Организация Объединенных Наций A/66/152

Генеральная Ассамблея

Distr.: General
15 July 2011
Russian
Original: English/Russian

Шестьдесят шестая сессия
Пункт 93 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/66/150.

11-41693 (R) 030811 030811

I. Введение

1. В пункте 3 своей резолюции 65/41 Генеральная Ассамблея просит все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[1], информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 2 указанной резолюции;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

2. В соответствии с этой просьбой 16 марта 2011 года государствам-членам была направлена вербальная нота, в которой им предлагалось представить информацию по данному вопросу. Полученные ответы содержатся в разделе II ниже. Любые дополнительные ответы будут опубликованы в качестве добавлений к настоящему докладу.

II. Ответы, полученные от правительств

Австралия

[Подлинный текст на английском языке]
[31 мая 2011 года]

Австралия с удовлетворением отмечает возможность представить в соответствии с резолюцией 65/41 Генеральной Ассамблеи этот ответ, содержащий нашу точку зрения на достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Австралия стремится быть одним из мировых лидеров в сфере кибербезопасности. Мы признаем важность и преимущества технического прогресса для глобальной цифровой экономики и безопасности всех стран. Австралия стремится к тому, чтобы благодаря нашим знаниям выгоды в сфере экономики и безопасности стали максимальными для всех стран.

По мере все более активного проникновения технологий в нашу жизнь правительство, частный сектор и физические лица оказываются во все большей зависимости от них при выполнении целого ряда задач и функций — от приобретения товаров и услуг онлайн, общения, поиска информации и управления финансами до контроля за оборудованием в горнодобывающей и обрабатывающей промышленности. Для максимального использования преимуществ

[1] A/65/201.

Интернета и цифровой экономики и укрепления кибербезопасности во всем мире настоятельно необходимо, чтобы страны вели совместную работу по созданию надежного, безопасного и устойчивого киберпространства. Австралия стремится к активному и инициативному участию в расширении киберпространства для всех пользователей — государств, частного сектора и физических лиц.

Общая оценка проблем информационной безопасности

Австралия считает кибербезопасность одним из важнейших национальных приоритетов в сфере безопасности. Во всем мире продолжается рост киберпреступности — как по масштабам и изощренности, так и по количеству совершенных деяний. С возрастанием объема и ценности электронной информации возросли и усилия преступников и других вредоносных субъектов, которые стали использовать Интернет в качестве более анонимного, удобного и экономически выгодного средства.

Противостояние этим рискам и их устранение необходимо соотносить с защитой индивидуальных гражданских свобод, в том числе правом на неприкосновенность частной жизни и необходимостью повышения эффективности и поощрения инноваций, с тем чтобы Австралия в полной мере использовала возможности цифровой экономики.

Национальная безопасность, экономическое благосостояние и социальное благополучие Австралии и каждой отдельной страны в значительной степени зависят от доступности, защищенности и конфиденциальности ряда информационно-коммуникационных технологий. В этой связи правительство Австралии выделило значительные ресурсы в целях превентивного содействия поддержанию надежной, безопасной и устойчивой электронной среды на благо всех пользователей.

Хотя политика правительства Австралии в сфере кибербезопасности в первую очередь направлена на обеспечение доступности, защищенности и конфиденциальности информационно-коммуникационных технологий Австралии, эта политика координируется с другими стратегиями и программами, такими как деятельность в сфере кибербезопасности, направленная в первую очередь на защиту физических лиц, и прежде всего детей, от агрессивного контента, издевательств, домогательств или завязывания онлайн-контактов в целях сексуальной эксплуатации.

Национальные усилия по укреплению информационной безопасности и международного сотрудничества в этой сфере

Национальные усилия по укреплению информационной безопасности

Австралия считает, что для содействия международному сотрудничеству в киберпространстве она должна сделать свою внутреннюю политику в этой сфере образцом передового опыта. В Австралии в деле защиты и укрепления кибербезопасности используется интегрированный подход, основанный на ведущей роли правительства. В 2009 году правительство обнародовало первый документ о стратегии в сфере кибербезопасности, в котором излагаются общая цель и задачи политики правительства Австралии в сфере кибербезопасности и устанавливаются стратегические приоритеты, которыми правительство Авст-

ралии будет руководствоваться при решении этих задач. В стратегии также представлены ключевые меры и шаги, которые будут предприняты в рамках всей деятельности правительства Австралии с целью осуществления этих стратегических приоритетов.

Целью политики Австралии в сфере кибербезопасности является поддержание надежной, безопасной и устойчивой электронной среды для защиты национальной безопасности Австралии и максимального использования преимуществ цифровой экономики. Ключевые инициативы стратегии включают в себя создание двух взаимодополняющих организаций: новой национальной группы по реагированию на чрезвычайные ситуации в компьютерной сфере и Оперативного центра по кибербезопасности. Созданная в 2010 году группа по реагированию на чрезвычайные ситуации в компьютерной сфере является единым контактным пунктом по предоставлению информации по кибербезопасности для всех физических лиц и представителей частного сектора Австралии; группа обеспечивает всем австралийцам-пользователям Интернета доступ к информации о киберугрозах и уязвимости их систем, а также о способах повысить защищенность их информационно-коммуникационных технологий. Группа поддерживает тесные рабочие связи с владельцами и операторами важнейших объектов инфраструктуры, а также с предприятиями, эксплуатирующими важные для национальных интересов Австралии системы. Она предоставляет этим предприятиям конкретную информацию об угрозах и уязвимости в области кибербезопасности с целью содействовать повышению защищенности их информационно-коммуникационной инфраструктуры. Оперативный центр, который также был создан в 2010 году, обеспечивает правительство Австралии получаемой из всех источников информацией о ситуации в киберпространстве и содействует созданию потенциала по оперативному реагированию на инциденты, угрожающие национальной кибербезопасности. Центр выявляет и анализирует сложные кибератаки и оказывает помощь в реагировании на компьютерные инциденты в государственных или ключевых частных системах и инфраструктуре.

Важнейшим приоритетом стратегии является проведение просветительских мероприятий для всех австралийцев и расширение их возможностей в данной сфере благодаря информированию, укреплению доверия и практическим инструментам онлайновой защиты. Стратегия основана на принципе общей ответственности, в соответствии с которым все пользователи, пользующиеся благами информационно-коммуникационных технологий, должны принимать разумные меры по обеспечению безопасности своих собственных систем, проявлять осмотрительность при передаче и хранении конфиденциальных сведений и соблюдать требования, касающиеся бережного отношения к информации и системам других пользователей. Для того чтобы физические лица играли активную роль в обеспечении информационной безопасности, необходимо, чтобы они осознавали и понимали киберсреду и связанные с ней риски. С этой целью Австралия проводит программу повышения осведомленности, в которую включено поддержание веб-сайта, на котором размещена информация о кибербезопасности, предназначенная для пользователей домашних компьютеров и малых предприятий, в том числе лиц с ограниченными компьютерными знаниями и навыками (см. www.staysmartonline.gov.au), а также проведение в партнерстве с частным сектором, обществами потребителей и местными организациями недели информации по вопросам кибербезопасности. Проведение

недели информации способствует распространению в Австралии знаний о рисках в области кибербезопасности и позволяет пользователям домашних компьютеров и сотрудникам малых предприятий ознакомиться с простыми шагами, которые они могут предпринять для защиты своей персональной и финансовой информации в Интернете. В ходе проведенной в 2010 году национальной недели информации по вопросам кибербезопасности около 150 правительственных учреждений, профессиональных и местных организаций и обществ потребителей объединили усилия с целью проведения мероприятий в крупных городах, регионах и сельских районах страны. В 2011 году неделя информации проводилась с 30 мая по 4 июня.

