Организация Объединенных Наций A/75/816*

Генеральная Ассамблея

Distr.: General
18 March 2021
Russian
Original: English

Семьдесят пятая сессия
Пункт 98 повестки дня
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить членам Генеральной Ассамблеи доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, подготовленный во исполнение резолюции 73/27 и решения 75/550 Ассамблеи.

* Переиздано по техническим причинам 12 октября 2021 года.

21-03673* (R) 120421 120421

Просьба отправить на вторичную переработку

Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

I. Введение

1. В своей резолюции 73/27 Генеральная Ассамблея постановила созывать, начиная с 2019 года, рабочую группу открытого состава, действующую на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств и путей их реализации; при необходимости внесения в них изменений или формулирования дополнительных правил поведения; изучения возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций; а также продолжения в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению и того, как международное право применяется к использованию информационно-коммуникационных технологий государствами, а также мер укрепления доверия и наращивания потенциала и представления доклада о результатах данного исследования Ассамблее на ее семьдесят пятой сессии; и предусмотреть возможность проведения за счет добровольных взносов межсессионных консультационных встреч с заинтересованными сторонами, а именно бизнесом, неправительственными организациями и научным сообществом, для обмена взглядами по вопросам, входящим в мандат группы. Ассамблея постановила также, что рабочая группа должна провести свою организационную сессию в июне 2019 года для согласования организационных мер, связанных с рабочей группой.

2. В своем решении 75/550 Генеральная Ассамблея, отметив, что в связи с пандемией коронавирусного заболевания (COVID-19) третья и заключительная основная сессия, запланированная на 6–10 июля 2020 года, была отменена, постановила, что Рабочая группа открытого состава, продолжая свою работу в соответствии со своим мандатом согласно резолюции 73/27 Ассамблеи, созовет свою третью и заключительную основную сессию 8–12 марта 2021 года.

II. Организационные вопросы

A. Открытие и продолжительность сессий

3. Рабочая группа провела свою организационную сессию 3 июня 2019 года, свою первую основную сессию 9–13 сентября 2019 года, свою вторую основную сессию 10–14 февраля 2020 года и свою третью основную сессию 8–12 марта 2021 года в Центральных учреждениях.

4. Основную поддержку Рабочей группе оказывали Управление по вопросам разоружения и Институт Организации Объединенных Наций по исследованию проблем разоружения. Секретариатское обслуживание обеспечивал Департамент по делам Генеральной Ассамблеи и конференционному управлению.

B. Участники

5. Список участников основных сессий приводится в документах A/AC.290/2019/INF/1, A/AC.290/2020/INF/1 и A/AC.290/2021/INF/1.

C. Должностные лица

6. На своей организационной сессии 3 июня 2019 года Рабочая группа путем аккламации избрала Председателем Юэрга Лаубера (Швейцария).

D. Утверждение повестки дня

7. На той же сессии Рабочая группа утвердила повестку дня всех своих сессий, содержащуюся в документе A/AC.290/2019/1. Повестка дня включает следующие пункты:

1. Выборы должностных лиц.
2. Утверждение повестки дня.
3. Организация работы.
4. Общий обмен мнениями.
5. Обсуждение вопросов существа, указанных в пункте 5 резолюции 73/27 Генеральной Ассамблеи:
   a) продолжение дальнейшей выработки норм, правил и принципов ответственного поведения государств, перечисленных в пункте 1 резолюции 73/27 Генеральной Ассамблеи, и путей их реализации и при необходимости внесение в них изменений или формулирование дополнительных правил поведения;
   b) изучение возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций;
   c) продолжение в целях выработки общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению;
   d) применимость международного права к использованию информационно-коммуникационных технологий государствами;
   e) меры укрепления доверия;
   f) наращивание потенциала и концепции, упомянутые в пункте 3 резолюции 73/27 Генеральной Ассамблеи.
6. Прочие вопросы.
7. Утверждение заключительного доклада.

8. Кроме того, на той же сессии Рабочая группа постановила проводить свою работу в соответствии с правилами процедуры главных комитетов Генеральной Ассамблеи, действуя при этом на основе консенсуса в соответствии с резолюцией 73/27 Ассамблеи. Группа постановила также, что в соответствии с

правилами процедуры и практикой Ассамблеи все государства-члены имеют право быть представленными в Группе. Государства, не являющиеся членами Организации Объединенных Наций, межправительственные организации и структуры, которым Ассамблея предоставила статус наблюдателя, получили постоянное приглашение участвовать в сессиях и работе Группы в качестве наблюдателей. Соответствующие подразделения системы Организации Объединенных Наций будут также приглашаться к участию исключительно в целях получения информации технического характера. Кроме того, соответствующие неправительственные организации, имеющие консультативный статус при Экономическом и Социальном Совете, согласно резолюции 1996/31 должны уведомлять секретариат Группы о своем желании принять участие в ее работе. Другие заинтересованные неправительственные организации, имеющие отношение к сфере деятельности и целям Группы и обладающие компетентностью в этой области, должны также сообщать секретариату Группы о своей заинтересованности, и, соответственно, им будет предложено принять участие в работе Группы в качестве наблюдателей на основе процедуры отсутствия возражений.

E. Организация работы

9. На первых заседаниях каждой из основных сессий, которые состоялись, соответственно, 9 сентября 2019 года, 10 февраля 2020 года и 8 марта 2021 года, Рабочая группа согласовывала порядок организации своей работы, содержащийся в документах A/AC.290/2019/2, A/AC.290/2020/1 и A/AC.290/2021/1.

F. Документация

10. С полным перечнем всех официальных документов, рабочих документов, технических документов и других документов, имеющихся в распоряжении Рабочей группы, можно ознакомиться на следующем специальном веб-сайте: www.un.org/disarmament/open-ended-working-group/.

G. Деятельность Рабочей группы

11. На своей первой основной сессии в ходе девяти пленарных заседаний Рабочая группа рассмотрела пункты 3–5 повестки дня.

12. На своей второй основной сессии в ходе девяти пленарных заседаний Рабочая группа продолжила рассмотрение пункта 5 повестки дня.

13. На своей третьей основной сессии Рабочая группа рассмотрела пункты 5–7 повестки дня.

14. С тем чтобы продолжить свою работу по время пандемии коронавирусного заболевания (COVID-19) Рабочая группа провела неофициальные виртуальные заседания 15, 17 и 19 июня и 2 июля 2020 года; 29 сентября — 1 октября 2020 года; 17–19 ноября 2020 года; 1–3 декабря 2020 года и 18, 19 и 22 февраля 2021 года.

15. В период со 2 по 4 декабря 2019 года Рабочая группа провела неофициальное межсессионное консультативное совещание с участием многих заинтересованных сторон. По просьбе Председателя Группы на этом совещании

председательствовал директор Агентства кибербезопасности Сингапура Дэвид Ко, и подготовленное им резюме работы было представлено и разослано членам Группы[1].

III. Утверждение доклада

16. На своей третьей основной сессии 12 марта 2021 года Рабочая группа рассмотрела пункт 7 повестки дня, озаглавленный «Утверждение доклада», и утвердила свой доклад, содержащийся в документе A/AC.290/2021/L.1 с внесенными в него устными исправлениями и в документе A/AC.290/2021/CRP.2.

17. Поскольку из-за ограничений, введенных в Центральных учреждениях Организации Объединенных Наций в связи с пандемией COVID-19, число заседаний Рабочей группы на ее третьей основной сессии было сокращено, подборка заявлений с разъяснением позиций будет издана в качестве документа A/AC.290/2021/INF.2.

[1] URL: www.un.org/disarmament/open-ended-working-group/.

Приложение I*

Окончательный предметный доклад

A. Введение

1. Несмотря на то, что со времени создания Организации Объединенных Наций 75 лет назад в мире произошли радикальные преобразования, цель ее деятельности и ее идеалы, не утратившие своей актуальности, сохраняют свое основополагающее значение. Помимо подтверждения своей приверженности фундаментальным правам человека и содействию улучшению экономического и социального положения всех людей и созданию условий для установления справедливости и соблюдения международного права государства заявили о решимости объединить свои силы для поддержания международного мира и безопасности[2].

2. Развитие информационно-коммуникационных технологий (ИКТ) затрагивает все три основные направления деятельности Организации Объединенных Наций: мир и безопасность, права человека и устойчивое развитие. Способствуя общественным и экономическим преобразованиям и расширяя возможности для сотрудничества, ИКТ и глобальная связь играют роль катализатора прогресса и развития человека.

3. Сегодня как никогда очевидна насущная необходимость установления и поддержания международного мира, безопасности, сотрудничества и доверия в сфере ИКТ. Негативные тенденции в сфере цифровых технологий могут подорвать международную безопасность и стабильность, негативно сказаться на экономическом росте и устойчивом развитии и помешать полному осуществлению прав человека и основных свобод. Речь идет о все более широком применении ИКТ со злым умыслом.

4. Текущий общемировой кризис в области здравоохранения наглядно показывает фундаментальные преимущества ИКТ и нашу зависимость от них, в том числе в плане предоставления жизненно важных государственных услуг, распространения важной информации по вопросам общественной безопасности, разработки новаторских решений для повышения устойчивости функционирования, ускорения исследований и содействия обеспечению непрерывности образования и социальной сплоченности с помощью средств виртуализации. В нынешних условиях неопределенности государства, а также частный сектор, ученые и другие субъекты используют цифровые технологии, с тем чтобы поддерживать связь между отдельными лицами и целыми сообществами и оказывать им услуги здравоохранения. В то же время пандемия коронавирусного заболевания (COVID-19) наглядно показала риски и последствия вредоносной деятельности, направленной на использование факторов уязвимости в то время, когда общество переживает тяжкие испытания. Она также подчеркнула необходимость преодоления цифрового разрыва, повышения устойчивости всех сообществ и секторов к потрясениям и неизменного применения подхода, ориентированного на интересы людей.

5. Поскольку ИКТ могут использоваться в целях, несовместимых с задачами поддержания международного мира, стабильности и безопасности, Генеральная

* Публикуется без официального редактирования.

[2] Преамбула Устава Организации Объединенных Наций.

Ассамблея отметила[3], что распространение и использование ИКТ затрагивают интересы всего мирового сообщества и что широкое международное взаимодействие способствует принятию наиболее действенных ответных мер.

6. В свете вышеизложенного создание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС) согласно резолюции 73/27 Генеральной Ассамблеи дало возможность добиться подвижек в рассмотрении этого важнейшего вопроса. Группа предоставила всем государствам демократичную, транспарентную и инклюзивную площадку для выражения их мнений и расширения сотрудничества в вопросах, касающихся ИКТ в контексте международной безопасности. Активное участие государств — членов Организации Объединенных Наций и вовлеченность целого ряда других соответствующих заинтересованных сторон свидетельствуют об общем стремлении и коллективной заинтересованности международного сообщества создать мирную и безопасную для всех ИКТ-среду и об их решимости сотрудничать в достижении этой цели.

7. Создание РГОС стало важной вехой в процессе международного сотрудничества на пути к обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Для изучения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению после 2003 года шесть раз создавались группы правительственных экспертов[4]. В трех принятых на основе консенсуса докладах (от 2010, 2013 и 2015 годов[5]), которые носят обобщающий характер, эти группы вынесли рекомендации в отношении 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств и констатировали, что со временем могут быть разработаны дополнительные нормы. Кроме того, в них содержались рекомендации в отношении конкретных мер в области укрепления доверия, создания потенциала и сотрудничества. В них также было подтверждено, что международное право, в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира, безопасности и стабильности в ИКТ-среде. В резолюции 70/237 Генеральной Ассамблеи государства-члены единогласно приняли решение при использовании ИКТ руководствоваться докладом группы правительственных экспертов 2015 года, тем самым закрепив первоначальные принципы ответственного поведения государств в области использования ИКТ. В этой связи РГОС приняла также к сведению резолюции 73/27 и 73/266 Генеральной Ассамблеи.

8. Опираясь на эти основополагающие принципы и подтверждая эту основу, РГОС стремится найти точки соприкосновения и взаимопонимания между всеми государствами — членами Организации Объединенных Наций по вопросу общемировой значимости. Для изучения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению РГОС в соответствии со своим мандатом рассмотрела вопросы, касающиеся дальнейшего развития норм, правил и принципов ответственного поведения государств, применимости норм международного права к использованию ИКТ государствами, мер укрепления доверия, укрепления потенциала и возможности организации регулярного институционального диалога с широким кругом участников под эгидой Организации Объединенных Наций. В своих усилиях по достижению консенсуса и содействию международному миру,

[3] См., например, шестой пункт преамбулы резолюции 53/70 Генеральной Ассамблеи.
[4] Резолюции 58/32, 60/45, 66/24, 68/243, 70/237 и 73/266 Генеральной Ассамблеи.
[5] A/65/201, A/68/98 и A/70/174.

безопасности, сотрудничеству и доверию РГОС руководствовалась принципами инклюзивности и транспарентности.

9. Организации Объединенных Наций следует и далее играть ведущую роль в содействии диалогу по вопросам использования государствами ИКТ. РГОС учитывает важность и взаимодополняющий характер специализированных обсуждений аспектов цифровых технологий в рамках других органов и форумов Организации Объединенных.

10. Главную ответственность за поддержание международного мира и безопасности несут государства, однако использовать ИКТ таким образом, чтобы не создавать угрозу миру и безопасности, обязаны все заинтересованные стороны. Поскольку во многих областях и дисциплинах проблема международной безопасности является сквозным аспектом ИКТ, ценным подспорьем для РГОС оказались опыт и знания, которыми поделились представители межправительственных организаций, региональных организаций, гражданского общества, частного сектора, научных кругов и технического сообщества. Трехдневное неофициальное консультативное совещание РГОС, состоявшееся в декабре 2019 года, позволило провести плодотворное обсуждение с участием государств и широкого круга других заинтересованных сторон[6]. Кроме того, в письменных материалах и в ходе неофициальных консультаций с РГОС эти заинтересованные стороны представили конкретные предложения и примеры передовой практики. Некоторые делегации по собственной инициативе также провели консультации с участием многих заинтересованных сторон, с тем чтобы отразить их мнения в материалах, которые они представили Рабочей группе открытого состава.

