



# Генеральная Ассамблея

Distr.: General  
22 July 2015  
Russian  
Original: Arabic/English/Spanish

## Семидесятая сессия

Пункт 93 предварительной повестки дня\*

### Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

#### Доклад Генерального секретаря

## Содержание

	<i>Стр.</i>
I. Введение . . . . .	2
II. Ответы, полученные от правительств . . . . .	2
Канада . . . . .	2
Куба . . . . .	4
Сальвадор . . . . .	6
Грузия . . . . .	6
Германия . . . . .	8
Нидерланды . . . . .	9
Панама . . . . .	10
Перу . . . . .	11
Португалия . . . . .	12
Катар . . . . .	14
Республика Корея . . . . .	14
Испания . . . . .	15
Соединенное Королевство Великобритании и Северной Ирландии . . . . .	16

\* A/70/150.



## I. Введение

1. 2 декабря 2014 года Генеральная Ассамблея приняла резолюцию 69/28, озаглавленную «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В пункте 3 этой резолюции Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/68/98), информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

- a) 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 2 резолюции;
- d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

2. В соответствии с этой просьбой 2 февраля 2015 года всем государствам-членам была разослана вербальная нота с предложением предоставить информацию по данной теме. В разделе II приводятся ответы, полученные ко времени составления доклада. Все остальные полученные ответы будут опубликованы в качестве добавлений к настоящему докладу.

## II. Ответы, полученные от правительств

### Канада

[Подлинный текст на английском языке]  
[4 июня 2015 года]

Киберпространство способствует активизации социального взаимодействия и преобразованиям в промышленности и системе государственного управления, продолжая выступать в качестве движущей силы экономического роста, инноваций и общественного развития. С ним также связано появление новых угроз и вызовов для общества.

Канада напоминает, что в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 года содержится четкое подтверждение государствами применимости норм международного права в киберпространстве как основы для норм и принципов, регулирующих ответственное поведение государств, и поддерживает будущую работу над нормами мирного времени.

Канада также считает, что обеспечение безопасности информационно-коммуникационных технологий неотделимо от уважения прав человека и ос-

новых свобод. Все права, которыми человек обладает вне Интернета, должны быть ему гарантированы при нахождении в сети.

Канада привержена идее построения свободного, открытого и безопасного Интернета посредством следующего:

a) реализация национальной стратегии и плана действий в области кибербезопасности остается приоритетным направлением нашей работы на страновом уровне. Эти меры позволяют обеспечивать надежное функционирование канадских киберсистем и защиту интернет-пользователей на основе активного взаимодействия с важнейшими инфраструктурными секторами (например, финансами, транспортом и энергетикой);

b) Канада разработала общие принципы ликвидации последствий киберпроисшествий, обеспечивающие консолидированный общенациональный подход к управлению и координации в контексте реагирования на потенциальные или реальные киберугрозы или инциденты;

c) новый закон Канады о борьбе со спамом помогает точнее уяснить юридические права и соответствующие обязанности государственных учреждений и повысить эффективность законодательных норм, регулирующих вопросы обеспечения соблюдения и международного сотрудничества;

d) что касается деятельности на международном уровне, то Канада обязалась направить 8 миллионов канадских долларов на поддержку проектов по наращиванию потенциала в области обеспечения кибербезопасности, в основном в странах Северной и Южной Америки и Юго-Восточной Азии. Кроме того, Канада выделила более 3,6 миллиона канадских долларов по линии Организации американских государств (ОАГ) (на 2007–2016 годы) на цели развития потенциала в области кибербезопасности стран — членов ОАГ, включая меры по созданию групп реагирования на инциденты в области компьютерной безопасности. Канада также вошла в состав членов — основателей Глобального форума по киберэкспертизе;

e) Канада поддерживает усилия Организации Североатлантического договора (НАТО), направленные на укрепление кибербезопасности альянса и его отдельных членов;

f) Канада участвует в работе Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН) над созданием потенциала в области укрепления доверия и повышения транспарентности, учитывая важное значение этих мер для обеспечения стабильности в киберпространстве;

g) в соответствии с двусторонним планом действий в сфере кибербезопасности Канада в партнерстве с Соединенными Штатами принимает меры, направленные на повышение надежности своей киберинфраструктуры и улучшение взаимодействия, сотрудничества и обмена информацией на оперативном и стратегическом уровнях;

h) кроме того, Канада принимает участие в инициативах по борьбе с киберпреступностью, реализуемых под эгидой Группы семи, Управления Организации Объединенных Наций по наркотикам и преступности, ОАГ и АСЕАН, и является членом Глобального альянса против сексуальных надругательств над детьми в Интернете;

i) Канада рекомендует всем государствам-членам, стремящимся повысить кибербезопасность и эффективность предупреждения киберпреступлений, обратить внимание на Конвенцию Совета Европы о киберпреступности.

