Организация Объединенных Наций A/56/164

# Генеральная Ассамблея

Distr.: General
3 July 2001
Russian
Original: English/Spanish

**Пятьдесят шестая сессия**
Пункт 81 первоначального перечня*
**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/56/50.

** От имени государств — членов Европейского союза, являющихся членами Организации Объединенных Наций.

01-44868 (R) 090801 100801
*0144868*

# I. Введение

1. В своей резолюции 55/28 от 20 ноября 2000 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея просила все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам: a) общая оценка проблем информационной безопасности; b) определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов; и c) содержание соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем; и просила Генерального секретаря представить на основе ответов, полученных от государств-членов, доклад по этому вопросу на ее пятьдесят шестой сессии.

2. 19 марта 2001 года Генеральный секретарь направил государствам-членам вербальную ноту с просьбой представить их мнения в ответ на просьбу Ассамблеи. Ответы, полученные от правительств по состоянию на 3 июля 2001 года, воспроизводятся в разделе II настоящего доклада; любые другие поступающие ответы будут издаваться в качестве добавлений к докладу.

# II. Ответы, полученные от правительств

## Боливия

[Подлинный текст на испанском языке]
[14 июня 2001 года]

Согласно информации, полученной из министерства иностранных дел Боливии, имею честь сообщить вам, что вооруженные силы Боливии в настоящее время не обладают надлежащими электронными средствами и не предусматривают их приобретения или производства в будущем.

## Мексика

[Подлинный текст на испанском языке]
[16 мая 2001 года]

1. Мексика считает необходимым уделять больше усилий в целях содействия гражданскому применению научно-технологических достижений и средств массовой информации. Мексика поддержала резолюции Генеральной Ассамблеи 53/70 от 4 декабря 1998 года и 54/49 от 1 декабря 1999 года, озаглавленные «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

2. В настоящее время основной озабоченностью в связи с проблемой безопасности является возможность уязвимости информационных систем, регулирующих оборонные программы некоторых стран, а также опасность использования информации и телекоммуникаций террористами или в целях устрашения.

3. В этой связи только международное сотрудничество и нормы международного права обеспечивают возможности для того, чтобы средства, которые будут созданы в связи с проблемами безопасности в области информации, никоим образом не ограничивали свободу информации и коммуникаций.

4. Значение этой сферы неоспоримо. Тем не менее необходимо также учитывать деятельность и обсуждения, осуществляемые в рамках других комитетов Генеральной Ассамблеи, которые могут в значительной степени содействовать выработке определения и уточнения концепций, которые могут использоваться для рассмотрения проблем, связанных с информационной безопасностью.

5. Что касается вопроса об определении основополагающих международных критериев и концепций в области информационной безопасности, Мексика считает, что концепция несанкционированного вмешательства может привести к нежелательным недоразумениям, поскольку это связано с возможностью принятия действий некоторыми государствами, которые, ссылаясь на гуманитарные или другие причины сомнительного характера, могут вмешаться на индивидуальной или коллективной основе во внутренние дела других государств.

6. В этом смысле возможно было бы лучше опустить эту концепцию и заменить ее концепцией «несанкционированного доступа» или просто «противоправного доступа» применительно к действиям, осуществляемым некоторыми физическими или юридическими лицами в отношении информационных систем.

7. Что касается необходимости разработки международных принципов, которые способствовали бы усилению безопасности международных информационных и телекоммуникационных систем, необходимо подчеркнуть, что такие принципы не только должны содействовать усилению безопасности таких систем, но также и самым эффективным образом гарантировать их законность.

8. Кроме того, представляется целесообразным осуществить тщательный анализ соответствующих положений, содержащихся в международных документах, принятых в течение последних лет как Генеральной Ассамблеей, так и другими международными организациями, прежде всего Организацией Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), в области международной безопасности, международного терроризма и информации с целью определения и оценки соответствующих имеющихся принципов, которые применяются в этой области.

9. В этой связи Мексика поддерживает положения резолюции 51/210 от 17 декабря 1996 года, касающейся средств борьбы с международным терроризмом, в частности пункт 3(c) части I, в котором содержится ссылка на возможную опасность использования террористами электронных или проводных систем и систем связи для совершения преступных действий и необходимость изыскания соответствующих национальному законодательству средств для предотвращения такого рода преступности и расширения сотрудничества для предотвращения такой преступной деятельности.

10. В ходе десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, который состоялся в Вене 10–17 апреля 2000 года, секретариат подготовил документ, озаглавленный «Преступления, затрагивающие информационные системы» (A/CONF.187/10), в котором отмечается, что для эффективной борьбы и предотвращения кибернетических преступлений необходимо применять согласованный международный подход на различных уровнях.

11. Что касается внутригосударственной деятельности, то расследование таких преступлений потребует использования экспертов, специализированных знаний и надлежащих процедур. В этой связи государствам предлагается рассмотреть возможность создания механизмов, которые позволили бы своевременно получать точные данные об информационных системах и сетях, когда такие данные требуются в качестве доказательства в ходе судебного разбирательства.