11. С учетом различий в условиях, возможностях и приоритетах государств и регионов РГОС констатирует, что распределение выгод, связанных с цифровыми технологиями, не является равномерным и что насущной задачей международного сообщества остается сокращение цифрового разрыва, в том числе за счет обеспечения всеобщего, инклюзивного и недискриминационного доступа к ИКТ и возможностей подключения к сети.

12. РГОС с удовлетворением отмечает высокий уровень участия женщин-делегатов в работе ее совещаний и то большое внимание, которое уделяется в ее обсуждениях гендерным аспектам. РГОС подчеркивает важность сокращения гендерного цифрового разрыва и содействия действенному и значимому участию и лидерству женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

13. РГОС подчеркивает, что отдельные элементы ее мандата связаны между собой и взаимно подкрепляют друг друга и в своей совокупности способствуют созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

B. Выводы и рекомендации

14. Рассмотрев основные аспекты мандата РГОС и напомнив, что в резолюции 73/27 Генеральной Ассамблеи особо отмечалась эффективная работа, выполненная в 2010, 2013 и 2015 годах Группой правительственных экспертов по

[6] См. “Chair’s Summary of the Informal intersessional consultative meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security”, URL: https://www.un.org/disarmament/open-ended-working-group/.

достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, и подготовленные в итоге соответствующие доклады, препровожденные Генеральным секретарем[7], государства пришли к следующим выводам и рекомендациям, которые включают конкретные действия и совместные меры по противодействию связанным с использованием ИКТ угрозам и содействию созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Существующие и потенциальные угрозы

15. По общему признанию государств, все большее беспокойство вызывают последствия использования ИКТ со злым умыслом для поддержания международного мира и, следовательно, для прав человека и развития. В частности, была выражена обеспокоенность по поводу расширения возможностей ИКТ, которые могут быть использованы для подрыва международного мира и безопасности. Вредоносные происшествия в сфере ИКТ становятся все более частыми и изощренными и постоянно эволюционируют и видоизменяются. Расширение коммуникационных возможностей и зависимости от ИКТ в отсутствие сопутствующих мер по обеспечению безопасности ИКТ может породить непреднамеренные риски, сделав общество более уязвимым для действующих в сфере ИКТ злоумышленников. Несмотря на неоценимую выгоду ИКТ для человечества, их использование со злым умыслом может иметь значительные и масштабные негативные последствия.

16. Государства напомнили, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей. Они напомнили также, что применение ИКТ в будущих конфликтах между государствами становится все более вероятным. Продолжающееся увеличение числа инцидентов, связанных со злонамеренным использованием ИКТ государственными и негосударственными субъектами, включая террористов и преступные группы, является тревожной тенденцией. Некоторые негосударственные субъекты продемонстрировали, что они располагают такими возможностями использования ИКТ, которые ранее были доступны только государствам.

17. Государства также пришли к выводу о том, что любое использование ИКТ государствами таким образом, который противоречит их обязательствам в рамках существующей системы, включающей добровольные нормы, международное право и меры укрепления доверия, подрывает международный мир и безопасность, доверие и стабильность в отношениях между государствами и может повысить вероятность возникновения в будущем межгосударственных конфликтов.

18. Государства пришли к выводу о том, что вредоносная деятельность в сфере ИКТ может иметь разрушительные последствия для безопасности, а также разрушительные экономические, социальные и гуманитарные последствия для критически важной инфраструктуры и критически важной информационной инфраструктуры, обеспечивающей оказание основных услуг населению. Хотя определение того, какие объекты инфраструктуры считаются критически важными, является прерогативой каждого отдельного государства, к таким объектам инфраструктуры могут относиться медицинские учреждения, финансовые службы, объекты энергетики и водоснабжения, транспорт и санитарные объекты.

[7] A/65/201, A/68/98 и A/70/174.

Реальную и растущую озабоченность вызывают злонамеренные действия с использованием ИКТ, направленные против объектов критически важной инфраструктуры и объектов критически важной информационной инфраструктуры и имеющие целью подрыв доверия к политическим и избирательным процессам и государственным институтам или ограничение общедоступности и надежности Интернета. Такие объекты инфраструктуры могут находиться в собственности, под управлением или в эксплуатации частного сектора, предоставляться в пользование другому государству или быть частью сети с участием другого государства или совместно эксплуатироваться несколькими государствами. Вследствие этого для поддержания их целостности, функционирования и доступности может потребоваться межгосударственное сотрудничество или сотрудничество государства и частного сектора.

19. Государства пришли также к выводу о том, что деятельность в сфере ИКТ, противоречащая обязательствам по международному праву и наносящая преднамеренный ущерб критически важной инфраструктуре или иным образом препятствующая использованию и функционированию критически важной инфраструктуры для обслуживания населения, может представлять угрозу не только безопасности, но и государственному суверенитету, а также экономическому развитию и источникам средств к существованию и, в конечном счете, безопасности и благополучию людей.

20. Поскольку все государства во все большей степени полагаются на цифровые технологии, государства пришли к выводу о том, что отсутствие осведомленности и надлежащих возможностей для выявления злоумышленных действий с использованием ИКТ, может сделать их более уязвимыми. Как наглядно показала нынешняя чрезвычайная ситуация в области здравоохранения в мире, во время кризиса действие существующих факторов уязвимости может многократно усилиться.

21. Государства пришли к выводу о том, что в зависимости от уровня цифровизации, имеющихся возможностей, а также безопасности и надежности, наличия инфраструктуры и уровня развития ИКТ государства могут воспринимать угрозы по-разному. Кроме того, угрозы могут по-разному воздействовать на различные группы и различных субъектов, включая молодежь, пожилых людей, женщин и мужчин, уязвимые группы населения, представителей отдельных профессий, малые и средние предприятия и т. д.

22. Учитывая все более тревожную обстановку в плане цифровых угроз и принимая во внимание, что от этих угроз не защищено ни одно государство, государства особо подчеркнули, что необходимо в срочном порядке применять совместные меры по борьбе с такими угрозами и продолжать разработку таких мер. Было подтверждено, что осуществление, когда это целесообразно, совместных и всеохватных действий может оказаться более результативным и дать более масштабные результаты. В этой связи была также подчеркнута ценность дальнейшего укрепления сотрудничества соответственно с гражданским обществом, частным сектором, научными кругами и техническим сообществом.

23. Государства особо подчеркнули положительные экономические и социальные возможности, которые могут быть получены благодаря ИКТ, и отметили, что обеспокоенность вызывают не сами технологии, а их ненадлежащее использование.

Правила, нормы и принципы ответственного поведения государств

24. Добровольные, не имеющие обязательной силы нормы ответственного поведения государств могут уменьшить риски для международного мира, безопасности и стабильности и могут играть важную роль в повышении предсказуемости и уменьшении риска неправильного восприятия, способствуя тем самым предотвращению конфликтов. Государства подчеркнули, что такие нормы отражают ожидания и стандарты международного сообщества в отношении поведения государств при использовании ими ИКТ и позволяют международному сообществу оценивать действия государств. Согласно положениям резолюции 70/237 Генеральной Ассамблеи и сообразно резолюции 73/27 Генеральной Ассамблеи к государствам был обращен призыв отказываться и воздерживаться от таких видов применения ИКТ, которые не соответствуют нормам ответственного поведения государств.

25. Государства подтвердили, что нормы не заменяют собой обязательства или права государств по международному праву, которые носят обязательный характер, и не изменяют их, а скорее содержат дополнительные конкретные указания в отношении того, что представляет собой ответственное поведение государства при использовании ИКТ. Нормы не направлены на ограничение или запрещение действий, которые не противоречат международному праву.

26. Согласившись с необходимостью защищать объекты критически важной инфраструктуры и объекты критически важной информационной инфраструктуры, обеспечивающие оказание основных услуг населению, а также с необходимостью обеспечения общедоступности и надежности Интернета, государства пришли также к выводу о том, что пандемия COVID-19 подтвердила важность защиты инфраструктуры систем здравоохранения, включая медицинские службы и объекты, посредством исполнения норм, касающихся объектов критически важной инфраструктуры, например таких норм, которые были утверждены на основе консенсуса в резолюции 70/237 Генеральной Ассамблеи Организации Объединенных Наций.

27. Государства подтвердили, что важно поддерживать и продолжать усилия по осуществлению на глобальном, региональном и национальном уровнях норм, с применением которых согласились государства.

28. Подтверждая резолюцию 70/237 Генеральной Ассамблеи и признавая резолюцию 73/27 Генеральной Ассамблеи, государства должны принимать разумные меры для обеспечения целостности каналов поставки, в том числе посредством разработки объективных коллективных мер, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ; должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций; и должны способствовать ответственному представлению информации о факторах уязвимости.

29. Государства подтвердили, что, принимая во внимание уникальные особенности ИКТ и учитывая представленные в рамках РГОС предложения в отношении норм, постепенную разработку дополнительных норм можно было бы продолжить. Государства также пришли к выводу о том, что дальнейшее развитие норм и применение существующих норм не являются взаимоисключающими, а могут происходить одновременно.

Рекомендации Рабочей группы открытого состава

30. Государствам следует добровольно анализировать национальные усилия по применению норм, накапливать опыт и передовую практику в части применения норм и обмениваться ими, а также продолжать информировать Генерального секретаря о своих национальных обзорах и оценках в этой связи.

31. 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. Кроме того, государствам следует продолжать укреплять меры по защите всей критически важной инфраструктуры от угроз, связанных с использованием ИКТ, и расширять обмен передовым опытом в области защиты критически важной инфраструктуры.

32. Государствам следует, действуя в партнерстве с соответствующими организациями, включая Организацию Объединенных Наций, продолжать содействовать внедрению и разработке норм ответственного государственного поведения. Следует призывать государства, которые в состоянии предоставить специалистов или ресурсы, делать это.

33. Ссылаясь на резолюцию 70/237 Генеральной Ассамблеи и подтверждая резолюцию 73/27 Генеральной Ассамблеи, государствам следует принять к сведению предложения, сделанные государствами относительно разработки правил, норм и принципов ответственного поведения государств в ходе будущих обсуждений в рамках Организации Объединенных Наций вопросов, касающихся ИКТ, и учесть, что резолюцией 75/240 Генеральной Ассамблеи была учреждена Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Международное право

34. Ссылаясь на резолюцию 70/237 Генеральной Ассамблеи и отмечая резолюцию 73/27 Генеральной Ассамблеи, согласно которой была учреждена РГОС, государства подтвердили, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. В этой связи к государствам был обращен призыв отказываться и воздерживаться от принятия каких бы то ни было мер, противоречащих международному праву, в частности Уставу Организации Объединенных Наций. Государства пришли также к выводу о том, что необходимо продолжить работу над углублением общего понимания применимости международного права к использованию ИКТ государствами.

35. Государства также подтвердили, что государствам следует стремиться урегулировать споры мирными средствами, в том числе путем переговоров, проведения расследований, посредничества, примирения, арбитража, судебного разбирательства и обращения к региональным учреждениям или механизмам, либо иными мирными средствами по их выбору.

36. Государства пришли к выводу о том, что, с учетом уникальных особенностей ИКТ-среды, улучшения общего понимания применимости международного

права к использованию ИКТ можно достичь благодаря обмену мнениями по этому вопросу между государствами и благодаря определению конкретных вопросов международного права для дальнейшего углубленного обсуждения в рамках Организации Объединенных Наций.

37. С тем чтобы улучшить понимание всеми государствами вопросов применимости международного права к использованию ИКТ государствами и содействовать формированию консенсуса и общего понимания в международном сообществе, необходимо, по общему мнению государств, предпринять, руководствуясь соображениями непредвзятости и объективности, дополнительные усилия по созданию потенциала в области международного права, национального законодательства и политики.

Рекомендации Рабочей группы открытого состава

38. Государствам следует продолжать добровольно информировать Генерального секретаря о национальных взглядах и оценках в отношении применимости международного права к использованию ими ИКТ в контексте международной безопасности и продолжать на добровольной основе обмениваться такими национальными взглядами и практикой по другим соответствующим каналам.

39. Государствам, которые имеют такую возможность, следует продолжать, руководствуясь соображениями непредвзятости и объективности и действуя в соответствии с принципами, содержащимися в пункте 56 настоящего доклада, поддерживать дополнительные усилия по созданию потенциала в области международного права, национального законодательства и политики, с тем чтобы все государства могли способствовать достижению общего понимания вопросов применимости международного права к использованию ИКТ государствами и содействовать достижению консенсуса в международном сообществе.

40. Государствам следует продолжать изучать и обсуждать в структуре будущих процессов в рамках Организации Объединенных Наций вопросы применимости международного права к использованию ИКТ государствами в качестве одного из важных шагов по уточнению и дальнейшему углублению общего понимания этого вопроса.

Меры укрепления доверия

41. Меры укрепления доверия, которые включают в себя меры обеспечения прозрачности, развития сотрудничества и повышения стабильности, могут способствовать предотвращению конфликтов, предупреждать случаи неправильного восприятия и недопонимания, а также могут использоваться для снижения напряженности. Они представляют собой одно из конкретных проявлений международного сотрудничества. При наличии необходимых ресурсов, возможностей и совместных усилий меры укрепления доверия могут способствовать укреплению общей безопасности, повышению устойчивости к потрясениям и использованию ИКТ в мирных целях. Кроме того, меры укрепления доверия могут способствовать практическому применению норм ответственного поведения государств, поскольку они способствуют укреплению доверия и повышению ясности, предсказуемости и стабильности в использовании ИКТ государствами. В сочетании с другими составляющими принципов ответственного поведения государств меры укрепления доверия могут также способствовать достижению

общего понимания между государствами, способствуя тем самым созданию более мирной международной обстановки.

