Организация Объединенных Наций A/60/95/Add.1

Генеральная Ассамблея

Distr.: General
21 September 2005
Russian
Original: English

Шестидесятая сессия
Пункт 86 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

Добавления

Содержание

05-51879 (R) 101005 101005
0551879

II. Ответы, полученные от правительств

Бразилия

[Подлинный текст на английском языке]
[24 июня 2005 года]

Анализ влияния достижений в сфере информатизации и телекоммуникаций на международную безопасность необходимо начинать с признания того факта, что взаимосвязь между обществами и развитием технологий нельзя определить как простое, одностороннее взаимодействие. Она характеризуется сложным взаимодействием между потребностями, творческим подходом, инициативами предпринимателей и коллективным использованием технологии. XXI век открывает новую эру, в которую, как предполагается, развитие «информационного общества» будет являться определяющим фактором глубоких преобразований во всех сферах деятельности человека: от взаимодействия отдельных людей и обществ — до структур производства и государственного управления.

Информация уже стала одним из чрезвычайно важных элементов обеспечения благосостояния и процветания народов, и она по праву рассматривается сегодня в качестве одного из их наиболее ценных ресурсов. Частные компании, банки, фондовые рынки и правительственные организации (включая оборонные структуры) связаны между собой через посредство всемирных информационных сетей, которые стали в той же степени жизненно необходимыми для экономического прогресса, что электроэнергия и вода. Однако эта все более высокая степень взаимосвязанности порождает также целый ряд новых факторов потенциальной уязвимости правительств и экономики, которые могут быть использованы как в ходе военных конфликтов, так и в контексте преступной и террористической деятельности.

В последние десятилетия широкомасштабное использование технологий и автоматического оборудования в целях ведения военных действий стало причиной того, что в контексте конфликтов между государствами больше внимания уделяется достижению военных целей таким образом, чтобы избежать больших сопряженных с этим потерь. В то же время все возрастающее влияние средств массовой информации и организаций гражданского общества затрудняет во многих отношениях проведение военных операций. Считается, что современные военные действия должны быть «чистыми» или даже «хирургически чистыми».

Ведение таких боевых действий вполне можно обеспечить благодаря реальным возможностям, которые дает «кибервойна». Вооруженные силы некоторых стран уже создают специализированные военные подразделения, обученные и имеющие все необходимое для того, чтобы вывести из строя или даже уничтожить жизненно важные объекты инфраструктуры посредством внедрения в информационные сети и совершения диверсий в них. В зависимости от цели и применяемых средств последствия таких нападений могут быть различными: от «частичного вывода из строя» вражеского оружия или сенсорных систем до практически полного разрушения электроэнергетических сетей в масштабах всей страны. Эффективность такой формы ведения военных действий еще более повышается благодаря тому, что многих из этих результатов можно добиться, используя относительно небольшие объемы инвестиций. В

силу этих факторов кибервойна вполне может стать в ближайшем будущем главным видом боевых действий в ходе военных межгосударственных конфликтов. Данные факторы уязвимости могут также быть использованы террористическими организациями, и это может обернуться еще более серьезными и непредсказуемыми негативными последствиями.

Такие наступательные информационно-технологические средства уже широко используются преступниками, хотя масштабы и результаты такого их применения менее значительны: ежегодно информационно-технологические системы многочисленных финансовых учреждений, коммерческих предприятий и государственных учреждений взламываются, и в них вторгаются отдельные лица или группы, пытающиеся незаконным образом получить прибыль и/или секретную информацию.

Сознавая важное значение данной проблемы с точки зрения поддержания международного мира и безопасности, Бразилия предлагает два различных пути ее решения. Во-первых, международному сообществу следует стремиться к созданию надлежащих инструментов, позволяющих противостоять преступной и террористической деятельности, осуществляемой с использованием информационных технологий. В контексте другого, дополняющего предыдущий, подхода ему следовало бы рассмотреть вопрос о возможных последствиях кибервойны и о потенциальной необходимости обеспечить учет многочисленных последствий такой войны в контексте режимов разоружения и нераспространения и международных законов и обычаях ведения войны.

С учетом возможных действий террористов и преступников мы предлагаем государствам-членам под руководством Организации Объединенных Наций и на основе сотрудничества принять следующие меры в целях:

- создания резервных и альтернативных сетей для защиты жизненно важных структур;
- изучения структур их сетей, анализа взаимозависимости и определения новых эффективных методов защиты;
- поощрения взаимодействия между государственным и частным секторами, направленного на достижение желаемого уровня защиты информации, которой обмениваются организации;
- создания систем защиты, позволяющих избежать или минимизировать последствия кибератак;
- создания инструментов и средств, позволяющих властям определять, откуда была совершена кибератака;
- создания возможностей для того, чтобы национальные учреждения могли проводить испытания и оценку информационных систем на предмет определения степени их защищенности;
- проведения переговоров в интересах принятия международной конвенции по киберпреступности;
- поощрения создания и разработки технологий, позволяющих создать средства и методы для защиты информации;

- гарантирования широким слоям общественности доступа к имеющейся информации и информационной технологии;
- недопущения создания механизмов, которые не дают странам возможности получить доступ к высоким технологиям в области телекоммуникаций и информационных систем;
- разработки процедур уведомления компетентных национальных органов о киберугрозах на взаимной основе;
- повышения уровня информированности населения о важном значении кибербезопасности.

