Организация Объединенных Наций A/65/201

Генеральная Ассамблея

Distr.: General
30 July 2010
Russian
Original: English

Шестьдесят пятая сессия
Пункт 94 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта группа была создана в соответствии с пунктом 4 резолюции 60/45 Генеральной Ассамблеи.

* A/65/150.

10-46959 (R) 170810 180810

Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Резюме

Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных проблем XXI века. Угрозы исходят из широкого круга источников и проявляются в подрывной деятельности, направленной в равной степени против физических и юридических лиц, национальной инфраструктуры и правительств. Ее последствия сопряжены со значительным риском для общественной безопасности, безопасности стран и стабильности объединенного в глобальную сеть международного сообщества в целом.

В результате роста применения информационных и коммуникационных технологий (ИКТ) в критической инфраструктуре возникают новые уязвимые места и возможности для совершения подрывных действий. В силу сложной взаимосвязанности телекоммуникационных сетей и Интернета любое устройство ИКТ может служить источником или объектом все более изощренных злонамеренных действий. Поскольку в силу самого характера ИКТ они могут использоваться двояко, те же технологии, которые применяются для обеспечения надежной системы электронной торговли, могут также использоваться в целях создания угрозы международному миру и национальной безопасности.

Установить источник подрывных действий, личность виновного в их совершении или мотивацию таких действий может быть нелегко. Во многих случаях виновных в совершении такой деятельности можно определить лишь по объекту этих действий, их последствиям или другим косвенным уликам, и они могут совершать такие действия, фактически где бы они ни находились. Эти факторы содействуют использованию ИКТ в целях осуществления подрывной деятельности. Неопределенность в плане определения источника действия и отсутствие общепринятого понимания создают риск нестабильности и неправильного восприятия.

Поступает все больше сообщений о том, что государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях. Все большее беспокойство вызывают физические лица, группы или организации, включая преступные организации, которые выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других. Растущая изощренность и масштабы преступной деятельности повышают вероятность оказания вредного воздействия. Хотя число свидетельств использования террористами ИКТ в целях ведения подрывных операций невелико, в будущем масштабы такого использования ИКТ могут возрасти.

Решение проблем XXI века зависит от успешного сотрудничества между партнерами, придерживающимися одинаковых убеждений. Сотрудничество между государствами и между государствами, частным сектором и гражданским обществом имеет важное значение, и для обеспечения эффективности мер по повышению информационной безопасности необходимо широкое международное сотрудничество. В докладе Группы правительственных экспертов выносятся рекомендации в отношении ведения дальнейшего диалога между государствами в целях снижения риска и защиты критической национальной и международной инфраструктуры.

Содержание

Предисловие Генерального секретаря

Десятилетие назад мы не могли себе представить, как глубоко информационные технологии и телекоммуникации войдут в нашу повседневную жизнь и сколь широко мы будем полагаться на их использование. Эти технологии привели к созданию объединенного в глобальную сеть международного сообщества, и хотя такое объединение создает огромные преимущества, оно порождает также уязвимость и риск.

В области принятия мер в связи с последствиями, обусловливаемыми новыми технологиями, достигнут значительный прогресс. Однако это трудная задача, и мы только начали разрабатывать нормы, законы и формы сотрудничества, необходимые в этой новой информационной среде.

С учетом этого я назначил группу правительственных экспертов из 15 государств для исследования существующих и потенциальных угроз в этой области и вынесения рекомендаций в отношении путей их устранения. Я благодарю Председателя Группы и экспертов за их кропотливую и усердную работу, результатом которой стал этот доклад, представляющий собой сжатое изложение проблемы и возможных последующих мер.

Генеральная Ассамблея призвана сыграть важную роль в процессе повышения безопасности информационных технологий и телекоммуникаций как на национальном, так и на международном уровнях. Для разработки общих концепций важное значение будет иметь диалог между государствами-членами. Жизненно важное значение имеет также практическое сотрудничество в целях обмена передовым опытом и информацией и создания потенциала в развивающихся странах, а также снижения риска неправильного восприятия, которое может ограничить возможности международного сообщества по принятию мер в случаях серьезных происшествий в киберпространстве.

Это насыщенная повестка дня будущей работы. Подготовка настоящего доклада призвана послужить первым шагом в направлении создания международной системы обеспечения безопасности и стабильности, необходимой в связи с этими новыми технологиями. Я предлагаю содержащийся в этом докладе анализ и рекомендации вниманию государств-членов и широкой мировой аудитории.

