Организация Объединенных Наций A/C.1/77/PV.19

Генеральная Ассамблея

Семьдесят седьмая сессия

Официальные отчеты

Первый комитет

19-е пленарное заседание

Понедельник, 24 октября 2022 года, 15 ч 00 мин

Нью-Йорк

Председатель: г-н Пиерис . . . . . (Шри-Ланка)

Заседание открывается в 15 ч 05 мин.

Пункты 90–108 повестки дня (*продолжение*)

Тематические обсуждения конкретных вопросов и внесение на рассмотрение и само рассмотрение проектов резолюций и решений, представленных по всем пунктам повестки дня, касающимся разоружения и международной безопасности

Председатель (*говорит по-английски*): Первый комитет продолжает тематические обсуждения по блоку вопросов «Другие меры в области разоружения и международная безопасность». Делегации, желающие воспользоваться своим правом на ответ, смогут сделать это после того, как Комитет заслушает всех ораторов, записавшихся для выступления по этому блоку вопросов. Если позволит время, во второй половине дня Комитет начнет рассмотрение блока вопросов «Региональное разоружение и безопасность».

Прежде чем предоставить слово желающим выступить, я хотел бы напомнить всем делегациям о том, что продолжительность выступлений в ходе тематических обсуждений ограничивается пятью минутами для выступлений в национальном качестве и семью минутами для выступлений от имени нескольких делегаций.

Г-н Лагардьен (Южная Африка) (*говорит по-английски*): Наша делегация присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Южная Африка поддержала итоги работы Группы правительственных экспертов (ГПЭ) за 2021 год по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и первой Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ. В то же время важно сохранять единство в отношении единого процесса, и мы с нетерпением ожидаем проведения четвертой и пятой сессий второй Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. В этой связи поздравляем государства-члены с единогласным принятием ежегодного доклада о ходе работы Рабочей группы открытого состава за 2022 год (см. A/77/275) и надеемся на достижение общего понимания по вопросам безопасности в сфере ИКТ.

Южная Африка по-прежнему обеспокоена растущей угрозой кибератак на важнейшие объекты инфраструктуры, включая информационную

инфраструктуру. Хотя мы считаем, что противостоять этим угрозам следует путем расширения сотрудничества и разработки соответствующих механизмов с учетом передовой практики, наши усилия следует направить на содействие выполнению приоритетных задач на национальном уровне и деятельности по выявлению и обозначению такой инфраструктуры. Поскольку государства, в частности развивающиеся страны, имеют различные возможности в части принятия мер реагирования на угрозы, создаваемые злонамеренными действиями в киберпространстве, они подвержены опасности в различной степени. В этой связи Южная Африка высоко оценивает важность как осуществления, так и дальнейшего развития существующих норм. Наша делегация отдает приоритет осуществлению, которое, по нашему мнению, позволит лучше понять пробелы в существующих нормах, если таковые имеются, и тем самым обосновать необходимость разработки новых норм. Осуществление также дает возможность выявить эффективные методы и потребности в области наращивания потенциала.

Южная Африка приветствует усилия по разработке программы действий в рамках работы РГОС. Убеждены в том, что в ходе наших обсуждений вопросов безопасности в сфере ИКТ в рамках Рабочей группы открытого состава мы сможем достичь общего понимания угроз и факторов уязвимости государств, которые необходимо будет учитывать в такой программе действий. Южная Африка давно поддерживает разработку такой программы действий и считает, что РГОС остается подходящим форумом для ее формулирования и внедрения. Поэтому напоминаем о рекомендации, содержащейся в ежегодном докладе о ходе деятельности РГОС и направленной на дальнейшую разработку программы действий в целях ее возможного принятия в качестве механизма содействия ответственному поведению государств при использовании ИКТ — механизма, который среди прочего будет поддерживать потенциал государств в плане выполнения обязательств, связанных с использованием ими ИКТ.

Считаем также, что привлечение к участию всех соответствующих субъектов, в том числе представителей гражданского общества и частного сектора, для обеспечения большего понимания характера таких угроз, сотрудничества и принятия в масштабах всего общества необходимых мер по борьбе с угрозами, исходящими от государственных и негосударственных субъектов, позволило бы повысить эффективность работы, проводимой при поддержке государств-членов.

