Организация Объединенных Наций A/57/166/Add.1

Генеральная Ассамблея

Distr.: General
29 August 2002
Russian
Original: Arabic/English/Spanish

Пятьдесят седьмая сессия
Пункт 62 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**

Содержание

* A/57/150.

** Информация, содержащаяся в настоящем докладе, была получена после представления основного доклада.

02-56151 (R) 200902 200902
0256151

Ответы, полученные от правительств

Куба

[Подлинный текст на испанском языке]
[15 июля 2002 года]

Общая оценка проблем информационной безопасности

1. Научно-технический прогресс человечества, достигнутый в последние десятилетия, является поистине огромным. Вне сомнения, прогресс в области информатизации и телекоммуникации является одним из аспектов технологической революции, которая охватывает все сферы человеческой деятельности. Сочетание процесса информатизации с прогрессом в области телекоммуникаций открывает невообразимые горизонты для потенциального развития обеих областей.

2. Создание быстро действующих компактных компьютеров, обладающих огромной оперативной мощностью, использование новых материалов, которые умножают скорость передачи информации и распространение спутниковой связи, — это лишь некоторые из примеров достигнутого прогресса.

3. Происходящий в настоящее время процесс глобализации является одним из ощутимых следствий так называемой технологической революции. Благодаря ему сокращаются расстояния, и средства связи и связанные с ними потоки информации осуществляются в реальном времени. В развитии промышленных технологий произошел резкий скачок, и средства информации все больше используются в реорганизации производственных процессов, что позволяет достичь невиданных никогда ранее уровней производительности.

4. Эти преобразования затрагивают не только гражданский сектор, но также и военную промышленность. В наши дни информатизация является неотъемлемым компонентом современных видов вооружений и их систем. В течение последнего десятилетия мы были свидетелями различных вооруженных конфликтов, в которых с большим эффектом применялись невиданные ранее современные виды вооружений, обладающих смертоносным разрушительным потенциалом и высоким уровнем точности для поражения своих целей; все это в значительной степени является следствием применения прогресса в области информатизации.

5. Информационные средства продемонстрировали свои возможности. Например, программное обеспечение находит все более широкий круг видов применения, среди которых все более стремительно распространяются вредные программы или программы, имеющие исключительно высокий уровень вредного воздействия, которые могут в течение относительно короткого времени причинить непоправимый ущерб в любой точке земного шара, учитывая распространение информационных сетей и уровень доступа к ним.

6. Зависимость, вызванная применением таких технологий, требует совместного размышления, с тем чтобы обеспечить надлежащее использование всех этих средств.

7. Сам факт включения этого вопроса в повестку дня Генеральной Ассамблеи свидетельствует о том, что международное сообщество сознает потенциальную опасность, которую представляет для международного мира и безопасности использование этих технологий в немирных целях.

8. С другой стороны, враждебное применение телекоммуникаций в некоторых случаях под объявленным или скрытым предлогом подрыва юридической и политической системы государств является еще одним негативным проявлением применения таких средств, последствия которого могут вызвать напряженность и неблагоприятные последствия для международного мира и безопасности, что вступает в явное противоречие с принципами и целями, воплощенными в Уставе Организации Объединенных Наций.

9. Резолюция 56/19 Генеральной Ассамблеи открывает перед нами возможность осуществить анализ всех аспектов информатизации и телекоммуникаций в контексте международной безопасности, включая возможность укрепления и усиления норм международного права, действующих в этой области.

Определение основных критериев, касающихся информационной безопасности, в частности несанкционированного вмешательства или противоправного использования информационных и телекоммуникационных сетей и информационных ресурсов

10. Ниже приводится перечень некоторых основополагающих критериев.

1. Согласование норм и процедур

11. Отсутствие кодекса общих этических норм для всех пользователей, учитывая свободный характер доступа к сетям Интернет и использование спутниковых и других средств связи, создают опасность для безопасности передаваемой с помощью этих средств информации.

12. Эффективность использования сети характеризуется такими элементами, как конфиденциальность, целостность и доступность. Эти элементы гарантируют использование информации только лишь санкционированными пользователями, без ее изменения и готовой для использования во всех случаях, когда это необходимо.

13. Когда не соблюдаются эти требования, уменьшается или же полностью исчезает безопасность. Каждый производитель информационных средств должен гарантировать, что его программное обеспечение или оборудование исключает противоправный доступ, а также не допускать производства информационного оружия, способного наносить ущерб некоторым из этих элементов информационных систем. В целом эти принципы имеют отношение ко всем видам использования услуг или производства информационно-коммуникационных товаров и технологических систем.

