Организация Объединенных Наций A/AC.290/2021/L.2

Генеральная Ассамблея

Distr.: Limited
19 January 2021
Russian
Original: English

Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Проект предметного доклада (первоначальный проект)*

A. Введение

1. С момента создания Организации Объединенных Наций 75 лет назад в мире произошли радикальные преобразования, однако ее цель и всегда актуальные идеалы сохраняют свое основополагающее значение. Государства обязались содействовать уважению прав человека и основных свобод, экономическому и социальному прогрессу всех народов и созданию условий для поддержания уважения к международному праву, а также заявили о решимости объединить силы для обеспечения международного мира и безопасности.

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 на общее благо человечества, ИКТ и глобальная связь играют роль катализатора прогресса и развития человека.

3. Сегодня как никогда очевидна насущная необходимость создания и поддержания доверия и безопасности в цифровой среде. 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 использовании 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 поддержанию социальной сплоченности с помощью средств виртуализации. В нынешних условиях неопреде-

* Настоящий документ публикуется без официального редактирования.

Просьба отправить на вторичную переработку

ленности 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 Ассамблея отметила[1], 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 без исключения государствам 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 последней 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[2]. В трех принятых на основе консенсуса докладах (от 2010, 2013 и 2015 годов[3]), которые носят обобщающий характер, эти группы подтвердили применимость норм международного права, в частности положений Устава Организации Объединенных Наций, и их ключевое значение для поддержания мира и стабильности в контексте ИКТ. В них также содержались рекомендации в отношении 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств и констатировалось, 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 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.

8. Опираясь на этот фундамент, РГОС стремилась найти точки соприкосновения и взаимопонимания между всеми государствами — членами Организации Объединенных Наций по вопросу общемировой значимости. Во имя достижения консенсуса с целью содействовать установлению и поддержания доверия в

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

своих обсуждениях она руководствовалась принципами всеохватности и прозрачности. 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.

9. 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[4]. 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.

10. С учетом различий в условиях, возможностях и приоритетах государств и регионов РГОС считает, что в цифровой сфере государства несут как индивидуальную, так и совместную ответственность. 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 расширения доступа к ИКТ и возможностей подключения к сети.

11. 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.

12. РГОС учитывает важность и взаимодополняющий характер специализированных обсуждений аспектов цифровых технологий в рамках других органов и форумов Организации Объединенных. Речь идет о вопросах, касающихся устойчивого развития, прав человека (в том числе защиты данных и неприкосновенности частной жизни, свободы выражения мнений и свободы информации), сотрудничества в цифровой сфере, управления Интернетом, киберпреступности и использования Интернета в террористических целях.

13. РГОС подчеркивает, что отдельные элементы ее мандата связаны между собой и взаимно подкрепляют друг друга и в своей совокупности способствуют

[4] See “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/.

созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Основой для действий государств является международное право, а его нормы дополнительно определяют ожидания в отношении ответственного поведения государств. Меры, направленные на укрепление доверия и потенциала, способствуют соблюдению норм международного права, стимулируют их перевод в практическую плоскость, открывают возможности для расширения сотрудничества между государствами и дают каждому государству возможность пользоваться преимуществами ИКТ в интересах своих граждан и экономики.

14. С учетом взаимоусиливающего характера этих элементов нижеследующие разделы настоящего доклада носят взаимодополняющий и взаимозависимый характер. Каждый из нижеследующих разделов (B–G) начинается с обзора мнений, высказанных в ходе обсуждения вопросов существа в Рабочей группе открытого состава, с последующим перечислением областей совпадения взглядов и конкретных рекомендаций.

B. Существующие и потенциальные угрозы

15. В ходе обсуждений в РГОС государства затронули широкий круг существующих и потенциальных угроз, что наглядно показало, что государства могут поразному воспринимать угрозы связанные с цифровой сферой. 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.

Обсуждение

16. Некоторые государства выразили озабоченность по поводу разработки или использования ИКТ в военных 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. 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.

17. 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 технический прогресс и новые прикладные программы могут не только создавать возможности в плане развития, но и расширять поле для атак, усиливать действие факторов уязвимости в ИКТ-среде или использоваться для осуществления новых вредоносных видов деятельности. 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.

