистана, Республики Корея, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Японии. Список экспертов приводится в приложении.

Группа провела всесторонний и углубленный обмен мнениями по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Группа провела четыре сессии: первую сессию с 21 по 25 июля 2014 года в Центральных учреждениях Организации Объединенных Наций, вторую — с 12 по 16 января 2014 года в Женеве, третью — с 13 по 17 апреля 2015 года и четвертую — с 22 по 26 июня 2015 года в Центральных учреждениях Организации Объединенных Наций.

Группа хотела бы поблагодарить экспертов, которые выступили в роли координаторов в ходе обсуждения проекта доклада: Флоренс Манжин (Франция), Кетрин Гетао (Кения), Аусафа Али (Пакистан), Рикардо Мора (Испания) и Оливию Престон (Соединенное Королевство).

Группа хотела бы выразить признательность за внесенный вклад Институту Организации Объединенных Наций по исследованию проблем разоружения, который консультировал Группу и от которого в ее работе участвовали Джеймс Льюис и Керстин Вигнард. Группа хотела бы также выразить свою признательность сотруднику Управления по вопросам разоружения Организа-

ции Объединенных Наций Юэну Бьюканану, который исполнял обязанности Секретаря Группы, и другим должностным лицам Секретариата, оказавшим содействие Группе.

(*Подпись*) Карлос Луис Дантас Кутинью **Перес**
Председатель Группы

I. Введение

1. В соответствии с резолюцией 68/243 Генеральной Ассамблеи, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральный секретарь создал на основе справедливого географического распределения группу правительственных экспертов, с тем чтобы продолжить в целях содействия выработке общего понимания исследование существующих и потенциальных проблем в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия, в вопросах использования информационно-коммуникационных технологий (ИКТ) в конфликтах и того, как международное право применяется к использованию ИКТ государствами, а также соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем.

2. Открытая, безопасная, стабильная, доступная и мирная ИКТ-среда имеет существенно важное значение для всех, а для ее создания необходимо эффективное сотрудничество между государствами в целях снижения угроз международному миру и безопасности. В настоящем докладе получили отражение рекомендации Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и используются результаты работы предыдущих групп (см. A/65/201 и A/68/98). Группа изучила соответствующие международные концепции и возможные совместные меры, имеющие отношение к ее мандату. Она вновь заявила, что деятельность по содействию использованию ИКТ в мирных целях и предупреждению конфликтов, связанных с их использованием, отвечает интересам всех государств.

II. Существующие и нарождающиеся угрозы

3. ИКТ открывают широчайшие возможности для социально-экономического развития и приобретают все большее значение для международного сообщества. Вместе с тем существуют тревожные тенденции в глобальной ИКТ-среде, включая резкое увеличение числа случаев злонамеренного использования ИКТ государственными и негосударственными субъектами. Такие тенденции создают угрозу для всех государств, а злонамеренное использование ИКТ может нанести ущерб международному миру и безопасности.

4. Ряд государств занимаются наращиванием потенциала в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным.

5. К числу наиболее пагубных нападений с использованием ИКТ относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной.

6. Существует все более реальная 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 вер-

бовки сторонников, финансирования, обучения и подстрекательства, причем, если не принять соответствующих мер, то это может поставить под угрозу международный мир и безопасность.

7. Многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов), их различные мотивы, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу. Государства с полным основанием обеспокоены опасностью дестабилизирующих последствий ошибочного понимания намерений другой стороны, потенциалом возникновения конфликта и возможностью нанесения ущерба их экономике.

8. Разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами может привести к повышению уязвимости в условиях взаимосвязанного мира.

III. Нормы, правила и принципы ответственного поведения государств

9. ИКТ-среда открывает возможности и одновременно создает проблемы для международного сообщества в деле определения применимости норм, правил и принципов к поведению государств при осуществлении деятельности, связанной с ИКТ. Одна из целей заключается в том, чтобы определить дополнительные добровольные и необязательные нормы ответственного поведения государств, а также укрепить общее понимание в целях повышения стабильности и безопасности в глобальной ИКТ-среде.

10. Принятие добровольных и необязательных норм ответственного поведения государств может привести к снижению угрозы международному миру, безопасности и стабильности. В соответствии с этим такие нормы не предусматривают ограничения или запрета действий, согласующихся с нормами международного права. Эти нормы отражают ожидания международного сообщества, определяют стандарты ответственного поведения и позволяют международному сообществу давать оценку действиям и намерениям государств. Эти нормы могут способствовать предупреждению конфликтов в ИКТ-среде и мирному использованию в целях обеспечения всесторонней реализации возможностей ИКТ по содействию глобальному социально-экономическому развитию.