Препроводительное письмо

16 июля 2010 года

Имею честь представить настоящим доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Эта Группа была создана в 2009 году в соответствии с пунктом 4 резолюции 60/45 Генеральной Ассамблеи. В качестве Председателя Группы я с удовлетворением сообщаю вам, что по этому докладу был достигнут консенсус.

В указанной резолюции, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея просила создать в 2009 году Группу правительственных экспертов на основе справедливого географического распределения с тем, чтобы продолжить исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем. Генеральная Ассамблея просила Генерального секретаря представить ей доклад о результатах данного исследования на ее шестьдесят пятой сессии.

В соответствии с положениями данной резолюции были назначены эксперты из 15 государств: Беларуси, Бразилии, Германии, Израиля, Индии, Италии, Катара, Китая, Республики Корея, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Южной Африки. Список экспертов приводится в приложении.

Группа правительственных экспертов провела четыре сессии: первую сессию с 24 по 26 ноября 2009 года в Женеве, вторую — с 11 по 15 января 2010 года в Центральных учреждениях Организации Объединенных Наций, третью — с 21 по 25 июня 2010 года в Женеве и четвертую — с 12 по 16 июля в Центральных учреждениях Организации Объединенных Наций.

В Группе состоялся всесторонний и углубленный обмен мнениями по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Кроме того, Группа приняла во внимание мнения, изложенные в ответах, направленных государствами-членами во исполнение резолюций 60/45, 61/54, 62/17 и 63/37 Генеральной Ассамблеи, соответственно озаглавленных «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также материалы и справочные документы, предоставленные отдельными членами Группы.

Группа хотела бы выразить свою признательность за внесенный вклад Институту Организации Объединенных Наций по исследованию проблем разоружения, который консультировал Группу и был представлен в лице Джеймса Льюиса и Керстина Вигнарда. Группа хотела бы также выразить свою признательность сотруднику по вопросам информации Сектора информации и пропаганды Управления по вопросам разоружения Секретариата Юэну Бьюканану, который исполнял обязанности Секретаря Группы, и другим должностным лицам Секретариата, оказавшим содействие Группе.

(*Подпись*) Андрей В. **Крутских**
Председатель Группы

I. Введение

1. Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных проблем XXI века. Реализация этих угроз может нанести серьезный ущерб экономике и национальной и международной безопасности. Угрозы исходят из широкого круга источников и проявляются в подрывной деятельности, направленной в равной степени против физических и юридических лиц, национальной инфраструктуры и правительств. Ее последствия сопряжены со значительным риском для общественной безопасности, безопасности стран и стабильности объединенного в глобальную сеть международного сообщества в целом.

2. Информационные и коммуникационные технологии (ИКТ) обладают особенностями, которые затрудняют принятие мер в связи с угрозами, с которыми могут сталкиваться государства и другие пользователи. ИКТ распространены повсеместно и широко доступны. По своей сути они не являются чисто гражданскими или чисто военными технологиями, и цель их использования диктуется главным образом мотивами, которыми руководствуются пользователи. Во многих случаях владельцами и операторами сетей являются частный сектор или физические лица. В силу сложной взаимосвязанности телекоммуникационных сетей и Интернета любое устройство ИКТ может служить источником или объектом все более изощренных злонамеренных действий. Злоумышленное использование ИКТ можно легко скрыть. Установить источник подрывных действий, личность виновного в их совершении или мотивацию может быть нелегко. Во многих случаях виновных в совершении такой деятельности можно определить лишь по объекту этих действий, их последствиям или другим косвенным уликам. Исполнители угроз могут действовать в значительной степени безнаказанно, практически где бы они ни находились. Эти факторы содействуют использованию ИКТ в целях осуществления подрывной деятельности.

3. С учетом последствий использования рассматриваемых достижений для международной безопасности Генеральная Ассамблея Организации Объединенных Наций просила Генерального секретаря с помощью правительственных экспертов провести исследование как угроз в сфере информационной безопасности, так и соответствующих международных концепций и предложить возможные совместные меры, осуществление которых могло бы укрепить безопасность глобальных информационных и коммуникационных систем.

II. Угрозы, риски и уязвимые места

4. Глобальная сеть ИКТ стала ареной для осуществления подрывной деятельности. Мотивы осуществления подрывной деятельности весьма разнообразны: начиная с простой демонстрации технического мастерства и кончая кражей денежных средств и информации или совершением такой деятельности в качестве дополнительной формы конфликта с государством. К источникам таких угроз относятся такие негосударственные субъекты, как преступные элементы и, потенциально, террористы, а также сами государства. ИКТ могут использоваться для целей нанесения ущерба информационным ресурсам и инфраструктурам. Поскольку в силу своего характера они могут использоваться двояко, те же ИКТ, которые применяются для обеспечения надежной системы

электронной торговли, могут также использоваться в целях создания угрозы международному миру и национальной безопасности.