Выводы

18. 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. Вредоносные происшествия в сфере ИКТ становятся все более частыми, целенаправленными и изощренными и постоянно эволюционируют и видоизменяются. Расширение коммуникационных возможностей и зависимость от ИКТ могут 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.

19. Продолжающееся увеличение числа инцидентов, связанных со злонамеренным использованием ИКТ государственными и негосударственными субъектами, включая посредников, является, по общему мнению государств, тревожной тенденцией. Как выясняется, некоторые негосударственные субъекты располагают такими возможностями использования ИКТ, которые ранее были доступны только государствам, в связи с чем была выражена озабоченность по поводу того, что эти возможности могут быть использованы для совершения террористических актов или преступных действий.

20. По общему мнению государств, всякое использование ИКТ государствами в целях, противоречащих их закрепленному в Уставе обязательству жить вместе, в мире друг с другом, как добрые соседи, а также другим их обязательствам по международному праву, подрывает доверие и стабильность в отношениях между государствами, что может увеличить риск неправильного восприятия и вероятность будущих межгосударственных конфликтов.

21. Государства согласились с тем, что нападения на объекты критически важной инфраструктуры и объекты критически важной информационной инфраструктуры, обеспечивающие оказание основных услуг населению, таких как медицинские учреждения и предприятия энергоснабжения, водоснабжения, транспорта и санитарии, могут иметь катастрофические гуманитарные последствия. Реальную и растущую озабоченность вызывают также такие нападения на объекты критически важной инфраструктуры и объекты критически важной информационной инфраструктуры, которые направлены на подрыв доверия к политическим и избирательным процессам и государственным институтам или на нарушение функционирования финансовой системы. 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.

22. Кроме того, использование ИКТ для нарушения работы, повреждения или уничтожения объектов критически важной инфраструктуры и объектов критически важной информационной инфраструктуры, по общему мнению государств, представляет угрозу не только для безопасности, но и для экономического развития и источников дохода и, в конечном счете, для безопасности и благополучия людей.

23. Поскольку все страны все шире пользуются цифровыми технологиями, отсутствие осведомленности и надлежащих возможностей для выявления злоумышленных действий с использованием ИКТ, защиты от них или реагирования на них, является, по общему мнению государств, непростой проблемой. Как наглядно показала нынешняя чрезвычайная ситуация в области здравоохранения в мире, во время кризиса действие существующих факторов уязвимости может многократно усилиться.

24. Государства согласились с тем, что в зависимости от уровня 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.

25. Учитывая все более тревожную обстановку в плане цифровых угроз и принимая во внимание, что от этих угроз не защищено ни одно государство, государства приняли решение о том, 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.

C. Международное право

26. Для продвижения к общему пониманию в вопросе о применимости международного права к использованию ИКТ государствами, государства, руководствуясь мандатом Группы, провели обмен мнениями о применимости международного права (общих принципов права, договоров и обычного международного права) в вопросах, касающихся ИКТ в контексте международной безопасности.

Обсуждение

27. В ходе обсуждений в рамках РГОС государства вновь указали, что международное право, и в частности Устав Организации Объединенных Наций, в полной мере применимо и имеет ключевое значение для поддержания мира и стабильности и содействия обеспечению открытой, безопасной, мирной и доступной ИКТ-среды. В то же время государства подчеркнули, что вопрос о применимости международного права к использованию ИКТ государствами требует дальнейшей проработки.

28. К упоминавшимся в ходе обсуждений конкретным принципам Устава Организации Объединенных Наций относятся, в частности, 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[5].

29. 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.

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

31. 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.

32. 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 некоторые 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.

33. 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,

[5] См. шестнадцатый пункт преамбулы резолюции 73/27 Генеральной Ассамблеи.

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

34. 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. Речь, в частности, идет о таких видах 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.

35. 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. Было отмечено, что такой обмен мнениями сам по себе может служить важной мерой укрепления доверия. Кроме того, государства предложили несколько способов добровольного обмена национальными мнениями по вопросу о международном праве, включая использование ежегодного доклада Генерального секретаря о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности или проведение 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.