Г-н Рётлин (Австрия) (*говорит по-английски*): Австрия полностью присоединяется к заявлению, сделанному от имени Европейского союза (см. A/C.1/77/PV.18). Позвольте высказать ряд дополнительных соображений в моем национальном качестве.

Со времени предыдущих специальных прений, прошедших в 2019 году по этому блоку вопросов, значение кибербезопасности заметно выросло. К сожалению, мы наблюдаем также, какой огромный вред может нанести безответственное и незаконное поведение в киберпространстве. В качестве примера можно привести незаконные кибератаки, которые сопровождали вторжение России на Украину и затрагивали не только Украину, но и имели косвенные последствия для других стран.

В этой связи мы приветствуем повышенное внимание, уделяемое Организацией Объединенных Наций теме кибербезопасности, и приветствуем важную работу, проводимую Рабочей группой открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий, которая успешно завершила первый год своей деятельности принятием доклада о проделанной работе (см. A/77/275), который Комитет, надеемся, примет консенсусом. Доклад и содержащиеся в нем рекомендации закладывают основы для дальнейшей работы Группы. Приветствуем активное участие различных заинтересованных сторон в работе РГОС, но вместе с тем сожалеем, что большое число важных заинтересованных сторон, представляющих промышленный сектор, научное сообщество и гражданское общество не были допущены к участию в ее работе в силу необоснованного использования права вето. Мы не можем работать над обеспечением кибербезопасности без взаимодействия с заинтересованными сторонами, которые определяют ее.

Австрия будет и впредь выступать за обеспечение открытого, свободного, стабильного и безопасного киберпространства на основе применимости международного права во всей его полноте, включая международное гуманитарное право и международное право прав человека, и руководствоваться принятой

консенсусом основой ответственного поведения государств в киберпространстве.

Многое еще предстоит сделать, особенно в том, что касается точной сферы применения международного права, мер по наращиванию потенциала и укреплению доверия. Мы продолжим работать в этом направлении в рамках РГОС и надеемся, что нам удастся изучить существующие передовые методы работы в этих областях, например, путем обмена информацией с региональными организациями по линии РГОС. Убеждены, что программа действий может стать идеальным инструментом для достижения прогресса в вопросах внедрения нормативной базы, и поэтому мы поддерживаем представленный Францией проект резолюции (A/C.1/77/L.73) по программе действий.

Мы с удовлетворением отмечаем, что проекты резолюций по этому блоку вопросов охватывают важные аспекты работы в области разоружения и международной безопасности, которые слишком долго не принимались во внимание. В этой связи хочу затронуть два вопроса.

Во-первых, мы приветствуем важную и все более активную работу, проводимую в последние годы Управлением по вопросам разоружения в области просвещения по вопросам разоружения. В эпоху роста глобальной напряженности повышается значение усилий по распространению информации о нашей работе. Такая деятельность будет способствовать повышению осведомленности и поможет нам подготовить следующие поколения экспертов, выполняющих важнейшую работу в области разоружения.

Во-вторых, в последние годы мир сталкивается не только с вооруженными конфликтами, но и с глобальной пандемией и все более тяжелыми последствиями изменения климата. Тем не менее ресурсы для преодоления каждого из этих трех аспектов кризиса распределяются неравномерно. Хотели бы вновь повторить наш прошлогодний призыв к отказу от опасного заблуждения, что безопасность может быть обеспечена только за счет вооружений. Возникновение кризисов, не связанных с военными действиями, должно послужить предупреждением и способствовать более глубокому пониманию нами вопросов безопасности и более эффективному использованию документов и принятию мер в области разоружения в рамках усилий по обеспечению и поддержанию безопасности.

Г-н Де Мартин Топранин (Италия) (*говорит по-английски*): Италия присоединяется к заявлению, сделанному от имени Европейского союза (см. A/C.1/77/PV.18), и хотела бы добавить следующие замечания в своем национальном качестве.

Развитие технологий и научный прогресс имеют решающее значение для благополучия человечества и должны рассматриваться как инструмент содействия миру и устойчивому росту. Информационно-коммуникационные технологии (ИКТ) и Интернет входят в число величайших достижений человечества всех времен и открывают беспрецедентные возможности. Наша работа по решению вопросов в области разоружения и безопасности сопряжена с большой ответственностью за создание надлежащей правовой основы для таких достижений и за предотвращение опасного и злонамеренного использования.

