Организация Объединенных Наций A/69/112/Add.1

Генеральная Ассамблея

Distr.: General
18 September 2014
Russian
Original: English/French/Spanish

Шестьдесят девятая сессия
Пункт 92 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Добавление**

Содержание

* A/69/150.

** Информация, приведенная в настоящем докладе, была получена после выхода основного доклада.

II. Ответы, полученные от правительств

Канада

[Подлинный текст на английском языке]
[12 июня 2014 года]

В свете доклада Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2013 год (A/68/98) Канада хотела бы поделиться с Генеральным секретарем следующими соображениями. Будучи движущей силой экономического роста, инноваций и социального развития, киберпространство позволяет активизировать социальное взаимодействие и осуществить преобразования в промышленности и системе государственного управления. С ним также связано появление новых угроз и вызовов для общества (таких как киберзапугивание, киберпреступность и использование Интернета в террористических целях).

Канада с удовлетворением отметила, что в докладе Группы правительственных экспертов за 2013 год содержится четкое подтверждение государствами применимости норм международного права в киберпространстве как основы для норм и принципов, регулирующих ответственное поведение государств.

Канада весьма заинтересована в поддержании открытого и свободного Интернета не только для обеспечения своего экономического процветания, но и для поддержки провозглашаемых ею ценностей и интересов, а также для защиты безопасности ее граждан.

Усилия, предпринимаемые Канадой на национальном уровне, включают осуществление ее Стратегии и Плана действий в области кибербезопасности, которые обеспечивают надежную работу киберсистем страны и охрану интересов канадцев при работе с Интернетом посредством активного взаимодействия с важнейшими инфраструктурными секторами (например финансами, транспортом и энергетикой).

Канада разработала основные принципы действий по ликвидации последствий киберпроисшествий, которые представляют собой общенациональную стратегию ликвидации последствий и координации действий в связи с потенциальными или явными киберугрозами или киберпроисшествиями.

В тесном сотрудничестве с многосторонними организациями и частным сектором Канада занимается укреплением информационной безопасности сетей, от которых зависит экономическое процветание и безопасность страны.

Что касается деятельности на международном уровне, то Канада выделила свыше 3,6 млн. долл. США по линии Организации американских государств (ОАГ) (на 2007–2016 годы) для наращивания потенциала в области кибербезопасности стран — членов ОАГ, в том числе путем создания групп реагирования на инциденты в области компьютерной безопасности.

В рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) Канада участвовала в подготовке ряда мер укрепления доверия и безопасности, призванных уменьшить опасность возникновения конфликтов, свя-

занных с использованием информационно-коммуникационных технологий в киберпространстве.

В рамках Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН) Канада работает над созданием потенциала, связанного с важностью мер укрепления доверия и повышения прозрачности в интересах стабильности в киберпространстве.

С помощью канадско-американского Плана действий в области кибербезопасности Канада сотрудничает с Соединенными Штатами в принятии мер для повышения надежности киберинфраструктуры Канады и улучшения взаимодействия, взаимопомощи и обмена информацией на оперативном и стратегическом уровнях.

Канада также принимает участие в инициативах по борьбе с киберпреступностью по линии Группы семи, Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) и ОАГ. Она является членом Глобального альянса против сексуальных надругательств над детьми в Интернете и в 2012–2013 годах принимала участие в работе Группы правительственных экспертов.

Канада рекомендует всем государствам-членам, желающим повысить кибербезопасность и предотвратить совершение киберпреступлений, обратить внимание на Конвенцию Совета Европы о киберпреступности.

Канада считает, что при решении проблемы безопасности информационно-коммуникационных технологий должно обеспечиваться уважение прав человека и основных свобод. Права, которыми люди пользуются в повседневной жизни, включая свободу выражения мнений, ассоциаций и собраний и неприкосновенность частной жизни, должны охраняться и в Интернете.

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

Франция

[Подлинный текст на французском языке]
[15 сентября 2014 года]

Франция хотела бы прежде всего вновь заявить, что вместо выражения «защита информации» она предпочитает использовать выражение «безопасность информационных систем» или просто «кибербезопасность». Будучи активным сторонником свободы выражения мнений в Интернете (см. резолюцию 20/8 Совета по правам человека, принятую в 2012 году), Франция не считают информацию как таковую потенциальным источником угрозы, от которой необходима защита, за исключением случаев, строго оговоренных законом, с соблюдением принципа соразмерности и прозрачности в соответствии со статьей 19 Международного пакта о гражданских и политических правах.

Функционирование нашего общества во все большей степени зависит от информационных систем и сетей, включая Интернет. Поэтому успешное нападение на какую-либо важнейшую информационную систему может иметь серь-

езные последствия как для людей, так и для экономики. По этой причине Франция разработала в 2011 году стратегию защиты и безопасности информационных систем, возведя кибербезопасность в ранг подлинно национального приоритета. В выпущенной в 2013 году Белой книге по вопросам обороны и национальной безопасности данная угроза была конкретизирована и разделена на два представляющих серьезную опасность для страны аспекта, к которым относятся кибершпионаж и киберсаботаж для нарушения работы важнейших объектов инфраструктуры.