Что касается использования «информационного оружия» в межгосударственных конфликтах, то мы полагаем, что Организации Объединенных Наций следует пропагандировать идею подготовки конвенций по следующим проблемам:

- идентификация, характеристики и классификация средств ведения информационной войны;
- идентификация и классификация информационного оружия и средств, которые могут использоваться в качестве информационного оружия;
- предотвращение применения кибернетического военного оружия или знаний террористическими группами;
- разработка кодекса поведения при использовании информационного оружия;
- гарантия равенства всех стран с точки зрения их прав на защиту от кибератак;
- создание международных механизмов, позволяющих обеспечивать регулирование конфликтов, связанных с актами киберагрессии;
- создание глоссария Организации Объединенных Наций, содержащего определения основных понятий, связанных с информационной безопасностью.

Канада

[Подлинный текст на английском языке]
[4 августа 2005 года]

Информационная инфраструктура является одним из ключевых компонентов жизненно важной инфраструктуры Канады, включающей следующие сектора: энергетика и коммунальное хозяйство; коммуникации и информационная технология; финансы; здравоохранение; продовольственное снабжение; водоснабжение; транспорт; государственное управление; и обрабатывающая промышленность. Проблемы обеспечения безопасности информационной инфраструктуры одинаковы во всех секторах, 90 процентов которых, по оценкам, находятся в частной собственности и управляются их владельцами. Важное значение информационной инфраструктуры Канады для всех жителей страны побудила правительство к проведению работы в целях обеспечения безопасно-

сти, функционирования и целостности ее систем на постоянной основе, предпринять шаги в целях предотвращения киберинцидентов и принятия оперативных мер реагирования в связи с любыми перебоями, информация о которых доводится до его сведения.

В декабре 2003 года премьер-министр объявил о создании нового министерства общественной безопасности и по чрезвычайным ситуациями (МОБЧС). В рамках этого нового министерства были объединены бывшие Управление по вопросам защиты национальной инфраструктуры и чрезвычайным ситуациям, Королевская канадская конная полиция (КККП) и Канадская разведывательная служба. МОБЧС несет ответственность за отслеживание и анализ киберугроз для правительственных систем, являясь центральным пунктом сбора информации о киберинцидентах, который обращает внимание министерств на новые угрозы и факторы уязвимости. Канадская разведывательная служба несет ответственность за расследование инцидентов, которые представляют собой угрозу для национальной безопасности. КККП отвечает за проведение расследований в связи со всеми преступными или потенциально преступными киберинцидентами. Кроме этого, Канадское управление по вопросам обеспечения безопасности коммуникаций (КУБК), являющееся техническим органом, занимается вопросами информационно-технологической безопасности и несет ответственность за разработку оперативных стандартов для сертификации и аккредитации систем, анализ риска и уязвимости, оценку продукции, а также за анализ степени безопасности систем и сетей.

В апреле 2004 года Канада впервые опубликовала программный документ под названием “National Security Policy” («Национальная политика в области безопасности»), в котором содержатся комплексная стратегия и план действий по борьбе с нынешними и будущими угрозами. В этом плане было подтверждено, в частности, что кибербезопасность является одним из элементов общественной безопасности, и было предложено создать национальную Целевую группу по вопросам кибербезопасности высокого уровня, члены которой, представляющие государственный и частный сектора, должны разработать национальную стратегию обеспечения кибербезопасности в целях решения данной проблемы. В настоящее время протекает процесс формирования Целевой группы.

В феврале 2005 года МОБЧС создало Канадский центр по реагированию на киберинциденты (КЦРКИ), который является национальным центром, координирующим ответные меры в связи с актами посягательства на кибербезопасность и отслеживающим киберугрозы. Центр функционирует в Правительственном оперативном центре, который работает круглосуточно на протяжении всего года и является частью Национальной системы реагирования на чрезвычайные ситуации Канады (НСРЧС).

Канадские провинции и территории концентрируют свое внимание на защите своих собственных жизненно важных инфраструктур, включая киберсистемы и сети, от которых зависит их нормальное функционирование. В настоящее время проводится работа в контексте инициатив по налаживанию сотрудничества между провинциями, в частности, в связи с созданием совместного механизма кибермониторинга.

Частный сектор активно участвует в реализации инициатив, направленных на обеспечение кибербезопасности. Компании частного сектора защищают

свои собственные чрезвычайно важные информационно-технологические инфраструктуры и, в рамках промышленных ассоциаций, обмениваются информацией о факторах киберуязвимости, киберинцидентах и соответствующих путях решения проблем в рамках их секторов. Промышленные ассоциации работают совместно с МОБЧС в рамках форума, который позволяет проводить широкий обмен информацией между всеми секторами промышленности.

Канада также является участником многосторонних инициатив, касающихся кибербезопасности. К их числу относятся Подгруппа по высокотехнологичной преступности «Группы восьми», которая была создана в 1997 году и приняла принципы борьбы против преступлений, связанных с использованием компьютеров; Конвенция о киберпреступности Совета Европы, нацеленная на согласование национальных законов, в которых определены виды различных преступлений и процедуры расследования и судебного преследования в целях борьбы с глобальными преступными сетями и создания оперативной и эффективной системы международного сотрудничества; и Организация американских государств (ОАГ), государства-члены которой согласились «рассмотреть вопрос о подготовке соответствующих межамериканских правовых инструментов и типового законодательства в целях укрепления в Западном полушарии сотрудничества в деле борьбы с киберпреступностью с учетом стандартов, касающихся неприкосновенности частной жизни, защиты информации, процедурных аспектов и предупреждения преступности».