12. На международном уровне эффективное расследование преступлений в электронной сфере требует принятия своевременных действий на основе сотрудничества между национальными правоохранительными органами и соответствующими юридическими властями.

## Филиппины

[Подлинный текст на английском языке]
[22 мая 2001 года]

### 1. Общая оценка проблем информационной безопасности

1. Сложность и масштабы этой проблемы и вопросов в области информационной безопасности являются огромными и безграничными, в результате чего информационная безопасность приобретает характер серьезной глобальной проблемы. Наблюдается стремительный рост угроз, связанных с проблемами, возникающими в сегодняшнюю информационную эпоху. Все технологические достижения и новшества также создают новые возможности, которые могут использоваться в ущерб благородным устремлениям человечества.

2. Проблема информационной безопасности в равной степени чревата такой же угрозой, как и оружие массового уничтожения. Она представляет опасность для всех аспектов жизни человека. Эта проблема, которую не смогут решить в одиночку ни одна страна, ни группа стран. Речь идет о глобальной проблеме, для решения которой настоятельно необходимы согласованные усилия всех стран независимо от того, являются ли они передовыми в технологическом отношении или нет.

### 2. Определение основных понятий, относящихся к информационной безопасности, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов

3. Ниже перечисленные основополагающие концепции можно определить следующим образом:

a) *несанкционированное вмешательство или несанкционированное проникновение*: i) неправительственный акт вмешательства; или ii) санкционированное правительством вмешательство, которое не вписывается в рамки установленного международного режима или протоколов в области информационной безопасности;

b) *санкционированное вмешательство*. «Вмешательство», осуществляемое по инициативе правительства, в соответствии с положениями международных договоров или в пределах границ установленного международного режима или протоколов в области информационной безопасности;

c) *несанкционированное использование информации*: i) противоправное использование публичной и частной информации, которая была законным путем получена без предварительного разрешения источников; ii) противоправное использование жизненно важной публичной и частной информации, которая была законным путем получена правительственными учреждениями для личных неправительственных интересов; iii) противоправное использование жизненно важной государственной и частной информации, которая была законным путем получена правительством вне рамок какого-либо установленного международного режима или протоколов в области информационной безопасности или других соответствующих договоров и международных законов;

d) *противоправное использование информационных и телекоммуникационных систем*: i) использование информационных и телекоммуникационных ресурсов, включая соответствующие инфраструктуры для противоправных целей; и ii) любой вид несанкционированного использования информации;

e) *информационные ресурсы*. Речь идет о необработанных и обработанных данных (например, статистические данные, факты, цифры, архивы и т.д.), программном обеспечении, технокибернетическом оборудовании/технике (например, персональные компьютеры, лэптопы, сканерные устройства и другие новые и передовые формы технологии), информационной технологии и других соответствующих средствах (например, трансляционные мачты, спутниковые антенны, контрольные мачты/здания), экспертах и специалистах в области информационных технологий (например, программисты, системные аналитики и т.д.), включая информационно-кибернетические сети и системы (Интернет);

f) *информационное оружие*. Информационные ресурсы, стратегически разработанные или созданные для ведения информационной войны или для причинения ущерба, замешательства, создания неудобств или любых других действий злонамеренного характера;

g) *информационная война*: i) действия с целью достижения информационного превосходства путем применения мер для эксплуатации, подрыва, уничтожения, дестабилизации и разрушения информационного потенциала противника и его функций; ii) меры с целью защиты собственных информационных ресурсов и телекоммуникационных систем; iii) действия с целью использования информационных ресурсов и телекоммуникационных систем другой стороны для достижения целей и интересов, например

электронная война (информационная война в оборонительном и военном контексте), война в Интернете (информационная война в более широком общественном контексте).

h) *информационный терроризм*. Террористические деяния в контексте информационной безопасности;

i) *электронно-кибернетические преступления или информационные преступления*: i) противоправные деяния, совершаемые с использованием элементов информационной безопасности; ii) действия злонамеренного характера, направленные против информационных ресурсов (например, технологический вандализм, несанкционированный технологический доступ и суперзаппинг); iii) любой вид несанкционированного вмешательства или проникновения.

j) *электронно-кибернетические/технологические преступники* : i) лица, совершающие действия в нарушение установленного международного режима или протоколов в области информационной безопасности; ii) лица, чьи преступные деяния связаны или в значительной степени зависят от использования информационной безопасности; iii) лица, которые неоднократно совершают деяния, направленные против информационных ресурсов (подозреваемые лица, являющиеся несовершеннолетними, должны быть освобождены от привлечения к ответственности в качестве технологических преступников);

k) *информационная колонизация*: i) действия, совершаемые одним государством или государствами против другого государства с целью установления господства и контроля в информационной области, предотвращения доступа к новейшим информационным технологиям и создания ситуации, когда другие государства становятся технологически зависимыми в информационной области; ii) акты информационной экспансии и установления монополии над национальными информационными и телекоммуникационными инфраструктурами другого государства с целью создания условий зависимости и контроля;

l) *технологически передовые государства*: i) страны, экономика которых более чем на 50 процентов охвачена информационными сетями; ii) может в целом относиться к развитым странам.