Международное сотрудничество имеет решающее значение для достижения этой цели, и нам необходимо расширять диалог, повышать транспарентность и эффективность мер укрепления доверия, чтобы способствовать более глубокому пониманию общих проблем, с которыми нам приходится сталкиваться. Италия по-прежнему привержена концепции киберстабильности и поддерживает усилия международного сообщества, направленные на создание киберпространства на основе применимости и соблюдения международного права во всей его полноте, начиная с Устава Организации Объединенных Наций, норм международного гуманитарного права и международного права прав человека.

Полностью поддерживаем нынешние усилия Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и приветствуем успешное завершение ее третьей основной сессии путем консенсусного принятия ежегодного доклада о проделанной работе. Поэтому мы полностью поддерживаем проект решения о принятии этого доклада консенсусом (см. A/77/275), который был представлен делегацией Сингапура от имени Председателя. Поскольку мы решительно поддерживаем многосторонний подход и методы работы, которые гарантируют инклюзивность и основаны на уже существующих правовых нормах, считаем необходимым в полной

мере использовать формат предстоящих обсуждений. Институциональный диалог должен быть упорядоченным, предсказуемым и инклюзивным, что позволит добиться конструктивного прогресса и разумно расходовать время и материальные средства.

Важно признать тот факт, что расширение применения ИКТ и их развитие привело к росту числа угроз. Это еще одна важная область, в которой РГОС следует активизировать свою работу, особенно когда речь идет о киберустойчивости цифровой инфраструктуры и угрозах, связанных с использованием цифровых технологий в вооруженных конфликтах. Эти вопросы особенно актуальны в нынешней сложной геополитической обстановке и в свете неспровоцированной и неоправданной агрессивной войны России против Украины.

Этот жестокий акт высветил зависимость жизненно важных видов деятельности в связанных цифровыми технологиями обществах от цифровой инфраструктуры, в частности телекоммуникационной инфраструктуры, и сопряженные с этим факторы уязвимости. Поэтому Италия подчеркивает важность защиты цифровой инфраструктуры от злонамеренного вмешательства и призывает все стороны уделять первостепенное внимание усилиям по поддержанию надежной работы информационной, коммуникационной и телекоммуникационной инфраструктуры. Это имеет решающее значение для обеспечения доступа к глобальной сети Интернет как ключевого средства получения информации, включая жизненно важную и деловую информацию.

Мы привержены делу укрепления киберустойчивости цифровой инфраструктуры, повышения осведомленности о киберугрозах и улучшения обмена соответствующей информацией, а также наращивания скоординированных действий по противодействию киберугрозам в соответствии с нашими программами в области кибер- и национальной безопасности и существующими и будущими инициативами в области сотрудничества и партнерства.

Киберпространство оказалось очень динамичной средой, и мы считаем, что необходимо предпринимать дальнейшие действия, чтобы воплотить наши обсуждения в ощутимые результаты, что будут способствовать развитию международного сотрудничества в области кибербезопасности. В этой связи Италия поддерживает предложение об учреждении программы действий по поощрению ответственного поведения в киберпространстве в качестве необходимой инициативы по разработке ориентированной на конкретные действия повестки дня (A/C.1/77/L.73). Это должен быть и будет всеохватный процесс, в котором ведущую роль играли бы государства — члены Организации Объединенных Наций. Считаем, что в этот напряженный момент нам необходимо объединиться и перевести наш институциональный диалог в практическую плоскость.

Поэтому мы полностью поддерживаем программу действий, касающуюся киберпространства, и приветствуем ее разработку как очень разумный, инклюзивный и сбалансированный проект, который может стать основой диалога, посвященного практической деятельности с упором на вопросы реализации и с опорой на нашу нормативно-правовую базу. Что касается практических шагов, то позвольте мне подчеркнуть, что усилия по наращиванию потенциала имеют решающее значение для обеспечения безопасного и защищенного киберпространства.

Г-н Шин (Российская Федерация): В начале своего выступления хотел бы еще раз подчеркнуть тот факт, что Россия последовательно продвигает объединительную повестку дня в области контроля над вооружениями, разоружения и нераспространения. Мы представили проект резолюции A/C.1/77/L.66 «Укрепление и развитие системы договоров и соглашений по контролю над вооружениями, разоружению и нераспространению». Рассчитываем на его принятие консенсусом и позитивный эффект под углом конструктивного взаимодействия по всему спектру вопросов обеспечения международного мира и безопасности.