5. Многие вредоносные инструменты и методологии являются порождением усилий преступников и хакеров. Растущая изощренность и масштабы преступной деятельности повышают вероятность оказания вредного воздействия.

6. До настоящего времени число свидетельств попыток террористов поставить под угрозу или вывести из строя инфраструктуру ИКТ или провести операции с использованием ИКТ было невелико, хотя в будущем такие попытки могут активизироваться. В настоящее время террористы используют эти технологии по большей части для обмена сообщениями, сбора информации, вербовки сторонников, организации деятельности, пропаганды своих идей и действий и сбора средств, однако в конечном счете они могут начать применять ИКТ для совершения нападений.

7. Поступает все больше сообщений о том, что государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях. Неопределенность в плане определения источника действия и отсутствие общепринятого понимания того, какие действия государства в этой связи приемлемы, могут создать риск нестабильности и неправильного восприятия.

8. Все большее беспокойство вызывают физические лица, группы или организации, включая преступные организации, которые выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других. Такие посредники, руководствуясь либо финансовой выгодой, либо другими причинами, могут предлагать государственным и негосударственным субъектам целый набор наносящих умышленный вред услуг.

9. В результате как роста применения ИКТ в критических инфраструктурах, так и расширения использования устройств мобильной связи и сетевых услуг возникают новые уязвимые места и возможности для совершения подрывных действий.

10. Государства обеспокоены также тем, что система поставок ИКТ может подвергнуться такому влиянию или быть нарушена таким образом, что это скажется на обычном, безопасном и надежном использовании ИКТ. Включение в ИКТ вредоносных скрытых функций может подорвать доверие к товарам и услугам, вызвать недоверие к торговле и сказаться на национальной безопасности.

11. Различия в степени оснащенности ИКТ и их безопасности в разных государствах повышают уязвимость глобальной сети. Различия в национальных законодательствах и практике могут создать проблемы на пути формирования безопасной и быстро восстанавливающейся цифровой среды.

III. Совместные меры

12. Риски, связанные с объединенными в глобальную систему сетями, требуют принятия согласованных мер. На протяжении прошедшего десятилетия государства-члены неоднократно подтверждали необходимость осуществления международного сотрудничества в области принятия мер в связи с угрозами в

сфере безопасности ИКТ для борьбы со злонамеренным применением информационных технологий в преступных целях, создания глобальной культуры кибербезопасности и поощрения других важных мер, которые могут уменьшить риск.

13. В течение прошедшего десятилетия усилия по борьбе с угрозой киберпреступности прилагались на международном уровне, в частности в рамках Шанхайской организации сотрудничества, Организации американских государств, Форума азиатско-тихоокеанского экономического сотрудничества, Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН), Экономического сообщества западноафриканских государств, Африканского союза, Европейского союза, Организации по безопасности и сотрудничеству в Европе и Совета Европы, а также в форме двусторонних усилий государств.

14. Следует уделять надлежащее внимание сферам непреступного применения ИКТ транснационального характера. Сюда относится риск неправильного восприятия в результате отсутствия общепринятого понимания международных норм, касающихся государственного использования ИКТ, что может сказаться на принятии мер в кризисных ситуациях, возникающих в результате серьезных происшествий. Это требует разработки мер, направленных на углубление сотрудничества в тех областях, где это возможно. Такие меры могут быть также направлены на обмен информацией и передовыми методами, устранение последствий происшествий, создание доверия, снижение риска и повышение транспарентности и стабильности.

15. Очевидно, что, поскольку подрывная деятельность с использованием информационно-коммуникационных технологий приобретает все более сложный и опасный характер, ни одно государство не может справиться с этими угрозами в одиночку. Решение проблем XXI века зависит от успешного сотрудничества между партнерами, придерживающимися одинаковых убеждений. Сотрудничество между государствами и между государствами, частным сектором и гражданским обществом имеет важное значение, и для обеспечения эффективности мер по повышению информационной безопасности необходимо широкое международное сотрудничество. В связи с этим международному сообществу следует изучить вопрос о необходимости осуществления совместных действий и создания совместных механизмов.