Признавая, что ответственность за безопасность киберпространства является общей, правительство Австралии вместе с Ассоциацией Интернет-отрасли выступило с инициативой по подготовке новаторского добровольного кодекса поведения Интернет-провайдеров в сфере кибербезопасности («i-кодекс»), использование которого началось в декабре 2010 года. В этом кодексе австралийским Интернет-провайдерам предлагается использовать последовательный подход к информированию своих клиентов о проблемах кибербезопасности, проведению для них просветительских мероприятий по этой тематике, а также к их защите в данной сфере. На многосторонних форумах представители Австралии сообщали об успехах в применении этого кодекса и об уроках, извлеченных в ходе его разработки. Такие сообщения были сделаны в декабре 2010 года в Рабочей группе по информационной безопасности и конфиденциальности Организации экономического сотрудничества и развития (ОЭСР), Рабочей группе по телекоммуникациям и информации «Азиатско-Тихоокеанского экономического сотрудничества» (АТЭС) и Азиатско-Тихоокеанском сообществе по электросвязи. Австралия готова поделиться информацией об этом кодексе с другими государствами в рамках двусторонних мероприятий по укреплению потенциала и многосторонних форумов, оказать другим государствам помощь в повышении эффективности сотрудничества с Интернет-провайдерами и повышении ответственности этих провайдеров за информирование и защиту конечных пользователей.

Содействие международному сотрудничеству

Австралия уделяет приоритетное внимание международному сотрудничеству в области кибербезопасности. С учетом транснационального характера Интернета, в котором для подлинного обеспечения кибербезопасности необходимы координированные глобальные действия, Австралия в своей деятельности на международной арене начала использовать активный, многоступенчатый подход. Он, в частности, включает совместную работу с правительствами иностранных государств и иностранными организациями как на двусторонней основе, так и на многосторонних форумах с целью содействия распространению передовой международной практики, обмена опытом, наращивания потенциала и укрепления скоординированного глобального подхода к борьбе с угрозами кибербезопасности.

Участие Австралии в деятельности Организации Объединенных Наций включает в себя совместную с другими странами подготовку резолюций о создании глобальной культуры кибербезопасности и оценке национальных усилий по защите важнейших информационных инфраструктур, а также о достижениях в сфере информатизации и телекоммуникаций в контексте международной

безопасности. Австралия также представила, в соответствии с рекомендациями, содержащимися в резолюции 64/211 Генеральной Ассамблеи, сведения о передовом опыте в защите важнейших информационных инфраструктур, в том числе информационно-коммуникационных технологий, в целях повышения кибербезопасности во всем мире. Австралия является членом Международного союза электросвязи (МСЭ) и участвует в работе исследовательских групп в секторах стандартизации и развития электросвязи. Австралия предоставляет финансирование сектору развития электросвязи для поддержки деятельности наращивания потенциала в Азиатско-Тихоокеанском регионе, в том числе в рамках инициатив, связанных с кибербезопасностью. Австралия — активный член Рабочей группы по информационной безопасности и конфиденциальности ОЭСР, предыдущий Председатель этой группы; в настоящее время — государство, на добровольной основе проводящее в рамках Рабочей группы сравнительный анализ стратегий кибербезопасности. Австралия сыграла ведущую роль в подготовке и осуществлении Сеульско-мельбурнского соглашения по борьбе со спамом, касающегося сотрудничества между странами Азиатско-Тихоокеанского региона, а также Лондонского плана действий, который предусматривает создание ведущей международной сети по обеспечению выполнения обязательств и сотрудничеству по борьбе со спамом.

Австралия поддерживает отношения сотрудничества со своими региональными партнерами и сохраняет приверженность совместной работе с ними. Мы тесно сотрудничаем с другими странами нашего региона в наращивании потенциала в целях обеспечения надежности, устойчивости и безопасности киберпространства. Австралия участвует в деятельности Рабочей группы по телекоммуникациям и информации «Азиатско-Тихоокеанского экономического сотрудничества» (РГТИ АТЭС) и Регионального форума по кибербезопасности Ассоциации государств Юго-Восточной Азии (АСЕАН). Австралия является заместителем руководителя Руководящей группы по безопасности и благосостоянию РГТИ АТЭС. В настоящее время Австралия стремится стать одним из государств, курирующих вопросы киберпреступности и транснациональной преступности в рамках плана работы Регионального форума АСЕАН.

На оперативном уровне австралийская Группа по реагированию на чрезвычайные ситуации в компьютерной сфере поддерживает тесные рабочие отношения с национальными группами по реагированию на чрезвычайные ситуации в компьютерной сфере во всем мире. В Австралии такая группа активно участвует в надежном и своевременном предоставлении информации, включая информацию об угрозах и уязвимости, на глобальном уровне и содействует этому процессу. Группа активно участвует в осуществлении инициатив по наращиванию потенциала, особенно в Азиатско-Тихоокеанском регионе, в том числе в своем качестве члена Азиатско-Тихоокеанской группы по реагированию на чрезвычайные ситуации в компьютерной сфере. Признавая, что информационная безопасность не имеет географических границ, данная группа тесно сотрудничает с другими партнерами в своем качестве члена Форума по реагированию на инциденты и Международной сети по наблюдению и предупреждению.

Возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

Все государства, в том числе Австралия, должны продолжать поиск как традиционных, так и новаторских мер по укреплению информационной безопасности. Глобальная проблема обеспечения кибербезопасности требует активизации усилий участников многосторонних форумов по повышению безопасности взаимодействующих между собой сетей. Это включает в себя усилия, прилагаемые в рамках Организации Объединенных Наций и МСЭ, региональных форумов, таких как АТЭС, и более специализированных международных групп, таких как Форум по реагированию на инциденты и группы по безопасности, а также Международная сеть по наблюдению и предупреждению.

Австралия выступает за разработку международных принципов ответственного поведения в киберпространстве, включая соглашения о широком наборе принципов нормативного поведения в киберпространстве, который должен содействовать повышению эффективности международного сотрудничества и укреплению доверия к киберпространству, а также вести к разработке международно признанных норм регулирования киберпространства. В качестве члена глобального сообщества Австралия будет по-прежнему выступать за прогресс в этой сфере как на двусторонних, так на многосторонних форумах с целью содействовать повышению безопасности, устойчивости и надежности киберпространства.