С полным текстом сообщения Канады можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).

## Куба

[Подлинный текст на испанском языке]  
[26 мая 2015 года]

Куба разделяет озабоченность, выраженную в резолюции 69/28 в связи с тем, что информационные технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам.

Кроме того, в резолюции 69/28 подчеркивается необходимость предотвратить использование информационных ресурсов и технологий в преступных или террористических целях.

В этой связи Куба выражает глубокую обеспокоенность по поводу скрытого и незаконного использования отдельными лицами, организациями и государствами компьютерных систем других стран для совершения нападений на третьи страны в силу того, что это в потенциальном плане способно провоцировать международные конфликты.

Единственным способом предотвращения и устранения этих новых угроз в целях недопущения превращения киберпространства в театр военных действий является сотрудничество между всеми государствами.

Использование телекоммуникаций в открытых или скрытых целях, заключающихся в подрыве юридического и политического строя государств, является нарушением международно признанных норм в этой области и может приводить к росту напряженности и возникновению ситуаций, не благоприятствующих международному миру и безопасности.

На состоявшемся в январе 2014 года в Гаване втором саммите Сообщества государств Латинской Америки и Карибского бассейна (СЕЛАК) главы государств и правительств стран Латинской Америки и Карибского бассейна провозгласили этот регион зоной мира и, среди прочего, обязались укреплять сотрудничество и дружественные отношения между собой и с другими государствами, вне зависимости от различий в их политических, экономических и социальных системах или уровнях развития, проявлять терпимость и жить вместе в мире друг с другом как добрые соседи.

В ходе третьего саммита СЕЛАК, проведенного 28 и 29 января 2015 года в Белене, Коста-Рика, государства-члены подчеркнули важность информационно-коммуникационных технологий, включая Интернет, и инноваций как инструментов содействия миру и поощрения благополучия, развития человека, образования, социальной включенности и экономического роста, особо отметив их вклад в расширение сферы охвата и улучшения качества социальных

услуг. Они подтвердили также принцип мирного использования информационно-коммуникационных технологий в соответствии с целями и принципами Устава Организации Объединенных Наций и нормами международного права и подчеркнули, что эти технологии ни при каких обстоятельствах не должны использоваться в целях разрушения общественного строя или создания ситуаций, способных провоцировать конфликты между государствами.

Но, невзирая на эти требования, правительство Соединенных Штатов продолжает непрерывные трансляции радио- и телепрограмм на территорию Кубы в нарушение целей и принципов Устава Организации Объединенных Наций и различных положений Международного союза электросвязи. К тому же, что не менее важно, подобные программы нарушают суверенитет Кубы.

Куба вновь заявляет, что использование информации в целях пропаганды и дестабилизации и подрыва внутригосударственного порядка других стран является нарушением их суверенитета и вмешательством в их внутренние дела и как таковое противозаконно и должно быть прекращено.

Мы вновь заявляем о своем самом решительном неприятии международно-противоправного использования информационно-коммуникационных технологий и всех действий такого рода. Мы подчеркиваем важность обеспечения того, чтобы использование этих технологий полностью согласовывалось с целями и принципами Устава Организации Объединенных Наций и международного права, в частности принципов суверенитета, невмешательства во внутренние дела и международно признанных норм сосуществования государств.

Куба подчеркивает, что обязательным условием успешного противодействия угрозам, порождаемым неправомерным использованием информационно-коммуникационных технологий, является международное сотрудничество. Кроме того, она отмечает важную роль Международного союза электросвязи в обсуждениях проблематики кибербезопасности на межправительственном уровне.