По пункту 94 повестки дня хотел бы сказать следующее: в 2020 году по инициативе Российской Федерации и при поддержке подавляющего большинства государств — членов Организации Объединенных Наций была создана Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. РГОС является единственным переговорным механизмом по данной проблематике в системе Организации. Ценность этого формата в том, что он позволяет всем без исключения государствам непосредственно участвовать в процессе принятия решений по вопросам, затрагивающим

интересы национальной безопасности, а также обсуждать любые профильные инициативы государств на подлинно демократичной, открытой и транспарентной основе.

В этом контексте приветствуем и разделяем прозвучавшую ранее позицию Движения неприсоединения, АСЕАН, КАРИКОМ и Группы арабских государств в поддержку деятельности РГОС (см. A/C.1/77/PV.18) и их готовность к продолжению конструктивной работы в данном формате.

Первый год деятельности РГОС завершился консенсусным принятием 29 июля 2022 года ежегодного промежуточного доклада (см. A/77/275). Документ содержит важные положения, которые позволяют заложить основу для формирования международно-правового режима регулирования сферы использования ИКТ и развития межгосударственного сотрудничества в данной области. Российская Федерация считает принципиально важным не только закрепить достигнутый успех, но и нацелить РГОС на дальнейшие конструктивные переговоры для согласования конкретных мер укрепления мира и безопасности в информационном пространстве, решения задач цифрового развития.

В этих целях представили в Первом комитете проект резолюции A/C.1/77/L.23/Rev.1 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», ежегодно вносимый Россией с 1998 года. Наш документ носит объединительный, неконфронтационный и деполитизированный характер, дополняет представленный Сингапуром проект решения A/C.1/77/L.54 об одобрении первого промежуточного доклада РГОС и приветствует неустанные усилия Председателя Группы, которые мы полностью поддерживаем. Наш текст основан на положениях ранее принятых государствами-членами резолюций Генеральной Ассамблеи, консенсусных докладах первой и ныне действующей РГОС. Цель — сохранить Группу в качестве ключевой переговорной площадки по всему комплексу вопросов международной информационной безопасности под эгидой Организации, предотвратить растаскивание этой проблематики по параллельным и дублирующим друг друга форматам. Таково стремление широкого мирового сообщества, достоянием которого является Группа.

Проект резолюции A/C.1/77/L.23/Rev.1 подтверждает ранее достигнутую государствами консенсусную договоренность о дальнейшей проработке национальных инициатив по вопросам безопасности в сфере использования ИКТ в рамках РГОС, содержит конкретные положения по наращиванию потенциала государств в сфере использования ИКТ, закрепляет необходимость принятия решения о будущем формате регулярного институционального диалога по данной проблематике на универсальной основе в рамках действующей Группы, причем подобный механизм должен быть запущен лишь по истечении срока ее деятельности в 2025 году. Мы должны дать РГОС возможность полностью раскрыть свой потенциал в оставшиеся три года мандата.

Принятие российского проекта резолюции A/C.1/77/L.23/Rev.1 приобретает особое значение именно в текущем году, когда группа государств выдвинула проект резолюции (проект резолюции A/C.1/77/L.23) с предложением о создании по сути альтернативного РГОС формата. Расцениваем это как очередную попытку подорвать деятельность Группы, политизировать переговоры и навязать международному сообществу преждевременное решение о формате будущей работы на данном направлении. Считаем такой подход категорически неприемлемым, противоречащим логике и интересам подавляющего числа стран. Призываем государства — члены Организации Объединенных Наций поддержать российский проект резолюции A/C.1/77/L.23/Rev.1, который направлен на сохранение и защиту формата РГОС. Голос за наш документ — это не голос за Россию: это голос за продолжение конструктивного межгосударственного взаимодействия и ориентированных на результат переговоров в интересах укрепления мира, безопасности и стабильности в информационном пространстве.

Г-н Айдид (Малайзия) (*говорит по-английски*): Малайзия присоединяется к заявлениям, с которыми выступили представитель Индонезии от имени Движения неприсоединившихся стран и представитель Филиппин от имени Ассоциации государств Юго-Восточной Азии (см. A/C.1/77/PV.18).