42. Поскольку меры укрепления доверия представляют собой добровольные обязательства, которые выполняются постепенно, они могут стать первым шагом к устранению между государствами недоверия, вытекающего из недопонимания, путем налаживания связей, наведения мостов и развития сотрудничества для достижения общей цели, представляющей взаимный интерес. Тем самым меры укрепления доверия могут способствовать формированию основы для заключения расширенных, дополнительных договоренностей и соглашений в будущем.

43. Государства пришли к выводу о том, что диалог в рамках РГОС сам по себе является мерой укрепления доверия, поскольку он стимулирует открытый и прозрачный обмен мнениями относительно восприятия угроз и факторов уязвимости, ответственного поведения государств и других субъектов, а также передовой практики, способствуя в конечном счете коллективной разработке и применению принципов ответственного поведения государств при использовании ИКТ.

44. Кроме того, государства пришли к выводу о том, что Организация Объединенных Наций играет решающую роль в разработке и поддержке реализации мер укрепления доверия на общемировом уровне. В каждом из принятых консенсусом докладов групп правительственных экспертов содержались рекомендации в отношении практических мер укрепления доверия. В дополнение к этим конкретным рекомендациям по ИКТ Генеральная Ассамблея в принятой консенсусом резолюции 43/78 H одобрила Руководящие принципы для мер укрепления доверия, разработанные в рамках Комиссии Организации Объединенных Наций по разоружению, в которых изложены ценные принципы, цели и характеристики мер укрепления доверия, которые могут учитываться при разработке новых мер применительно к ИКТ.

45. Государства пришли к выводу о том, что региональные и субрегиональные организации, используя имеющееся у них в активе доверие и налаженные связи, прилагают значительные усилия для разработки мер укрепления доверия с учетом их конкретных условий и приоритетов, тем самым повышая осведомленность и способствуя распространению информации среди своих членов. Кроме того, региональные, межрегиональные и межорганизационные обмены могут способствовать созданию новых возможностей для сотрудничества, взаимодействия и взаимного обучения. Было отмечено, что, так как не все государства являются членами той или иной региональной организации и не все региональные организации разработали меры укрепления доверия, такие меры дополняют работу Организации Объединенных Наций и других организаций по продвижению мер укрепления доверия.

46. На основе обмена информацией об уроках и практике, который состоялся в рамках РГОС, государства пришли к общему мнению о том, что для обеспечения того, чтобы меры укрепления доверия выполнили свое предназначение, необходимо существование уже функционирующих национальных и региональных механизмов и структур, а также создание адекватных ресурсов и возможностей, таких как национальные группы реагирования на компьютерные происшествия.

47. Государства пришли к выводу о том, что такая конкретная мера, как создание национальных контактных центров, является не только самостоятельной

мерой укрепления доверия, но и полезным средством для принятия многих других мер укрепления доверия и имеет неоценимое значение в условиях кризиса. Государства могут счесть целесообразным создание контактных центров, в частности, для координации по дипломатическим, политическим, правовым и техническим вопросам, а также для уведомления об инцидентах и реагирования на них.

Рекомендации Рабочей группы открытого состава

48. Государствам следует продолжать добровольно информировать Генерального секретаря о своих взглядах и оценках и представлять дополнительную информацию об извлеченных уроках и передовой практике в отношении соответствующих мер укрепления доверия на двустороннем, региональном или многостороннем уровне.

49. Государствам следует добровольно определять меры укрепления доверия и рассматривать возможность их принятия с учетом их конкретных обстоятельств, а также сотрудничать с другими государствами в принятии таких мер.

50. Государствам следует добровольно принимать меры обеспечения прозрачности посредством распространения соответствующей информации и сделанных выводов в подходящей форме и на соответствующих форумах, в том числе на портале по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения.

51. Государствам, которые еще не сделали этого, следует, учитывая различия в возможностях, рассмотреть вопрос о создании национальных контактных центров, в частности, на техническом, политическом и дипломатическом уровнях. Государствам следует также продолжать рассматривать способы создания справочника таких контактных центров на глобальном уровне.

52. Государствам следует изучить механизмы регулярного межрегионального обмена опытом и передовой практикой в области мер укрепления доверия, принимая во внимание различия в региональных условиях и структурах соответствующих организаций.

53. Государствам следует продолжать рассматривать вопрос о мерах укрепления доверия на двустороннем, региональном и многостороннем уровнях и способствовать созданию возможностей для совместного принятия мер укрепления доверия.

Укрепление потенциала

54. Способность международного сообщества предотвращать вредоносную деятельность в области ИКТ или смягчать ее последствия зависит от возможностей каждого государства в плане обеспечения готовности и реагирования. Это особенно важно для развивающихся государств и необходимо для того, чтобы содействовать их полноценному участию в обсуждении вопросов ИКТ в контексте международной безопасности и обеспечить их способность устранять факторы уязвимости в критически важной инфраструктуре. Укрепление потенциала способствует развитию навыков, людских ресурсов, политики и институтов, повышающих устойчивость государств к потрясениям и их безопасность, с тем чтобы они могли в полной мере пользоваться благами цифровых технологий. Оно играет важную вспомогательную роль, выступая стимулом для соблюдения

норм международного права и реализации норм ответственного поведения государств, а также для поддержки принятия мер укрепления доверия. В мире, где существует цифровая взаимозависимость, выгоды от укрепления потенциала не ограничиваются первоначальными получателями, а способствуют созданию более безопасной и стабильной ИКТ-среды для всех.

55. Обеспечение открытой, безопасной, стабильной, доступной и мирной ИКТ-среды требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Укрепление потенциала является важным аспектом такого сотрудничества и осуществляется в добровольном порядке как передающей, так и получающей стороной.

56. Принимая во внимание широко признанные принципы и необходимость их дальнейшей проработки, государства пришли к выводу, что деятельность по укреплению потенциала в области использования ИКТ государствами в контексте международной безопасности должна осуществляться на основе перечисленных ниже принципов.

Сфера действия и предназначение

- Процесс укрепления потенциала должен носить поступательный характер и включать в себя конкретные мероприятия, проводимые различными субъектами и в интересах этих субъектов.

- Конкретные мероприятия должны иметь четкую цель и практическую ориентацию, способствуя при этом достижению общей цели создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

- Деятельность по укреплению потенциала должна быть научно обоснованной, нейтральной в политическом плане, прозрачной, подотчетной и носить необусловленный характер.

- Деятельность по укреплению потенциала должна осуществляться при полном соблюдении принципа государственного суверенитета.

- Для этого, возможно, потребуется облегчить доступ к соответствующим технологиям.

Партнерские отношения

- Деятельность по укреплению потенциала должна быть основана на взаимном доверии, определяться спросом, соответствовать национальным потребностям и приоритетам и должна осуществляться при полном признании принципа национальной ответственности. Участие партнеров в деятельности по укреплению потенциала носит добровольный характер.

- Поскольку деятельность по укреплению потенциала должна осуществляться с учетом конкретных потребностей и условий, все стороны являются активными партнерами, несущими общую, но дифференцированную ответственность, в том числе в отношении сотрудничества в разработке, осуществлении и мониторинге и оценке мероприятий по укреплению потенциала.

- Все партнеры обязаны обеспечивать и соблюдать конфиденциальный характер национальной политики и планов.

Интересы людей

• В основе деятельности по укреплению потенциала, которая должна носить всеохватный, универсальный и недискриминационный характер, должны лежать уважение прав человека и основных свобод и учет гендерных аспектов.

• Должна обеспечиваться конфиденциальность информации частного характера.

57. Государства пришли к выводу, что деятельность по укреплению потенциала представляет собой своего рода улицу с двусторонним движением, где участники прилагают совместные усилия и учатся друг у друга, а все стороны извлекают пользу из общего улучшения положения дел с безопасностью в сфере ИКТ во всем мире. Была также упомянута ценность сотрудничества Юг — Юг, Юг — Север, трехстороннего сотрудничества и сотрудничества региональной направленности.

58. Государства пришли к выводу о том, что укрепление потенциала должно способствовать превращению «цифровой пропасти» в цифровые возможности. В частности, наращивание потенциала должно быть ориентировано на содействие реальному участию развивающихся стран в соответствующих дискуссиях и форумах и на повышение устойчивости развивающихся стран в ИКТ-среде.

59. Государства пришли к выводу о том, что укрепление потенциала может способствовать пониманию и устранению системных и других рисков, обусловленных отсутствием безопасности в сфере ИКТ, недостаточно тесной увязкой технических и директивных возможностей на национальном уровне и сопутствующими проблемами неравенства и цифрового разрыва. Было сочтено, что особо важное значение имеет деятельность по укреплению потенциала, которая позволяет государствам выявлять и защищать объекты национальной критически важной инфраструктуры и обеспечивать совместную защиту критически важной информационной инфраструктуры. Наращивание потенциала может также помочь государствам углубить понимание по вопросу о применимости международного права. Повышению эффективности деятельности по укреплению потенциала, приданию ей более стратегического характера и более тесной ее увязке с национальными приоритетами могут способствовать обмен информацией и координация на национальном, региональном и международном уровнях.

60. Государства пришли к выводу о том, что в дополнение к техническим навыкам, институциональному строительству и механизмам сотрудничества крайне необходимо накапливать экспертные знания в целом ряде областей дипломатии, права, политики, законодательства и нормативного регулирования. В этой связи была подчеркнута важность укрепления дипломатического потенциала для участия в международных и межправительственных процессах.

61. Государства напомнили о том, что в связи с укреплением потенциала необходимо применять конкретный и ориентированный на действия подход. Государства пришли к выводу о том, что такие конкретные меры могли бы предусматривать поддержку как на уровне политики, так и на техническом уровне и охватывать, например, разработку национальных стратегий кибербезопасности, предоставление доступа к соответствующим технологиям, оказание поддержки группам реагирования на компьютерные происшествия или группам по расследованию происшествий в области кибербезопасности, а также разработку специализированных программ обучения и специальных учебных планов, включая

программы подготовки инструкторов и профессиональную сертификацию. Были признаны преимущества создания платформ для обмена информацией, включая передовую юридическую и административную практику, а также ценный вклад других соответствующих заинтересованных сторон в деятельность по наращиванию потенциала.

62. Государства пришли к выводу о том, что подведение итогов работы, проделанной государствами в связи с выводами и рекомендациями, содержащимися в данном докладе, а также в связи с оценками и рекомендациями, которым государства-члены согласились следовать, приняв на основе консенсуса резолюцию 70/237, является ценным мероприятием для оценки прогресса и определения сфер, в которых требуется дальнейшее наращивание потенциала.

Рекомендации Рабочей группы открытого состава

63. Государствам следует руководствоваться принципами, изложенными в пункте 56, в своей связанной с ИКТ работе по укреплению потенциала в сфере международной безопасности, а другим субъектам рекомендуется учитывать эти принципы в осуществляемой ими деятельности по укреплению потенциала.

64. Государствам следует продолжать добровольно информировать Генерального секретаря о своих взглядах и оценках относительно достижений в области ИКТ в контексте международной безопасности и включать дополнительную информацию об извлеченных уроках и передовой практике в отношении программ и инициатив по укреплению потенциала.

65. Государствам следует добровольно использовать типовое обследование «Обзор хода осуществления на национальном уровне резолюции 70/237 Генеральной Ассамблеи Организации Объединенных Наций» (будет доступен в онлайн-режиме) для облегчения представления отчетности. Государства-члены, возможно, пожелают также добровольно использовать типовое обследование для структурирования информации в рамках своих вышеупомянутых документов, посредством которых они информируют Генерального секретаря о своих взглядах и оценках.

66. Государствам и другим субъектам, которые в состоянии предложить финансовую, натуральную или техническую помощь в целях создания потенциала, следует делать это. Следует продолжать содействовать координации и обеспечению ресурсами усилий по укреплению потенциала, в том числе с участием соответствующих организаций и Организации Объединенных Наций.

67. Государствам следует продолжать рассматривать вопрос об укреплении потенциала на многостороннем уровне, включая обмен мнениями, информацией и передовой практикой.

Регулярный институциональный диалог

68. РГОС, которая была создана во исполнение резолюции 73/27 Генеральной Ассамблеи, впервые позволила всем государствам провести под эгидой Организации Объединенных Наций специализированное обсуждение достижений в области ИКТ в контексте международной безопасности.

69. В дополнение к решению задачи добиться общего понимания между всеми государствами РГОС содействовала развитию дипломатических сетей и способствовала установлению доверительных отношений между участниками.

Участие широкого круга неправительственных заинтересованных сторон продемонстрировало готовность более широкого сообщества субъектов использовать имеющийся опыт для оказания государствам поддержки в решении стоящей перед ними задачи обеспечения открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Обсуждения, состоявшиеся в рамках РГОС, подтвердили важность регулярного и организованного обсуждения вопросов использования ИКТ под эгидой Организации Объединенных Наций.

70. Государства пришли к выводу о том, что регулярный диалог под эгидой Организации Объединенных Наций способствует достижению общих целей укрепления международного мира, стабильности и предотвращения конфликтов в ИКТ-среде. Государства пришли также к выводу о том, что с учетом растущей зависимости от ИКТ и масштабов угроз, возникающих в результате их злонамеренного использования, налицо настоятельная необходимость в дальнейшей работе по углублению общего понимания, укреплению доверия и активизации международного сотрудничества.

71. Государства указали, что главную ответственность за национальную безопасность, общественную безопасность и соблюдение законности несут государства, в связи с чем они подтвердили, что важно поддерживать регулярный межправительственный диалог и определить надлежащие механизмы для взаимодействия с другими группами заинтересованных сторон в рамках будущих процессов.

72. Рассмотрение вопроса о достижениях в сфере ИКТ в контексте международной безопасности в Организации Объединенных Наций сосредоточено на тех аспектах их использования, которые связаны с международным миром, стабильностью и предотвращением конфликтов. Государства пришли к выводу о том, что планируемый в будущем регулярный институциональный диалог не должен дублировать существующие мандаты, усилия и мероприятия Организации Объединенных Наций, посвященные цифровым аспектам других проблем[8]. Государства пришли к выводу о том, что установление более тесных связей между этими форумами и процессами, инициированными Первым комитетом, могло бы способствовать повышению их взаимодополняемости и согласованности при одновременном уважении экспертного характера или специализированного мандата каждого органа.