Конкретные усилия, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне, включают в себя:

a) разработку глобальных стандартов, включая соглашение о широком наборе международных принципов нормативного поведения в киберпространстве в целях содействия повышению эффективности международного сотрудничества и укреплению доверия;

b) расширение возможностей международной правовой системы в борьбе с киберпреступностью, включая введение единообразных правовых норм (например, увеличение числа участников Конвенции Совета Европы о киберпреступности, требованиям которой Австралия рассчитывает соответствовать к концу 2011 года), а также расширение сотрудничества в области обеспечения выполнения законодательства с целью позволить странам эффективно учреждать внутренние законы;

c) развитие и поощрение передовой практики в сфере информирования о ситуациях, стратегического предупреждения и реагирования на инциденты, включая создание национальных групп по реагированию на чрезвычайные ситуации в компьютерной сфере с целью осуществления такой деятельности и координации ее проведения во всех странах;

d) проведение инициатив по повышению осведомленности и мероприятий по наращиванию потенциала со стороны имеющих опыт и давно сформировавшихся государств с целью оказать помощь развивающимся государствам в обеспечении надежности, безопасности и устойчивости киберпространства на благо всех;

e) применение более последовательного подхода к привлечению отрасли к выработке руководящих принципов поведения в киберпространстве, таких как кодекс поведения австралийской Интернет-отрасли.

Соответствующие международные концепции

Существующие нормы международного права представляют собой основу для защиты от угроз в сфере информационной безопасности, связанных с деятельностью различных субъектов. Целый ряд существующих правовых принципов может быть применен к использованию киберпространства, включая принципы суверенного равенства государств и запрет применения силы и актов агрессии, а также принципы международного гуманитарного права. Государствам необходимо продолжать обсуждение этого вопроса на международных и региональных форумах в целях более четкого определения сферы охвата и применения этих принципов к угрозам, исходящим от киберпространства.

Грузия

[Подлинный текст на английском языке]
[1 июня 2011 года]

В Грузии особое внимание проблемам информационной безопасности стали уделять после августа 2008 года, когда Российская Федерация провела против Грузии массированную распределенную атаку типа «отказ в обслуживании».

С учетом оценки этих событий и недавнего быстрого и крупномасштабного внедрения связанных с идеей «электронного управления» проектов и услуг информационная безопасность стала одним из важных аспектов концепции национальной безопасности. Для улучшения регулирования информационной безопасности правительство Грузии за последние годы осуществило ряд важных инициатив.

В 2010 году под эгидой министерства юстиции Грузии была создана юридическая структура — Агентство по обмену данными, несущее прямую ответственность за разработку и осуществление политики в сфере информационной безопасности в государственном секторе. Посредством создания Агентства по обмену данными правительство Грузии учредило механизм для координации деятельности в сфере «электронного управления» и информационной безопасности.

Агентство по обмену данными сотрудничает, в рамках своих определенных законом и ее уставом функций, с министерством юстиции Грузии в проведении политики в сфере информационной безопасности, которая должна соответствовать Стандарту 27 000 Международной организации по стандартизации (ИСО). Агентство также координирует правоприменение и внедрение других документов или стандартов, необходимых для обеспечения информационной безопасности государственного и частного секторов, особенно путем проведения мероприятий разной степени значимости. Одним из самых важных таких мероприятий является ежегодно проводимая в Грузии конференция по инновациям в сфере информационных технологий, в повестку дня которой всегда включаются вопросы информации и кибербезопасности; конференция также получала от Агентства полномочия по разработке и проведению политики по повышению осведомленности общественности по вопросам информации и кибербезопасности.

Что касается повседневного обеспечения кибербезопасности, то Агентство по обмену данными несет ответственность за создание и обеспечение функционирования группы по реагированию на чрезвычайные ситуации в компьютерной сфере, которая в настоящее время действует в Агентстве для принятия необходимых мер в случае возникновения в киберпространстве Грузии инцидентов, угрожающих информационной безопасности. Агентство также наблюдает за функционированием компьютерной сети правительства Грузии в целях обеспечения безопасности этой сети.

К функциям Агентства в сфере информационно-коммуникационных технологий также относятся повышение качества профессионального обучения (в целях подготовки специалистов по информационной безопасности), подготовка предложений, наблюдение за безопасностью и удостоверение цифровых подписей. В сфере профессионального обучения Агентство планирует осуществить ряд специальных проектов при поддержке международных доноров (таких как Европейский союз (ЕС) и Всемирный банк). Эти проекты обеспечат соответствующий уровень профессиональной подготовки; что касается безопасности цифровых подписей, то Агентство начнет выполнение своих функций в этой сфере после начала выдачи электронных удостоверений личности граждан (с цифровыми подписями) Агентством актов гражданского состояния.

Помимо деятельности Агентства по обмену данными, которое играет руководящую и координирующую роль в сфере информационной безопасности, необходимо отметить другие инициативы, которые в настоящее время осуществляет правительство Грузии и в которых Агентство по обмену данными активно участвует:

a) под эгидой Совета национальной безопасности Грузии была создана рабочая группа экспертов для подготовки стратегии кибербезопасности и плана действий (конкретно определенных в следующей части);

b) был подготовлен ряд законодательных инициатив, включая административное законодательство и закон о государственной тайне, которые должны быть внесены на рассмотрение парламента Грузии в 2011 году. Необходимо особо отметить проект закона об информационной безопасности, который сейчас готовится в Агентстве по обмену данными и должен быть представлен на рассмотрение парламента в 2011 году;

c) в 2010 году министерство юстиции и министерство финансов Грузии при содействии Агентства подготовили внутренние положения в области информационной безопасности (политика и руководящие указания) и сейчас вводят их в действие. Ожидается, что аналогичные инициативы будут осуществляться и в других государственных учреждениях.

Германия

[Подлинный текст на английском языке]
[6 июня 2011 года]

За последние годы положение в сфере безопасности киберпространства кардинально изменилось. С одной стороны, наблюдается процесс развития технологически обусловленных инноваций, поскольку в экономике растет количество процессов, которые управляются с помощью электронных средств и соединены друг с другом, а иногда прямо или косвенно подключены к Интер-

нету. Связанные с информационными технологиями системы постоянно становятся все более сложными. Инновационные циклы становятся все более короткими. С другой стороны, организованная преступность и другие негосударственные субъекты атакуют созданные информационными технологиями сети, базы данных и веб-сайты. В ряде случаев эти атаки имеют последствия, которым до сих пор не была дана реалистичная оценка.

В этой связи в феврале 2011 года федеральное правительство приняло новую стратегию кибербезопасности. Ядром этой стратегии является защита важнейшей инфраструктуры. Все правительственные органы, занимающиеся проблемами кибербезопасности, должны тесно и напрямую сотрудничать друг с другом, а также с частным сектором в рамках нового центра киберреагирования в целях быстрого выявления и анализа крупных инцидентов в сфере информационных технологий и выработки рекомендаций по принятию мер защиты. В сфере политики новый Совет кибербезопасности на уровне государственного секретариата занимается проблемами кибербезопасности и выработкой позиции Германии по отношению к ним.

Это включает в себя координацию внешней киберполитики, включающей ряд аспектов внешней политики, экономической политики и политики в области обороны и безопасности. Наличие международных соединений в киберпространстве означает необходимость скоординированных действий на международном уровне. Поэтому Германия будет решительно выступать в ЕС и международных организациях за укрепление кибербезопасности.

В связи с глобальной взаимопереплетенностью информационных технологий Германия в рамках своей стратегии кибербезопасности выступает за разработку широких, не вызывающих разногласий и политически обязывающих норм поведения государств в киберпространстве. Эти нормы должны быть приемлемыми для значительной части международного сообщества и включать меры по укреплению доверия и безопасности.