Куба надеется, что на новом этапе ее двусторонних отношений с Соединенными Штатами, провозглашенном 17 декабря 2014 года в заявлениях президентов Рауля Кастро Руса и Барака Обамы, объявивших также о намерении восстановить дипломатические отношения и приступить к нормализации отношений, этой агрессивной политике будет положен конец, и будет снята экономическая, торговая и финансовая блокада, которая причиняет огромный ущерб кубинскому народу и негативно отражается на положении в сфере информации и телекоммуникаций и других областях повседневной жизни кубинцев.

18–20 февраля 2015 года в рамках программы информатизации на Кубе был проведен первый общенациональный семинар-практикум по вопросам компьютеризации и кибербезопасности под названием «Становление компьютеризованного общества». В этом мероприятии приняли участие более 11 500 специалистов в области информационно-коммуникационных технологий со всей страны. Среди обсуждавшихся тем были вопросы безопасности, контроля и регулирования сферы информационно-коммуникационных технологий.

Куба учредила Совет по информатизации и кибербезопасности под руководством высшего государственного органа — правительства и Коммунистиче-

ской партии Кубы. В задачи Совета входит вынесение рекомендаций по вопросам выработки всеобъемлющей политики и стратегий в этой области, координация и контроль за ходом их осуществления. Кроме того, ведется работа по созданию Кубинского союза специалистов в области информационных технологий.

Куба поддержала резолюцию 69/28 и намерена продолжать вносить свой вклад в усилия, направленные на мирное развитие информационно-коммуникационных технологий во всем мире и их применение на благо всего человечества.

## **Сальвадор**

[Подлинный текст на испанском языке]  
[21 апреля 2015 года]

В целях защиты информационных и телекоммуникационных систем вооруженными силами Сальвадора создана централизованная информационно-телекоммуникационная сеть передачи голосовой и визуальной информации и данных, функционирующая независимо от открытых сетей. Создана и укомплектована группа по периметральной системе защиты информационных систем; предусмотрена также система шифрования официальной информации в целях защиты всех категорий данных от попыток любого проникновения извне и кибератак.

## **Грузия**

[Подлинный текст на английском языке]  
[26 мая 2015 года]

Правительство Грузии относит вопросы безопасности информационных систем и кибербезопасности к числу своих важнейших политических задач и рассматривает противодействие киберугрозам в качестве неотъемлемого компонента национальной политики в области безопасности, особенно в условиях реализуемых по всей стране реформ, направленных на развитие электронного управления, и возросшей зависимости жизненно-важной инфраструктуры от информационно-коммуникационных технологий. Руководствуясь этими соображениями и стремлением повысить информационную безопасность, правительство Грузии претворяет в жизнь ряд стратегических, правовых, организационных и институциональных мер.

Первая общенациональная стратегия кибербезопасности была оформлена в виде стратегии и плана действий по обеспечению безопасности в киберпространстве на 2013–2015 годы — основного документа, в котором излагается политика государства в сфере кибербезопасности, включая стратегические цели и руководящие принципы, а также основные направления деятельности и задачи. Кибербезопасность является одним из главных приоритетов государственной политики в сфере безопасности, и для национальной безопасности охрана киберпространства не менее важна, чем защита, земельного, водного и воздушного пространства страны.

Еще одним шагом в направлении институционализации безопасности информационных систем явилось создание в 2010 году при министерстве юстиции Грузии агентства по обмену данными в качестве центрального правительственного органа, ответственного за разработку и осуществление политики и стандартов в области информационной и кибербезопасности. В частности, перед агентством поставлены следующие задачи:

- утверждение и осуществление стратегий и стандартов в области информационной безопасности в государственном секторе и на жизненно важных объектах инфраструктуры;
- выполнение мандата на обеспечение кибербезопасности путем создания национальной группы по реагированию на чрезвычайные ситуации в компьютерной сфере;
- предоставление консультативных услуг по вопросам информационной и кибербезопасности, проведение проверок на предмет соблюдения информационной безопасности и оказание услуг по обеспечению кибербезопасности;
- проведение информационно-просветительских мероприятий по вопросам информационной безопасности и кибербезопасности.

Нормативно-правовую основу политики Грузии в сфере информационной безопасности составляет Закон об информационной безопасности и дополняющие его подзаконные акты, принятые в 2011–2012 годах. Основные концепции, используемые в грузинских нормативно-правовых актах, регулирующих обеспечение информационной безопасности, разработаны на базе стандартов серии 27000 Международной организации по стандартизации. Закон наделяет объекты важнейшей инфраструктуры определенными правами и обязанностями в контексте осуществления политики в области информационной безопасности и предусматривает создание механизмов сотрудничества между национальными правительственными группами по реагированию на чрезвычайные ситуации в компьютерной сфере.

