Генеральная Ассамблея

Distr.: General
11 December 2018

Семьдесят третья сессия
Пункт 96 повестки дня

Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года

[*по докладу Первого комитета (A/73/505)*]

73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Генеральная Ассамблея,

ссылаясь на свои резолюции 36/103 от 9 декабря 1981 года, 43/78 H от 7 декабря 1988 года, 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года, 67/27 от 3 декабря 2012 года, 68/243 от 27 декабря 2013 года, 69/28 от 2 декабря 2014 года, 70/237 от 23 декабря 2015 года и 71/28 от 5 декабря 2016 года,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

особо отмечая стремление международного сообщества к мирному использованию информационно-коммуникационных технологий (ИКТ) в интересах всеобщего блага человечества и дальнейшему устойчивому развитию всех стран вне зависимости от их научного и технологического развития,

отмечая, что наращивание потенциала имеет существенно важное значение для сотрудничества государств и укрепления доверия в области обеспечения безопасности в сфере использования ИКТ,

признавая, что некоторым государствам может потребоваться помощь в связи с их усилиями по преодолению разрыва в уровне потенциала в области безопасности при использовании ИКТ и самих ИКТ,

отмечая, что оказание по запросу помощи в деле наращивания потенциала в сфере обеспечения безопасности при использовании ИКТ имеет существенно важное значение для международной безопасности,

подтверждая, что меры по наращиванию потенциала должны способствовать использованию ИКТ в мирных целях,

подтверждая также, что ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях,

выражая обеспокоенность, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей, а использование ИКТ в будущих конфликтах становится все более вероятным,

подчеркивая, что все государства заинтересованы в поощрении использования ИКТ в мирных целях с целью создания для человечества сообщества общего будущего в киберпространстве и что государства также заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ,

отмечая, что Организация Объединенных Наций должна играть ведущую роль в поощрении диалога между государствами-членами для выработки общего понимания в отношении обеспечения безопасности при использовании ИКТ и самих ИКТ, а также в выработке единого понимания в вопросах применимости международного права и норм, правил и принципов ответственного поведения государств в этой сфере, поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта,

выражая озабоченность по поводу возможности включения в ИКТ скрытых вредоносных функций, которые могут использоваться для подрыва безопасности и надежности использования ИКТ и всей системы производства и сбыта информационных товаров и информационно-технических услуг, а также для подрыва доверия между контрагентами в сфере торговли и причинения ущерба национальной безопасности,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

подчеркивая важность уважения прав человека и основных свобод в сфере использования ИКТ,

приветствуя результативную работу Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленные в итоге соответствующие доклады, препровожденные Генеральным секретарем[1],

приветствуя содержащийся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 года[2] вывод при рассмотрении вопроса о применимости норм международного права к использованию ИКТ государствами, что важнейшее значение имеют обязанности государств в соответствии со следующими принципами Устава Организации Объединенных Наций и другими нормами международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или ее применения как

[1] A/65/201, A/68/98 и A/70/174.

[2] A/70/174.

против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединенных Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств,

подтверждая содержащийся в докладах Группы правительственных экспертов 2013[3] и 2015[2] годов вывод, что международное право, и в частности Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания международного мира и стабильности, а также создания открытой, безопасной, стабильной, доступной и мирной информационной среды, что добровольные и необязывающие нормы, правила и принципы ответственного поведения государств в сфере использования ИКТ могут снизить риск нарушения международного мира, безопасности и стабильности и что с учетом уникальных особенностей ИКТ могут быть разработаны дополнительные нормы,

подтверждая, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территории,

вновь подтверждая право и обязанность государства бороться, в рамках своих конституционных полномочий, против распространения фальшивых или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств или как наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями,

осознавая обязанность государства воздерживаться от любых клеветнических кампаний, оскорбительной или враждебной пропаганды с целью осуществления интервенции или вмешательства во внутренние дела других государств,

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

1. *приветствует* следующий свод международных правил, норм и принципов ответственного поведения государств, закрепленных в докладах групп правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013[3] и 2015[2] годов, принятых консенсусом и рекомендованных резолюцией «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 71/28, принятой Генеральной Ассамблеей 5 декабря 2016 года:

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

[3] A/68/98.

1.2 Государства должны выполнять свои международные обязательства в отношении международно-противоправных деяний, приписываемых им в соответствии с международным правом. Вместе с тем 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 недостаточным для присвоения этой деятельности указанному государству. Обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. 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.

1.3 Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и использовать посредников для совершения международно-противоправных деяний с использованием ИКТ и должны стремиться обеспечивать, чтобы их территории не использовались негосударственными субъектами для совершения таких деяний.

1.4 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 рассмотреть вопрос о разработке новых мер в этой сфере.

1.5 Государства в процессе обеспечения безопасного использования ИКТ должны соблюдать положения резолюций Совета по правам человека 20/8 от 5 июля 2012 года[4] и 26/13 от 26 июня 2014 года[5] о поощрении, защите и осуществлении прав человека в Интернете и резолюций Генеральной Ассамблеи 68/167 от 18 декабря 2013 года и 69/166 от 18 декабря 2014 года о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение.

1.6 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.

1.7 Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи от 23 декабря 2003 года о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

1.8 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

[4] См. *Официальные отчеты Генеральной Ассамблеи, шестьдесят седьмая сессия, Дополнение № 53* (A/67/53), гл. IV, разд. A.

[5] Там же, *шестьдесят девятая сессия, Дополнение № 53* (A/69/53), гл. V, разд. A.

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.

1.9 Государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ.

1.10 Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

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

1.12 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.

1.13 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 должны сотрудничать с частным сектором и организациями гражданского общества в области осуществления правил ответственного поведения государств в информационном пространстве с учетом их потенциальной роли.

2. *призывает* государства-члены далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

3. *полагает*, что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

4. *просит* все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[1] информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

а) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 3 выше;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне;

5. *постановляет* созвать, начиная с 2019 года, в целях придания переговорному процессу в Организации Объединенных Наций по безопасности в сфере использования информационно-коммуникационных технологий более демократического, инклюзивного и транспарентного характера рабочую группу открытого состава, действующую на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств, перечисленных в пункте 1, 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 исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению и того, как международное право применяется к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала и концепций, упомянутых в пункте 3 выше, и представления доклада о результатах данного исследования Генеральной 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;

6. *постановляет,* что рабочая группа открытого состава должна провести организационную сессию в июне 2019 года для согласования организационных мер, связанных с рабочей группой;

7. *постановляет* включить в предварительную повестку дня своей семьдесят четвертой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

45-е пленарное заседание,
5 декабря 2018 года