Меры по укреплению доверия и безопасности в киберпространстве

Киберпространство является общественным благом и публичным пространством. В этой связи мы должны рассматривать безопасность киберпространства с точки зрения устойчивости инфраструктуры, а также сохранности систем и данных и их защищенности от сбоев. Поскольку киберпространство является публичным пространством, государства обязаны содействовать безопасности в нем, особенно безопасности от преступлений и вредоносной деятельности, путем защиты тех, кто прибегает к программам проверки подлинности против хищения личных данных, и обеспечения сохранности и конфиденциальности данных и сетей.

Киберпространство по своей природе глобально. Обеспечение кибербезопасности, обеспечение соблюдения прав и защита важнейшей информационной инфраструктуры требуют от государства значительных усилий как на национальном уровне, так и в сотрудничестве с международными партнерами.

В этих условиях Германия готова работать над подготовкой комплекса норм, которые регулировали бы поведение государств по отношению друг к другу в киберпространстве, включая прежде всего меры укрепления доверия, транспарентности и безопасности, и которые получили бы одобрение как можно большего числа стран.

На состоявшейся 9 и 10 мая 2011 года конференции Организации по безопасности и сотрудничеству в Европе (ОБСЕ), посвященной вопросам кибербезопасности, Германия представила следующие возможные элементы такого кодекса международных норм поведения:

a) подтверждение общих принципов доступности, конфиденциальности, конкурентоспособности, сохранности и подлинности данных и компьютерных сетей, защиты персональных данных и прав интеллектуальной собственности;

b) выполнение обязательств по защите важнейшей инфраструктуры;

c) расширение сотрудничества, направленного на укрепление доверия, осуществление мер по сокращению рисков, повышение транспарентности и стабильности посредством:

- обмена сведениями о национальных стратегиях, передовым опытом и национальными концепциями международного регулирования киберпространства;
- обмена мнениями на межгосударственном уровне относительно международных правовых норм, касающихся использования киберпространства;
- создания контактных центров и уведомления о них;
- создания механизмов раннего предупреждения и расширения сотрудничества между группами по реагированию на чрезвычайные ситуации в компьютерной сфере;
- обновления линий связи в кризисных ситуациях с целью учета случаев компьютерных инцидентов, содействия разработке технических рекомендаций, направленных на поддержание надежной и безопасной глобальной киберинфраструктуры;
- выполнения задач по противодействию терроризму, включая обмен опытом и расширение сотрудничества по проблемам, связанным с негосударственными субъектами;
- поддержки укрепления потенциала развивающихся стран в сфере кибербезопасности и разработки принимаемых на добровольной основе мер по обеспечению кибербезопасности крупных мероприятий (таких как Олимпийские игры).

Кроме того, мы считаем необходимым приступить к обсуждению возможностей международного сотрудничества по вопросам установления лиц, ответственных за кибератаки, что обычно крайне сложно сделать; установления ответственности государств за кибератаки, осуществленные с их территории, в случаях, когда государства, несмотря на получение информации, ничего не предпринимают для того, чтобы им воспрепятствовать; а также установления ответственности государств за отсутствие противодействия появлению в ки-

берпространстве внеправовых зон, например, в случае осведомленности государства о хранении незаконно собранных персональных данных на его территории и его попустительства этому.

Военные аспекты кибербезопасности

Поскольку вооруженные силы во все большей степени применяют информационные технологии для успешного осуществления все более сложных сценариев на всех уровнях командования, защита информации и средств ее обработки стала первоочередной задачей.

Тем не менее, с военной точки зрения, угрозу для информационной безопасности представляют не только потенциальный противник, который в ходе операций применяет оружие с целью физического уничтожения информационной инфраструктуры, но и безответственные пользователи, технические сбои, преступники или обычные инциденты.

Поэтому необходимо прилагать целый ряд усилий — от повышения осведомленности каждого индивидуального пользователя и обеспечения надежности цепочки поставок в сфере информационных технологий до создания механизмов реагирования для противостояния кибератакам и укрепления общей устойчивости используемой архитектуры информационных технологий.

По существу необходимо всеобъемлющее управление рисками и принятие мер по укреплению информационной безопасности в национальном и глобальном масштабе.

В вооруженных силах Германии (бундесвере) создана устойчивая структура командования и контроля, технологий и процедур безопасности, а также такая организация безопасности информационных технологий, которая охватывает все виды вооруженных сил и включает независимую группу по реагированию на чрезвычайные ситуации в компьютерной сфере, которая располагает потенциалом для принятия мер в случае критических нарушений функционирования информационных технологий. Адаптация технического и кадрового потенциала к постоянно возрастающему уровню угроз является одной из постоянных задач.

Вооруженные силы Германии тесно взаимодействуют с федеральным министерством внутренних дел Германии и твердо поддерживают укрепление информационной безопасности в Организации Североатлантического договора (НАТО) и ЕС, а также разработку политики и наращивание потенциала в данной области. Кроме того, вооруженные силы поддерживают регулярные контакты с рядом стран по вопросам информационной безопасности как на уровне разработки политики, так и на рабочем уровне.

Вооруженные силы Германии приветствуют инициативы по принятию международных документов в целях дальнейшей защиты полезной роли мировых информационных сетей, такие как подготовка рассчитанного на применение на добровольной основе международного кодекса поведения в киберпространстве, и совместно с другими министерствами федерального правительства Германии прилагают усилия в этой сфере.

Кибероборона в НАТО

Угроза кибербезопасности определяется НАТО как одна из ключевых проблем безопасности. В стратегической концепции, принятой главами государств и правительств на саммите НАТО, состоявшемся в ноябре 2010 года в Лиссабоне, говорится, что «кибератаки... могут достичь уровня, который угрожает национальным и евроатлантическим процветанию, безопасности и стабильности».

Главы государств и правительств в принятой на саммите декларации поставили перед Североатлантическим советом задачу «к июню 2011 года разработать, используя прежде всего существующие международные структуры, на основе обзора нашей нынешней политики, глубоко продуманную политику НАТО в сфере кибероборонs и подготовить план действий для ее осуществления».

В качестве первого шага в процессе перехода к этой новой политике министры обороны стран НАТО в марте 2011 года приняли концепцию кибероборонs.

В концепции основное внимание уделяется защите компьютерных сетей НАТО и национальных компьютерных сетей государств-членов, которые подключены к сетям НАТО или обрабатывают информацию НАТО (включая разработку общих принципов и критериев в целях обеспечения минимального уровня кибероборонs во всех государствах-членах). С целью уменьшить глобальные угрозы, исходящие от киберпространства, НАТО намеревается сотрудничать с государствами-партнерами, соответствующими международными организациями, такими как Организация Объединенных Наций и ЕС, частным сектором и университетскими кругами.

Германия приветствует приверженность НАТО обеспечению кибербезопасности и активно поддерживает проводимые обсуждения.

Кибербезопасность в Организации по безопасности и сотрудничеству в Европе

В Организации по безопасности и сотрудничеству в Европе проблемы кибербезопасности обсуждаются в течение нескольких лет. На саммите ОБСЕ, состоявшемся в 2010 году в Астане, главы государств и правительств 56 стран — членов ОБСЕ подчеркнули необходимость добиться «большего единства целей и действий в противостоянии появляющимся транснациональным угрозам». В Астанийской юбилейной декларации говорится, что киберугрозы входят в число появляющихся транснациональных угроз.