73. Государства пришли к выводу о том, что будущий диалог по вопросам международного сотрудничества в области ИКТ в контексте международной безопасности должен, в частности, способствовать повышению информированности, укреплению доверия и способствовать дальнейшему изучению и обсуждению тех областей, в отношении которых общее понимание еще не достигнуто. Государства признали пользу изучения механизмов, предназначенных для контроля за осуществлением согласованных норм и правил, а также для разработки дополнительных норм и правил.

74. Государства пришли к выводу о том, что любые будущие механизмы поддержания регулярного институционального диалога под эгидой Организации Объединенных Наций должны быть ориентированным на практические

[8] См. справочный документ, подготовленный Председателем РГОС и озаглавленный “An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme”, декабрь 2019 года, URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

действия процессом с конкретными целями, который основан на достигнутых ранее результатах и носит всеохватный, прозрачный, консенсусный и ориентированный на результаты характер.

Рекомендации Рабочей группы открытого состава

75. Государствам следует продолжать активно участвовать в регулярном институциональном диалоге под эгидой Организации Объединенных Наций.

76. Государствам следует обеспечить продолжение всеохватного и транспарентного процесса переговоров по ИКТ в контексте международной безопасности под эгидой Организации Объединенных Наций при участи и признании Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, учрежденной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

77. Государствам следует принимать к сведению различные предложения 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.

78. Государствам следует учитывать содержащиеся в настоящем докладе выводы и рекомендации во всех будущих процессах, связанных с регулярным институциональным диалогом под эгидой Организации Объединенных Наций.

79. Государствам, которые в состоянии сделать это, следует рассмотреть вопрос о создании или поддержке спонсорских программ и других механизмов для обеспечения широкого участия в вышеупомянутых процессах в рамках Организации Объединенных Наций.

C. Заключительные замечания

80. На протяжении всего процесса в рамках РГОС государства последовательно и активно участвовали в нем, что позволило провести плодотворный обмен мнениями. Отчасти ценность такого обмена заключается в том, что были высказаны различные точки зрения, новые идеи и важные предложения, включая возможность принятия дополнительных юридически обязательных обязательств, хотя и не все государства поддержали их. Различные точки зрения представлены в прилагаемом резюме Председателя по итогам дискуссий и обсуждения конкретных предложений по формулировкам в рамках пункта повестки дня «Правила, нормы и принципы». Эти точки зрения следует дополнительно изучить в рамках будущих процессов под эгидой Организации Объединенных Наций, в том числе в Рабочей группе открытого состава, созданной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

Приложение II*

Резюме Председателя

A. Общая информация

1. РГОС предоставила всем государствам историческую возможность на равных основаниях принять участие в проводимом под эгидой Организации Объединенных Наций целенаправленном и непрерывном обсуждении вопросов, связанных с ИКТ в контексте международной безопасности. Благодаря всеохватным и прозрачным обсуждениям деятельность Рабочей группы открытого состава не только позволила достичь согласия по многим вопросам, отраженным в ее докладе, но и стала ценной мерой усиления международного мира и безопасности благодаря укреплению доверия и взаимопонимания между государствами, а также помогла создать глобальную дипломатическую сеть национальных экспертов. Активное и широкое участие всех делегаций продемонстрировало решимость государств продолжать совместную работу по этому вопросу, имеющему основополагающее значение для всех.

2. Отличительным признаком всех заседаний РГОС стал интерактивный обмен мнениями по вопросам существа с участием государств, а также гражданского общества, частного сектора, научных кругов и технического сообщества. Решимость, которую государства и другие заинтересованные стороны продемонстрировали на всем протяжении работы РГОС, и готовность работать даже в условиях перевода некоторых заседаний Группы в виртуальный формат являются бесспорным доказательством растущей универсальной актуальности рассматриваемых ею тем, а также растущего признания насущной необходимости коллективных действий для устранения угроз международной безопасности, которые возникают вследствие использования ИКТ со злым умыслом.

3. В настоящем резюме, ответственность за опубликование которого несет Председатель, представлено его понимание основных вопросов, которые обсуждались на заседаниях Рабочей группы открытого состава. В нем может быть представлена не вся информация об участии в работе всех делегаций, и его не следует рассматривать как документ с изложением консенсусной точки зрения государств по каким-либо конкретным вопросам, которые в нем затрагиваются. Полная подборка заявлений и предложений государств, которые были представлены для распространения, размещена на веб-сайте https://www.un.org/disarmament/open-ended-working-group.

B. Обзор хода обсуждений

4. Процесс РГОС предоставила всем государствам возможность высказать свою точку зрения, обеспокоенность или пожелания в рамках демократичной, транспарентной и всеохватной процедуры. Хотя РГОС стремилась определить сферы сближения позиций и достижения консенсуса, обсуждения в ней также свидетельствуют о разнообразии высказанных государствами-членами мнений, идей и предложений и могут послужить полезной основой для будущей работы,

* Публикуется без официального редактирования.

направленной на дальнейшее углубление общего понимания по вопросам использования ИКТ государствами в контексте международной безопасности.

5. В ходе обсуждений в РГОС государства подчеркивали взаимосвязанный и взаимоусиливающий характер всех элементов ее мандата. Так, международное право регулирует действия государств и их отношения, а добровольные, не имеющие обязательной силы нормы содержат дополнительные указания в отношении того, что представляет собой ответственное поведение государства. Оба этих элемента отражают ожидания в отношении поведения государства в связи с использованием ИКТ в контексте международной безопасности. Тем самым они также способствуют укреплению доверия за счет повышения прозрачности и развития сотрудничества между государствами и уменьшению риска возникновения конфликтов. В свою очередь укрепление потенциала позволяет всем государствам содействовать укреплению стабильности и безопасности во всем мире. В совокупности эти элементы составляют глобальную основу для принятия совместных мер по устранению существующих и потенциальных угроз в области ИКТ. Регулярный институциональный диалог даст возможность продолжить развитие и практическое использование этой основы за счет углубления общего понимания, обмена извлеченными уроками и передовой практикой в области осуществления, укрепления доверия между государствами и укрепления потенциала всех государств.

Существующие и потенциальные угрозы

6. В ходе обсуждений в РГОС государства затронули широкий круг существующих и потенциальных угроз, что наглядно показало, что государства могут по-разному воспринимать угрозы связанные с ИКТ-средой. Всеохватный формат работы РГОС предоставляет государствам возможность глубже понять, как действия и поведение в ИКТ-среде воспринимается другими, а также ознакомиться с мнениями других о том, что они считают наиболее значительными угрозами и рисками.

7. Некоторые государства выразили озабоченность по поводу разработки или использования ИКТ в целях, несовместимых с целями поддержания международного мира и безопасности. Некоторые из них были озабочены тем, что особенности ИКТ-среды могут способствовать не столько урегулированию споров мирными средствами, сколько принятию односторонних мер. Некоторые государства отметили свою озабоченность по поводу развития потенциала ИКТ в военных и других подобных целях, что может подорвать международный мир и безопасность. Другие государства отметили, что угроза заключается в использовании государствами такого потенциала вопреки их обязательствам по международному праву. Была также выражена озабоченность по поводу накопления факторов уязвимости и отсутствия прозрачности и четко определенных процедур для раскрытия информации о них, использования вредоносных скрытых функций, целостности глобальных цепочек поставок в области ИКТ и обеспечения безопасности данных. Некоторые государства выразили обеспокоенность по поводу того, что ИКТ могут использоваться для вмешательства в их внутренние дела, в том числе посредством информационных операций и кампаний по распространению дезинформации. В качестве конкретной проблемы было названо стремление к повышению уровня автоматизации и автономии операций в сфере ИКТ, а также принятие мер, которые могут привести к ограничению или нарушению связи, непреднамеренной эскалации или негативным последствиям для

третьих сторон. В качестве отдельной проблемы некоторые государства также отметили отсутствие ясности в отношении обязанностей частного сектора.

8. Государства особо отметили, что меры, направленные на поощрение ответственного поведения государств, должны оставаться нейтральными с технической точки зрения, подчеркнув при этом, что проблемой являются не сами технологии, а их ненадлежащее использование. Государства признали, что даже с учетом того, что технический прогресс и новые прикладные программы могут открывать возможности для развития, они могут также способствовать расширению сферу нападений, усиливать уязвимость ИКТ-среды или использоваться для осуществления новых видов деятельности со злым умыслом. В этой связи отмечались конкретные направления развития техники и технические достижения, в том числе прогресс в области машинного обучения и квантовых вычислений, повсеместное использование подключенных устройств («Интернет вещей»), новые способы хранения и получения данных с использованием технологий распределенного реестра и облачных вычислений, и бурный рост объема больших данных и оцифрованных личных данных.

Международное право

9. Действуя в рамках мандата Группы и преследуя цель поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды и поощрения общего понимания, государства провели обмен мнениями о применимости международного права к вопросам, касающимся ИКТ в контексте международной безопасности.

10. В ходе обсуждений в РГОС, государства напомнили, что международное право, и в частности Устав Организации Объединенных Наций во всей своей полноте, применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, мирной и доступной ИКТ-среды. В этой связи государства особо отметили, что необходимо предпринимать шаги к тому, чтобы не допускать и воздерживаться от введения любых мер, не соответствующих Уставу Организации Объединенных Наций и международному праву и препятствующих всестороннему обеспечению экономического и социального развития населения затрагиваемых стран и тормозящих улучшение их благосостояния. В то же время государства подчеркнули также, что вопрос о применимости международного права к использованию ИКТ государствами требует дальнейшей проработки.

11. В ходе обсуждений были подтверждены конкретные принципы международного права, в том числе государственный суверенитет, суверенное равенство, разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость, отказ в международных отношениях от применения силы или угрозы силой 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 и невмешательство во внутренние дела других государств.

12. Было вновь отмечено, что международное право является основой стабильности и предсказуемости в отношениях между государствами. В частности, снижению рисков и уменьшению потенциального ущерба для гражданских лиц и гражданских объектов, а также комбатантов в контексте вооруженного конфликта способствует международное гуманитарное право. В то же время

государства подчеркнули, что международное гуманитарное право не поощряет милитаризацию и не узаконивает применение силы в какой бы то ни было области.

13. Было также отмечено, что в соответствии с обычным международным правом ответственность государств за международно-противоправные деяния распространяется на использование ИКТ.

14. Было вновь отмечено, 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, действующими по указанию государства или под его контролем. Была также отмечена ответственность государств в отношении субъектов, принадлежащих государству или находящихся под его контролем.

15. Государства вновь отметили, 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 присвоения этой деятельности указанному государству и что обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. Некоторые государства подчеркнули важность подлинных, надежных и достаточных доказательств в этом контексте.

16. По мнению некоторых государств, существующих норм международного права, дополняемых добровольными, не имеющими обязательной силы нормами, которые отражают консенсус между государствами, в настоящее время достаточно для решения проблемы использования ИКТ государствами. Предлагалось также сосредоточить усилия на достижении общего понимания в отношении того, каким образом разработка дополнительных руководящих указаний способствует применению уже согласованной нормативной базы и как переводу ее в практическую плоскость может содействовать ее более активное применение всеми государствами. В то же время другие государства высказали мнение о том, что ввиду быстро меняющегося характера угроз и серьезности риска необходима согласованная на международном уровне и имеющая обязательную юридическую силу нормативная база в отношении использования ИКТ. Была также высказана мысль о том, что такая имеющая обязательную силу нормативная база может способствовать более эффективному выполнению обязательств на глобальном уровне и может стать более надежной основой для привлечения субъектов к ответственности за совершенные действия. Государства подчеркнули, что при разработке любых международно-правовых рамок для решения проблем, вызванных таким использованием ИКТ, которое может иметь последствия для международного мира и безопасности, следует учитывать озабоченность и интересы всех государств, руководствоваться правилом консенсуса, и что этим следует заниматься в рамках Организации Объединенных Наций при активном и равноправном участии в нем всех государств.

17. Было подчеркнуто, что, хотя существующие своды норм международного права не содержат конкретных ссылок на использование ИКТ в контексте международной безопасности, международное право может прогрессивно развиваться, в том числе на основе убежденности в правомерности и практики государств. Был поднят вопрос о возможности постепенной разработки одновременно с применением норм дополнительных обязательных мер. Кроме того,

было высказано предложение о том, что одним из перспективных направлений могло бы стать принятие политического обязательства.

18. Напомнив о том, что международное право, и в частности Устав Организации Объединенных Наций, применимы к использованию ИКТ, государства подчеркнули, что некоторые вопросы, касающиеся применимости международного права к использованию ИКТ, еще предстоит прояснить в полной мере. Некоторые государства предложили отнести к таким вопросам, среди прочего, такие виды связанной с ИКТ деятельности, которые могут быть истолкованы другими государствами как угроза силой или ее применение (статья 2 4) Устава) или могут дать государству основание воспользоваться своим неотъемлемым правом на самооборону (статья 51 Устава). Кроме того, речь идет о вопросах, касающихся применимости к операциям с использованием ИКТ таких принципов международного гуманитарного права, как гуманность, необходимость, соразмерность, различие и предосторожность. В связи с этим некоторые государства отметили необходимость осмотрительного подхода к обсуждению вопроса о применимости международного гуманитарного права к использованию ИКТ государствами. Государства отметили необходимость дальнейшего изучения этих важных тем в ходе будущих обсуждений.

19. Кроме того, в перспективе, по предложению государств, одним из важнейших первых шагов по уточнению и дальнейшему углублению общего понимания могло бы стать расширение обмена мнениями и углубленное обсуждение государствами вопроса о применении международного права к использованию ИКТ государствами. Было отмечено, что такой обмен мнениями сам по себе может служить важной мерой укрепления доверия. Кроме того, некоторые государства предложили несколько способов добровольного обмена национальными мнениями о применимости международного права, включая использование ежегодного доклада Генерального секретаря о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности[9], портала по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения или использование обзора национальной практики применения международного права. Были также отмечены позитивные результаты, достигнутые в реализации региональных и других договоренностей об обмене мнениями и выработке общего понимания в отношении применимости международного права.