Стремительное развитие информационно-коммуникационных технологий (ИКТ), безусловно, приводит к появлению бесценных возможностей для народов всего мира, способствуя социально-экономическому росту и трансграничному взаимодействию в различных областях.

Платформы ИКТ сыграли ключевую роль в обеспечении непрерывной работы государственных и частных организаций на национальном, региональном и международном уровнях в течение всего периода пандемии коронавирусного заболевания (COVID-19), и их использование позволило уменьшить издержки, связанные с нарушением хода всех мировых процессов. Наша беспрецедентная зависимость от ИКТ в настоящее время является суровым напоминанием о характере сопутствующих проблем и важности принятия коллективных мер для их решения. Сейчас, когда мы преодолеваем многоаспектные последствия пандемии COVID-19, мы должны гарантировать оптимальное использование наших ограниченных ресурсов в целях обеспечения безопасности ИКТ. Особое внимание следует уделять потребностям развивающихся стран как в плане внедрения существующих правил, норм и принципов, так и в плане глобального обсуждения их дальнейшего развития.

Вызывает обеспокоенность тот факт, что угрозы, возникающие в киберпространстве, становятся все более сложными и изощренными. Мы должны сохранять бдительность в отношении любого злонамеренного использования ИКТ, особенно против критически важной инфраструктуры и систем предоставления основных услуг. Необходимо постоянно поддерживать диалог и прилагать усилия на многосторонних платформах, с тем чтобы ликвидировать разрыв в развитии и использовать все преимущества ИКТ. В этой связи Малайзия подчеркивает центральную роль Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих информационно-коммуникационных технологий в период 2021–2025 годов и приветствует принятие ее ежегодного доклада о ходе работы в 2022 году (см. A/77/275). Являясь универсальной платформой, РГОС представляет собой площадку для всех государств-членов, в частности для дальнейшей выработки норм, правил и принципов ответственного поведения государств, а также средств их реализации. Кроме того, РГОС предоставляет государствам-членам возможность поддерживать постоянное взаимодействие с заинтересованными сторонами, которые являются неотъемлемыми участниками процесса разработки, введения в действие и обеспечения безопасности платформ ИКТ.

В прошлом году Малайзия была рада присоединиться к числу авторов резолюции 76/19, в которой, в частности, подчеркивается поддержка государствами-членами РГОС в ее нынешнем формате и ее мандата. С удовлетворением отмечаем принятие этой резолюции без голосования, поскольку это свидетельствует о том, что после нескольких лет острых споров о различных механизмах члены Организации Объединенных Наций готовы коллективно решать связанные с ИКТ вопросы в рамках единой платформы. К сожалению, на текущей сессии Первого комитета мы стали свидетелями представления различными делегациями рекомендаций, касающихся основных идей и существенных преимуществ предложений, которые выдвигали другие стороны. Это тенденция, с которой мы, к сожалению, хорошо знакомы. Малайзия искренне надеется, что заинтересованные стороны приложат все усилия для конструктивного взаимодействия друг с другом и не допустят утраты с таким трудом достигнутого консенсуса, который, несмотря на свой хрупкий характер, способствует продвижению вперед работы РГОС. Очевидно, что все стороны признают большое значение РГОС и необходимость сохранения ее целостности и авторитета. Малайзия, как и многие другие страны, твердо убеждена в том, что РГОС является наиболее подходящей структурой для обеспечения безопасности в сфере использования ИКТ. Мы будем и далее активно участвовать в заседаниях РГОС, которая сама по себе является важнейшим механизмом укрепления доверия и которой необходимо дать возможность полностью реализовать свой потенциал в соответствии с ее мандатом.

Г-н Ли Сун (Китай) (*говорит по-китайски*): Я взял слово, чтобы изложить позицию Китая относительно мирного использования и обеспечения безопасности информационно-коммуникационных технологий. Использование науки и техники в мирных целях, а также осуществление международного сотрудничества в этой области являются неотъемлемым правом всех государств. К сожалению, на протяжении многих лет права развивающихся стран на использование науки и техники в мирных целях и на международное сотрудничество не всегда гарантируются. В итоговом документе Саммита Движения неприсоединившихся стран, который прошел в Баку, четко указываются необоснованные ограничения, с которыми по-прежнему сталкиваются развивающиеся

страны в области экспорта материалов, оборудования и технологии для использования в мирных целях. Китай считает, что следует принять меры в ответ на призыв стран Движения неприсоединения, уважать законные права развивающихся стран на использование науки и техники в мирных целях и как можно скорее устранить неоправданные ограничения на такое использование.