Германия приняла активное участие в конференции ОБСЕ по всеобъемлющему подходу к кибербезопасности под названием «Исследование будущей роли ОБСЕ», состоявшейся 9 и 10 мая 2011 года в Вене. На этой конференции обсуждались конкретные рекомендации по проведению последующей деятельности в рамках ОБСЕ.

Германия будет по-прежнему активно поддерживать проводимые в ОБСЕ обсуждения по вопросу о будущей роли этой организации в сфере кибербезопасности.

Греция

[Подлинный текст на английском языке]
[6 июня 2011 года]

В настоящее время вопросам информационной безопасности уделяется все большее внимание. Рассматриваются меры противодействия современным угрозам, возникающим вследствие глобализации сетей и систем на современном этапе. Разрабатываются и осуществляются меры для защиты свободного распространения информации на национальном и трансграничном уровнях.

Отслеживаются и анализируются современные международные и многонациональные концепции. Необходимо разработать международные рекомендации для оценки существующих рисков. Кроме того, нужно заняться решением вопросов кибероборонны. Еще одна задача заключается в сохранении национального суверенитета в сфере информационной безопасности в процессе глобального информационного обмена.

Государства-члены должны продолжать информировать Генерального секретаря о своей точке зрения и об оценках по соответствующим вопросам. В этой связи необходимо отметить следующее:

a) все вопросы, связанные с информационной безопасностью, являются приоритетными;

b) необходимо принимать меры для изучения и обеспечения возможностей свободного обмена информацией через национальные и международные границы при сохранении необходимого уровня конфиденциальности, сохранности и доступности информации;

c) необходимо разработать и согласовать такие механизмы подключения сетей друг к другу, которые бы предусматривали единые возможности как на национальном, так и на международном уровне. Нужно уделять особое внимание оценке рисков, связанных с подключением сетей друг к другу, и разработать соответствующие международные рекомендации. Кроме того, поскольку всем странам приходится самым серьезным образом заниматься принятием мер в сфере кибероборонны, необходимо разработать согласованные международные рекомендации по вопросам сотрудничества и в целях обеспечения эффективности и экономии. Наконец, важно отметить, что при разработке любой концепции нужно учитывать право стран на сохранение своего суверенитета и собственной информационной базы;

d) международное сообщество могло бы принять следующие меры для укрепления информационной безопасности на глобальном уровне:

i) детальная разработка и согласование соответствующих международных концепций;

ii) разработка директивного плана создания согласованной общей инфраструктуры, который охватывал бы вопросы базового законодательства, в целях обеспечения необходимой информационной безопасности в процессе электронной обработки всех видов корреспонденции и сообщений для пользователей, что будет гарантировать разнообразие способов коммуникации;

iii) согласование концепций, которых придерживаются многонациональные союзы и группы малых государств, и их адаптация для глобальных условий. Достигнутые договоренности в отношении определения характера угроз и их негативных последствий должны предусматривать не только разработку самых современных технических средств, но и меры для их защиты от злоумышленников;

iv) в дополнение к перечисленным выше мерам необходимо учитывать, что в основе любых действий в направлении глобализации должен в качестве основополагающего условия лежать суверенитет стран. Необходимо разработать международную концепцию для определения национальных шлюзов информационного обмена, а также соответствующие сценарии, отражающие желаемый уровень интеграции, и использовать такую концепцию в качестве руководства для всех усилий, прилагаемых на национальном, многонациональном и международном уровнях.

Казахстан

[Подлинный текст на русском языке]
[7 июня 2011 года]

В Республике Казахстан в 2010 году в целях обеспечения кибербезопасности информационно-коммуникационных технологий создана Служба реагирования на компьютерные инциденты.

В этой связи информация об обнаруженных в домене kz или казахстанском хостинге вирусах, кодах безопасности, программах для создания систем-ботов и нарушениях требований законодательства (порнография, насилие, нарушение авторских прав и т.д.), полученная от пользователей Казнета, направляется в Службу реагирования на компьютерные инциденты для анализа.

Нидерланды

[Подлинный текст на английском языке]
[6 июня 2011 года]

Общая оценка проблем информационной безопасности

Нидерланды выступают за безопасные и надежные информационно-коммуникационные технологии и защиту открытого, свободного Интернета и соблюдение прав человека. Безопасные и надежные информационно-коммуникационные технологии имеют огромное значение для нашего процветания и благосостояния и служат катализатором устойчивого экономического роста.

Информационно-коммуникационные технологии открывают новые возможности, но также делают наше общество более уязвимым. В силу трансграничной природы угроз международное сотрудничество имеет огромное значение. Многие меры будут эффективными только в том случае, если они будут приниматься или координироваться на международном уровне. В этой связи Нидерланды придают большое значение государственно-частным партнерствам и индивидуальной ответственности всех пользователей информационно-коммуникационных технологий.

Национальные усилия по укреплению информационной безопасности и международного сотрудничества в этой сфере

Нидерланды прилагают усилия как на национальном, так и на международном уровне с целью обеспечить безопасность цифровой среды. На национальном уровне в феврале 2011 года правительство Нидерландов представило национальную стратегию кибербезопасности под названием «Сила через сотрудничество». В июле 2011 года в рамках этой стратегии правительство создаст национальный совет по кибербезопасности с целью обеспечить применение подхода, основанного на совместной работе государственного и частного секторов, университетских и исследовательских учреждений. Правительство также создаст национальный центр по вопросам кибербезопасности, задачей которого будет выявление тенденций и угроз, а также содействие по преодолению последствий инцидентов и кризисных ситуаций. Главной задачей центра станет анализ киберугроз на основе данных из государственных и частных источников. В состав центра войдет существующая правительственная группа по реагированию на чрезвычайные ситуации в компьютерной сфере.

На международном уровне Нидерланды принимают активное участие в соответствующей деятельности ЕС, НАТО, Форума по вопросам управления Интернетом, МСЭ и других партнерств. Нидерланды содействуют практическому сотрудничеству между центрами по вопросам кибербезопасности (включая группы по реагированию на чрезвычайные ситуации в компьютерной сфере) и укреплению Международной сети наблюдения и предупреждения. Быстрый рост киберпреступности требует эффективных правоохранных мер с целью сохранить доверие к цифровому обществу. Что касается правоохранных мер, то Нидерланды ставят перед собой задачу содействовать активизации трансграничных расследований в сотрудничестве с правоохранительными органами других европейских и не только европейских стран. Нидерланды являются участником Конвенции о киберпреступности Совета Европы и рекомендуют другим странам присоединиться к этой конвенции.

Возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне

Нидерланды понимают важность продолжения диалога по разработке стандартов поведения государств с целью обеспечить безопасное использование киберпространства. Нидерланды стремятся к активному участию в этом диалоге. Отправной точкой для страны является открытый Интернет, который содействует инновациям, стимулирует экономический рост и защищает основные свободы.

Нидерланды придают большое значение вовлечению в этот диалог частного сектора, а также образовательных и научных учреждений и готовы делиться своим опытом и передовой практикой.