36. В связи с вопросом поддержания мира и предотвращения конфликтов было отмечено, что можно было бы также уделять больше внимания урегулированию споров 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.

Выводы и рекомендации

37. Во исполнение резолюции 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, мирной и доступной ИКТ-среды. Государства также согласились с тем, что необходимо продолжить работу над углублением общего понимания применимости международного права к использованию ИКТ государствами.

38. Государства также подтвердили важность урегулирования споров мирными средствами, в том числе путем переговоров, проведения расследований, посредничества, примирения, арбитража, судебного разбирательства и обращения к региональным учреждениям или механизмам.

39. Государства согласились с тем, что достижению общего понимания применимости международного права к использованию ИКТ государствами может способствовать как развитие обмена мнениями по этому вопросу между государствами, так и определение для дальнейшего углубленного обсуждения конкретных вопросов международного права.

40. С тем чтобы обеспечить выработку всеми государствами собственного понимания вопросов применимости международного права к использованию ИКТ государствами и содействовать формированию консенсуса в международном сообществе, настоятельно 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

41. Государствам следует продолжать добровольно информировать Генерального секретаря о национальных взглядах и практике в отношении применимости международного права к использованию ими ИКТ в контексте международной безопасности, информация о которых будет включаться в его ежегодный доклад о достижениях в области ИКТ в контексте международной безопасности.

42. Государствам следует добровольно представлять информацию о национальных взглядах и практике в отношении применимости международного права к использованию ИКТ государствами для размещения на портале по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения.

43. Государствам, которые имеют такую возможность, следует продолжать, руководствуясь соображениями непредвзятости и объективности и действуя в соответствии с принципами, содержащимися в пункте 85 настоящего доклада, поддерживать дополнительные усилия по созданию потенциала в области международного права, национального законодательства и политики, с тем чтобы все государства могли выработать собственное понимание вопросов применимости международного права к использованию ИКТ государствами и содействовать достижению консенсуса в международном сообществе.

44. Государствам следует продолжать проводить на многостороннем уровне обсуждения для содействия выработке общего понимания применимости международного права к использованию ИКТ государствами в контексте международной безопасности и рассматривать возможность осуществления дополнительных инициатив в этой связи.

D. Правила, нормы и принципы ответственного поведения государств

45. Важную роль в повышении предсказуемости и уменьшении риска неправильного восприятия, способствуя тем самым предотвращению конфликтов, играют добровольные, не имеющие обязательной силы нормы ответственного поведения государств. Государства подчеркнули, что в таких нормах отражаются ожидания международного сообщества и устанавливаются стандарты в отношении поведения государств при использовании ИКТ.

Обсуждение

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

47. Государства напомнили о том, что в принятой консенсусом резолюции 70/237 к государствам обращен призыв руководствоваться при использовании ИКТ положениями доклада группы правительственных экспертов 2015 года, в котором сформулированы 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств. Некоторые государства подчеркнули, что эти 11 согласованных норм составляют основу функционирования РГОС, а некоторые государства также напомнили о том, что в резолюции 73/27 Генеральной Ассамблеи содержится свод из 13 правил, норм и принципов ответственного поведения государств. Было отмечено, что постепенное применение добровольных норм в соответствии с национальными приоритетами и возможностями является прерогативой государств.

48. Государства подчеркнули необходимость повышения осведомленности о существующих нормах и поддержки перевода их в плоскость практического применения одновременно с постепенной 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.

49. 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.

50. В ходе обсуждений высказывались предложения в отношении дальнейшей разработки существующих норм. Государства вновь заявили о важности защиты объектов критически важной инфраструктуры, к которым должны относиться медицинские учреждения. Они также обратили внимание на важность сотрудничества в защите трансграничных или международных объектов критически важной инфраструктуры, 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»[6]. 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.

51. В дополнение к сказанному выше был подготовлен перечень внесенных в РГОС письменных предложений государств по дальнейшей проработке существующих норм, разработке указаний по их применению и выработке новых норм, который был включен в неофициальный документ для последующего размещения в Интернете[7].