14. Это возможно лишь в той степени, в какой каждый производитель информационных систем сможет создать оптимальный контроль над процессами производства, технологиями и системами и, кроме того, обеспечит с учетом этих же целей контроль за последующей эксплуатацией и использованием этих систем и технологий. В этой связи необходимо располагать механизмами сотрудничества, которые позволят обеспечить взаимное заблаговременное предупреждение на уровне поставщиков и пользователей о любом нарушении, а также установит ответственность производителей за решение проблем, связанных с обеспечением безопасности продаваемых ими товаров.

15. Необходимо разработать минимальные стандарты для производства технологий в условиях безопасности. Эти стандарты должны также сертифицироваться, учитывая необходимость согласования этих механизмов. В этом смысле Куба готова развивать сотрудничество, учитывая свой собственный опыт в этой области с теми странами, которые проявят заинтересованность.

2. Несанкционированное вмешательство в информационные или телекоммуникационные системы

16. Необходимо усилить международные положения, которые будут препятствовать нарушению работы таких систем. Государства в одиночку не могут решить эту проблему. Уровень взаимозависимости, определяющий универсальный характер информационных сетей и телекоммуникационных систем, исключает возможность того, что эту задачу сможет решить только одно государство.

17. Необходимо соблюдать уже существующие международные нормы. Доступ к информационным или телекоммуникационным системам другого государства может иметь место только с предварительного согласия соответствующего государства в той степени и в том объеме, который будет санкционирован этим государством.

18. Нападение на информационные или телекоммуникационные системы иностранных государств может поставить под угрозу международный мир и безопасность. Эти процедуры уже использовались в качестве средства осуществления враждебной политики.

19. Куба является объектом такой агрессии, осуществляемой при поддержке и с согласия правительства Соединенных Штатов Америки. Для того чтобы получить представление о серьезности этого вопроса, следует отметить, что наша страна на протяжении нескольких десятилетий подвергалась радио- и телевизионной агрессии со стороны Соединенных Штатов Америки, которые провозгласили цель подрыва внутреннего строя и свержения правительства Республики Куба.

20. В этих целях, например, начиная с января 2001 года по март 2002 года с территории Соеди-

ненных Штатов Америки в среднем осуществляли вещание 15 радио- и телевизионных станций, передавая лживую и тенденциозную информацию, имеющую явно подрывной характер.

21. Эти станции ежедневно в течение этого периода вещали порядка 312–319 часов на средних и коротких волнах и в диапазоне частотного модулирования. В среднем это означает 2257 часов в неделю. Если к этому добавить телевизионное вещание, то эта цифра составит порядка 2288 часов в неделю в целом.

22. В рамках этой радио- и телевизионной агрессии правительство Соединенных Штатов Америки осуществляло начиная с 1990 года инвестиции на сумму более 20 млн. долл. США в год и, в частности, в течение нынешнего финансового года — порядка 24 млн. долл. США.

23. В большинстве своих случаев эта информация подстрекает к гражданскому неповиновению и совершению актов вандализма и терроризма. Так, совсем недавно одна радиостанция правительства Соединенных Штатов Америки спровоцировала инцидент, имевший своей целью создание ситуации внутреннего беспорядка на Кубе, и в этом инциденте, кроме того, было замешено дипломатическое представительство третьей страны, что создало ситуацию напряженности, которая могла нанести ущерб дипломатическим отношениям Кубы с этой страной.

3. Противоправное использование информационных и телекоммуникационных систем

24. Речь идет об использовании таких систем вне рамок существующих международных процедур и норм и в нарушение соответствующих национальных положений. Государства, которые еще не сделали этого, должны принять все необходимые меры для укрепления соответствующих национальных положений.

25. Необходимо осуществлять периодический обзор международных положений в этой области, учитывая стремительное развитие соответствующих технологий, с тем чтобы эффективность и результативность этих норм соответствовали темпам развития технологий.

26. В настоящее время практически ни одна сфера деятельности общества, ни один вид человеческой деятельности не остается в стороне от влияния информационных или телекоммуникационных систем, в результате чего противоправное использование этих средств может иметь невообразимые последствия.

4. Информационно-технологические системы как технологии двойного использования

27. Одной из особенностей исторического развития в этой области является то, что возникновение новых технологий происходило одновременно как в гражданской, так и военной областях. Иначе говоря, многие из технологий, которые сегодня обширно используются в гражданской жизни, зародились в военной области и наоборот.