Грузия прилагает большие усилия в целях наращивания международного сотрудничества и обмена накопленными знаниями со своими партнерами. Наглядным свидетельством этого служит ряд двусторонних соглашений о сотрудничестве и меморандумов о взаимопонимании, заключенных агентством по обмену данными с военным штабом Европейского союза (из Австрии, Эстонии, Польши и других стран) и своими соседями (Азербайджан, Армения, Республика Молдова, Турция и др.).

Грузия признает возросшее значение механизмов регионального и международного сотрудничества в противостоянии вызовам в области информационной безопасности. Исходя из этого необходимо направлять значительные усилия на проведение мероприятий международного уровня, посвященных этим весьма важным вопросам, повышение степени доверия между основными заинтересованными сторонами и продолжение работы над выработкой стратегических доктрин и правовых концепций при участии международного сообщества.

## Германия

[Подлинный текст на английском языке]  
[27 мая 2015 года]

Открытый, свободный, безопасный и надежный Интернет открывает широкие возможности для экономического роста, социального развития и научного прогресса, равно как и для поощрения демократии, благого управления и верховенства права. Одновременно с этим растет обеспокоенность по поводу угроз международной безопасности, исходящих из киберпространства. В последние месяцы нападениям с применением вредоносных программных средств все чаще подвергаются такие весьма заметные объекты, как средства массовой информации. Нападения на объекты жизненно важной инфраструктуры могут иметь особенно тяжкие последствия.

Сегодня перспектива развязывания тотальной «кибервойны» представляется маловероятной. Однако ограниченное использование возможностей киберпространства в контексте более масштабных военных кампаний, в том числе в условиях гибридных конфликтов, уже стало реальностью. Более того, инциденты в кибернетическом пространстве могут приводить к эскалации конфликтов в реальной жизни.

Для успешного реагирования на такое развитие событий Германия призывает придерживаться трехцелевого подхода, предусматривающего: согласование норм ответственного поведения государств в киберпространстве, проведение мероприятий по укреплению доверия и наращивание потенциала противодействия киберугрозам.

Решающая роль в установлении таких норм ответственного поведения государств в киберпространстве принадлежит Организации Объединенных Наций. Важной отправной точкой является достигнутый Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2012–2013 годах консенсус о том, что сфера действия международного права, и в частности Устава Организации Объединенных Наций, распространяется на киберпространство. Этот вывод получил дальнейшее развитие в работе сформированной на период 2014–2015 годов Группы правительственных экспертов, активным участником которой вновь выступает Германия.

Общее понимание правил, норм и принципов ответственного поведения государств в киберпространстве могло бы способствовать повышению уровня транспарентности и предсказуемости в международных отношениях и тем самым содействовать обеспечению мира и стабильности. Например, было бы полезно иметь более полное общее понимание порядка применения права вооруженных конфликтов в условиях использования кибернетических сил и средств ведения войны, развитием которых сегодня занимается все большее число государств.

В сфере укрепления доверия, по мнению Германии, чрезвычайно важную роль играют региональные организации. В 2013 году Организация по безопасности и сотрудничеству в Европе согласовала первоначальный пакет мер по укреплению доверия в киберпространстве. В настоящее время эти меры успешно выполняются и ведутся переговоры по второму пакету, охватываю-

чему вопросы укрепления доверия и сотрудничества. В рамках своего предстоящего председательства в этой организации Германия намерена уделять обеспечению кибербезопасности первостепенное внимание.

Германия занимается разработкой закона о безопасности информационных технологий в целях усиления потенциала противодействия киберугрозам на национальном уровне. В законопроекте определены минимальные требования безопасности информационных систем на объектах важнейшей инфраструктуры. Он устанавливает обязанность сообщать о всех значимых инцидентах в целях повышения общей безопасности и систем и защиты интересов населения. Кроме того, Германия готова оказывать поддержку другим государствам в повышении их способности противостоять угрозам кибербезопасности.

С полным текстом сообщения Германии можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).