20. Что касается вопроса о поддержании мира и предотвращении конфликтов, то государства подтвердили необходимость урегулировать споры мирными средствами и воздерживаться от угрозы силой или ее применения. В этой связи государства напомнили о существующих органах, механизмах и средствах предупреждения и мирного урегулирования споров. Некоторые государства высказали мысль о том, что разработка под эгидой Организации Объединенных Наций пользующегося всеобщим признанием общего подхода и понимания источника инцидентов в сфере ИКТ на техническом уровне на основе обмена передовым опытом с учетом уважения принципа государственного суверенитета могла бы привести к повышению ответственности и прозрачности и могла бы способствовать применению средств правовой защиты теми, кому в результате злоумышленных действий был причинен ущерб.

[9] Резолюция 75/32 Генеральной Ассамблеи.

Правила, нормы и принципы ответственного поведения государств

21. В ходе обсуждений в рамках РГОС государства напомнили о том, что добровольные, не имеющие обязательной силы нормы ответственного поведения самих государств не изменяют и не подменяют собой международное право и цели и принципы Организации Объединенных Наций, включая поддержание международного мира и безопасности и поощрение прав человека, а должны рассматриваться как соответствующие международному праву и целям и принципам Организации Объединенных Наций. Государства также отметили резолюцию 2131 (XX) Генеральной Ассамблеи «Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета».

22. Государства сослались на резолюцию 73/27 Генеральной Ассамблеи и представили свод из 13 правил, норм и принципов ответственного поведения государств, в частности подтвердив 11 добровольных, не имеющих обязательной силы норм, «закрепленных в докладах групп правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 и 2015 годов, принятых консенсусом и рекомендованных резолюцией 71/28»[10].

23. Государства подчеркнули необходимость повышения осведомленности о существующих нормах и поддержки перевода их в плоскость практического применения одновременно с разработкой новых норм. Государства подчеркнули необходимость выработки указаний в отношении применения норм на практике. В этой связи государства призвали осуществлять обмен передовым опытом и извлеченными уроками в области практического применения норм и распространять их. Предлагалось использовать различные совместные подходы, такие как разработанная государствами «дорожная карта» для содействия их усилиям по осуществлению, а также добровольные обследования для обмена опытом и передовой практикой.

24. Государства отметили, что нормы могут способствовать предотвращению конфликтов в ИКТ-среде и способствовать использованию ИКТ в мирных целях и полной реализации выгод от их использования в целях ускорения социального и экономического развития во всем мире. Государства подчеркнули, что применение норм не должно приводить к неоправданным ограничениям для международного сотрудничества и передачи технологий, а также не должно препятствовать новаторству в мирных целях и экономическому развитию государств в условиях справедливости и недискриминации. Государства также подчеркнули, что между нормами, укреплением доверия и созданием потенциала существует взаимосвязь, и особо указали на необходимость учитывать гендерные факторы проблематики при применении норм.

25. В ходе обсуждений высказывались предложения в отношении дальнейшей разработки существующих норм. Государства вновь заявили также о важности защиты всех объектов критически важной инфраструктуры, которые обеспечивают оказание основных услуг населению и к которым следует относить медицинские и медико-санитарные учреждения. С учетом потенциальных последствий причинения любого ущерба объектам критически важной инфраструктуры, которые используются для предоставления трансграничных или международных услуг, государства обратили также внимание на важность

[10] Резолюция 73/27 Генеральной Ассамблеи, пункт 1 постановляющей части.

сотрудничества в защите таких объектов, а также на важность обеспечения общедоступности и надежности Интернета. Государства сослались на резолюцию 64/211 Генеральной Ассамблеи «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»[11]. Кроме того, государства, выразив обеспокоенность по поводу включения в ИКТ-продукты вредоносных скрытых функций, также предложили дополнительно обеспечить надежность цепочки поставок ИКТ и ответственность за уведомление пользователей при выявлении серьезных факторов уязвимости. Более того, государства выразили озабоченность по поводу накопления факторов уязвимости. Некоторые государства предложили сформулировать объективные международные правила и стандарты безопасности цепочек поставок.

26. В дополнение к сказанному в приложении к настоящему резюме представлены письменные предложения государств по дальнейшей проработке существующих норм, разработке указаний по их применению и выработке новых норм.

27. Некоторые государства также отметили представленное в 2015 году предложение о разработке международного кодекса поведения в области информационной безопасности[12].

28. Некоторые государства отметили, что необходимо поощрять и поддерживать дополнительные усилия на региональном уровне, а также налаживать партнерские отношения с другими заинтересованными сторонами, например с частным сектором и техническим сообществом, по вопросам применения норм. Такие партнерские отношения можно было бы выстраивать, например, для обеспечения того, чтобы усилия по укреплению потенциала для устранения различий в возможностях в плане применения носили постоянный характер. В этой связи государства сослались на пункт 1.13 постановляющей части резолюции 73/27 Генеральной Ассамблеи, в котором, в частности, подчеркивается, что «государства должны содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в укреплении безопасности при использовании ИКТ и самих ИКТ, включая безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг». Государства отметили важное значение информационно-разъяснительной работы и принятия совместных мер для обеспечения того, чтобы различные заинтересованные стороны, включая государственный и частный сектор и гражданское общество, выполняли свои обязанности в связи с использованием ИКТ.

Меры укрепления доверия

29. В ходе обсуждений в рамках РГОС государства отметили сохраняющуюся актуальность мер укрепления доверия, рекомендованных в согласованных докладах группы правительственных экспертов. Был отмечен ряд мер, требующих первоочередного внимания, таких как регулярный диалог и добровольный обмен информацией о существующих и потенциальных угрозах, национальной политике, законодательной базе или доктрине, национальных взглядах на применимость международного права к использованию ИКТ государствами, а также о

[11] В приложении к этой резолюции содержится инструмент добровольной самооценки национальных усилий по защите объектов критически важной информационной инфраструктуры.

[12] Документ A/69/723, упоминаемый в п. 12 документа A/70/174.

национальных подходах к определению критически важной инфраструктуры и классификации происшествий, связанных с ИКТ. Было высказано мнение о том, что обмен передовым опытом в области цифровой криминалистики и расследования инцидентов, связанных с применением вредоносных компьютерных программ, мог бы способствовать укреплению как сотрудничества, так и потенциала. Было также подчеркнуто, что одним из ценных практических шагов в направлении развития международного сотрудничества и укрепления доверия является выработка общего понимания концепций и терминологии. К числу других таких мер относятся разработка руководства по осуществлению мер укрепления доверия, подготовка дипломатов, обмен опытом создания и использования защищенных каналов связи в кризисных ситуациях, обмен персоналом, проведение учений на основе сценариев на директивном уровне, а также оперативные учения на техническом уровне с участием групп реагирования на компьютерные происшествия или групп по расследованию происшествий в области кибербезопасности. Было высказано предложение о том, что еще одним направлением деятельности по укреплению доверия и повышению уверенности в отношении намерений и обязательств государств могут быть национальные меры обеспечения прозрачности, такие как добровольный обмен ответами на опрос о ходе осуществления или публикация национальных деклараций о приверженности принципам ответственного поведения государств.

30. Был рассмотрен вопрос о целесообразности создания централизованного глобального справочника контактных центров, в связи с чем был проанализирован опыт региональных органов в связи с созданием и эксплуатацией сетей контактных центров и была принята во внимание информация о функционировании существующих сетей. В то же время было отмечено, что решающее значение для эффективности такого справочника будут иметь не только его надежность и порядок функционирования, но и отказ от дублирующих друг друга или чрезмерно детализованных процедур. Была также подчеркнута значимость регулярного проведения учений в рамках сети контактных центров, поскольку это может способствовать поддержанию готовности и повышению оперативности, а также обеспечению постоянного обновления указателей контактных центров.

31. Поскольку меры укрепления доверия могут разрабатываться на двустороннем, региональном или многостороннем уровнях, государства также обсудили желательность и целесообразность создания глобального хранилища информации о мерах укрепления доверия под эгидой Организации Объединенных Наций, с тем чтобы обеспечить обмен информацией о политике, передовой практике, опыте и анализе осуществления мер укрепления доверия и содействовать взаимному обучению и направлению средств на укрепление потенциала. Такое хранилище могло бы также помочь государствам в определении дополнительных мер укрепления доверия, которые бы отвечали их национальным и региональным условиям, и стать источником возможных образцов для воспроизведения в других областях. Было отмечено, что в любом случае вновь создаваемое глобальное хранилище не должно дублировать существующие механизмы и что условия функционирования такого хранилища требуют дальнейшего обсуждения.

32. Государства также обратили внимание на функции и обязанности других субъектов, включая гражданское общество, частный сектор, научные круги и техническое сообщество, в деле содействия укреплению доверия и повышения уверенности в связи с использованием ИКТ на национальном, региональном и глобальном уровнях. Государства отметили разнообразие инициатив с участием

многих заинтересованных сторон, благодаря которым на основе разработки принципов и обязательств были созданы новые сети для обмена информацией, взаимодействия и сотрудничества. Точно так же инициативы в конкретных секторах или областях наглядно демонстрируют растущее понимание функций и обязанностей других участников и тот уникальный вклад, который они могут внести в обеспечение безопасности ИКТ благодаря добровольным обязательствам, кодексам профессионального поведения и стандартам.

Укрепление потенциала

33. В ходе обсуждений в рамках РГОС государства особо отметили, что укрепление потенциала может играть важную роль в предоставлении всем государствам возможности в полной мере участвовать в обсуждении на международном уровне принципов ответственного поведения государств, способствуя при этом выполнению таких совместных обязательств, как Повестка дня в области устойчивого развития на период до 2030 года[13]. В этой связи государства подчеркнули необходимость обеспечения программ по укреплению потенциала достаточными финансовыми и людскими ресурсами.

34. Государства особо отметили важную работу, проводимую в области укрепления потенциала, связанного с ИКТ, другими субъектами, включая международные организации, региональные и субрегиональные органы, гражданское общество, частный сектор, научные круги и специализированные технические органы, и призвали подумать над тем, как содействовать координации, поступательному характеру, эффективности и сокращению дублирования всех этих усилий.

35. Организация Объединенных Наций призвана сыграть важную роль в оказании государствам поддержки в повышении значимости деятельности по укреплению потенциала и в поддержке более тесной координации деятельности различных субъектов, занимающихся вопросами укрепления потенциала, на основе использования ее организаторских возможностей. Государства предложили использовать существующие платформы в рамках Организации Объединенных Наций, ее специализированных учреждений и международного сообщества в целом для укрепления уже налаженной координации. Эти платформы можно было бы использовать для обмена национальными мнениями о потребностях в укреплении потенциала, содействия распространению выводов и опыта как получателями, так и поставщиками помощи и облегчения доступа к информации о программах укрепления потенциала и оказания технической помощи. Эти платформы могли бы также способствовать мобилизации ресурсов или содействовать направлению имеющихся ресурсов для удовлетворения просьб об оказании поддержки в создании потенциала и технической помощи. Была высказана мысль о том, что разработка под эгидой Организации Объединенных Наций глобальной программы укрепления потенциала в области ИКТ могла бы способствовать повышению слаженности усилий по укреплению потенциала и что добровольные обследования для целей самооценки могут помочь государствам в

[13] К соответствующим целям и задачам в области устойчивого развития относятся, в частности, существенное расширение доступа к информационно-коммуникационным технологиям (9.C), расширение сотрудничества по линии Север — Юг и Юг — Юг, а также трехстороннего регионального и международного сотрудничества в областях науки, техники и новаторства и доступа к соответствующим достижениям (17.6) и усиление международной поддержки эффективного и целенаправленного наращивания потенциала (17.9).

выявлении и определении важности потребностей в области укрепления потенциала или возможностей в области оказания поддержки.

36. Одновременно с главной ответственностью государств за поддержание безопасной, надежной и пользующейся доверием ИКТ-среды была также подчеркнута важность многостороннего подхода к укреплению потенциала, позволяющего устранять технические и нормативные недостатки во всех соответствующих секторах общества. Государства отметили, в частности, что поступательный характер деятельности по укреплению потенциала может быть обеспечен с помощью подхода, предполагающего взаимодействие и партнерство с местным гражданским обществом, техническим сообществом, научно-образовательными учреждениями и субъектами частного сектора, а также за счет создания реестров экспертов и специализированных узловых центров. В этой связи было также подчеркнуто, что благоприятное воздействие на национальные подходы к безопасности ИКТ могло бы оказать принятие межсекторального, целостного и междисциплинарного подхода к укреплению потенциала, в том числе путем укрепления национальных координационных органов с участием соответствующих заинтересованных сторон для оценки эффективности программ. Такой подход может также способствовать решению проблем, возникающих в связи с появлением новых технологий.

37. Государства обратили внимание на гендерный цифровой разрыв и настоятельно призвали принять конкретные меры на национальном и международном уровнях для решения проблемы гендерного неравенства и обеспечения конструктивного участия женщин в международных дискуссиях и программах по созданию потенциала в области ИКТ и международной безопасности, в том числе путем сбора дезагрегированных по признаку пола данных. Государства дали высокую оценку программам, которые способствуют участию женщин в многосторонних обсуждениях по вопросам безопасности ИКТ. Была также подчеркнута необходимость укрепления связи этой темы с повесткой дня Организации Объединенных Наций по вопросам женщин, мира и безопасности.

38. Государства отметили, что существуют многочисленные факторы, которые препятствуют повышению эффективности деятельности по укреплению потенциала или снижают ее эффективность. В качестве серьезных проблем были отмечены недостаточная координация и взаимодополняемость при выборе направлений и осуществлении деятельности по укреплению потенциала. Государства также подняли вопросы практического характера, касающиеся определения потребностей в укреплении потенциала, оперативного реагирования на просьбы об оказании помощи в укреплении потенциала, а также разработки, осуществления, устойчивости и доступности мероприятий по укреплению потенциала и отсутствия конкретных показателей для измерения их воздействия. Во многих случаях деятельность по укреплению потенциала и прогресс в деле сокращения цифрового разрыва затрудняются отсутствием достаточных людских, финансовых и технических ресурсов. В условиях повышенного спроса на ИКТ-специалистов после создания потенциала некоторые страны, которые занимаются укреплением только что созданного потенциала, сталкиваются с проблемой удержания квалифицированных кадров. Государства отметили, что проблемой является также отсутствие доступа к технологиям, связанным с обеспечением безопасности ИКТ.