11. В предыдущих докладах Группы был отражен консенсус в отношении ответственного поведения государств в сфере обеспечения безопасности и использования ИКТ, формирующейся на основе существующих международных норм и обязательств. Перед Группой этого созыва стояла задача продолжить в целях содействия выработке общего понимания изучение норм ответственного поведения государств, определить, в каких случаях существующие нормы могут быть применимы к ИКТ-среде, способствовать более широкому принятию норм и выяснить, в каких случаях может потребоваться разработка дополнительных норм, которые бы учитывали сложные и уникальные особенности ИКТ.

12. Группа приняла к сведению Правила поведения в области обеспечения международной информационной безопасности, предложенные Казахстаном, Китаем, Кыргызстаном, Российской Федерацией, Таджикистаном и Узбекистаном (см. A/69/723).

13. С учетом существующих и нарождающихся угроз, рисков и факторов уязвимости, а также в развитие оценок и рекомендаций, содержащихся в докладах групп предыдущих созывов за 2010 и 2013 годы, настоящая группа предлагает государствам рассмотреть следующие рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды:

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;

b) в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий;

c) государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

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. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере;

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

f) государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

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 о создании глобальной куль-

туры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

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 должны также 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;

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 пагубных скрытых функций;

j) государства должны способствовать ответственному представлению информации о 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;

k) государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

14. Группа отметила, что, хотя такие меры могут иметь существенно важное значение для содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, их безотлагательное осуществление может оказаться невозможным, в частности для развивающихся государств, которые еще не располагают необходимым потенциалом.

15. С учетом уникальных особенностей ИКТ со временем может возникнуть необходимость в разработке дополнительных норм.

IV. Меры укрепления доверия

16. Меры укрепления доверия способствуют поддержанию международного мира и безопасности. Они могут способствовать расширению межгосударственного сотрудничества, повышению степени транспарентности, предсказуемости и стабильности. В стремлении укрепить доверие в целях создания мирной ИКТ-среды государства должны принимать во внимание Руководящие принципы для мер по укреплению доверия, принятые Комиссией по разоружению в 1988 году и утвержденные консенсусом Генеральной Ассамблеей в резолюции 43/78 (H). В целях повышения доверия и расширения сотрудничества, а

также снижения угрозы конфликта Группа рекомендует государствам рассмотреть следующие добровольные меры укрепления доверия:

a) определение надлежащих контактных центров на политическом и техническом уровнях для рассмотрения серьезных инцидентов в сфере ИКТ и создание перечня таких центров;

b) создание и поддержка механизмов и процессов для проведения двусторонних, региональных, субрегиональных и многосторонних консультаций, сообразно обстоятельствам, в целях укрепления доверия между государствами и снижения риска ошибочного восприятия, эскалации и конфликта, которые могут быть вызваны инцидентами в сфере ИКТ;

c) содействие на добровольной основе повышению транспарентности на двустороннем, субрегиональном, региональном и многостороннем уровнях, сообразно обстоятельствам, в целях повышения доверия и определения направлений будущей работы. Это может включать добровольное распространение национальных мнений и информации о различных аспектах национальных и транснациональных угроз ИКТ и в сфере использования ИКТ; факторах уязвимости и установленных пагубных скрытых функций в продуктах ИКТ; передовых методах обеспечения безопасности ИКТ; мерах укрепления доверия, разработанных в рамках региональных и многосторонних форумов; национальных организациях, политике и программах, имеющих отношение к безопасности ИКТ;

d) добровольное представление государствами информации об их национальных мнениях в отношении категорий инфраструктуры, которые они считают критически важными, а также о национальных усилиях по ее защите, включая информацию о национальных законах и стратегиях обеспечения безопасности данных и инфраструктуры, зависящей от ИКТ. Государства должны стремиться укреплять трансграничное сотрудничество в устранении транснациональных факторов уязвимости критически важной инфраструктуры ИКТ. Такие меры могут включать:

i) создание базы данных по национальному законодательству и стратегиям обеспечения безопасности данных и инфраструктуры, зависящей от ИКТ, а также публикация материалов, считающихся важными для целей распространения информации об этих национальных законах и стратегиях;

ii) создание механизмов и процессов для проведения двусторонних, субрегиональных, региональных и многосторонних консультаций по вопросам защиты критически важной инфраструктуры, зависящей от ИКТ;

iii) создание двусторонних, субрегиональных, региональных и многосторонних основ технических, правовых и дипломатических механизмов для рассмотрения запросов, связанных с ИКТ;

iv) принятие добровольных национальных договоренностей о классификации инцидентов в сфере ИКТ с точки зрения масштабов и серьезности инцидента для целей содействия обмену информацией об инцидентах.