## Нидерланды

[Подлинный текст на английском языке]  
[29 мая 2015 года]

Международное сообщество имеет общую заинтересованность в сохранении открытости, свободы и безопасности киберпространства и несет за это общую ответственность. По мнению Нидерландов, обеспечению безопасности может способствовать широкое признание и соблюдение свода норм ответственного поведения государств. Большая работа уже проделана Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Вместе с тем в перечисленных ниже областях было бы полезно продолжить работу и принять следующие конкретные меры:

- выработка более глубокого понимания государствами того, каким образом существующие нормы международного права и нормы, регулирующие правила поведения государств, применяются в киберпространстве; в частности, это касается международно-правовых принципов, применимых к кибероперациям, не достигающим порога, после которого они могут быть расценены как вооруженное нападение;
- выработка норм или дополнительных мер самоограничения или взаимопомощи с уделением особого внимания идее создания механизмов особой нормативной защиты определенных систем и сетей, включая важнейшие объекты инфраструктуры основного обслуживания населения, структуры гражданской обороны и некоторые ключевые компоненты глобальной сети Интернет;
- наращивание правового, дипломатического и стратегического потенциала и активизация обмена информацией о передовых методах в области международного мира и безопасности в киберпространстве. Важную роль в этом может играть Глобальный форум по киберэкспертизе, основанный в Гааге во время проведения четвертой Глобальной конференции по киберпространству.

Сегодня, когда Интернет становится стратегическим активом для всех нас, эта проблематика нуждается в широком международном обсуждении. Нидерланды намерены продолжать активно содействовать расширению такого диалога.

С полным текстом сообщения Нидерландов можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).

## **Панама**

[Подлинный текст на испанском языке]  
[3 июня 2015 года]

Сегодня информационно-коммуникационные технологии переживают стремительный рост. В результате технологии и средства связи постепенно входят в жизнь всего населения, становясь более доступными.

Очевидно, что наша жизнь сегодня неотделима от эволюции средств передачи и обработки информации.

Правительство Панамы, действуя в русле этой тенденции, принимает меры к тому, чтобы адаптировать ее к особым нуждам органов национальной безопасности. С этой целью ведется работа по совершенствованию технических средств, что позволит повысить качество связи и уровень ее защиты.

В рамках этих усилий правительство Панамы занимается поэтапной разработкой плана развития системы коммуникаций, включающего элементы сетевой инфраструктуры, защиты и телефонии. Соответствие всех этих средств международным стандартам подтверждается их производителями.

Правительство Панамы обеспечивает защиту целостности государственной информации в сети Интернет и системах передачи данных и телефонии при помощи инфраструктуры внутренней межсетевой защиты и посредством подключения к национальной многофункциональной сети.

Для обеспечения сохранности конфиденциальных данных и защиты информации в ходе сеансов передачи данных правительство Панамы использует межсетевые защитные экраны.

Мы полагаем, что дальнейшее совершенствование телекоммуникационных решений с учетом потребностей служб безопасности позволит оснастить эти службы средствами, которые будут способствовать гармонии в информационной сфере на основе активных и превентивных мер. Органы безопасности должны использовать преимущества нынешней ситуации в области информационных технологий, особенно с учетом нашей миссии по защите общества, как на местном, так и на международном уровнях.

## Перу

[Подлинный текст на испанском языке]  
[30 июня 2015 года]

### **Общая оценка проблем информационной безопасности, подготовленная управлением по информационным технологиям**

- Общеорганизационная сеть данных Национальной полицейской службы Перу обеспечивает постоянный контроль работы своих систем с использованием различных протоколов безопасности для каждого уровня ее целостной и функциональной структуры.
- Защита информационных систем в составе общеорганизационной сети обеспечивается внешним подрядчиком, привлеченным службой управления безопасностью при оперативном центре безопасности.
- Запланированы меры по формированию ролей и идентификаторов пользователей; это позволит контролировать и фиксировать операции каждого пользователя и проводить соответствующие проверки.