28. В результате этого усилия международного сообщества в этом вопросе должны осуществляться по двум направлениям: предотвращение, пресечение и искоренение использования информационных и телекоммуникационных систем во враждебных целях и обеспечение возможностей для того, чтобы международное сообщество могло их использовать в мирных целях.

29. Это означает, в частности, анализ следующих элементов, связанных с информационными и телекоммуникационными системами:

a) разработка и повсеместное применение процедур, исключающих несанкционированный доступ к этим системам;

b) транспарентность использования этих средств;

c) разработка конкретных мер для защиты информационных систем, связанных с оружием массового уничтожения и другими видами современного оружия;

d) применение мер с целью недопущения несанкционированного доступа к информационным системам ядерных электростанций, тепловых электростанций и других стратегически важных объектов страны;

e) обмен информацией между государствами о противоправной деятельности физических или юридических лиц, находящихся под их контролем или юрисдикцией, который имел бы в качестве сво-

ей основополагающей цели воспрепятствовать совершению противоправных деяний;

f) расширение международного сотрудничества в целях содействия передаче технологий и профессиональной подготовке или развитию соответствующего национального потенциала;

g) запрещение размещения этих средств в космическом пространстве в военных целях;

h) укрепление основополагающего принципа международных отношений, касающегося невмешательства во внутренние дела государств с помощью, в частности, принятия мер, запрещающих использование информационных и телекоммуникационных систем в этих целях.

5. Информационное оружие

30. Информационные и телекоммуникационные системы могут использоваться в качестве оружия, когда их разработка и/или их применение осуществляется с целью нанесения ущерба инфраструктуре другого государства. Например, нападение на национальные сети с использованием иностранного программного обеспечения или с помощью внутренних источников в государстве, которые были разработаны при иностранном содействии или поставлены из-за границы; осуществление радио- или телевизионных передач с помощью несанкционированных средств или без согласия подвергшегося агрессии государства; воздействие на поведение людей с целью дестабилизировать общество, свергнуть правительство или изменить социальный и политический строй других стран.

6. Терроризм в отношении информационных и телекоммуникационных систем

31. Необходимо вести борьбу с терроризмом и отвергать его во всех формах и проявлениях независимо от того, кто его осуществляет и против кого он осуществляется. Эти технологии также могут использоваться для совершения террористических актов. Их широкое распространение, относительно легкий доступ к ним и низкие издержки, связанные с их применением, делают эти технологии привлекательными для террористов.

32. Эти действия могут иметь весьма разнообразный и весьма опасный характер, включая нарушение работы автоматизированных систем в аэропортах; нарушение работы навигационных систем пассажирских воздушных судов; нанесение ущерба системам управления электростанциями, источникам водоснабжения и автотранспортным магистралям; нанесение ущерба коммуникационным сетям и т.д.

33. Оценка прогресса в области информатизации и телекоммуникаций в контексте международной безопасности неизбежно требует учета проблем, связанных с терроризмом. Очевидно, что одним из путей для рассмотрения этого вопроса являются переговоры, которые ведутся в рамках Организации Объединенных Наций по вопросам международной борьбы с терроризмом в целях разработки международных норм и положений, а также другие соответствующие многосторонние инициативы.

34. Куба готова осуществить анализ этих и других основополагающих критериев, которые будут предложены, и считает, что Организация Объединенных Наций как основной гарант международного мира и безопасности является самым подходящим форумом для обсуждения этих вопросов.

35. Кроме того, в обсуждении этих вопросов должны участвовать специализированные международные учреждения, занимающиеся информационными и телекоммуникационными системами.

Целесообразность разработки международных принципов в целях повышения безопасности всемирных информационных и телекоммуникационных систем и содействия борьбе против терроризма и преступности в области информации

36. Очевидно, что необходимо укрепить нормы международного права в области информации и телекоммуникации. Мы не начинаем с нуля, ибо уже существуют международные принципы, положения и процедуры, которые необходимо учитывать. Также необходимо учитывать существующий национальный опыт.

37. Необходимо работать как над разработкой не имеющих обязательного характера руководящих принципов, так и над принятием норм, которые могут принять форму международных, многосторонних и имеющих юридически обязательную силу протоколов или конвенций.