Регулярный институциональный диалог

39. В ходе состоявшихся в Рабочей группе открытого состава обсуждений государства напомнили о содержащемся в резолюции 73/27 Генеральной Ассамблеи мандате Рабочей группы изучить возможность организации регулярного институционального диалога и подтвердили, что одним из ключевых результатов работы Группы станут подготовленные ею оценки и рекомендации.

40. Государства высказали ряд мнений относительно целей, которые должны стать приоритетными для будущего регулярного институционального диалога, и относительно того, какой формат регулярного диалога мог бы наилучшим образом способствовать достижению этих целей. Некоторые государства выразили желание, чтобы в рамках регулярного диалога приоритетное внимание уделялось выполнению существующих обязательств и рекомендаций, включая разработку руководящих указаний по поддержке и проверке их выполнения, координации и повышению эффективности деятельности по созданию потенциала и определению передового опыта и обмену им. Другие государства выразили желание, чтобы в рамках регулярного диалога приоритетное внимание уделялось дальнейшей проработке существующих обязательств и выработке дополнительных обязательств, включая выработку юридически обязательного документа и создание институциональных структур в поддержку его применения.

41. Некоторые государства внесли конкретное предложение о разработке Программы действий по содействию ответственному поведению государств в киберпространстве с целью создания постоянного форума Организации Объединенных Наций для рассмотрения вопросов использования ИКТ государствами в контексте международной безопасности. Было предложено отразить в Программе действий политическое обязательство государств следовать согласованным рекомендациям, нормам и принципам, проводить регулярные совещания по вопросам осуществления, укреплять сотрудничество между государствами и активизировать их деятельность по созданию потенциала и проводить регулярные конференции по обзору. В рамках Программы действий было также предложено обеспечить участие широкого круга сторон и проведение консультаций.

42. Государства отметили учреждение в соответствии с резолюцией 75/240 от 31 декабря 2020 года новой Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, которая начнет функционировать по завершении деятельности Рабочей группы открытого состава, учрежденной во исполнение резолюции 73/27, и рассмотрит результаты ее работы.

43. Государства также выразили пожелание, чтобы международное сообщество в конечном счете вернулось к единому основанному на консенсусе процессу под эгидой Организации Объединенных Наций. В этой связи государства отметили, что различные предлагаемые форматы диалога не обязательно являются взаимоисключающими. Была высказана мысль о том, что различные форматы могут дополнять друг друга или могут быть объединены, с тем чтобы использовать уникальные особенности каждого из них и сократить дублирование усилий.

44. Кроме того, была отмечена необходимость продолжить рассмотрение вопроса о продолжительности и устойчивости будущего диалога, а также были подняты вопросы, касавшиеся выбора между консультативным и

ориентированным на практические действия характером диалога, сроков и возможных мест его проведения и бюджетных соображений.

45. Государства приняли во внимание уникальную роль и ответственность государств в обеспечении национальной и международной безопасности, но при этом подчеркнули, что ответственное поведение других субъектов в немалой степени способствует созданию открытой, безопасной, доступной и мирной ИКТ-среды. В этой связи было отмечено, что формированию более устойчивой и безопасной ИКТ-среды может способствовать расширение сотрудничества и партнерских связей с участием многих заинтересованных сторон.

Приложение к резюме Председателя

Конкретные предложения относительно формулировок по пункту повестки дня «Правила, нормы и принципы» из материалов, представленных делегациями в письменном виде

С учетом того, что в своих письменных материалах многие делегации ссылались на существующие нормы, ниже приводятся лишь дополнительные предложения относительно формулировок.

Армения

- Государства воздерживаются от любых действий, которые могут привести к попыткам нарушения работоспособности объектов критически важной инфраструктуры и деятельности правительства, и по защищенным каналам своевременно направляют разъяснения во избежание дальнейшей возможной эскалации.

Австралия, Казахстан, Соединенные Штаты Америки, Чешская Республика, Эстония и Япония

Текст с указаниями по осуществлению норм в пунктах 13 f) и g) доклада 2015 года

- При подготовке указаний относительно осуществления этих норм государствам следует учитывать, что выделение отдельных секторов в качестве объектов критически важной инфраструктуры не предполагает составления исчерпывающих перечней и не влияет на определение государством какого-либо другого сектора в качестве приоритетного, а также не означает косвенного попустительства в отношении злонамеренных действий против какой-либо категории объектов, не включенной в перечень.

- РГОС готовила свой доклад в условиях пандемии COVID-19. В этих обстоятельствах РГОС подчеркнула, что все государства рассматривают медицинские службы и медицинские учреждения в качестве объектов критически важной инфраструктуры для целей норм f) и g).

Беларусь

- Государства должны подтвердить свою приверженность принципу отказа от милитаризации существующих ИКТ и создания новых ИКТ, специально предназначенных для нанесения ущерба информационным ресурсам, инфраструктуре и важнейшим объектам других стран.

Канада

Предлагаемый текст указания к норме для включения в пункт 41

Хотя в нормах, подготовленных группой правительственных экспертов в 2015 году, определены меры, которые государства должны и не должны принимать, государства подчеркнули необходимость в указаниях по их практическому применению и предложили следующие указания в отношении этих норм. В понимании РГОС и нормы, и указания не наносят ущерба существующим правам и обязанностям государств по международному праву и никоим образом не изменяют и не умаляют их.

> 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, признаваемых вредоносными или способных создать угрозу международному миру и безопасности (2015 ¶13 a)).

i. Настоящая норма носит общий характер. Осуществление всего комплекса норм, а также изложенных ниже конкретных указаний будет способствовать дальнейшей практической реализации этой нормы. Государствам следует применять совместный подход к работе друг с другом и с неправительственными заинтересованными сторонами, включая отраслевые предприятия, научные круги и гражданское общество.

ii. Для этого государствам следует, по мере необходимости и когда это возможно, делать следующее:

– утверждать и реализовывать всеобъемлющие национальные стратегии кибербезопасности. По возможности это должно способствовать международному сотрудничеству в сфере кибербезопасности;

– создавать и поддерживать структуры для реагирования на инциденты, например, группы реагирования на компьютерные происшествия, которые способны координировать деятельность, обмениваться передовым опытом и сотрудничать в реагировании на инциденты в сфере ИКТ;

– публиковать заявления о том, что они будут действовать в рамках норм ответственного поведения государств в киберпространстве, сформулированных в докладе, подготовленном в 2015 году группой правительственных экспертов Организации Объединенных Наций;

– принимать участие в региональных и двусторонних инициативах, направленных на разработку и осуществление мер укрепления доверия.

iii. Государствам-членам следует рекомендовать подготавливать и упорядочивать информацию об осуществлении ими принятых норм, которую они должны представлять.

b. Государства должны изучить в случае инцидентов в сфере ИКТ всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности в ИКТ-среде, а также характер и масштабы ответственности (2015 ¶13 b)).

i. Государства могли бы создать структуры, установить регламенты, процессы и координационные механизмы, необходимые для содействия тщательному рассмотрению серьезных инцидентов в сфере ИКТ и определения надлежащих мер реагирования.

ii. После создания этих структур и процессов государства могли бы разработать типовые формы для описания инцидентов в сфере ИКТ или степени их значимости, с тем чтобы оценивать и анализировать инциденты в сфере ИКТ.

iii. Транспарентность таких типовых форм и их унификация региональными организациями могли бы обеспечить общность подходов государств к рассмотрению инцидентов в сфере ИКТ и улучшить коммуникацию между государствами. Когда это возможно, типовые формы следует соотносить с устоявшейся практикой и избегать дублирования усилий.

iv. При рассмотрении всей релевантной информации, касающейся происшествия в сфере ИКТ, государствам следует изучать возможные гендерно-дифференцированные последствия и проводить совместную работу со всеми заинтересованными сторонами, с тем чтобы понимать более широкий контекст инцидента в сфере ИКТ, включая его воздействие на осуществление прав ЛГБТ и женщин.

v. Государствам следует рассматривать воздействие инцидентов в сфере ИКТ на права человека, включая права на свободу выражения мнений, ассоциации и мирных собраний, право на свободу от произвольного или незаконного вмешательства в частную жизнь, а также права инвалидов.

vi. Государствам следует признать, что реагирование на инциденты в сфере безопасности часто требует участия не только групп реагирования на компьютерные происшествия/групп по расследованию происшествий в области кибербезопасности, но и различных заинтересованных сторон, а также следует развивать сотрудничество посредством подготовки кадров и укрепления потенциала совместно со всеми группами заинтересованных сторон. Государствам следует стимулировать организацию учебной подготовки по вопросам безопасности в цифровой среде и другие мероприятия по укреплению потенциала и оказанию содействия со стороны заинтересованных кругов, включая гражданское общество, в целях предотвращения инцидентов в области безопасности, особенно для уязвимых групп населения и других пользователей, подвергающихся опасности.

c. Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ (2015 ¶13 c)).

i. Замечания относительно применения данной нормы:

– Если государство обнаруживает, что злонамеренная кибердеятельность осуществляется с территории другого государства или с использованием его киберинфраструктуры, то первым шагом может стать уведомление этого государства. Группы реагирования на компьютерные происшествия имеют крайне важное значение для возможностей выявлять такую деятельность.

– С учетом того, что инциденты в сфере ИКТ могут быть спровоцированы с территории третьих государств или при их участии, подразумевается, что уведомление государства не означает ответственности такого государства за инцидент.

– Получившему уведомление государству следует подтвердить получение запроса через национальный контактный центр.

– Когда государству известно, что его территория или киберинфраструктура используются для совершения международно-противоправного деяния с применением ИКТ, которое может привести к серьезным неблагоприятным последствиям в государстве, первому государству следует попытаться принять разумные, доступные и практически осуществимые меры в пределах своей территории и возможностей в соответствии со своими обязательствами по внутреннему и международному праву, с тем чтобы добиться прекращения международно-противоправного деяния или смягчить его последствия.

– Государство может узнать о таком деянии после получения уведомления от затронутого государства. Такое уведомление должно быть сделано добросовестно и должно быть подкреплено сопроводительной информацией. Сопроводительная информация может включать индикаторы компрометации, такие как IP-адрес и данные компьютера, использованного для совершения злонамеренных действий с использованием ИКТ, и данные о вредоносных программах.

– Государства следует поощрять к обеспечению того, чтобы негосударственные субъекты, включая частный сектор, не могли осуществлять злонамеренную деятельность с использованием ИКТ в своих собственных целях или в целях государственных или других негосударственных субъектов в ущерб третьим сторонам, в том числе тем, которые находятся на территории другого государства. Эта цель может быть достигнута посредством сотрудничества с частным сектором в определении допустимых действий с использованием подхода, основанного на оценке риска, и в разработке конкретных инструментов: процессов сертификации, руководств по передовой практике, механизмов реагирования на инциденты и, в соответствующих случаях, национальных нормативных актов.

– Эту норму не следует интерпретировать как требование к государству осуществлять опережающий мониторинг всех ИКТ на своей территории или принимать другие превентивные меры.

ii. Государство, которому стало известно об осуществляемой с его территории вредоносной деятельности в сфере ИКТ и которое не располагает возможностями для реагирования, может по своему усмотрению обратиться за помощью к другим государствам, в том числе используя для этого типовые формы запросов об оказании помощи.

– В таких случаях помощь может запрашиваться у других государств или у частной организации, и такая помощь, если она оказывается, должна соответствовать национальному законодательству и международному праву прав человека.

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 следует рассмотреть вопрос о разработке новых мер в этой сфере (2015 ¶13 d)).

i. При применении этой нормы государствам следует:

– рассматривать, в соответствующих случаях, вопрос о поддержке работы Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, в том числе путем продления мандата межправительственной группы экспертов открытого состава и поддержки ее текущей работы по всестороннему изучению проблемы киберпреступности;

– поддерживать усилия Управления Организации Объединенных Наций по наркотикам и преступности, направленные на то, чтобы продолжать оказывать государствам-членам, по их просьбе и исходя из национальных потребностей, техническую помощь и содействие в деле устойчивого наращивания потенциала для борьбы с киберпреступностью через Глобальную программу борьбы с киберпреступностью и, в частности, через ее региональные отделения, в том, что касается предупреждения, выявления, расследования и судебного преследования киберпреступности во всех ее формах, признавая, что сотрудничество с государствами-членами, соответствующими международными и региональными организациями, частным сектором, гражданским обществом и другими соответствующими заинтересованными сторонами может способствовать этой деятельности;

– принимать предусмотренные меры в соответствии с их обязательствами и рассмотреть вопрос о принятии новых мер, таких как введение национального законодательства, направленного на борьбу с киберпреступностью, таким образом, чтобы это соответствовало обязательствам государств в области прав человека и обеспечивало судебные гарантии.

e. Государства в процессе обеспечения безопасного использования ИКТ должны соблюдать положения резолюций Совета по правам человека 20/8 и 26/13 (Поощрение, защита и осуществление прав человека в Интернете) и резолюций Генеральной Ассамблеи 68/167 и 69/166 (Право на неприкосновенность личной жизни в эпоху цифровых технологий), чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение (2015 ¶13 e))

i. Государствам следует:

– выполнять свои обязательства по национальному и международному праву при рассмотрении, разработке или применении национальной политики или законодательства в области кибербезопасности или при разработке и реализации инициатив или создании структур, связанных с кибербезопасностью, включая меры по обеспечению защиты всех прав человека;

– при этом государствам следует учитывать мнения всех соответствующих и затронутых заинтересованных сторон на самых ранних этапах разработки и реализации политики в области кибербезопасности, с тем чтобы обеспечить целостное рассмотрение последствий мер по обеспечению кибербезопасности;

– вовлечение гражданского общества особенно важно с учетом его роли как одного из основных субъекта в содействии соблюдению государством его обязательств и обязанностей в области прав человека;

– принимать во внимание, что отдельные лица имеют в онлайновом режиме те же права, что и в физическом мире, и учитывать различные угрозы, с которыми могут сталкиваться женщины и лица, принадлежащие к меньшинствам и уязвимым группам, в контексте прав человека;

– проводить гендерную экспертизу национальной и региональной политики в области кибербезопасности для выявления областей, в которых необходимы улучшения;

– рассмотреть вопрос о включении мер по устранению последствий ИКТ для прав человека в свои национальные планы действий в области предпринимательства и прав человека.