17. Государства должны рассмотреть возможность принятия дополнительных мер укрепления доверия, которые бы способствовали расширению сотрудничества на двусторонней, субрегиональной, региональной и многосторонней основах. Такие меры могут предусматривать принятие государствами добровольных соглашений по следующим вопросам:

a) укрепление механизмов взаимодействия между соответствующими ведомствами по противодействию инцидентам в сфере безопасности ИКТ и создание дополнительных технических, правовых и дипломатических механизмов для рассмотрения запросов, касающихся инфраструктуры ИКТ, в том числе рассмотрения вопроса о проведении обмена кадрами в таких сферах, как реагирование на инциденты и правоохранительная деятельность, сообразно обстоятельствам, и поддержка обменов между научно-исследовательскими учреждениями;

b) расширение сотрудничества, в том числе создание координационных центров для обмена информацией о случаях злонамеренного использования ИКТ и оказания помощи в проведении расследований;

c) создание национальной группы экстренной готовности к компьютерным инцидентам и/или группы реагирования на инциденты в сфере кибербезопасности или же официальное назначение какой-либо организации для выполнения этих функций. Государства могут рассмотреть возможность создания таких органов с учетом своего определения критически важной инфраструктуры. Государства должны поддерживать и обеспечивать функционирование таких национальных групп реагирования и иных уполномоченных органов и сотрудничество между ними;

d) расширение и поддержка сотрудничества между группами экстренной готовности к компьютерным инцидентам и группами реагирования на инциденты в сфере кибербезопасности, сообразно обстоятельствам, например обмен информацией о факторах уязвимости, моделях нападений и передовой практике в сфере смягчения последствий нападения, включая координацию мер реагирования, организацию учений, поддержку деятельности по пресечению инцидентов в сфере ИКТ и расширение регионального и отраслевого сотрудничества;

e) выполнение с учетом норм национального законодательства и международного права поступающих от других государств просьб в рамках расследования преступлений, связанных с ИКТ или использованием ИКТ для террористических целей, или смягчения последствий злонамеренной деятельности в сфере ИКТ, проистекающей с их территории.

18. Группа вновь заявляет, что, учитывая темпы развития ИКТ и масштабы угрозы, необходимо способствовать углублению общего понимания и активизации сотрудничества. В этой связи Группа рекомендует поддерживать регулярный институциональный диалог с широким кругом участников под эгидой Организации Объединенных Наций, а также регулярный диалог в рамках двусторонних, региональных и многосторонних форумов и других международных организаций.

V. Международное сообщество и помощь в сфере обеспечения безопасности ИКТ и наращивания потенциала

19. Государства несут главную ответственность за обеспечение государственной безопасности и безопасности своих граждан, в том числе в ИКТ-среде, однако некоторые государства могут не обладать достаточным потенциалом для защиты своих ИКТ-сетей. Отсутствие такого потенциала может сделать граждан и критически важную инфраструктуру государства уязвимыми или же превратить такое государство в невольное убежище для злоумышленников. Международное сообщество и помощь могут сыграть существенно важную роль в наращивании потенциала государств по обеспечению безопасности ИКТ и их мирного использования. Оказание помощи в деле наращивания потенциала в сфере обеспечения важности ИКТ также имеет существенно важное значение для международной безопасности, поскольку это позволяет расширять возможности государств для сотрудничества и принятия совместных мер. Группа пришла к единому мнению о том, что меры по наращиванию потенциала должны способствовать использованию ИКТ в мирных целях.

20. Группа одобрила рекомендации о наращивании потенциала, содержащиеся в докладах за 2010 и 2013 годы. В докладе за 2010 год государствам было рекомендовано определить меры по содействию наращиванию потенциала в менее развитых странах. В докладе за 2013 год к международному сообществу был обращен призыв принять совместные меры для оказания помощи в сфере повышения безопасности критически важной инфраструктуры ИКТ; развития технических навыков и разработки соответствующего законодательства, стратегий и нормативно-правовой базы, чтобы государства могли выполнять свои обязанности; преодоления разрыва в сфере обеспечения безопасности ИКТ и их использования. Группа этого созыва также особо отмечает, что деятельность по наращиванию потенциала выходит за рамки передачи знаний и информации о навыках от развитых государств развивающимся, поскольку все государства могут обмениваться информацией об угрозах, с которыми они сталкиваются, и эффективных мерах реагирования на такие угрозы.