38. В рамках обеих методологий необходимо рассмотреть изложенные в этом документе основополагающие критерии, а также другие предложения, в частности вопрос о несанкционированном вмешательстве или противоправном использовании информационных и телекоммуникационных систем и информационных ресурсов; вопросов суверенитета, связанных с этими темами; вопрос мирного использования информационных и телекоммуникационных средств во всех его аспектах; предотвращение, пресечение и искоренение враждебных методов использования этих систем; применение национальных средств, обеспечивающих более строгий контроль со стороны государства над информационными и телекоммуникационными системами, и борьба с соответствующими преступными деяниями.

Панама

[Подлинный текст на испанском языке]
[24 июня 2002 года]

1. Республика Панама с озабоченностью признает, что огромный технологический прогресс в области информатизации и телекоммуникации превратил так называемое «поле виртуальной битвы» в новый вызов для международной безопасности: эта технология используется не только в ходе вооруженных конфликтов, но также и для их урегулирования (сбор разведданных, выбор мишеней, соотношение качества и количества оружия).

2. Осуществление нападения с использованием новых информационных и телекоммуникационных технологий может причинить бóльший ущерб, чем, например, бомбардировка с применением обычного оружия. В настоящее время электронно-вычислительные средства регулируют финансовую информацию, потоки нефти и газа по газо- и нефтепроводам, запасы воды и мониторинга водохранилищ, контроль за воздушным движением, контроль за транзитом по Панамскому каналу и работу чрезвычайных служб и т.д. Соответственно, определение основополагающих критериев, касающихся информационной безопасности, в частности несанкционированного вмешательства в информационные и телекоммуникационные системы и информационные ресурсы или противоправного использования этих систем, требует создания систем защиты, которые соответствовали бы этому новому виду насилия. Тем не менее такие системы защиты (брандмауэр и т.д.) требуют использования большого объема финансовых и людских ресурсов, которых недостает во многих из наших стран.

3. Так, например, усиление безопасности глобальных информационных и телекоммуникационных систем требует создания надежной системы, которая позволила бы осуществлять обмен информацией между государствами в целях контроля и пресечения деятельности или общения между отдельными лицами или сетями отдельных лиц, которые используют коммуникационные технологии для осуществления своей преступной деятельности. Тем не менее эта необходимость приобретает форму обязательства и является обязанностью технологически развитых стран предоставить и передать такие технологии и осуществить профессиональную подготовку тех, кто ее не имеет. Кроме того, эти страны должны взять на себя обязательство не использовать свои технологические преимущества в целях торгового или промышленного шпионажа в ущерб остальным менее развитым в технологическом отношении странам.

4. Несмотря на ущерб, который может причинить Интернет и новые информационные и телекоммуникационные технологии, они являются теми средствами, которые при надлежащем использовании могут реально содействовать укреплению международной безопасности путем обеспечения необходимых средств для достижения целей безопасности человечества.

Сирийская Арабская Республика

[Подлинный текст на арабском языке]
[28 августа 2002 года]

Ниже воспроизводятся соображения заинтересованных сторон в Сирийской Арабской Республике по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности.

– Эмбарго на информационные технологии и средства и на их импорт в развивающиеся государства — члены Организации Объединенных Наций должно быть отменено.

– Организации Объединенных Наций следует играть активную роль в законодательной и

практической деятельности, связанной с преодолением цифрового разрыва между развитыми в научно-техническом плане и развивающимися государствами.

– Необходимо принять законы, препятствующие несанкционированному вмешательству государств, организаций и частных лиц в информационные и телекоммуникационные системы других государств, причем соответствующее законодательство должно предусматривать применение санкций в отношении нарушителей.

– Необходимо обеспечить осуществление резолюций Международного союза электросвязи, которые предусматривают защиту каждого государства — члена Организации Объединенных Наций от создания помех на используемых ими радиочастотах и от противоправного использования этих частот любым другим государством или любой иной стороной.

– Необходимо принять основополагающие принципы и международные нормы, касающиеся включения информации об истории цивилизации и культуре народов в базы данных и ее распространения по каналам информационных сетей (Интернет) и предполагающие воздержание от использования вводящих в заблуждение данных и принятие соответствующих мер в отношении нарушителей.

– Необходимо учредить пользующийся широкой поддержкой международный орган, задача которого заключалась бы в оказании государствам помощи в подготовке обоснований и проведении исследований по вопросам, касающимся сотрудничества в обеспечении режима информационной безопасности. В круг обязанностей этого международного органа входило бы, в частности, обеспечение предоставления этим государствам материально-технической помощи, позволяющей им выполнять поставленные перед ними задачи, и помощи в подготовке кадров национальных специалистов — на основе сотрудничества в решении технологических вопросов обеспечения безопасности информационных и телекоммуникационных систем.