В прошлом году Генеральная Ассамблея приняла резолюцию 76/234, озаглавленную «Поощрение международного сотрудничества в области мирного использования в контексте международной безопасности», которая положила начало диалогу по вопросу о мирном использовании и прочем соответствующем международном сотрудничестве. Согласно этой резолюции, Генеральный секретарь собрал мнения всех сторон и представил доклад (A/77/96), участие в котором приняло весьма большое число стран и для подготовки которого было направлено наибольшее количество материалов по сравнению с другими докладами по разоружению, опубликованными в прошлом году, что в полной мере продемонстрировало широкую волю к участию в диалоге по соответствующим вопросам и настоятельную необходимость в нем. В этом году Китай вновь представил проект резолюции по этой теме (A/C.1/77/L.56). Сохраняя приверженность целям и основной концепции резолюции прошлого года, мы в полной мере учли предложения всех сторон и намерены продолжать процесс диалога в рамках Генеральной Ассамблеи и обеспечивать площадку, на которой все стороны могли бы обсуждать соответствующие вопросы, вызовы и возможности для сотрудничества.

Некоторые страны обеспокоены тем, что инициатива Китая направлена на подрыв существующего режима экспортного контроля в сфере нераспространения. Это полный абсурд. Конфронтацию по поводу проекта резолюции о мирном использовании начал не Китай, и она не должна сохраняться на протяжении текущей сессии. Напротив, процесс диалога, созданный под эгидой Организации Объединённых Наций в соответствии с проектом резолюции, должен служить связующим звеном для коммуникации и ведения диалога между режимом экспортного контроля в сфере нераспространения и развивающимися странами. Я хотел бы подчеркнуть, что нераспространение и мирное использование не являются конкурирующими процессами; наоборот, они должны осуществляться параллельно, дополняя друг друга. Китай призывает развивающиеся страны оказать проекту резолюции более широкую поддержку, настоятельно просит страны Запада не препятствовать процессу диалога в рамках Организации Объединенных Наций и обращается к государствам-членам Организации Объединенных Наций с призывом предпринять согласованные усилия в целях оказания содействия на сбалансированной основе как мирному использованию, так и нераспространению – двум целям, которые не являются взаимоисключающими.

В настоящее время глобальная ситуация в области кибербезопасности претерпевает глубокие изменения, регулирование киберпространства и управление цифровыми технологиями осуществляются крайне неэффективно, и наряду со всем этим в области киберпространства сохраняются мощные факторы нестабильности и неопределенности. Китай считает, что все стороны должны ставить общественное благо международного сообщества выше своих собственных геополитических эгоистических интересов, отдавать приоритет единству и сотрудничеству, а не разногласиям и конфронтации, применять подлинный многосторонний подход, а также совместно разрабатывать и соблюдать основанные на консенсусе международные правила регулирования киберпространства. Все страны, в частности крупные страны, должны добросовестно выполнять свои международные обязательства, стремиться к созданию мирного, безопасного, открытого и совместного киберпространства, а также не просто претворять в жизнь, но и совместно соблюдать букву и дух разработанной Организацией Объединенных Наций основы ответственного поведения государств в киберпространстве при использовании информационно-коммуникационных технологий. Страны должны воздерживаться от внесения идеологических разногласий в сферу киберпространства, политизации, инструментализации и милитаризации научных, технических, экономических и торговых вопросов, фрагментации Интернета и дестабилизации промышленных цепочек поставок.

Все страны должны принимать совместное участие в планировании будущего киберпространства, будь то в рамках Группы правительственных экспертов (ГПЭ) по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности или Рабочей группы открытого состава (РГОС) по вопросам

безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. Достигнутый между странами консенсус заключается в том, что в рамках Организации Объединенных Наций должен существовать только один процесс по вопросам кибербезопасности. В этом году Рабочая группа открытого состава (РГОС) успешно составила свой первый ежегодный доклад о проделанной работе (см. A/77/275), что является немалым достижением с учетом нынешних обстоятельств и свидетельствует о доверии всех сторон к Рабочей группе.