21. Продолжая работу, начатую в предыдущих резолюциях и докладах Организации Объединенных Наций, в том числе в резолюции 64/211 Генеральной Ассамблеи, озаглавленной «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», государствам необходимо рассмотреть следующие добровольные меры по оказанию технической и иной помощи в целях наращивания потенциала обеспечения безопасности ИКТ в странах, нуждающихся в помощи, и обращающихся с просьбами об оказании такой помощи:

a) оказание помощи в деле укрепления механизмов взаимодействия с национальными группами экстренной готовности к компьютерным инцидентам и иным уполномоченным органам;

b) оказание помощи и обеспечение подготовки кадров для развивающихся стран в деле укрепления безопасности в сфере использования ИКТ, в том числе критически важной инфраструктуры, а также обмен информацией о передовой практике в правовой и административной сферах;

c) оказание помощи в обеспечении доступа к технологиям, которые считаются существенно важными для обеспечения безопасности ИКТ;

d) разработка процедур взаимопомощи в деле реагирования на инциденты и решения краткосрочных проблем в сфере обеспечения безопасности сетей, включая процедуры оказания оперативной помощи;

e) содействие трансграничному сотрудничеству в деле устранения трансграничных факторов уязвимости критически важной инфраструктуры;

f) разработка стратегий непрерывного принятия мер для наращивания потенциала в сфере обеспечения безопасности ИКТ;

g) уделение особого внимания распространению информации и наращиванию потенциала в сфере обеспечения безопасности ИКТ в национальных планах и государственных бюджетах, а также придание этому вопросу надлежащего значения в разработке планов в сфере развития и оказания помощи. Это может включать программы повышения осведомленности по вопросам обеспечения безопасности в сфере ИКТ, разработанные для обучения и информирования сотрудников соответствующих учреждений и отдельных граждан. Такие программы могли бы осуществляться в сочетании с усилиями международных организаций, включая Организацию Объединенных Наций и ее учреждения, частный сектор, научные круги и организации гражданского общества;

h) содействие продолжению деятельности по наращиванию потенциала, в частности в сфере проведения криминалистической экспертизы или принятия совместных мер по противодействию преступному или террористическому использованию ИКТ.

22. Представляется целесообразной разработка региональных подходов к деятельности по наращиванию потенциала, поскольку в них можно было бы учитывать конкретные культурные, географические, политические, экономические или социальные аспекты и обеспечивать учет конкретных потребностей.

23. В интересах наращивания потенциала в сфере обеспечения безопасности ИКТ государства могли бы рассмотреть вопрос о выдвижении инициатив по двустороннему и многостороннему сотрудничеству, которое бы основывалось на существующих партнерских отношениях. Такие инициативы могли бы способствовать улучшению условий для оказания эффективной взаимопомощи между государствами в их деятельности по реагированию на инциденты в сфере ИКТ и могли бы далее развиваться компетентными международными организациями, включая Организацию Объединенных Наций и ее учреждения, частный сектор, научные круги и организации гражданского общества.

VI. Применимость норм международного права к использованию ИКТ

24. В докладе за 2013 год указывается, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет существенно важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной ИКТ-среды. В соответствии со своим

мандатом Группа нынешнего созыва рассмотрела вопрос о применимости норм международного права к использованию ИКТ государствами.

25. Соблюдение государствами международного права, в частности их обязанностей по Уставу, является существенно важной основой, определяющей их действия в сфере использования ИКТ и создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Эти обязанности имеют важнейшее значение для рассмотрения вопроса о применимости норм международного права к использованию ИКТ государствами.

26. При рассмотрении вопроса о применимости норм международного права к использованию ИКТ государствами Группа определила, что важнейшее значение имеют обязанности государств в соответствии со следующими принципами Устава и другими нормами международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединенных Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств.

27. Суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

28. В дополнение к работе предыдущих групп, а также руководствуясь Уставом и мандатом, сформулированным в резолюции 68/243 Генеральной Ассамблеи, Группа нынешнего созыва предлагает следующие неисчерпывающие мнения в отношении применимости норм международного права к использованию ИКТ государствами:

a) государства обладают юрисдикцией над ИКТ-инфраструктурой, расположенной на их территориях;

b) в процессе использования ИКТ государства должны соблюдать, наряду с другими принципами международного права, такие принципы, как государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств. Существующие обязательства по международному праву применимы к использованию ИКТ государствами. Государства должны выполнять их обязательства по международному праву, касающиеся уважения и защиты прав человека и основных свобод;

c) особо отмечая стремление международного сообщества к мирному использованию ИКТ в интересах всеобщего блага человечества и напоминая о применимости Устава в полном объеме, Группа отмечает неотъемлемое право государств принимать меры, соответствующие международному праву и признанные в Уставе. Группа отмечает необходимость дальнейшего изучения этого вопроса;

d) Группа отмечает существующие принципы международного права, в том числе, в соответствующих случаях, принципы гуманности, необходимости, пропорциональности и индивидуализации;

e) государства не должны использовать представителей для совершения международно противоправных деяний с использованием ИКТ и должны стремиться обеспечивать, чтобы их территория не использовалась негосударственными субъектами для совершения таких деяний;

f) государства должны выполнять свои международные обязательства в отношении международно противоправных деяний, приписываемых им в соответствии с международным правом. Вместе с тем указание 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 недостаточным для присвоения этой деятельности указанному государству. Группа отмечает, что обвинение в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными.

29. Группа отмечает, что общее понимание применимости норм международного права к использованию ИКТ государствами имеет важное значение для содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

VII. Выводы и рекомендации в отношении дальнейшей работы

30. Удалось добиться существенных успехов в признании угроз международному миру и безопасности, проистекающих из злонамеренного использования ИКТ. Отметив, что ИКТ могут являться одним из факторов ускорения прогресса на пути развития, и осознавая необходимость сохранения глобальной взаимосвязанности и обеспечения беспрепятственного и надежного обмена информацией, Группа сочла целесообразным определить возможные меры для дальнейшей работы, включающие, в частности, следующее:

a) дальнейшее развитие государствами на совместное и индивидуальной основе концепций международного мира и безопасности в сфере использования ИКТ на правовом, техническом и политическом уровнях;

b) расширение сотрудничества на 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 критически важной инфраструктуры, зависящий от ИКТ.

31. Государства несут главную ответственность за поддержание безопасной и мирной ИКТ-среды, однако определение механизмов участия, сообразно обстоятельствам, частного сектора, научных кругов и организаций гражданского общества могло бы способствовать повышению эффективности международного сотрудничества.

32. В числе вопросов, которые можно было бы изучить более детально и основательно, можно назвать концепции, имеющие отношение к использованию ИКТ государствами. Обслуживающему все государства-члены Институту Ор-

ганизации Объединенных Наций по исследованию проблем разоружения, наряду с другими соответствующими аналитическими структурами и исследовательскими организациями, можно было бы предложить провести соответствующие исследования.

33. Организация Объединенных Наций должна играть лидирующую роль в деле содействия развитию диалога по вопросам безопасности ИКТ в их использовании государствами и выработке единого понимания в вопросах применимости международного права и норм, правил и принципов ответственного поведения. В рамках дальнейшей работы можно было бы рассмотреть инициативы в отношении проведения международного диалога и обмена информацией по вопросам безопасности ИКТ. Эти усилия не должны дублировать текущую работу других международных организаций и форумов, занимающихся такими вопросами, как преступное и террористическое использование ИКТ, права человека и регулирование Интернета.

34. Группа отметила важность рассмотрения в Генеральной Ассамблее вопроса о созыве новой Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2016 году, с тем чтобы продолжить в целях содействия выработке общего понимания исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также применимости международного права к использованию ИКТ государствами, включая нормы, правила или принципы ответственного поведения государств, меры укрепления доверия и наращивания потенциала.

35. Группа отмечает ценные усилия в сфере обеспечения безопасности ИКТ, прилагаемые международными организациями и региональными группами. Эти усилия необходимо учитывать в рамках межгосударственной деятельности по вопросам обеспечения безопасности в использовании ИКТ, и государства-члены должны, в соответствующих случаях, способствовать созданию новых двусторонних, региональных и многосторонних платформ для диалога, консультаций и наращивания потенциала.

36. Группа рекомендует государствам-членам внимательно изучить содержащиеся в настоящем докладе рекомендации о путях содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, а также проанализировать возможные пути доработки и осуществления этих рекомендаций.

