Организация Объединенных Наций A/56/164/Add.1

Генеральная Ассамблея

Distr.: General
3 October 2001

Original: Russian

Пятьдесят шестая сессия
Пункт 69 повестки дня
Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Доклад Генерального секретаря

Добавление

Содержание

01-56159 (R) 111001 111001
0156159

II. Ответы, полученные от правительств

Российская Федерация

[Подлинный текст на русском языке]
[21 июня 2001 года]

Общая оценка проблем информационной безопасности

Угрозы международной информационной безопасности

В пункте 1 своей резолюции 55/28 Генеральная Ассамблея призывает государства-члены содействовать рассмотрению существующих и потенциальных угроз в сфере информационной безопасности. В предложенном Российской Федерацией проекте документа «Принципы, касающиеся международной информационной безопасности» (см. A/55/140, глава II) угрозы информационной безопасности определяются как факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве.

К таким основным факторам, по мнению Российской Федерации, относятся следующие:

1. **Разработка, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам другого государства**

- средств радиоэлектронного или энергоинформационного воздействия, используемых незаконными (антиконституционными) вооруженными формированиями, террористическими группами и отдельными лицами для временного или необратимого подавления радиоэлектронных средств и систем;
- средств воздействия на программные ресурсы электронных управляющих модулей с целью их вывода из строя или изменения алгоритма их работы;
- средств воздействия на процесс передачи информации с целью его прекращения или дезорганизации за счет воздействия на среду распространения сигналов и алгоритмов функционирования;
- средств дезинформации, создания в информационном пространстве виртуальной картины обстановки, отличающейся от действительности или прямо ее искажающей;
- средства воздействия на психику и подсознание человека с целью дезорганизации, подавления воли или временного вывода из строя.

2. **Целенаправленное информационное воздействие на критически важные структуры другого государства**

Наиболее опасно применение информационного оружия в отношении военных и гражданских объектов, систем и институтов государств, нарушение нормального функционирования которых создает прямые угрозы национальной безопасности.

Несанкционированные проникновения, например, в компьютеризированные системы управления энергообеспечения могут спровоцировать полный «паралич» инфраструктуры жизнеобеспечения страны, а в случаях с ядерными электростанциями — вызвать катастрофический результат, подобный трагедии Чернобыля.

Несанкционированный доступ преступных и террористических сообществ к информации о научно-технических разработках оборонного характера или двойного применения может использоваться ими как для производства новейших типов оружия в своих преступных целях, так и для политического шантажа.

Базы данных и другие информационные ресурсы правоохранительных органов могут подвергнуться искажению или полному уничтожению путем информационного воздействия извне, создавая, таким образом, самые серьезные препятствия осуществлению правосудия, эффективной борьбе с преступностью, поддержанию законности и порядка.

Воздействие на информационные ресурсы в кредитно-финансовой сфере, такие, как несанкционированный перевод или прямое хищение банковских средств, «обнуление» счетов и тем более блокирование путем «электронных атак» компьютерных сетей центральных банковских учреждений, очевидно, могут создать кризисные ситуации не только в этой конкретной сфере, но и в целом коллапс в экономике страны и, соответственно, серьезные осложнения в ее международных отношениях.

Массированное поражение инфраструктуры телекоммуникаций с помощью информационного оружия вызывает блокаду государственных систем управления и принятия решений.

Враждебное информационное воздействие на системы связи и управления противоздушных, противоракетных и других систем обороны обезоруживает государство перед лицом потенциального агрессора, лишает его возможностей использования законного права на самооборону.

Не менее бедственные последствия может иметь спровоцированная дезорганизация производственного процесса на предприятиях повышенной технической и экологической опасности (химическое, биологическое, топливное производство).

Дезорганизация средств связи, управления и транспорта служб, привлекаемых к спасению людей и ликвидации последствий стихийных бедствий природного характера или иных чрезвычайных ситуаций, может многократно усугубить материальный ущерб и людские потери в таких ситуациях.

3. Информационное воздействие с целью подрыва политической, экономической и социальной системы других государств, психологической обработки населения с целью дестабилизации общества

Целенаправленное информационное воздействие на противника (конкурента, оппонента) не является новейшим изобретением. Однако сегодня благодаря широчайшему распространению современных телекоммуникационных технологий и формированию глобальных информационных сетей средства такого воздействия приобретают качественно иной потенциал. Возможности проведения информационных акций массированного, тотального характера переводит информационное оружие из категории вспомогательного средства в разряд одного из основных инструментов противоборства.

Одновременно информационная сфера приобретает характер принципиального системообразующего фактора жизни любого общества и активно влияет на состояние практически всех составляющих безопасности государства. Соответственно по мере прогресса в информационно-технологической сфере эта зависимость будет возрастать. Доминирующее информационное давление, возникающее в результате преобладания ограниченного круга источников информации, может быть использовано для целенаправленного негативного психологического воздействия на население страны в целом, персонал критически важных структур, административный и правительственный аппарат, законодательные органы.