52. Государства также отметили представленной в 2015 году предложение о разработке международного кодекса поведения в области информационной безопасности[8].

53. 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 партнерства можно было бы создавать, например, для обеспечения того, чтобы усилия по укреплению потенциала для устранения различий в возможностях в плане применения носили постоянный характер. Можно было бы обратиться к государствам с призывом провести необходимую информационно-разъяснительную работу и принять совместные меры для обеспечения того, чтобы различные заинтересованные стороны, включая государственный и частный сектор и гражданское общество, выполняли свои обязанности в связи с использованием ИКТ.

Выводы и рекомендации

54. Государства согласились с тем, что нормы не заменяют собой обязательства 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.

55. Пандемия COVID-19, по общему мнению государств, подчеркнула важность защиты инфраструктуры здравоохранения, включая медицинские службы и объекты, которая охватывается нормами, касающимися критически важной инфраструктуры.

56. Государства согласились с тем, что важно поддерживать и продолжать усилия по применению норм на глобальном, региональном и национальном уровне.

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

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

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

57. 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 согласились с тем, что дальнейшее развитие норм и применение существующих норм не являются взаимоисключающими, а могут происходить одновременно.

Рекомендации Рабочей группы открытого состава

58. Государствам следует добровольно анализировать национальные усилия по применению норм и продолжать информировать Генерального секретаря об этих национальных обзорах, информация о которых будет включаться в его ежегодный доклад о достижениях в области ИКТ в контексте международной безопасности. Государствам следует просить Секретариат Организации Объединенных Наций собирать полученную в результате такого анализа информацию в поддержку усилий по укреплению потенциала.

59. Государствам следует, действуя в партнерстве с соответствующими организациями, включая Организацию Объединенных Наций, разрабатывать дополнительные добровольные указания по осуществлению норм ответственного государственного поведения и широко распространять эти добровольные указания на национальном, региональном, межрегиональном и глобальном уровне. Государствам, которые в состоянии предоставить специалистов или ресурсы для подготовки и распространения таких руководящих принципов, следует делать это.

60. Государствам следует, принимая во внимание положения резолюции 70/237 и резолюции 73/27, а также при необходимости неофициальный документ с предложениями, которые были сделаны государствами в ходе работы настоящей РГОС и о которых говорится в пункте 51, продолжать рассматривать и обсуждать на многостороннем уровне вопрос о международных правилах, нормах и принципах ответственного поведения государств при использовании ИКТ в контексте международной безопасности, включая их применение.

E. Меры укрепления доверия

61. 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 быть своего рода предохранительным клапаном 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.

62. Поскольку меры укрепления доверия представляют собой добровольные обязательства, которые выполняются постепенно, они могут стать первым шагом к устранению недоверия между государствами 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 или более структурированных договоренностей и соглашений в будущем.

Обсуждение

63. 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 или доктрине, национальных взглядах на применимость международного права к использованию ИКТ государствами, а также о национальных подходах к определению критически важной инфраструктуры и классификации происшествий, связанных с ИКТ. 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. Еще одним направлением деятельности по укреплению доверия и повышению уверенности в отношении намерений и обязательств государств являются национальные меры обеспечения прозрачности, такие как добровольный обмен ответами на опрос о ходе осуществления или публикация национальных деклараций о приверженности принципам ответственного поведения государств.

64. 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.

65. Поскольку меры укрепления доверия могут разрабатываться на двустороннем, региональном или многостороннем уровне, 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 дополни-

тельных 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.

66. 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 уровне. 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.

Выводы и рекомендации

67. Государства согласились с тем, 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.

68. Кроме того, государства согласились с тем, 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.

69. Государства согласились с тем, 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.

70. 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.

71. Государства согласились с тем, что такая конкретная мера, как создание национальных контактных центров, является не только самостоятельной мерой укрепления доверия, но и необходимым условием для осуществления многих других мер укрепления доверия и имеет неоценимое значение в условиях кризиса. Государства могут счесть целесообразным создать контактные центры, 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

72. Государствам следует продолжать добровольно информировать Генерального секретаря о своих взглядах и оценках, которые будут отражаться в его ежегодном докладе о достижениях в области ИКТ в контексте международной безопасности, и представлять дополнительную информацию об извлеченных уроках и передовой практике в отношении соответствующих мер укрепления доверия на двустороннем, региональном или многостороннем уровне.