### **Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности**

#### **Превентивные меры**

- Назначение сетевых администраторов
- Учебная подготовка сотрудников по вопросам использования информационных технологий
- Лицензирование программного обеспечения серверов центра хранения и обработки данных Национальной полицейской службы
- Создание «частного облачного сервиса»
- Резервное копирование данных
- Создание системы резервного энергоснабжения (бесперебойное питание)
- Модернизация электрораспределительных панелей и электрических соединений
- Передача на внешний подряд функций периметральной защиты на случай нападений или отказа в обслуживании

#### **Содержание концепций, упомянутых в пункте 2 резолюции**

- Модернизация технологической платформы и информационных систем Национальной полицейской службы, предусматривающая консолидацию информационных средств в целях повышения уровня как внутригосударственной, так и международной безопасности посредством имплементации сервисов, обеспечивающих функциональную совместимость систем между странами.

### **Меры, которые могло бы принять международное сообщество для укрепления информационной безопасности на глобальном уровне**

- Стандартизация средств связи, в том числе в части видов оборудования и протоколов связи
- Стандартизация технологической платформы с гарантией высокой степени доступности для обеспечения эксплуатационной совместимости систем разных стран, занимающихся вопросами международной безопасности
- Стандартизация механизмов защиты информации
- В рамках концепции «сфера информатизации»: определение факторов риска, существующих в каждой стране, участвующей в решении вопросов международной безопасности, и возможное согласование общих целей с указанием явлений, которые необходимо пресекать и/или сдерживать, и с созданием автоматизированных информационных механизмов. Например, в случае Перу к таким проблемам можно отнести: оборот наркотиков, терроризм, организованную преступность, контрабанду, отмывание денег и торговлю людьми.

### **Португалия**

[Подлинный текст на английском языке]  
[24 апреля 2015 года]

В своей резолюции 69/28 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея напомнила о роли науки и техники в контексте международной безопасности, признав, что достижения в этих областях могут иметь как гражданское, так и военное применение. Хотя прогресс в области информатизации и телекоммуникаций означает появление новых возможностей для развития цивилизации, сотрудничества между государствами, укрепления созидательного потенциала человечества и обмен информацией в масштабе всего мирового сообщества, мы видим, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут иметь негативные последствия для национальной целостности государств.

В той же резолюции Генеральная Ассамблея призвала государства-члены представить, принимая во внимание доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/68/98), свои соображения и замечания по следующим четырем вопросам:

- а) общая оценка проблем информационной безопасности;
- б) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;
- в) содержание концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем;

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

В докладе Группы правительственных экспертов содержатся рекомендации относительно следующих областей: нормы, правила и принципы ответственного поведения государств; меры укрепления доверия и обмен информацией; и меры по наращиванию потенциала.

С учетом этих рекомендаций мы можем охарактеризовать наш национальный контекст следующим образом.

### **Нормы, правила и принципы ответственного поведения государств**

По мнению Португалии, безопасность в области сетевой информации имеет большое значение и ее уровень повышается.

Мы должны особо отметить активизацию усилий по введению в действие законодательства в области обеспечения безопасности и целостности сетей на основе определения методик оценки риска; для этого необходимо принять надлежащие совместные меры безопасности, как на техническом, так и на организационном уровнях, и установить требование в отношении информирования о случаях нарушения безопасности или утраты целостности сетей, которые существенно сказываются на функционировании служб.

На концептуальном уровне важно закрепить понимание того, что регулирование должно основываться главным образом на международных нормах.

На международном уровне важно расширять обмен информацией и деятельность по проведению учебных мероприятий в приграничных районах.

### **Меры по укреплению доверия и обмен информацией**

Крайне важно поощрять обмен информацией среди всех заинтересованных сторон (как государственных, так и частных) с учетом расширения процесса глобализации.

В своих усилиях на национальном уровне мы уделяем особое внимание проведению совместных учебных мероприятий, в которых участвуют государственные и частные структуры, поощрению технической стандартизации, а также организации конференций и семинаров, в том числе с участием международных представителей.

### **Меры по наращиванию потенциала**

Важно разработать меры по наращиванию потенциала. Тем не менее существуют трудности, связанные с организацией учебной подготовки и обеспечением людских ресурсов, необходимых для проведения этих мероприятий.

Необходимо содействовать расширению доступа к знаниям и развивать коллективные формы обучения по ряду направлений, включая безопасность, среди всех основных заинтересованных сторон.