Все стороны должны приветствовать текущую активную динамику Рабочей группы и уважать ее авторитет как единственного в Организации Объединенных Наций процесса обеспечения безопасности в сфере информационно-коммуникационных технологий в соответствии с его мандатом, учрежденным в исполнение резолюции 75/240, и должны принимать участие в обсуждениях по вопросу о будущих институциональных диалогах в рамках Рабочей группы. Все стороны должны воздерживаться от попыток создать новую программу действий вне Группы и не допускать дублирования процесса Организации Объединенных Наций в области киберпространства на параллельных направлениях. Китай будет сотрудничать со всеми сторонами в целях полного использования возможностей механизма Рабочей группы, укрепления контактов и расширения обмена информацией, а также совместного создания более справедливого, рационального, открытого, инклюзивного, безопасного, стабильного и динамичного киберпространства.

Г-жа Лыхмус (Эстония) (*говорит по-английски*): Эстония присоединяется к заявлению, сделанному от имени Европейского союза (см. A/C.1/77/PV.18), и я также хотела бы остановиться на некоторых моментах в своем национальном качестве.

Эстония придает исключительно большое значение мобилизации усилий, направленных на предотвращение и устранение угроз международному миру и безопасности, обусловленных злонамеренным использованием киберпространства. С февраля мы наблюдаем жестокую агрессию России против Украины, в ходе которой Россия, наряду с реальными военными действиями, проводит злонамеренные кибероперации против объектов критически важной инфраструктуры и основных служб Украины, а также кампании по дезинформации. Злонамеренная кибероперация России против спутниковой сети KA-SAT имела серьезные последствия в виде массовых перебоев со связью и сбоев в работе частных и государственных организаций на Украине. В результате этого нападения ущерб также был нанесен третьим странам, что свидетельствует об опасных побочных последствиях кибератак.

Эстония решительно осуждает такие злонамеренные кибероперации и считает их намеренным игнорированием разработанной Организацией Объединенных Наций основы ответственного поведения государств. В этой связи мы вновь заявляем о том, что международное право – включая Устав Организации Объединенных Наций во всей его полноте, международное право прав человека и международное гуманитарное право – в полной мере применимо к поведению государств в киберпространстве. Как отражено в консенсусом докладе Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий за 2021 год, который был одобрен резолюцией 76/135, государства-члены согласились с тем, что государства не должны осуществлять и заведомо поддерживать какую-либо деятельность в сфере информационно-коммуникационных технологий, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для предоставления услуг населению.

Эстония высоко оценивает деятельность Рабочей группы открытого состава и приветствовала принятие ее ежегодного доклада о проделанной работе (см. A/77/275) в июле 2022 года. Несмотря на тяжелую геополитическую ситуацию, в данном докладе направляется важный сигнал о необходимости продолжить обсуждение вопросов разработки и применения норм ответственного поведения государств, а также о готовности государств-членов Организации Объединенных Наций делать это. Призываем государства продолжать конструктивные обсуждения в целях достижения

взаимопонимания относительно путей эффективного уменьшения киберугроз и вносить вклад в наращивание глобального потенциала в области противодействия киберугрозам. Что касается достижения прогресса в обсуждении вопроса о претворении в жизнь согласованной основы ответственного поведения государств и оказания поддержки усилиям по наращиванию потенциала, то Эстония заявляет о своей решительной поддержке учреждения программы действий в качестве постоянного, всеохватного и ориентированного на практические действия механизма. Поэтому мы поддерживаем проект резолюции A/C.1/77/L.73, который направлен на обеспечение начала работы над программой действий после завершения мандата РГОС в 2025 году и на продолжение работы последней, а также предыдущей РГОС, равно как и работы Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности.

Наконец, мы подчеркиваем неотъемлемый многосторонний характер киберпространства и приветствуем дальнейшее сотрудничество с частным сектором и гражданским обществом. Благодаря выступлениям высококвалифицированных специалистов и обмену разнообразных мнений разных сторон участники обсуждений вопросов кибербезопасности в Организации Объединенных Наций получают более полную информацию по этой теме. Эстония считает, что многостороннему сообществу заинтересованных сторон необходимо предоставить достаточные возможности для выражения своего мнения в ходе предстоящих обсуждений в рамках РГОС.