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

74. В качестве меры укрепления доверия государствам следует публично подтвердить обязательство руководствоваться при использовании ИКТ положениями доклада группы правительственных экспертов 2015 года[9].

75. 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.

76. Государствам, которые еще не сделали этого, следует, учитывая различия в возможностях, создавать национальные контактные центры, в частности, на техническом, политическом и дипломатическом уровне. Государствам следует также продолжать рассматривать способы создания справочника таких контактных центров на глобальном уровне.

77. 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.

78. Государствам следует продолжать рассматривать вопрос о мерах укрепления доверия на двустороннем, региональном и многостороннем уровне и способствовать созданию возможностей для совместного осуществления мер укрепления доверия.

[9] A/70/174, см. также резолюцию 70/237 Генеральной Ассамблеи.

F. Укрепление потенциала

79. Способность международного сообщества предотвращать вредоносную деятельность в области ИКТ или смягчать ее последствия зависит от возможностей каждого государства в плане обеспечения готовности и реагирования. 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. Укрепление потенциала является важным аспектом международного сотрудничества и осуществляется в добровольном порядке как передающей, так и получающей стороной. Оно играет важную вспомогательную роль, выступая стимулом для соблюдения норм международного права и реализации норм ответственного поведения государств, а также для поддержки осуществления 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.

Обсуждение

80. В ходе обсуждений в рамках РГОС государства особо отметили, что укрепление потенциала может играть важную роль в предоставлении всем государствам и другим соответствующим субъектам 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[10]. В этой связи государства подчеркнули необходимость обеспечения программ по укреплению потенциала достаточными финансовыми и людскими ресурсами.

81. 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.

82. 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 получате-

[10] 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).

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

83. 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.

84. 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.

85. 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 занима-

ются 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.

Выводы и рекомендации

86. Обеспечение открытой, безопасной, стабильной, доступной и мирной ИКТ-среды является общей, но дифференцированной ответственностью, которая требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Одним из важнейших элементов такого сотрудничества является укрепление потенциала. Принимая во внимание широко признанные принципы и необходимость их дальнейшей проработки, государства согласились с тем, 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 связи

- 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.

87. Государства согласились с тем, что деятельность по укреплению потенциала представляет собой своего рода улицу с двусторонним движением, где совместная ответственность участников дополняется их взаимными усилиями и где участники 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.

88. Государства согласились с тем, 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. 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.

89. Государства согласились с тем, 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.

90. Государства напомнили о том, что в связи с укреплением потенциала необходимо применять конкретный и ориентированный на действия подход. Государства согласились с тем, 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 отмечены выгоды от создания центров передового опыта и других механизмов обмена информацией, включая передовую правовую и административную практику.

Рекомендации Рабочей группы открытого состава

91. В своей деятельности по созданию потенциала в области ИКТ в сфере международной безопасности государствам следует руководствоваться принципами, сформулированными в пункте 86.

92. 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.

93. 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.

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

G. Регулярный институциональный диалог

95. 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.

96. В дополнение к решению задачи добиться общего понимания между всеми государствами на основе предметных обсуждений, о чем говорилось в предыдущих разделах настоящего доклада, 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, на что также указывается в принятых консенсусом докладах групп правительственных экспертов.

Обсуждение

97. 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.

98. 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.

99. 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.

100. Государства также выразили пожелание, чтобы международное сообщество в конечном счете вернулось к единому процессу, основанному на консенсусе и глобальной поддержке, с тем чтобы обеспечить коллективную ответственность за этот процесс. 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. Было предложено, чтобы РГОС разработала «дорожную карту», в которой были бы определены приоритетные темы и вопросы, а также график будущего регулярного институционального диалога.

101. 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.

102. 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, и поэтому ведется в Первом комитете Генеральной Ассамблеи. Рассматривать цифровые аспекты других вопросов, включая терроризм, преступность, развитие и права человека, а также управление Интернетом, уполномочены другие органы Организации Объединенных Наций. Была высказана мысль 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.