16. Существующие соглашения включают нормы, касающиеся использования ИКТ государствами. С учетом особенностей ИКТ со временем могут быть разработаны дополнительные нормы.

17. Создание потенциала имеет жизненно важное значение для достижения успеха в обеспечении глобальной безопасности ИКТ, оказания помощи развивающимся странам в их усилиях по повышению безопасности их критических национальных информационных инфраструктур и устранения нынешней пропасти в уровне безопасности ИКТ. Для создания потенциала в государствах, которым может быть необходима помощь в решении вопросов безопасности их ИКТ, потребуется тесное международное сотрудничество.

IV. Рекомендации

18. С учетом существующих и потенциальных угроз, рисков и уязвимых мест в области информационной безопасности Группа правительственных экспертов считает полезным рекомендовать дальнейшие шаги по разработке мер укрепления доверия и прочих мер в целях снижения риска возникновения неправильного восприятия в результате дезорганизации или нарушений, связанных с применением ИКТ:

i) продолжение диалога между государствами в целях обсуждения норм, касающихся государственного использования ИКТ, сокращения коллективного риска и защиты критической национальной и международной инфраструктуры;

ii) принятие мер по укреплению доверия, обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах;

iii) осуществление обмена информацией о национальных законах и национальных стратегиях обеспечения безопасности информационно-коммуникационных технологий и технологиях, принципах и передовых методах;

iv) определение мер оказания содействия созданию потенциала в менее развитых странах;

v) нахождение возможностей для выработки общей терминологии и определений в связи с положениями резолюции 64/25 Генеральной Ассамблеи.

Приложение

Список членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Г-н Владимир Н. Герасимович
Начальник Управления международной безопасности и контроля над вооружениями
Министерство иностранных дел
Беларусь

Г-н Александр Пономарев (третья сессия)
Советник Постоянного представительства Республики Беларусь при Отделении Организации Объединенных Наций в Женеве

Г-н Александр Мариано Фейтоза
Командующий
Корпус морских фузилеров, Военно-морской флот Бразилии
Управление политики, стратегии и по международным делам
Министерство обороны
Бразилия

Г-н Ли Сун (первая и вторая сессии)
Заместитель Генерального директора
Департамент по контролю над вооружениями и разоружению
Министерство иностранных дел
Китай

Г-н Кан Юн (третья и четвертая сессии)
Заместитель Генерального директора
Департамент по контролю над вооружениями и разоружению
Министерство иностранных дел
Китай

Г-н Линнар Вик
Адъюнкт-профессор Эстонского информационно-технологического колледжа
Эстония

Г-н Аймерик Симон
Международные отношения
Национальное управление безопасности информационных систем
Генеральный секретариат национальной обороны и безопасности
Франция

Г-н Грегор Кёбель
Начальник Отдела по контролю над обычными вооружениями
Федеральное министерство иностранных дел
Германия

Г-н Б. Дж. Сринатх
Старший директор
Группа быстрого реагирования на нарушения компьютерной безопасности Индии
Министерство информационных технологий
Индия

Г-жа Родика Радиан-Гордон
Директор
Департамент по контролю над вооружениями
Министерство иностранных дел
Израиль

Г-н Винченцо Делла Корте (первая и третья сессии)
Директор Сектора безопасности систем связи
Аппарат при Председателе Совета министров
Италия

Г-н Вальтер Меккиа (вторая и четвертая сессии)
Сектор безопасности систем связи
Аппарат при Председателе Совета министров
Италия

Г-н Рашид А. Аль-Моханнади (первая сессия)
Командир роты связи сухопутных сил
Войска связи эмира
Катар

Г-н Саад М. Р. Аль-Кааби
Подполковник (инженер)
Министерство обороны
Катар

Г-н Лю Кван-чхуль
Посол
Министерство иностранных дел и торговли
Республика Корея

Г-н Андрей В. Крутских
Заместитель директора
Департамент по вопросам новых вызовов и угроз
Министерство иностранных дел
Российская Федерация

Г-жа Пализа Банда (первая сессия)
Заместитель директора, Отдел регулирования Интернета
Министерство связи
Южная Африка

Генерал-майор Марио Сильвино Брацколи
Сотрудник Государственного управления информационных технологий
Министерство обороны
Южная Африка

Г-н Гавин Уиллис
Группа по международным отношениям
Национальное техническое управление информационной безопасности
Соединенное Королевство Великобритании и Северной Ирландии

Г-жа Мишель Маркофф
Старший советник по политическим вопросам
Управление по вопросам киберпространства
Государственный департамент США
Соединенные Штаты Америки