Для решения этих проблем в 2009 году было создано Национальное управление сетевой и информационной безопасности, ресурсы и полномочия которого с тех пор постоянно увеличивались. В настоящее время Управление, действуя от имени премьер-министра, отвечает за все мероприятия по предотвращению и реагированию, касающиеся кибербезопасности жизненно важных объектов инфраструктуры Франции, включая инфраструктуру государственного управления. Министерство обороны, у которого есть собственный план обеспечения безопасности сетей, также активно работает в этой области, о чем свидетельствует выпущенный в феврале 2014 года масштабный стратегический документ под названием «Пакт о кибероборо не».

В то же время Франция активно участвует в укреплении международного сотрудничества в области кибербезопасности, без которого национальные усилия будут носить ограниченный характер. С момента проведения в 2011 году встречи Группы восьми в Довиле Франция проявляла особый интерес к укреплению международного регулирования киберпространства. В этой связи страна в настоящее время активно участвует в работе Группы правительственных экспертов Организации Объединенных Наций и Организации по безопасности и сотрудничеству в Европе (ОБСЕ) по выработке международной нормативной базы на основе действующих норм международного права, а также мер укрепления доверия и конкретных норм поведения в киберпространстве. Наконец, Франция прилагает большие усилия для достижения цели международной деятельности по укреплению потенциала в области кибербезопасности с помощью конкретных программ двустороннего и многостороннего характера (по линии Европейского союза и Организации Североатлантического договора (НАТО)).

С полным текстом сообщения Франции можно ознакомиться по адресу http://www.un.org/disarmament/topics/informationsecurity/.

Республика Корея

[Подлинный текст на английском языке]
[30 июня 2014 года]

Киберпространство открывает неограниченные возможности для экономического и социального развития и процветания во всем мире. Открытое и безопасное киберпространство имеет важное значение для расширения достижений человеческой мысли и поощрения демократического участия. Но при этом оно ведет к появлению новых проблем, таких как киберпреступность, кибертерроризм и информационные войны.

Для решения этих проблем правительство Республики Корея объявило в июле 2013 года о принятии Всеобъемлющей национальной стратегии противо-

действия киберугрозам, в которой изложены меры реагирования на кибернападения и укрепления безопасности особо охраняемых объектов информационной инфраструктуры.

Республика Корея считает, что в число ключевых направлений международного сотрудничества входят согласование комплекса международных норм и мер укрепления доверия, создание киберпотенциала развивающихся стран и развитие сотрудничества между группами реагирования на чрезвычайные ситуации в компьютерной сфере.

В этой связи правительство Кореи регулярно проводит двусторонние консультации с целым рядом стран и принимает активное участие в региональных и международных обсуждениях вопросов кибербезопасности, в том числе в рамках Регионального форума Ассоциации государств Юго-Восточной Азии, Саммита по ядерной безопасности и Организации Объединенных Наций. Относительно недавно, 17 и 18 октября 2013 года, Республика Корея принимала Сеульскую конференцию по киберпространству. Предыдущие конференции были проведены в Лондоне (2011 год) и Будапеште (2012 год). Конференция способствовала привлечению внимания к необходимости укрепления международного сотрудничества в целях устранения растущей угрозы при одновременном поиске точек соприкосновения по основным вопросам использования киберпространства. Страны-участницы приняли «Сеульские принципы и обязательства в отношении открытого и безопасного киберпространства» в качестве составной части подготовленного Председателем итогового документа.

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

Испания

[Подлинный текст на испанском языке]
[30 июня 2014 года]

Испания считает, что правительства должны поддерживать открытое, доступное и безопасное киберпространство и обеспечивать защиту таких основополагающих ценностей, как демократия, права человека и верховенство права.

Кибербезопасность является для Испании одним из стратегических приоритетов. В связи с этим и в соответствии с положениями Стратегии в области кибербезопасности ее партнеров по Европейскому союзу Испания приняла 5 декабря 2013 года Национальную стратегию в области кибербезопасности, в которой отражен комплексный подход к обеспечению кибербезопасности и в соответствии с которой для реагирования на кризисные ситуации создается система межведомственной координации (Национальный совет по кибербезопасности).

В Стратегии также предусмотрены меры по развитию международного сотрудничества и привлечению учреждений и предприятий, в первую очередь стратегического характера. К важнейшим компонентам Стратегии относятся воспитательные и информационно-просветительские мероприятия, направлен-

ные на углубление понимания гражданским обществом проблем, связанных с кибербезопасностью.

Испания считает, что Организация Объединенных Наций призвана сыграть весьма важную роль в деле формирования международного консенсуса в этой области, и поддерживает проведение институционального диалога в рамках Организации Объединенных Наций для обеспечения мирного и безопасного использования информационных технологий. Испания также поддерживает рекомендации, содержащиеся в докладе Группы правительственных экспертов Организации Объединенных Наций за 2013 год.