## Катар

[Подлинный текст на арабском языке]  
[24 июня 2015 года]

Государство Катар продолжает отслеживать существующие и потенциальные угрозы в сфере информационной безопасности. Им разработаны стратегии противодействия этим угрозам таким образом, чтобы это учитывало необходимость сохранения свободного потока информации. Государство Катар уверено, что информационная безопасность имеет решающее значение для национальной и международной безопасности. В целях обеспечения информационной безопасности Государство Катар приняло ряд мер по обновлению соответствующих технологий и повышению эффективности законодательных, регулятивных и правоприменительных функций. Кроме того, принимаются меры для улучшения координации и расширения сотрудничества в решении соответствующих вопросов на региональном и международном уровнях, если это не противоречит внутреннему законодательству.

Государство Катар считает, что международное сообщество может внести свой вклад в укрепление информационной безопасности, продолжив заниматься разработкой имеющего обязательную силу международного документа о гарантиях информационной безопасности. Такой документ должен предусматривать разработку программных средств защиты от хакеров и требования по обеспечению совместимости информационных систем.

## Республика Корея

[Подлинный текст на английском языке]  
[11 июня 2015 года]

Сегодня киберпространство — это новый горизонт, открывающий бескрайние возможности и уникальные экономические и социальные преимущества. Вместе с тем в силу его открытого, анонимного и трансграничного характера в нем формируются киберугрозы, представляющие собой серьезный вызов международной безопасности.

В последнее время Республика Корея подверглась серии кибератак, включая недавние случаи посягательства на безопасность систем оператора атомных электростанций страны, имевшие место в 2014 году. В целях более эффективного реагирования на киберугрозы в марте 2015 года Республика Корея разработала всеобъемлющие планы действий по укреплению кибербезопасности и учредила должность секретаря президента по делам кибербезопасности. Республика Корея убеждена в важности согласования набора норм международного регулирования киберпространства и осуществления мер по укреплению доверия и наращиванию потенциала в киберпространстве.

В этой связи Республика Корея с удовлетворением отмечает выводы Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, изложенные в ее докладе 2013 года, в котором признается возможность распространения сферы действия международного права на поведение государств в киберпространстве. Республика Корея надеется на продолжение обсуждений возможного порядка применения согласованных принципов в отношении поведе-

ния государств в киберпространстве. В 2014 году Республика Корея выступила в качестве принимающей стороны Азиатско-Тихоокеанского регионального семинара по вопросам международного права и поведения государств в киберпространстве, организованного совместно с Институтом Организации Объединенных Наций по исследованию проблем разоружения для того, чтобы страны региона смогли обсудить вопросы, связанные с кибербезопасностью.

Кроме того, правительство Республики Корея работает над укреплением двустороннего и трехстороннего сотрудничества с ведущими странами и активно участвует в региональных и международных форумах по кибертематике, включая Региональный форум Ассоциации государств Юго-Восточной Азии и Группу правительственных экспертов Организации Объединенных Наций. В качестве принимающей стороны Сеульской конференции по киберпространству, состоявшейся в 2013 году, Республика Корея тесно сотрудничала с Нидерландами в рамках подготовки к проведению в 2015 году в Гааге Глобальной конференции по киберпространству и намерена и впредь активно участвовать в проведении конференций под эгидой лондонского процесса.

С полным текстом сообщения Республики Корея можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).

## **Испания**

[Подлинный текст на испанском языке]  
[29 мая 2015 года]

Испания считает, что информационно-коммуникационные технологии являются важнейшим средством обслуживания общества во всем мире, однако их глобализация порождает серьезные риски и угрозы, включая кибершпионаж, кибертерроризм, «хактивизм» и кибервойны.

После учреждения Национального совета кибербезопасности Испания продолжила работу по реализации планов, составленных на основе Национальной стратегии в области кибербезопасности и направленных на наращивание потенциала противодействия киберугрозам в контексте деятельности по предупреждению, защите, выявлению, анализу, реагированию, восстановлению и координации.

Испания продолжает активно участвовать в усилиях, направленных на поощрение международного сотрудничества, и внимательно отслеживает ход реализации всех стратегических инициатив в области кибербезопасности, как в Европейском союзе, так и на других крупных международных форумах, включая Организацию по безопасности и сотрудничеству в Европе, Организацию Североатлантического договора и Совет Европы.