103. 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. Формированию более устойчивой и безопасной ИКТ-среды может способствовать расширение сотрудничества и партнерских связей с участием многих заинтересованных сторон.

Выводы и рекомендации

104. Государства согласились с тем, что с учетом растущей зависимости от ИКТ и масштабов угроз, возникающих в результате их ненадлежащего использования, налицо настоятельная необходимость в углублении общего понимания, укреплении доверия и активизации международного сотрудничества.

105. Государства согласились с тем, что регулярный диалог способствует достижению общих целей укрепления международного мира, стабильности и предотвращения конфликтов в ИКТ-среде.

106. Государства указали, что главную ответственность за национальную безопасность, общественную безопасность и соблюдение законности несут государства, в связи с чем они согласились, что важно поддерживать регулярный межправительственный диалог, и подчеркнули важность определения надлежащих механизмов для взаимодействия с другими группами заинтересованных сторон в рамках будущих процессов.

107. Государства согласились с тем, что регулярный институциональный диалог в рамках Первого комитета по-прежнему должен быть сосредоточен на вопросах международного мира и безопасности, с тем чтобы не дублировать существующие мандаты, усилия и мероприятия Организации Объединенных Наций, посвященные цифровым аспектам других проблем, включая терроризм, преступность, развитие, права человека и управление Интернетом[11].

108. Государства договорились 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.

109. Государства согласились с тем, что регулярный институциональный диалог под эгидой Организации Объединенных Наций должен быть ориентированным на практические действия процессом с конкретными целями, который основан на достигнутых ранее результатах и носит всеохватный, прозрачный, консенсусный и ориентированный на результаты характер.

110. Рассмотрев основные аспекты мандата, отраженные в разделах B-F настоящего доклада, государства рекомендовали по каждому разделу набор конкретных действий и совместных мер по противодействию связанным с использованием ИКТ угрозам и содействию созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Государства также согласились с тем, что необходимо продолжать диалог, в том числе обмен национальными мнениями или передовым опытом по вопросам применимости международного права к использованию ИКТ, применение норм и их дальнейшее постепенное развитие, а также разработку и осуществление мер укрепления доверия и мер по укреплению потенциала.

[11] See background paper issued by the Chair of the OEWG, “An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme”, December 2019, URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

Рекомендации Рабочей группы открытого состава

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

112. Государствам следует учредить программу, направленную на дальнейшую реализацию существующих соглашений и обязательств, касающихся использования ИКТ государствами, которые изложены в соответствующих резолюциях Генеральной Ассамблеи, в частности в резолюции 70/237, а также выводов и рекомендаций нынешней Рабочей группы открытого состава. Такие обсуждения следует проводить в Первом комитете Генеральной Ассамблеи Организации Объединенных Наций в качестве Программы действий по содействию ответственному поведению государств в киберпространстве.

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

114. 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.

H. Заключительные замечания

115. Деятельность РГОС предоставила всем государствам историческую возможность провести под эгидой Организации Объединенных Наций целенаправленное и непрерывное обсуждение вопросов, связанных с ИКТ и международной безопасностью. Благодаря всеохватным и прозрачным обсуждениям деятельность Рабочей группы открытого состава не только позволила достичь согласия по многим вопросам, отраженным в настоящем докладе, но и стала ценной мерой укрепления 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.

116. Отличительным признаком официальных, неофициальных и виртуальных 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.

117. Деятельность РГОС наглядно продемонстрировала коллективную решимость международного сообщества продолжать совместную работу в направлении создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды на благо всех государств и народов. В ходе обсуждений в РГОС государства подчеркивали взаимосвязанный и взаимоусиливающий характер всех элементов ее мандата. Так, добровольные, не имеющие обязательной силы нормы усиливают и дополняют существующие обязательства по международному

праву. Оба этих элемента определяют 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 на основе углубления общего понимания, обмена извлеченными уроками и передовой практикой в области осуществления, укрепления доверия между государствами и укрепления потенциала всех государств.