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 (2015 ¶13 f)).

i. Каждое государство определяет, какие объекты инфраструктуры или сектора оно считает критически важными, в соответствии с национальными приоритетами и методами определения объектов критически важной инфраструктуры. К объектам критически важной инфраструктуры, которые используются для оказания населению базовых услуг, могут относиться объекты энергетики, водоснабжения, санитарии, здравоохранения, образования, финансов, транспорта, телекоммуникаций и реагирования на кризисные ситуации. К критически важной инфраструктуре может также относиться техническая инфраструктура, необходимая для проведения выборов, референдумов или плебисцитов, и техническая инфраструктура, необходимая для обеспечения общедоступности и надежности Интернета. 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 против каких-либо объектов критически важной инфраструктуры, не указанных выше.

ii. Государствам следует учитывать потенциально вредные последствия их деятельности в области ИКТ для технической инфраструктуры, имеющей важное значение для общедоступности и надежности Интернета.

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 культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции (2015 ¶13 g)).

i. В целях содействия формированию глобальной культуры кибербезопасности государствам следует рассматривать, в соответствующих случаях, вопрос об обмене информацией о передовой практике в области защиты критически важной инфраструктуры, в том числе относительно всех составляющих, указанных в этой резолюции, к которым относятся:

– основные требования в сфере безопасности;

– процедуры уведомления об инцидентах;

– инструменты и методы работы в случае инцидентов;

– устойчивость в случае чрезвычайных ситуаций;

– выводы, сделанные в результате предыдущих инцидентов.

ii. Укрепление потенциала и другие меры по созданию глобальной культуры кибербезопасности должны разрабатываться на основе широкого участия и должны быть направлены на обеспечение учета гендерных аспектов кибербезопасности.

iii. С учетом того, что объекты критической инфраструктуры могут относиться к сфере ответственности разных субъектов различной организационной формы, государствам следует по возможности и в консультации с соответствующими заинтересованными сторонами содействовать внедрению минимальных стандартов безопасности критически важной инфраструктуры и способствовать сотрудничеству с частным сектором, научными кругами и техническим сообществом в усилиях по защите критически важной инфраструктуры.

iv. Государствам следует по возможности участвовать в добровольных инициативах по оценке рисков и планированию мероприятий по обеспечению бесперебойного функционирования (устойчивость, восстановление и непредвиденные обстоятельства), в которых участвуют другие заинтересованные стороны и которые направлены на повышение безопасности и устойчивости критически важных объектов инфраструктуры, задействованных на региональном или международном уровнях, перед лицом существующих и нарождающихся угроз.

v. Усилия по защите объектов критически важной информационной инфраструктуры следует предпринимать с должным учетом применимых национальных законов, касающихся защиты частной жизни, и другого соответствующего законодательства.

vi. При подготовке указаний по осуществлению норм f) и g) государствам следует учитывать, что выделение отдельных секторов в качестве объектов

критически важной инфраструктуры не предполагает составления исчерпывающих перечней и не влияет на определение государством какого-либо другого сектора в качестве приоритетного, а также не означает косвенного попустительства в отношении злонамеренных действий против какой-либо категории объектов, не включенной в перечень.

vii. РГОС подчеркнула, что все государства рассматривают инфраструктуру системы здравоохранения, медицинские службы и медицинские учреждения в качестве объектов критически важной инфраструктуры для целей норм f) и g). С учетом того, что РГОС вела подготовку своего доклада в условиях пандемии COVID-19, необходимость подтверждения того, что инфраструктура систем здравоохранения нуждается в защите, ощущалась особенно остро.

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 (2015 ¶13 h)).

i. Осуществление этой нормы предполагает рассмотрение соответствующих просьб об оказании помощи и учет характера помощи, которая может быть своевременно предложена. Государствам, получающим должным образом оформленную просьбу об оказании помощи после инцидента в сфере ИКТ, следует, когда это возможно, рассматривать ее как обоснованную и надлежащую и в этой связи сделать следующее:

– подтвердить получение просьбы через соответствующий национальный контактный центр;

– оперативно определить, располагает ли оно возможностями и ресурсами для оказания запрашиваемой помощи. Для этого может потребоваться уточнение у ряда заинтересованных сторон информации об имеющихся в стране знаниях и опыте;

– в своем первоначальном ответе государство указывает характер, объем и условия оказания помощи, которая может быть предоставлена, включая сроки ее предоставления;

– в случае, если оказание помощи согласовано, необходимо оперативно оказать помощь, о которой была достигнута договоренность.

– необходимо обеспечить, чтобы запрос об оказании помощи, включая соответствующие процессы и ресурсы, такие как правовые основания и типовые формы, а также ответы, соответствовали обязательствам в области прав человека.

ii. Осуществлению данной нормы будут дополнительно способствовать ранее существовавшие национальные структуры и механизмы, включая национальный контактный центр, типовые формы запросов об оказании помощи и формы

для подтверждения оказываемой помощи, а также целенаправленное наращивание потенциала и оказание технической помощи. Инициативы по двустороннему и многостороннему сотрудничеству, международные и региональные организации и форумы могут играть определенную роль в содействии их развитию.

Подходы, которые могли бы внести положительный вклад в осуществление данной нормы, могут включать расширение сотрудничества на национальном и международном уровнях между государственными учреждениями, частным сектором и организациями гражданского общества, особенно в целях принятия превентивных мер; укрепление потенциала групп реагирования на происшествия на основе целенаправленного подхода к наращиванию потенциала в области киберпространства; и специализированная подготовка в целях создания потенциала в области киберпространства на всех уровнях государственных учреждений и общества в целом.

> 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 (2015 ¶13 i)).

i. Для применения этой нормы государствам следует:

- предпринимать шаги, в том числе через существующие площадки, для предотвращения распространения злонамеренных программных и технических средств в сфере ИКТ. При этом государствам следует поощрять законную деятельность по обеспечению безопасности систем ИКТ, осуществляемую научно-исследовательскими сообществами, научными кругами, промышленными предприятиями, правоохранительными органами, группами реагирования на компьютерные происшествия/группами по расследованию происшествий в области кибербезопасности и другими учреждениями, занимающимися вопросами кибербезопасности;
- рассмотреть вопрос об обмене информацией о факторах уязвимости ИКТ и/или вредных скрытых функциях в продуктах ИКТ;
- проводить работу по внедрению средств контроля безопасности, основанных на управлении рисками.

> j. Государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться 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 (2015 ¶13 j)).

i. Для применения этой нормы государствам следует:

– создавать национальные структуры, которые позволяют со всей ответственностью сообщать о факторах уязвимости в сфере ИКТ и устранять их;

– содействовать созданию механизмов координации между субъектами государственного и частного секторов.

ii. Кроме того, во избежание недоразумений или неправильного толкования, в том числе в результате нераскрытия информации о потенциально вредных факторах уязвимости в сфере ИКТ, государствам рекомендуется в максимально широком объеме обмениваться, когда это целесообразно, технической информацией о серьезных инцидентах в сфере ИКТ, используя существующие координационные механизмы в рамках групп реагирования на компьютерные происшествия и групп по расследованию происшествий в области кибербезопасности, а также механизмы, созданные региональными организациями (такие, как сети контактных центров). Государствам следует обеспечивать, чтобы такая информация обрабатывалась ответственно и, при необходимости, в координации с другими заинтересованными сторонами.

k. Государства не должны заведомо осуществлять и поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группами готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности (2015 ¶13 k)).

Китай

• Государства должны взять на себя обязательство не использовать ИКТ и ИКТ-сети для осуществления деятельности, противоречащей задаче поддержания международного мира и безопасности.

Государственный суверенитет в киберпространстве

• Государствам следует на своей территории распространять свою юрисдикцию на ИКТ-инфраструктуру и ИКТ-ресурсы, а также на деятельность, связанную с ИКТ.

• Государства имеют право проводить государственную политику в сфере ИКТ сообразно национальным условиям для распоряжения собственными делами в сфере ИКТ и защиты законных интересов своих граждан в киберпространстве.

• Государствам следует воздерживаться от использования ИКТ для вмешательства во внутренние дела других государств и подрыва их политической, экономической и социальной стабильности.

• Государствам следует на равноправной основе участвовать в распоряжении международными Интернет-ресурсами и их распределении.

Защита критически важной инфраструктуры

• Государства имеют права и обязанности в отношении правовой защиты их критически важных ИКТ-инфраструктур от ущерба, возникшего в результате угроз, вмешательства, нападений и саботажа.

• Государствам следует воздерживаться от кибератак на критически важные инфраструктуры других государств.

• Государствам не следует использовать политические и технические преимущества для подрыва безопасности и целостности критически важных инфраструктур других государств.

• Государствам следует расширять обмен стандартами и передовым опытом в области защиты критически важных инфраструктур и поощрять предприятия к таким обменам.

Безопасность данных

• Государствам следует применять сбалансированный подход в отношении технического прогресса, развития предпринимательства и защиты национальной безопасности и общественных интересов.

• Государства имеют права и обязанности по обеспечению безопасности личной информации и важных данных, связанных с национальной безопасностью, общественной безопасностью, экономической безопасностью и социальной стабильностью.

• Государствам не следует осуществлять или поддерживать шпионаж с использованием ИКТ в отношении других государств, включая массовое наблюдение и хищение важных данных и личной информации.

• Государствам следует уделять равное внимание как развитию, так и безопасности и добиваться законной, упорядоченной и свободной передачи данных. Государствам следует содействовать обмену передовым опытом и сотрудничеству в этой области.

Безопасность цепочек поставок

• Государствам не следует использовать свое доминирующее положение в сфере ИКТ, в том числе доминирующее положение в отношении ресурсов, критически важных ИКТ-инфраструктур и основных технологий, товаров и услуг в сфере ИКТ, для ущемления права других государств на независимый контроль над товарами и услугами в сфере ИКТ, а также компрометации их безопасности.

• Государствам следует запретить поставщикам товаров и услуг в сфере ИКТ незаконно получать данные пользователей, контролировать пользовательские устройства и системы и манипулировать ими, создавая в продуктах пути обхода систем защиты. Государствам следует также запретить поставщикам товаров и услуг в сфере ИКТ преследовать свои незаконные интересы, пользуясь зависимостью пользователей от их продукции или вынуждая пользователей обновлять свои системы или устройства. Государствам следует обратиться к поставщикам товаров и услуг в сфере ИКТ с просьбой взять на себя обязательство своевременно уведомлять своих партнеров по сотрудничеству и пользователей в случае обнаружения в их продуктах серьезных факторов уязвимости.

• Государствам следует проявлять приверженность созданию справедливой, равноправной и недискриминационной деловой среды. Государствам не следует использовать национальную безопасность в качестве предлога для ограничения развития и сотрудничества в сфере ИКТ и ограничения доступа на рынки для продукции ИКТ и экспорта высокотехнологичной продукции.

Борьба с терроризмом

• Государствам следует запретить террористическим организациям использовать Интернет для создания веб-сайтов, онлайновых форумов и блогов для осуществления террористической деятельности, включая производство, воспроизводство, хранение и трансляцию аудио- и видеоматериалов террористического характера, распространение агрессивной террористической риторики и идеологии, сбор средств, вербовку, подстрекательство к террористической деятельности и т.д.

• Государствам следует осуществлять обмен разведывательными данными и сотрудничество между правоохранительными органами в сфере борьбы с терроризмом. Например, по поступившему от других государств запросу, связанному с террористической деятельностью в киберпространстве, государству следует обеспечить оперативный сбор в сети Интернет соответствующих данных и доказательств и их хранение, оказать помощь в проведении расследования и обеспечить своевременное реагирование.

• Государствам следует развивать на основе сотрудничества партнерские отношения с международными организациями, предприятиями и гражданами в борьбе с кибертерроризмом.

• Государствам следует обратиться к Интернет-провайдерам с просьбой перекрывать онлайновые каналы распространения материалов террористической направленности, блокируя веб-сайт и учетные записи, с которых ведется пропаганда, и удаляя материалы террористического и экстремистского толка.

Словения, Финляндия, Франция и Хорватия

• Государства следует поощрять к принятию мер, препятствующих осуществлению негосударственными субъектами, включая частный сектор, деятельности с использованием ИКТ в своих собственных целях или в целях других негосударственных субъектов в ущерб третьим сторонам, в том числе тем, которые находятся на территории другого государства.

• Эта цель может быть достигнута посредством сотрудничества с частным сектором в определении допустимых действий с использованием подхода, основанного на оценке риска, и в разработке конкретных инструментов: процессов сертификации, руководств по передовой практике, механизмов реагирования на инциденты и, в соответствующих случаях, национальных нормативных актов.

Куба

Сложившаяся ситуация требует осуществления конкретных положений, дополняющих международное право и направленных, в частности, на решение следующих не менее важных задач:

- предотвращение применения односторонних мер и направленных против государств мер, препятствующих всеобщему доступу к преимуществам от использования ИКТ;

- смягчение негативных последствий установления ответственности в условиях совершения кибератак;

- предотвращение милитаризации киберпространства;

- обеспечение более эффективной защиты личных данных граждан посредством содействия принятию в этой сфере международных норм;

- дополнение законодательства о кибертерроризме в целях противодействия инцидентам и проблемам, связанным с кибербезопасностью, таким как кибератаки; выработка на основе консенсуса определения кибератаки;

- практическое применение, с большей объективностью, принципов международного права в этой области.