Испания продолжает отстаивать значимость роли Организации Объединенных Наций в деле достижения международного консенсуса по вопросам кибербезопасности и поддерживает идею проведения системного диалога с участием других международных организаций, направленного на поощрение регионального сотрудничества и выработку общемировых стандартов, передовой практики, правил поведения государств и мер укрепления доверия и имеющего своей конечной целью гарантировать мирное и безопасное использование информационных технологий.

Испания считает, что государствам следует выработать консенсус по четырём направлениям. Во-первых, необходимо согласовать коллективные меры укрепления доверия в целях повышения транспарентности в отношениях между государствами в области кибербезопасности и расширения их возможностей в плане нейтрализации любых возможных нападений, совершаемых с территории третьих стран.

Во-вторых, Испания считает, что государствам следует продолжать рассматривать вопрос о том, каким образом принципы и нормы международного права должны толковаться и применяться в киберпространстве; в первую очередь речь идет о нормах и принципах, касающихся угрозы силой или ее применения, гуманитарного права и защиты прав и основных свобод человека.

В-третьих, Испания считает необходимым укреплять международное сотрудничество путем совершенствования каналов связи, учреждения механизмов координации деятельности групп реагирования на чрезвычайные ситуации в компьютерной сфере, проведения совместных учений и других аналогичных операций и развития сотрудничества между судебными и полицейскими органами.

И наконец, следует продолжать поощрять усилия по наращиванию потенциала в тех странах, где это необходимо, и оказывать помощь государствам, по их просьбе, в разработке внутригосударственных законов, устанавливающих нормы кибербезопасности.

С полным текстом сообщения Испании можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).

## **Соединенное Королевство Великобритании и Северной Ирландии**

[Подлинный текст на английском языке]  
[29 мая 2015 года]

Соединенное Королевство Великобритании и Северной Ирландии приветствует возможность откликнуться на резолюцию 69/28 Генеральной Ассамблеи «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», взяв за основу свой ответ на резолюцию 68/243, представленный в 2013 году. В своем ответе во избежание путаницы Соединенное Королевство использует предпочитаемый им термин «кибербезопасность» и связанные с ним концепции, поскольку в данном контексте существуют различные толкования термина «информационная безопасность».

Соединенное Королевство признает, что киберпространство является одним из основных элементов жизненно важной национальной и международной инфраструктуры и необходимой основой для экономической и социальной деятельности в Интернете. Фактические и потенциальные угрозы, создаваемые в результате деятельности в киберпространстве, вызывают серьезную озабоченность. В нашем ответе приводится подробная информация о национальных и международных подходах, которые применялись и будут применяться в целях укрепления безопасности и развития сотрудничества в этой области. Эти подходы были подкреплены национальной стратегией Соединенного Королевства в области кибербезопасности, которая была обнародована в ноябре 2011 года.

Соединенное Королевство продолжает играть одну из ведущих ролей в международных дискуссиях по вопросам кибербезопасности. Наши эксперты вошли в состав всех четырех групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, и мы считаем, что доклад, подготовленный группой предыдущего состава на основе консенсуса, свидетельствует о значимом прогрессе в деле достижения общего понимания в отношении норм поведения государств в киберпространстве и признания применимости международного права в киберпространстве. Мы с нетерпением ожидаем результатов обсуждений в Группе нынешнего состава в июне 2015 года. Соединенное Королевство также приветствует продолжающиеся в Организации по безопасности и сотрудничеству в Европе обсуждения возможных последующих мер укрепления доверия в киберпространстве, в основу которых будут положены меры, успешно согласованные в 2013 году, а также аналогичную работу в других региональных организациях.

В этом ответе вкратце изложены усилия Соединенного Королевства, направленные на обеспечение и укрепление кибербезопасности и обмен передовым опытом, как на внутригосударственном, так и на общемировом уровне, в том числе в сотрудничестве с международными партнерами в рамках борьбы с киберпреступностью и серьезными инцидентами и расширения возможностей в компьютерной сфере. Соединенное Королевство рассчитывает на достижение дальнейшего прогресса во всех этих областях. Соединенное Королевство радо играть активную роль в решении этих важных вопросов и надеется на дальнейшее участие в укреплении потенциала и международного сотрудничества в области кибербезопасности.

С полным текстом сообщения Соединенного Королевства можно ознакомиться по адресу: [www.un.org/disarmament/topics/informationsecurity/](http://www.un.org/disarmament/topics/informationsecurity/).