Внушение неспособности решать собственные проблемы, недоверия к институтам власти, безысходности, подавление воли, провоцирование противоречий на религиозной, этнической или иной социальной почве подрывает государственные устои, дестабилизирует общество. В итоге такая ситуация может вести к антагонистическому расслоению социальных групп, гражданской войне, полной дезинтеграции государства.

4. Несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерное использование

Практически любое государство сегодня сталкивается или может столкнуться с фактами несанкционированного вмешательства в свои информационные системы, причем число таких актов имеет явную тенденцию к увеличению. Опасность такого вмешательство в том, что при этом может создаваться цепь опасных последствий: опыт «хакеров» используется преступными группировками, а их «достижения», в свою очередь, потенциально могут быть приняты на вооружение при осуществлении враждебных, и в том числе военных, акций на межгосударственном уровне.

При этом современные условия социально-экономического развития вызывают обострение противоречий между потребностями общества в расширении свободного обмена и доступа к информации, с одной стороны, и очевидной необходимостью сохранения регламентирующих ограничений на такой обмен и доступ — с другой.

В то же время несанкционированное вмешательство в информсистемы или их неправомерное использование, если как-то и определяется в национальных законах и правилах, то трактуется весьма широко — от мелкого административного нарушения до уголовного преступления. Многие страны вообще не определились в своем отношении к таким действиям.

Таким образом, нарушитель, действуя по каналам международных информсетей со своей территории и не нарушая собственного законодательства, может оставаться вне юрисдикции государства, в отношении которого им фактически совершено правонарушение.

Совершенствование технологической защиты информсетей может быть выходом, но только для тех государств, которые имеют для этого соответствующие технические, а главное — финансовые возможности.

Очевидно, что такая ситуация логично подводит к необходимости кодификации существующего национального законодательства и создании универсальной международно-правовой базы ответственности за указанные правонарушения и преступления.

5. Действия, ведущие к доминированию и контролю в информационном пространстве

Процесс глобализации в отношении информационного пространства характеризуется, помимо прочего, более высоким уровнем стандартизации, облегчающим странам с развитой экономической и информационной структурой проникновение на телекоммуникационные рынки развивающихся государств. У слаборазвитых стран нет другого выбора, как принять эти стандарты и позволить использовать новые технологии в своем информационном пространстве. В условиях либерализованного рынка информтехнологий и свободного обмена информацией они оказываются в доминирующем информационном поле других государств, что может быть использовано в ущерб интересам их национальной безопасности.

6. Противодействие доступу к новейшим информационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам

Причины возможного противодействия или создания ограничений в получении другими странами новейших информационных технологий, видимо, аналогичны тем, которые возникают в отношении любых других высоких технологий. Такие ограничения могут быть, с одной стороны, связаны с чисто экономическими соображениями, желанием монополизировать определенную сферу рынка, а с другой — определяться политическими мотивами (санкции, ответные действия в отношении «недружественных» стран, соображения собственной безопасности и т.д.). И в том, и в другом случае не исключено стремление сохранить или создать технологическую зависимость одних стран от других в информационной сфере.

В любом случае, критический для любого государства характер, который приобретают в XXI веке информационные технологии, ставит вопрос о доступе к ним как проблему выживания.

Необходимо также принимать во внимание специфику создания информационного оружия, которая заключается в том, что применяемые для этого информационные технологии первоначально появляются, как правило, в гражданском секторе и лишь затем могут переходить в военный.

Учитывая эти факторы, вопрос ограничения доступа к информационным технологиям должен, очевидно, решаться исключительно в свете предотвращения их использования в качестве оружия, создания с их помощью новых разрушительных видов оружия или использования таких технологий в противоправных и иных, не отвечающих общей безопасности целях. Любые иные мотивировки ограничений условиями перспективного режима международной информационной безопасности должны рассматриваться как неприемлемые.

7. Поощрение действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным структурам государств

Беспрецедентное развитие корпоративных, государственных и международных информационных систем и одновременное расширение возможностей доступа к ним достигли такого уровня, что сегодня практически все члены международного сообщества сталкиваются с реальной опасностью электронного нападения со стороны преступников и террористов. Характерно, что масштабы этой опасности будут возрастать по мере развития глобальной инфраструктуры таких систем и, соответственно, приобретать трансграничный характер.

Как информационная преступность, так и информационный терроризм представляют собой противоправные действия, отличающиеся, однако, характером преследуемых целей. Если информационный криминал действует исходя из сугубо корыстных или хулиганских намерений, то террористы действуют в киберпространстве с целями, свойственными политическому терроризму вообще.

Средства осуществления таких действий могут включать различные виды информационного оружия.

Используя специальные компьютерные программы, технику и технологии, террористы способны:

- разрушать, искажать, манипулировать с отдельными элементами информационной инфраструктуры;
- похищать важную информацию;
- модифицировать официальную, фактическую информацию в своих целях;
- захватывать или блокировать каналы средств массовой информации для распространения дезинформации, панических слухов, угроз террористических актов и объявления собственных требований;
- выводить из строя системы связи, вызывая их искусственную перегрузку;
- распространять угрозы террористических актов в информационном пространстве, влекущие тяжелые политические, экономические, социальные или иные опасные последствия.