В этой связи 21 марта 2014 года Испания организовала в Мадриде совещание по вопросам кибербезопасности на уровне постоянных представителей. Испания также принимает участие в работе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и активно участвует в осуществлении различных международных инициатив в области кибербезопасности на таких форумах, как Организация по безопасности и сотрудничеству в Европе, Организация Североатлантического договора, Управление Организации Объединенных Наций по наркотикам и преступности, Совет по правам человека Организации Объединенных Наций и меридианные конференции по защите важнейших объектов информационной инфраструктуры. Кроме того, Испания является государством — участником Будапештской конвенции о киберпреступности.

Испания считает, что для укрепления глобальной информационной безопасности международному сообществу следует принять меры в следующих четырех областях деятельности:

1) меры укрепления доверия: прозрачность, обмен информацией и передовым опытом;

2) международное право: международному сообществу и особенно Организации Объединенных Наций следует продолжать рассматривать вопрос о том, каким образом принципы и нормы международного права должны толковаться и применяться в киберпространстве;

3) международное сотрудничество: повышение эффективности связи на случай происшествий, а также создание более совершенных и гибких механизмов для сотрудничества между полицейскими и судебными органами;

4) создание потенциала: в тех странах, где существует необходимость в создании потенциала, соответствующие меры должны приниматься как на двусторонней основе, так и в рамках международных организаций.

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

Швеция

[Подлинный текст на английском языке]
[12 сентября 2014 года]

Поскольку развитие киберпространства открывает практически неограниченные возможности, в рамках международного сотрудничества необходимо надлежащим образом учитывать соображения безопасности, связанные с использованием информационных технологий и телекоммуникаций.

В Швеции уже в течение многих лет ведется работа над национальной стратегией обеспечения безопасности информационно-коммуникационных технологий, и в настоящее время правительство разрабатывает национальную стратегию в области кибербезопасности. В последнее время шведская Комиссия по обороне подготовила ряд оценок, касающихся кибербезопасности и кибероборонь, подчеркнув необходимость общего наращивания потенциала Швеции в области кибербезопасности.

Швеция участвует в работе и активно сотрудничает с другими участниками различных международных форумов по киберпространству, стремясь также наладить двусторонний и региональный диалог по вопросам использования киберпространства, в том числе в регионе Северной Европы и Балтии. Особое внимание Швеция уделяет поощрению прав человека в киберпространстве и применению модели управления Интернетом с участием большого числа заинтересованных сторон, а также необходимости выработки основополагающих принципов организации международного наблюдения.

Швеция выступает за последовательное проведение политики Европейского союза по вопросам киберпространства исходя из основных ценностей и интересов Европейского союза. Одним из важных событий стало принятие в 2013 году всеобъемлющей Стратегии Европейского союза в области кибербезопасности. Швеция была одним из инициаторов создания «Коалиции за свободу в Интернете» — группы, которая привержена идее свободного пользования Интернетом во всем мире. На протяжении трех лет подряд Швеция принимает Стокгольмский форум по проблемам Интернета, который представляет собой конференцию с участием многих заинтересованных сторон, направленную на углубленное обсуждение вопросов, связанных со свободой и глобальным развитием Интернета. Швеция была в составе основной группы государств, выступивших инициаторами принятия резолюции 20/8 (2012) Совета по правам человека, в которой Совет подтвердил, что права, которыми люди пользуются в повседневной жизни, должны охраняться и в Интернете. На протяжении трех лет подряд Швеция представила совместные заявления в Первом комитете Генеральной Ассамблеи, указывая, среди прочего, на необходимость последовательного применения правозащитного и основанного на участии большого числа заинтересованных сторон подхода при решении проблем в области информационно-коммуникационных технологий и международной безопасности. Швеция также активно участвовала в принятии первоначального комплекса мер укрепления доверия ОБСЕ для уменьшения опасности конфликтов, связанных с использованием информационно-коммуникационных технологий, и повышения прозрачности, особенно подчеркивая при этом необходимость уважать и поощрять права человека.

Для выработки основных принципов, регулирующих использование информационно-коммуникационных технологий и международные отношения в киберпространстве, необходимы усилия всех стран мира; ниже приводятся некоторые предварительные соображения. Международному сообществу, включая все заинтересованные стороны, необходимо наладить практическое сотрудничество в укреплении кибербезопасности, для чего можно было бы разработать добровольный свод правил поведения или норм международного поведения в киберпространстве. Глобальные игроки должны стремиться к разработке мер укрепления доверия для повышения прозрачности и предсказуемости, что позволит снизить опасность непонимания или конфликта в киберпространстве.

С полным текстом сообщения Швеции можно ознакомиться по адресу http://www.un.org/disarmament/topics/informationsecurity/.