Приложение

Список членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Беларусь

Александр Чесновский (третья и четвертая сессии)
Заместитель начальника Управления международной безопасности и контроля над вооружениями министерства иностранных дел

Посол Владимир Н. Герасимович (первая сессия)
Начальник Управления международной безопасности и контроля над вооружениями министерства иностранных дел

Иван Гриневич (вторая сессия)
Советник Постоянного представительства Беларуси при Отделении Организации Объединенных Наций в Женеве

Бразилия

Карлос Луис Дантас Кутинью Перес
Министр, начальник канцелярии заместителя министра по политическим вопросам министерства иностранных дел

Китай

Хайтао У (третья и четвертая сессии)
Координатор министерства иностранных дел по вопросам деятельности в киберпространстве

Цун Фу (первая и вторая сессии)
Координатор министерства иностранных дел по вопросам деятельности в киберпространстве

Колумбия

Хорхе Фернандо Бехарно
Директор Отдела по стандартам и архитектуре информационных технологий министерства информационных технологий и связи

Египет

Самех Абул-Энеин
Посол, заместитель помощника министра иностранных дел по вопросам разоружения, международной безопасности и мирного использования ядерной энергии министерства иностранных дел

Амр Алджовайли (третья сессия)
Посланник, Постоянное представительство Египта при Организации Объединенных Наций

Эстония

Марина Кальюранд
Вице-канцлер по юридическим вопросам министерства иностранных дел

Франция

Флоренс Манжин
Посол, координатор по вопросам кибербезопасности министерства иностранных дел

Леонар Роллан (первая сессия)
Департамент стратегических вопросов, безопасности и разоружения министерства иностранных дел

Германия

Карстен Гайер
Начальник Отдела по координации политики в киберпространстве министерства иностранных дел

Гана

Марк-Оливер Кевор
Член Совета директоров Национального управления коммуникаций

Израиль

Иддо Моед
Координатор по вопросам кибербезопасности министерства иностранных дел

Япония

Такаси Окада (третья и четвертая сессии)
Посол по делам Организации Объединенных Наций и посол по вопросам политики в сфере кибербезопасности, заместитель Генерального директора Бюро внешней политики министерства иностранных дел

Акира Коно (вторая сессия)
Посол по делам Организации Объединенных Наций и посол по вопросам кибербезопасности, заместитель Генерального директора Бюро внешней политики министерства иностранных дел

Такао Имафуку (первая сессия)
Старший представитель на переговорах по вопросам международной безопасности Бюро внешней политики министерства иностранных дел

Кения

Катрин Гетао
Секретарь по вопросам ИКТ министерства информации, связи и коммуникационных технологий

Малайзия

Нур Хайуна Абд Карим (четвертая сессия)
Первый помощник Секретаря Отдела по кибер- и космической безопасности Совета национальной безопасности

Мд Шах Нури бин Мд Заин (первая, вторая и третья сессии)
Заместитель Секретаря Отдела по кибер- и космической безопасности Совета национальной безопасности

Мексика

Эдгар Сурита
Атташе в Соединенных Штатах Америки и Канаде, Комиссия по национальной безопасности Мексики — федеральная полиция

Пакистан

Аусаф Али (первая, вторая и четвертая сессии)
Генеральный директор Технической группы Отдела стратегического планирования Генерального штаба

Халиль Хашими (третья сессия)
Посланник, Постоянное представительство Пакистана при Организации Объединенных Наций

Республика Корея

Чуль Ли (вторая и четвертая сессии)
Директор Отдела международной безопасности министерства иностранных дел

Хюнчеоль Янг (первая и третья сессии)
Советник посольства Республики Корея в Королевстве Бельгия и Европейском союзе

Российская Федерация

Андрей В. Крутских
Специальный представитель президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям

Испания

Рикардо Мор (четвертая сессия)
Посол по особым поручениям, ответственный за вопросы кибербезопасности министерства иностранных дел и сотрудничества

Алисия Мораль (первая, вторая и третья сессии)
Посол по особым поручениям, ответственный за вопросы кибербезопасности министерства иностранных дел и сотрудничества

Соединенное Королевство Великобритании и Северной Ирландии

Оливия Престон
Помощник директора Управления кибербезопасности и обеспечения сохранности информации, секретариат Кабинета министров

Соединенные Штаты Америки

Мишел Маркофф
Заместитель координатора по вопросам киберпространства, Канцелярия Государственного секретаря, государственный департамент Соединенных Штатов Америки