Для обеспечения еще большей безопасности и надежности киберпространства необходим активный международный обмен знаниями и информацией между всеми заинтересованными сторонами и организациями. Другим важным вопросом, заслуживающим международного внимания, является единообразное применение существующих международных правовых норм.

Соединенные Штаты Америки

[Подлинный текст на английском языке]
[7 июня 2011 года]

I. Введение

Информационно-коммуникационные технологии имеют большую важность для развития всех государств-членов. Эти технологии, будучи взаимосвязанными в рамках киберпространства, помогают реализовать общую концепцию информационного общества, разработанную на Всемирной встрече на высшем уровне по вопросам информационного общества, проведенной в 2003 и 2005 годах. Информационно-коммуникационные технологии способствуют осуществлению основных функций повседневной жизни, коммерческой деятельности и предоставлению товаров и услуг, проведению исследований, инновациям, предпринимательской деятельности и свободному потоку информации между людьми, организациями и правительствами. Они являются мощным новым инструментом, позволяющим применять электронные методы управления, способствующим экономическому развитию, облегчающим предоставление гуманитарной помощи и обеспечивающим функционирование жизненно необходимой гражданской инфраструктуры, инфраструктуры государственной и национальной безопасности. Кроме того, нельзя переоценить возможности, которые предоставляют сетевые средства связи для устранения препятствий на пути международного взаимопонимания и сотрудничества.

Хотя степень зависимости от информационно-коммуникационных технологий возрастает, также возрастают риски, связанные с этой зависимостью. Целый ряд явлений и видов деятельности природного и антропогенного характера угрожает надежному функционированию жизненно важных национальных инфраструктур, глобальных сетей и целостности информации, которая через них проходит или в них хранится. Возрастает число, сложность и серьезность вызванных человеком угроз. Некоторые из них исходят от государства, но многие другие — от негосударственных субъектов и связаны с преступной или террористической деятельностью. Мотивировки могут отличаться — от кражи денег или информации или создания сбоев в работе конкурентов до национализма и перенесения традиционных форм государственного конфликта в киберпространство. Целями создателей этих угроз в равной мере являются отдельные лица, корпорации, важнейшие национальные инфраструктуры и правительства, и их воздействие имеет существенные последствия для благосостояния и безопасности отдельных наций и глобально взаимосвязанного международного сообщества в целом.

Какие бы шаги на национальном уровне ни предпринимали правительства в целях защиты своих информационных сетей, для обеспечения всеобщей безопасности необходимо международное взаимодействие по выработке стратегий уменьшения рисков для информационно-коммуникационных технологий. Правительства должны быть уверены в том, что сети, обеспечивающие их национальную безопасность и экономическое процветание надежны и жизнестойки. Создание заслуживающей доверия инфраструктуры информационно-коммуникационных технологий обеспечит реализацию всеми возможностей информационной революции.

Это не будет легкой задачей. Перед международным сообществом стоит проблема поддержания условий, способствующих эффективности, инновациям, экономическому процветанию и свободной торговле, но при этом также обеспечивающих безопасность, гражданские свободы и право на частную жизнь. Эту задачу еще больше усложняют уникальные особенности информационно-коммуникационных технологий. Сети, являющиеся доступными для всех, часто принадлежат частному сектору, а не правительствам, и этот сектор обеспечивает их функционирование. В отличие от традиционного оружия разрушительные средства информационной технологии скрыты и невидимы. Их использование может осуществляться через цепочку нескольких стран, при этом сложно установить происхождение и идентифицировать нарушителя и его спонсоров. Все чаще негосударственные субъекты создают потенциал, позволяющий государствам и негосударственным субъектам осуществлять разрушительные действия в киберпространстве с использованием посредников. Эти свойства делают традиционные стратегии, такие как меры, аналогичные применяемым в процессе контроля за вооружениями, неэффективными в противодействии создателям угроз или их сдерживании. В этой связи для уменьшения рисков необходимы неординарные новые подходы. Несмотря на сложность этой задачи, государства-члены должны объединить усилия в реализации этой общей цели сохранения и расширения вклада, который информационные технологии вносят в обеспечение их безопасности и целостности.

Перед государствами-членами стоят задачи на двух уровнях: национальном и международном. Обеспечение безопасности национальной информационной инфраструктуры представляет собой задачу, которую правительства должны осуществлять на национальном уровне в координации с соответствующими заинтересованными представителями гражданского общества. В то же время национальные усилия должны подкрепляться международным сотрудничеством в реализации стратегий, направленных на решение проблем, связанных с транснациональным характером различных угроз сетевым информационным системам. Эти усилия должны включать в себя сотрудничество в деле ликвидации и смягчения последствий инцидентов и принятия ответных мер; проведение транснационального уголовного расследования и судебное преследование виновных; представление технических рекомендаций по улучшению надежности кибернетической инфраструктуры; и утверждение применяемых на международном уровне норм поведения, подкрепленных мерами укрепления доверия, направленными на повышение стабильности и уменьшение риска ошибочного восприятия.

II. Угрозы, риски и уязвимые места

Угрозы сетевым системам, образующим киберпространство, и передаваемой через них информации являются одной из серьезных глобальных проблем XXI века. Государственные и негосударственные субъекты с помощью информационно-коммуникационных технологий могут совершать действия против обычных граждан, коммерческих предприятий, важнейшей промышленной инфраструктуры и правительств. Слияние информационно-коммуникационных технологий, Интернета и других инфраструктур создает беспрецедентные возможности для выведения из строя телекоммуникационных сетей, электроснабжения, трубопроводов и нефтеперерабатывающих заводов, финансовых сетей и другой жизненно важной инфраструктуры.

Уникальные особенности информационной технологии облегчают ее использование в деструктивных целях и создают серьезные проблемы для правительств, стремящихся сократить риск. В отличие от традиционных военных технологий сети, образующие киберпространство, не являются монополией правительства, и во многих случаях принадлежат частному сектору и управляются им. Сама по себе информационная технология — это широко доступная технология, не являющаяся по своему характеру ни чисто гражданской, ни чисто военной, и ее использование зависит исключительно от мотивации пользователя.

Применяемые для создания сбоев программные средства, по крайней мере их базовые элементы, доступны всем. Любой, кто обладает необходимыми навыками, может разработать более сложные подходы. Кроме того, эти средства быстро совершенствуются с учетом выявляемых новых уязвимых мест. Такие средства невидимы в традиционном смысле, являются достаточно скрытыми и могут иметь латентный и легко воспроизводимый «почерк». С учетом характера Интернета маршрут движения вредоносного кода от исходной точки до места назначения может пролегать через целый ряд стран, в результате чего выявление его происхождения становится обременительным процессом, требующим больших затрат времени и зачастую широкого транснационального сотрудничества. Даже при выявлении происхождения кода, идентификация нарушителя или его спонсоров может оказаться невозможной. Таким образом, злоумышленники могут действовать в условиях достаточной секретности и безнаказанности практически из любой точки планеты.

Неясность сведений о злоумышленнике дополняется неясностью мотивов вторжения в киберпространство. Организованные преступники и другие лица или группы могут действовать ради достижения собственных интересов, но могут выступать и в роли посредников как государственных, так и негосударственных субъектов. Отсутствие своевременной надежной идентификации и возможность несанкционированного входа в системы с помощью ложной информации может вызвать у правительств сомнения и замешательство, повысив тем самым вероятность кризиса, нестабильности, неадресного реагирования и потери контроля эскалации во время крупных киберинцидентов.