## 3. Содержание концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем, упомянутых в пункте 2 резолюции 55/28

4. Предложение о создании международного режима в области информационной безопасности является исключительно важным в настоящее время. Такие предложения должны обеспечить отчетность со стороны государств, которые нарушают соответствующие протоколы в области информационной безопасности. Это должно также содействовать созданию баланса между технологически передовыми странами и странами, которые таковыми не являются. Данный режим должен осуществлять контроль за технологически передовыми странами, которые уже в настоящее время осуществляют свое собственное «вмешательство» в других странах, которые находятся в невыгодном положении. Наконец, этот режим должен в

значительной степени учитывать, что «обеспечение соблюдения законов» является важным фактором в усилении международной информационной безопасности. Это может быть осуществлено на практике путем создания международного центра, который будет координировать деятельность правоохранных подразделений различных стран в деле поиска подозреваемых лиц, а также в оказании содействия этим странам в осуществлении их внутригосударственных операций.

## Швеция*

[Подлинный текст на английском языке]
[26 июня 2001 года]

1. На пятьдесят пятой сессии Генеральная Ассамблея Организации Объединенных Наций и государства — члены Европейского союза поддержали принятую консенсусом резолюцию 55/28 Ассамблеи, озаглавленную «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Государства — члены ЕС хотели бы направить следующий общий ответ в связи с пунктом 3 резолюции, в котором государствам — членам Организации Объединенных Наций предлагается информировать Генерального секретаря о своей точке зрения и об оценках.

### 1. Общая оценка проблем информационной безопасности

2. Информационные и телекоммуникационные технологии содействуют в значительной степени свободному потоку информации и создают огромные выгоды для отдельных лиц, предпринимателей и правительств во всем мире. Они способствуют развитию демократии и свободы слова, а также прогрессу гражданского общества. Европейский союз считает, что важно развивать и гарантировать дальнейший прогресс в области информационных и телекоммуникационных технологий, а также в области усиления принципа свободы информации. Европейский союз признает, что существует потенциальная опасность несанкционированного вмешательства или противоправного использования информационных и телекоммуникационных систем, нарушения целостности информационных инфраструктур и информационных ресурсов отдельных лиц, предприятий, учебных или медицинских учреждений и организаций частного сектора, а также правительств.

3. Информационная и сетевая безопасность означает защиту личной информации об отправителях и получателях, защиту информации от несанкционированных изменений, защиту от несанкционированного доступа к информации и создание надежного источника поставок оборудования, услуг и информации.

4. Информационная безопасность охватывает также защиту информации, касающейся военного потенциала и других аспектов национальной безопасности. Недостаточная защита жизненно важных информационных ресурсов и информационных и телекоммуникационных систем может создать опасность для международной безопасности.

### 2. Возможное содержание соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем

5. В качестве исходного пункта ЕС хотел бы подчеркнуть, что, хотя международное сотрудничество является исключительно важным для

*От имени государств — членов Европейского союза, являющихся членами Организации Объединенных Наций.

эффективного решения новых и сложных вопросов, связанных с информационной безопасностью, в первую очередь каждое государство имеет право и несет ответственность за защиту своей собственной информации и базирующихся на информации систем.

6. Европейский союз считает, что существующие риски имеют трансграничный характер и что имеется широкий доступ к технологиям, позволяющим совершать нападения на информационные и телекоммуникационные системы. Экономика всех стран зависит от свободного потока информации и мирного использования информационных технологий. Любые превентивные меры, направленные на ограничение потенциального ущерба от преступных или террористических нападений, включая опасность для международной безопасности, должны осуществляться с учетом необходимости защиты информационных ресурсов и базирующихся на информации систем.

7. В настоящее время уже предпринимаются различные многосторонние усилия, связанные с международным сотрудничеством в области информационной безопасности, например: Советом Европы; десятым Конгрессом Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, 10–17 апреля 2000 года (см. A/CONF.187/15); Комиссией Организации Объединенных Наций по предупреждению преступности и уголовному правосудию; Рабочей группой по информатике Экономического и Социального Совета; Целевой группой Организации Объединенных Наций по информационно-коммуникационным технологиям; Организацией экономического сотрудничества и развития; Международным союзом электросвязи; Группой по высокотехнологическим преступлениям Группы восьми и Организацией американских государств

8. Европейский союз считает, что государства — члены Организации Объединенных Наций должны следить за работой на этом и других форумах, с тем чтобы давать своевременную оценку тем основополагающим действиям, которые могут внести полезный вклад в этой области. Европейский союз считает, что Генеральная Ассамблея и Первый комитет не должны быть основным форумом для обсуждения проблемы информационной безопасности. Поскольку этот вопрос в основном охватывает другие темы, помимо разоружения и международной безопасности, ЕС считает, что другие комитеты в лучшей степени приспособлены для обсуждения по крайней мере некоторых аспектов этой проблемы.