Тактика информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен и имел большой общественный резонанс. Незащищенные информационные системы представляют для этого, к сожалению, весьма широкие возможности.

8. Разработка и принятие планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн

Одним из основных направлений современной оборонной стратегии многих технологически развитых государств является наращивание информационной мощи, которое подразумевает наличие как оборонного, так и наступательного военного информационного потенциала. Такая стратегия закрепляется в соответствующих национальных доктринах. С учетом возрастания роли информационной войны и средств информационного противоборства происходит пересмотр традиционных пониманий угроз национальному суверенитету, соблюдению принципов и норм международного права, природы экономического соревнования, роли отдельных государств в международных делах. При этом все большее внимание уделяется такой новой категории конфликта, как стратегическая информационная война.

Сочетание экономического и информационного могущества позволяет, отказываясь от традиционных «жестких» форм принуждения при помощи военной силы, не менее эффективно влиять на развитие ситуации в международной политике.

В обоснование таких новых стратегий приводятся следующие особенности:

– развитие информационных технологий не вызывает такой острой негативной реакции общественности, как дальнейшее наращивание обычных вооружений и тем более оружия массового уничтожения;

– упор на развитие информационных систем является выгодным, поскольку такие системы наиболее близко отвечают понятию технологий двойного применения и во многих случаях могут одновременно использоваться как в военных, так и в гражданских, коммерческих целях;

– лидирующее положение государства в развитии и применении информационных технологий закрепляет его монополию на обладание стратегической информацией и, соответственно, возможность наиболее оперативно реагировать в случаях нарастания международной напряженности.

При этом считается, что применение информационного оружия может значительно снизить потери и ущерб по сравнению с «традиционными» военными действиями. Очевидно, что, таким образом, предпринимаются попытки создать впечатление «гуманного характера» информационных операций.

Понятно, однако, что и выгоды и угрозы, связанные с развитием информтехнологий, видят все государства, и они будут стремиться адекватно реагировать на изменение ситуации. Дальнейшее развитие планов и доктрин информационной войны способно привести к значительному расширению круга стран, владеющих информационным арсеналом и, соответственно, к началу гонки вооружений на новом технологическом уровне. В итоге положение в области контроля над вооружениями может вернуться к состоянию, характерному для периода «холодной войны».

9. Использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере

Интересы личности в информационной сфере заключаются в реализации прав и свобод человека на доступ к информации, использование информации в интересах осуществления законной деятельности, духовного и интеллектуального развития, обеспечении личной и семейной тайны, тайны переписки и других телекоммуникационных сообщений, защиты чести и достоинства.

Развитие и широкое применение новейших информационных технологий и средств создает сегодня беспрецедентные возможности осуществления права на информацию. Однако прогресс в информатизации общественной жизни, развитие информационных сетей приводит к тому, что все больше данных, касающихся личной жизни граждан, становятся доступны через открытые базы данных. С другой стороны, возникает угроза неправомерного ограничения властями доступа граждан к открытым информационным ресурсам федеральных органов, органов местного самоуправления, архивов, к другой открытой, социально значимой информации.

Перспективный режим международной информационной безопасности должен гарантировать унифицированный запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и на ограничение доступа граждан к информации, за исключением случаев, предусмотренных правом.

10. Трансграничное распространение информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран

Глобализация информационного пространства размывает традиционные понятия географических, государственных, административных границ или зон юрисдикции, связанных с обеспечением национальной безопасности. В этих условиях возникает задача четкого определения источников угроз в отношении их внутреннего или внешнего характера. Например, враждебная информационная военная операция против другого государства может маскироваться под действия «местных» преступников. Иначе говоря, государства, способные ранее обеспечивать правовой режим информационного обмена на собственном внутреннем уровне в новой обстановке, оказываются незащищенными от проникновения на свою территорию извне информации, запрещенной к распространению или имеющей деструктивный характер (порнография, дезинформация, информация, имеющая признаки расовой

дискриминации и нетерпимости, направленная на разжигание социальной, национальной и религиозной вражды, подрывного характера, исходящая и используемая в интересах от международных криминальных и террористических групп).

11. Манипулирование информационными потоками, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей

Характер информационной среды и информационного воздействия может существенно изменять массовое сознание и поведение больших социальных групп. Особую опасность при этом приобретает такая форма информационного влияния, как манипуляция — вид психологического воздействия, реализация которого ведет к возбуждению у индивидуума или социальной группы намерений, не совпадающих с действительными. Нестабильная, стрессовая политическая ситуация усиливает «эффективность» манипулирования информацией. Массированные «вбросы» дезинформации или, напротив, сокрытие реальной информации в этой ситуации приводят к тому, что объективная оценка событий и факторов становится невозможной. Наиболее восприимчивым к такого рода воздействию является общественное мнение.

Подкрепленные всей мощью современной информационной структуры, такие операции могут вести к разрушению психологической среды общества, его культурных и других духовных ценностей (война культур). Деморализация общества, в свою очередь, создает предпосылки к размыванию национального самосознания, подавлению воли к сопротивлению возможной агрессии.