В число основных субъектов, которые представляют угрозу для надежного функционирования киберпространства, входят следующие:

a) **Преступники**. Многие из вредоносных средств изначально создаются в рамках предпринимательской деятельности организованной преступности и хакеров. Все более усложняющийся характер преступной деятельности и ее растущие масштабы чреваты тем, что вредоносная деятельность в киберпространстве может негативно сказаться на национальной конкурентоспособности, привести к общему снижению доверия к использованию Интернета в коммерческой деятельности и торговле и даже к нарушению функционирования гражданской инфраструктуры. Объем и масштабы этой деятельности постоянно возрастают.

b) **Государства**. Все чаще появляются сообщения о том, что государства создают и используют потенциал, позволяющий перенести традиционные формы государственных конфликтов в киберпространство или использовать киберпространство для этих целей. Между тем по-прежнему сложно найти неопровержимые доказательства в отношении источника или намерений, связан-

ных с действиями, предположительно совершаемыми государствами. Как это часто бывает, идентифицировать и понять мотивировку нарушителя(ей) можно лишь исходя из цели атаки, ее последствий и других косвенных доказательств, связанных с инцидентом.

c) **Террористы**. В настоящее время у террористов отсутствуют возможности нарушить функционирование информационных сетей или провести операции физического воздействия с помощью информационно-коммуникационных технологий, хотя нельзя исключать, что такие возможности могут возникнуть в будущем. Большинство экспертов соглашаются с тем, что в настоящее время террористы используют информационно-коммуникационные технологии для целей вербовки, организации и мобилизации финансовых средств. Конкретные угрозы, связанные с использованием террористами Интернета, могут включать его использование для организации и осуществления конкретной боевой террористической операции.

d) **Посредники**. Все большую обеспокоенность вызывают отдельные лица или группы, осуществляющие вредоносную сетевую деятельность от имени других — будь то государственные или негосударственные субъекты — для извлечения финансовых выгод или исходя из националистических или иных политических мотивов. По сообщениям, так называемые «ботмастеры» предлагают различные вредоносные услуги тому, кто предложит за них наибольшую цену. Уникальные особенности информационной технологии позволяют обеспечить таким лицам высокую степень анонимности и эффективно скрыть какую-либо связь со спонсором, что дает спонсору убедительные аргументы для отрицания своей вины.

Стоящие перед государствами проблемы, связанные с устранением таких угроз, огромны. Особенности информационно-коммуникационных технологий таковы, что действия каждого из этих создателей угроз можно увидеть лишь по их последствиям. Поэтому невозможно своевременно — или вообще когда-либо — идентифицировать нарушителей, и успех часто зависит от высокой степени транснационального сотрудничества. Эта возрастающая роль посредников еще больше усложняет процесс установления источника, поскольку пострадавшая сторона должна выявить не только исполнителя, но и спонсора, и эта проблема, вероятно, будет еще более сложной в будущем.

Такие вызовы требуют, чтобы национальные правительства взяли на себя подготовку и осуществление внутренних мер по разработке и развертыванию надежных и многоуровневых систем защиты информационно-коммуникационной инфраструктуры, независимо от источника угрозы. В то же время сложный транснациональный характер этих угроз требует международного сотрудничества в реализации стратегий по устранению рисков на глобальной основе.

III. Принципы, правила и нормы поведения

A. Ответственность государств за обеспечение кибербезопасности

За последнее десятилетие государства-члены признали свою национальную ответственность за принятие систематических внутренних мер по собственной защите от угроз кибербезопасности и подтвердили необходимость международного сотрудничества. В пяти резолюциях Генеральной Ассамблеи

было обращено внимание на основные меры защиты, которые правительства могут осуществить для уменьшения рисков для их безопасности. Хотя цель этих резолюций заключалась в повышении информированности, в них при этом выдвигался ряд полезных норм поведения для отдельных лиц и государств в интересах обеспечения кибербезопасности:

a) в резолюции 55/63 о борьбе с преступным использованием информационных технологий Генеральная Ассамблея подчеркнула необходимость наличия современных эффективных национальных законов для надлежащего судебного преследования киберпреступников и содействия своевременному транснациональному сотрудничеству в проведении расследования;

b) в резолюции 56/121 Генеральная Ассамблея особо отметила работу международных и региональных организаций в борьбе с высокотехнологичной преступностью, включая работу Совета Европы по разработке конвенции о кибернетической преступности. В этой области Организация Объединенных Наций и другие организации проводили активную деятельность. В число организаций системы Организации Объединенных Наций, которые в первую очередь занимаются проблемой использования Интернета в преступных целях, входят Управление Организации Объединенных Наций по наркотикам и преступности, Комиссия Организации Объединенных Наций по предупреждению преступности, Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Международный союз электросвязи и другие;

c) в резолюции 57/239 Генеральная Ассамблея подтвердила необходимость создания глобальной культуры кибербезопасности, признала ответственность правительств за обеспечение понимания всеми элементами общества их роли и ответственности в отношении кибербезопасности и указала взаимодополняющие элементы, которые все участники информационного общества должны учитывать;

d) в резолюции 58/199 Генеральная Ассамблея, в частности, уделила внимание мерам, которые государства-члены должны рассматривать в рамках своих усилий по созданию глобальной культуры кибербезопасности и защите жизненно важной информационной инфраструктуры. Они также могут рассматриваться как комплекс норм, которым правительства должны следовать, и они составляют важную основу и являются необходимым условием для содействия международному сотрудничеству в области сокращения рисков;

e) в резолюции 64/211 Генеральная Ассамблея предложила всем государствам-членам провести детальный обзор предпринятых ими к настоящему времени национальных усилий по обеспечению кибербезопасности в вышеуказанных и других областях, используя для этого содержащийся в приложении к резолюции инструмент самооценки, и поделиться примерами успешных мер и действий, которые могли бы помочь другим государствам-членам в их усилиях.

B. Нормы, применимые в контексте военных действий

Несмотря на уникальные особенности информационно-коммуникационных технологий, существующие принципы международного права служат надлежащей основой для определения и анализа правил и норм поведения, которые должны регулировать использование киберпространства в связи с воен-

ными действиями. Существуют две различные, но взаимосвязанные нормативно-правовые основы, которые следует рассматривать в этой связи: jus ad bellum и jus in bello. Первая является основой для рассмотрения вопроса о том, дает ли степень серьезности инцидента в киберпространстве основания приравнивать его к применению силы, что влечет за собой осуществление страной права на самооборону. Вторая представляет собой основу для определения правил, регулирующих использование киберпространства в контексте вооруженного конфликта.

Jus ad bellum. Значительная часть правовых норм, регулирующих применение силы и самооборону, основана на трех положениях Устава Организации Объединенных Наций:

a) статья 2(4) Устава Организации Объединенных Наций гласит: «Все Члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения против территориальной неприкосновенности или политической независимости любого государства...»;

b) согласно статье 39 Устава Совет Безопасности определяет существование любой угрозы миру, любого нарушения мира или акта агрессии и делает рекомендации или решает о том, какие надлежащие ответные меры следует предпринять в соответствии со статьями 41 и 42 Устава;

c) в статье 51 Устава признается и подкрепляется принцип о том, что «настоящий Устав ни в коей мере не затрагивает неотъемлемого права на индивидуальную или коллективную самооборону, если произойдет вооруженное нападение на члена Организации, до тех пор пока Совет Безопасности не примет мер, необходимых для поддержания международного мира и безопасности».