Чешская Республика

- Государства не должны осуществлять или сознательно поддерживать в киберпространстве деятельность, которая может нанести ущерб медицинским службам или медицинским учреждениям, и должны принимать меры по защите медицинских служб от причинения вреда[14].

- Необходимо соблюдать существующие обязательства по международному праву прав человека при рассмотрении, разработке и применении национальной политики и законодательства в области кибербезопасности[15].

- Необходимо учитывать мнения всех соответствующих и затронутых заинтересованных сторон на самом раннем этапе разработки политики в области кибербезопасности для обеспечения всестороннего рассмотрения последствий мер по обеспечению кибербезопасности для прав человека[16].

Эквадор

- Указание относительно нормы 13 b) (доклад группы правительственных экспертов 2015 года)[17]:

i) Государства могли бы создать структуры, установить регламенты, процессы и координационные механизмы, необходимые для содействия тщательному рассмотрению серьезных инцидентов в сфере ИКТ и определения надлежащих мер реагирования;

ii) затем государства могли бы разработать типовые формы для описания инцидентов в сфере ИКТ или степени их значимости, с тем чтобы оценивать и анализировать инциденты в сфере ИКТ;

[14] URL: https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-buildinternational-law.

[15] URL: https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[16] URL: https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[17] Государства должны изучить в случае инцидентов в сфере ИКТ всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности в ИКТ-среде, а также характер и масштабы ответственности.

iii) транспарентность таких типовых форм и их унификация региональными организациями могли бы обеспечить общность подходов государств к рассмотрению инцидентов в сфере ИКТ и улучшить коммуникацию между государствами;

iv) при рассмотрении всей релевантной информации, касающейся происшествия в сфере ИКТ, государствам следует изучать возможные гендерно-дифференцированные последствия и проводить совместную работу со всеми заинтересованными сторонами, с тем чтобы понимать более широкий контекст инцидента в сфере ИКТ, включая его воздействие на осуществление прав женщин.

• Для осуществления нормы 13 c)[18] предлагаются следующие указания:

i) Если государство обнаруживает, что злонамеренная кибердеятельность осуществляется с территории другого государства или с использованием его киберинфраструктуры, то первым шагом может стать уведомление этого государства. Группы реагирования на компьютерные происшествия имеют крайне важное значение для возможностей выявлять такую деятельность.

ii) С учетом того, что инциденты в сфере ИКТ могут быть спровоцированы с территории третьих государств или при их участии, подразумевается, что уведомление государства не означает ответственности такого государства за инцидент.

iii) Получившему уведомление государству следует подтвердить получение запроса через национальный контактный центр.

iv) Когда государству известно, что его территория или киберинфраструктура используются для совершения международно-противоправного деяния, которое может привести к серьезным неблагоприятным последствиям в государстве, первому государству следует попытаться принять разумные, доступные и практически осуществимые меры в пределах своей территории и возможностей в соответствии со своими обязательствами по внутреннему и международному праву, с тем чтобы добиться прекращения международно-противоправного деяния или смягчить его последствия.

v) Эту норму не следует интерпретировать как требование к государству осуществлять опережающий мониторинг всех ИКТ на своей территории или принимать другие превентивные меры.

vi) Государство, которому стало известно об осуществляемой с его территории вредоносной деятельности в сфере ИКТ и которое не располагает возможностями для реагирования, может по своему усмотрению обратиться за помощью к другим государствам, в том числе используя для этого типовые формы запросов об оказании помощи.

vii) В таких случаях помощь может запрашиваться у других государств или у частной организации в порядке, установленном национальным законодательством. Приверженность государств сотрудничеству с другими странами и оказанию им помощи в случае кризиса имеет важное значение; при этом следует особо учитывать, что инциденты в сфере ИКТ могут по-разному повлиять на конкретные объекты инфраструктуры развивающихся стран.

• В проект следует также включить новые нормы, в том числе следующую:

[18] Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

«Государства не должны осуществлять с использованием ИКТ операции, направленные на разрушение технической инфраструктуры, имеющей важнейшее значение для политических процессов, таких как выборы, референдумы или плебисциты».

Индия

• (Относительно ПУНКТА 39): Предложение о новой норме, касающейся необходимости принятия согласованного стандарта основных параметров безопасности в киберпространстве в отношении наиболее эффективных способов оптимизации использования перспективных технологий при одновременной защите интересов общества. Для этого государства должны решительно поддержать повсеместное принятие и гарантированное внедрение основных правил личной безопасности в киберпространстве.

• Защита критически важной информационной инфраструктуры является одним из элементов ответственного поведения государств. Угроза критически важной информационной инфраструктуре может нарушить целостность информации и навредить экономике и экономическому развитию страны. Государства должны рассмотреть вопрос о защите критически важной информационной инфраструктуры на основе государственно-частного партнерства. Государства не должны проводить с использованием ИКТ операции, направленные на нарушение функционирования критически важной информационной инфраструктуры. Государства не должны закладывать вредные функции в ИКТ-продукты. Государства должны нести ответственность за уведомление пользователей при выявлении существенных факторов уязвимости и уведомление поставщиков, которые должны устранять такие факторы уязвимости. Государства должны сотрудничать в сфере критически важной информационной инфраструктуры, обмениваться информацией об угрозах и инструментах и методах смягчения их последствий.

Исламская Республика Иран

• Роль государств, несущих главную ответственность за поддержание безопасной, надежной и заслуживающей доверия ИКТ-среды, должна быть усилена в том, что касается управления ИКТ-средой, включая политику и принятие решений на глобальном уровне. Такого рода управление ИКТ-средой должно осуществляться таким образом, чтобы укреплять государственный суверенитет и не затрагивать права государств при выборе ими моделей развития, управления и законодательства в ИКТ-среде.

• Государства должны воздерживаться от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства в рамках и посредством ИКТ-среды.

• Ни одно государство не имеет права прямо или косвенно и по какой бы то ни было причине вмешиваться во внутренние или внешние дела других государств с использованием киберсредств. Все формы вмешательства и воздействия или попытки угроз в отношении политических, экономических, социальных и культурных систем, а также в отношении связанной с киберпространством критически важной информационной инфраструктуры государств должны осуждаться и предотвращаться (резолюция 2131 Генеральной Ассамблеи Организации Объединенных Наций от 21 декабря 1965 года).

• Государства не должны использовать достижения в сфере ИКТ в качестве инструментов для принятия экономических, политических или любых других видов принудительных мер, включая меры ограничительного или блокирующего характера против отдельных государств (резолюция 2131 Генеральной Ассамблеи Организации Объединенных Наций от 21 декабря 1965 года).

• Государства должны обеспечивать принятие надлежащих мер, с тем чтобы предприятия частного сектора, деятельность которых имеет экстерриториальные последствия, включая платформы, несли ответственность за свою деятельность в ИКТ-среде. Государства должны осуществлять полноценный контроль за ИКТ-компаниями и платформами, находящимися под их юрисдикцией, в противном случае они несут ответственность за намеренное нарушение национального суверенитета, безопасности и общественного порядка других государств.

• Государства должны воздерживаться от злоупотреблений и предотвращать злоупотребления в отношении разработанных под их контролем и юрисдикцией цепочек поставок в сфере ИКТ; такие злоупотребления осуществляются в целях создания или содействия созданию факторов уязвимости продуктов, товаров и услуг, что наносит ущерб суверенитету и сохранности данных отдельных государств.

Япония

Новое предложение Японии в адрес РГОС заключается в добавлении следующей формулировки в качестве указания к норме i) по обеспечению целостности цепочек поставок:

• «Государства имеют право и несут ответственность за обеспечение использования проверенных поставщиков и продавцов оборудования и систем ИКТ, в особенности при решении вопросов, касающихся национальной безопасности и защиты частной жизни. Разумные шаги в этой связи могут включать принятие законодательства или административных мер для обеспечения безопасности цепочек поставок, поддержки развития надежных и заслуживающих доверия технологий и промышленных решений и для диверсификации поставщиков».

Нидерланды

• «Государственные и негосударственные субъекты не должны вести или сознательно допускать деятельность, которая намеренно и существенно нарушает общедоступность или надежность основного ядра Интернета и, следовательно, стабильность киберпространства» — [такая формулировка могла бы использоваться как] указание, касающееся выполнения рекомендации 13 f), содержащейся в докладе группы правительственных экспертов Организации Объединенных Наций 2015 года, и, соответственно, подводящее его также под сферу действия рекомендации 13 g), содержащейся в докладе группы правительственных экспертов Организации Объединенных Наций 2015 года.

• «Государственные и негосударственные субъекты не должны осуществлять, поддерживать или допускать кибероперации, направленные на разрушение технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов» — [такая формулировка могла бы использоваться как] указание, касающееся выполнения рекомендации 13 f), содержащейся в докладе группы правительственных экспертов Организации Объединенных Наций 2015 года, и, соответственно, подводящее его также под сферу действия

рекомендации 13 g), содержащейся в докладе группы правительственных экспертов Организации Объединенных Наций 2015 года.

Движение неприсоединения

- Следует рекомендовать государствам-членам подготавливать и упорядочивать информацию, которую они представляют относительно выполнения ими международных норм и относительно соответствующего предлагаемого хранилища, в целях регулирования конкретных аспектов использования ИКТ государствами с точки зрения международной безопасности и в целях выявления областей, которые вызывают обоюдную озабоченность.

- Государства-члены не должны проводить или сознательно поддерживать любые мероприятия в сфере ИКТ, которые в нарушение международного права преднамеренно наносят ущерб или вред в том, что касается использования и функционирования критически важной инфраструктуры других государств-членов.

- Следует настоятельно призвать государства-члены рассмотреть вопрос об обмене информацией о факторах уязвимости ИКТ и/или вредных скрытых функциях в ИКТ-продуктах, а также призвать их уведомлять пользователей в случае выявления существенных факторов уязвимости.

- Государствам-членам следует также учитывать резолюцию 73/27 Генеральной Ассамблеи Организации Объединенных Наций при осуществлении любой деятельности, связанной с ИКТ.

- Движение неприсоединения вновь заявляет о своей глубокой обеспокоенности по поводу все более широкого применения одностороннего подхода и в этой связи подчеркивает, что в соответствии с Уставом Организации Объединенных Наций многосторонность и согласование решений на многосторонней основе представляют собой единственный надежный способ решения вопросов международной безопасности.

- Движение неприсоединения вновь заявляет, что все государства должны воздерживаться от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства в рамках и посредством ИКТ-среды.

- Движение неприсоединения призывает активизировать усилия, направленные на то, чтобы киберпространство не превратилось в арену конфликтов, а обеспечило бы исключительное мирное использование, которое позволило бы в полной мере реализовать потенциал ИКТ для содействия социально-экономическому развитию.

- Движение неприсоединения подчеркивает важность недопущения неоправданных ограничений, в том числе посредством односторонних принудительных мер, на использование ИКТ в мирных целях, международное сотрудничество или передачу технологий.

- Движение неприсоединения подчеркивает, что государства несут главную ответственность за то, чтобы ИКТ-среда оставалась открытой, безопасной, стабильной, доступной и мирной.

- Движение неприсоединения подчеркивает, что государства не должны преднамеренно осуществлять или поддерживать деятельность в сфере ИКТ, противоречащую их обязательствам по международному праву и преднамеренно

наносящую ущерб или вред в том, что касается использования и функционирования критически важной инфраструктуры.

Пакистан

- Следует поощрять государства-члены к тому, чтобы они и далее рассматривали по мере необходимости возможность принятия юридически и/или политически обязывающего нормативного акта (актов) для регулирования конкретных аспектов использования ИКТ государствами в контексте международной безопасности.

- Государствам-членам следует рекомендовать выработать согласованное общее определение «критически важной инфраструктуры», с тем чтобы достичь договоренности о запрещении деятельности в сфере ИКТ, которая наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры.

- Следует поощрять государства-члены сотрудничать в целях достижения договоренности о запрещении включения в ИКТ-продукты вредоносных скрытых функций или накопления факторов уязвимости, а также взять на себя обязательство ответственно и своевременно представлять информацию о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости.

- Государствам-членам следует стремиться содействовать сотрудничеству с поставщиками ИКТ-продуктов и услуг, с тем чтобы предотвратить недобросовестное использование ими личных данных пользователей или сведений о частной жизни и злоупотребление такими данными и сведениями.

- Государства-члены должны взять на себя обязательство не использовать ИКТ для осуществления деятельности, противоречащей задаче поддержания международного мира и безопасности, и воздерживаться от использования ИКТ для вмешательства каким-либо образом во внутренние дела других государств.

- Государства-члены должны сотрудничать в целях решения проблем, связанных с установлением ответственности в ИКТ-среде. Разработка общего подхода к установлению ответственности в рамках универсальной процедуры под эгидой Организации Объединенных Наций остается наиболее эффективным способом продвижения вперед в этом направлении.

- Необходимо настоятельно призвать государства-члены прийти к соглашению о запрещении деятельности в сфере ИКТ, направленной на разрушение технической инфраструктуры, необходимой для проведения выборов, референдумов или плебисцитов.

- Следует поощрять государства-члены к разработке и применению норм таким образом, который позволял бы избежать необоснованных ограничений на использование ИКТ в мирных целях, международное сотрудничество в этой области или передачу технологий.

Республика Корея

Предложение, касающееся указания в отношении пункта 13 c) доклада группы неправительственных экспертов 2015 года:

- Когда затронутое государство уведомляет другое государство о том, что инциденты в сфере ИКТ были спровоцированы с территории уведомляемого государства или при его участии, и сопровождает это проверенной информацией, получающее уведомление государство должно, в соответствии с международным правом и внутренним законодательством и в рамках своих возможностей, предпринять все разумные шаги на своей территории, с тем чтобы прекратить эту деятельность или смягчить ее последствия.

- Следует понимать, что такое уведомление не подразумевает ответственности получающего уведомление государства за инцидент.

- К числу минимальных требований к проверенной информации могут относиться индикаторы компрометации, такие как IP-адрес, местонахождение нарушителей и компьютеров, использованных для злонамеренных действий с использованием ИКТ, и данные о вредоносных программах.