Возможно сложно прийти к окончательному правовому заключению о том, что подрывная деятельность в киберпространстве представляет собой вооруженное нападение, влекущее за собой осуществление права на самооборону. Например, в тех случаях, когда источник угрозы и мотив неизвестны, а последствия не приводят к массовой гибели или физическим разрушениям, возможны различные выводы о том, имело ли место вооруженное нападение. Тем не менее такая неопределенность и возможность расхождений во мнениях не означают необходимости разработки новой правовой основы конкретно для киберпространства. Они просто отражают проблемы в применении правовой основы Устава, которая уже существует во многих контекстах. Тем не менее в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение. В этом контексте могли бы применяться следующие закрепившиеся принципы:

a) право на самооборону от неизбежного или фактического вооруженного нападения применяется независимо от того, является ли нападающий государственным или негосударственным субъектом;

b) применение силы в порядке самообороны должно ограничиваться необходимыми потребностями для устранения неизбежного или фактического вооруженного нападения и должно быть пропорционально существующей угрозе;

c) государства должны принять все необходимые меры для обеспечения того, чтобы их территории не использовались другими государственными или негосударственными субъектами для целей вооруженной деятельности, в том числе путем планирования, угрозы, осуществления или предоставления материальной поддержки для вооруженных нападений против других государств и их интересов.

Jus in bello. В праве вооруженных конфликтов изложен комплекс правил, известных как jus in bello, которые применяются при ведении вооруженного конфликта, включая использование инструментов информационной технологии в контексте вооруженного конфликта. В частности важную роль в определении законности кибератак в ходе вооруженного конфликта могли бы играть следующие ключевые принципы права вооруженных конфликтов:

a) принцип разграничения требует, чтобы нападения ограничивались законными военными целями и чтобы гражданские объекты не становились объектами нападения;

b) запрещение неизбирательных нападений включает в себя запрещение нападений, в которых применяются методы и способы ведения войны, которые не могут обоснованно быть направлены против конкретной военной цели;

c) принцип пропорциональности запрещает нападения, которые могут привести к сопутствующей гибели гражданских лиц, нанесению увечий гражданским лицам или ущербу гражданским объектам, которые будут чрезмерными по отношению к ожидаемому достижению конкретного и непосредственного военного преимущества.

Эти принципы запрещают нападения на чисто гражданскую инфраструктуру, сбой работы или разрушение которой не приведет к достижению значимых военных преимуществ. Кроме того, до планирования нападения на военную цель необходимо оценивать возможный сопутствующий ущерб. Иными словами, для совершения нападений с использованием информационных технологий необходимо проводить анализ целей в той же степени, как и при совершении нападений с использованием кинетического (обычного и стратегического) оружия.

Хотя вышеизложенные принципы являются общепризнанными и применяются в контексте киберпространства, также верно и то, что толкование этих нормативно-правовых основ в контексте деятельности в киберпространстве может представлять собой новые и уникальные вызовы, которые потребуют консультаций и сотрудничества между странами. В этом нет ничего необычного. Когда разрабатываются новые технологии, они часто вызывают проблемы в плане применения существующих правовых норм.

C. Использование посредников

Использование посредников для проведения подрывных операций является примером области, в которой уникальные особенности информационно-коммуникационных технологий создают новые вызовы для государств. Действие через посредников существенно повышает возможности государства осуществлять нападения, имея при этом убедительные доводы в пользу своей невиновности. Хотя в существующем международном праве имеются положения,

регулирующие использование наемников, использование посредников в киберпространстве поднимает новые и важные вопросы, имеющие далеко идущие последствия. Государствам необходимо совместно работать над разработкой эффективных решений этой проблемы.

D. Ответственность за обеспечение свободного потока информации

Права на свободу выражения мнения и свободный поток информации закреплены во Всеобщей декларации прав человека и в Международном пакте о гражданских и политических правах, в которых в целом предусматривается, за рядом ограничений, что каждый человек имеет право на свободу выражения убеждений, включая свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Эти принципы были подтверждены на многочисленных международных форумах, в том числе в Генеральной Ассамблее, Международном союзе электросвязи и на Всемирной встрече на высшем уровне по вопросам информационного общества.

E. Ответственность за борьбу с терроризмом

По меньшей мере в 16 существующих резолюциях Совета Безопасности содержится призыв к борьбе с терроризмом. Эти обязательства в полной мере применимы к ситуациям, когда террористы или пособники террористов используют киберпространство для вербовки людей, мобилизации средств, перевода денег, приобретения оружия или планирования нападений. Все государства обязаны делиться информацией об осуществляемых через Интернет финансировании, вербовке, планировании или содействии осуществлению террористической деятельности и принимать меры против этой деятельности при одновременном уважении суверенитета других государств и соблюдении их собственных обязательств по обеспечению свободного потока информации.

IV. Транспарентность, стабильность и сокращение рисков и совместные меры

Как подчеркивалось выше, государства-члены сталкиваются с проблемой устранения весьма разнородных и сложных угроз. За последнее десятилетие на международном уровне предпринимались активные усилия по борьбе с угрозой киберпреступности. Меры по подготовке специалистов по расследованию киберпреступлений и судебному преследованию киберпреступников предпринимались, в частности, в Организации американских государств, организации «Азиатско-тихоокеанское экономическое сотрудничество», Экономическом сообществе западноафриканских государств, Африканском союзе и Совете Европы. Широкое международное сотрудничество в вопросах проведения расследований и судебного преследования в сфере киберпреступности осуществлялось в рамках Конвенции о киберпреступности, а также двусторонних усилий соответствующих государств, и это сотрудничество остается наиболее эффективным средством устранения угроз информационно-коммуникационным технологиям, создаваемых преступной деятельностью.

Другим областям, вызывающим озабоченность в различных странах, еще предстоит уделить аналогичное внимание. В их число входят риски неправильного восприятия, возникающие в результате отсутствия общего понимания международных норм, касающихся поведения государств в киберпространстве, которое может сказаться на мерах по урегулированию кризиса в случае крупных киберинцидентов. Это является доводом в пользу разработки мер по расширению сотрудничества и укреплению доверия, снижению рисков и повышению транспарентности и стабильности:

Меры по повышению транспарентности

- Обмен национальными стратегиями и передовым опытом (извлеченными уроками);
- обмен национальными мнениями относительно международных норм, регулирующих использование киберпространства;
- обмен информацией о национальных структурах по вопросам кибербезопасности и о контактных центрах.

Меры по укреплению стабильности и снижению рисков

- Создание или совершенствование каналов связи и соответствующих протоколов с целью охвата киберинцидентов;
- расширение сотрудничества в борьбе с организованными негосударственными субъектами (преступниками, террористами, посредниками);
- создание процедур, позволяющих осуществлять плановый обмен информацией между национальными группами по реагированию на инциденты в области компьютерной безопасности.

Совместные меры

- Оказание поддержки укреплению потенциала в менее развитых странах.