Г-н Молла (Бангладеш) (*говорит по-английски*): Бангладеш присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Формат обсуждения вопросов разоружения постоянно претерпевает изменения, обусловленные стремительными темпами технического прогресса, в том числе в области оружейных технологий, разработки искусственного интеллекта и биотехнологий. В частности, революция в области информационно-коммуникационных технологий (ИКТ) и Интернета коренным образом изменила наш образ жизни. Сейчас, когда вследствие развития цифровой связи жизнь человека претерпевает коренные изменения, нельзя недооценивать риски, которые такое развитие представляет для международного мира и безопасности. Поэтому мы должны сохранять бдительность и выявлять случаи злонамеренного использования технологий, которые могут поставить под угрозу нашу коллективную безопасность.

Киберпространство необходимо рассматривать как глобальное общественное благо, которое должно служить в интересах всех людей во всем мире без дискриминации. Для того, чтобы воспользоваться огромными преимуществами цифровых технологий, международное сообщество должно создать безопасную, защищенную, надежную и открытую ИКТ-среду на основе применимости международного права к киберпространству, четко определенных норм ответственного поведения государств, эффективных мер укрепления доверия и скоординированных усилий по наращиванию потенциала. Кибербезопасность – это вопрос международного мира и безопасности, и поэтому в этой сфере необходимо наладить тесное международное сотрудничество. В своем докладе «Наша общая повестка дня» (A/75/982) Генеральный секретарь также рассматривает военные действия в киберпространстве в качестве одной из основных стратегических угроз. Ни одна страна не может справиться с угрозой кибератак в одиночку. Поэтому государства-члены должны создать условия, при которых все государства могут в полной мере пользоваться преимуществами киберпространства. Наша единственная надежда – создание свободной, безопасной, стабильной, доступной и мирной ИКТ-среды на основе многостороннего подхода. Подчеркиваем, что Организация Объединенных Наций должна играть ведущую роль в разработке международных норм в области киберпространства.

Бангладеш считает учрежденную в соответствии с резолюцией 73/27 Рабочую группу открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности одним из важных и всеохватных механизмов Организации Объединенных Наций. Мы подтверждаем наше стремление к конструктивному взаимодействию в целях обеспечения успеха работы нынешней РГОС и приветствуем принятие на основе консенсуса первого ежегодного доклада о проделанной работе (см. A/77/275), который, по нашему мнению, будет

служить «дорожной картой» для наших дальнейших обсуждений. Поддерживаем проект решения A/C.1/77/L.54, представленный Сингапуром. Также отмечаем работу предыдущих групп правительственных экспертов и их доклады, которые содержат важные рекомендации относительно содействия созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

В отсутствие глобально принятой структуры норм мы поддерживаем применение принципов Устава Организации Объединенных Наций и соответствующих норм международного права к киберпространству для поддержания мира и стабильности. В Бангладеш мы осуществляем инвестиции в развитие надлежащей культуры кибербезопасности в правительстве и обществе. Мы разработали и внедрили необходимые механизмы, программы и стратегии, а также непрерывно совершенствуем их. Мы стремимся к налаживаю международного сотрудничества в рамках наших усилий, в частности в области мер по наращиванию потенциала и укреплению доверия.

Бангладеш придает большое значение задействованию и соблюдению соответствующих экологических норм в рамках международного правового режима, касающегося разоружения и контроля над вооружениями. Вопрос о применимости таких правовых норм к разоружению на морском дне и в космическом пространстве или их актуальности должен стать предметом дальнейших обоснованных исследований и анализа.

Бангладеш вновь подчеркивает важность образования по вопросам разоружения и нераспространения. Образование играет основополагающую роль в углублении понимания гуманитарных и экономических последствий, связанных с вооружениями. Мы хотели бы официально выразить нашу признательность Институту Организации Объединенных Наций по исследованию проблем разоружения за проводимую им полезную работу. Подчеркиваем необходимость предоставления Институту дополнительных и предсказуемых ресурсов, которые ему необходимы для выполнения своего мандата и, соответственно, расширения своей базы знаний и управления ею для общего использования всеми государствами-членами.

В заключение хочу сказать, что мы должны ставить людей в центр наших усилий в области разоружения и добиваться разоружения, которое спасает жизни сегодня и будет спасать их завтра. Давайте продолжать работать сообща в целях обеспечения более безопасного мира.

Г-н Диак (Сенегал) (*говорит по-французски*): Сенегал присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Мы рады принимать участие в этих тематических обсуждениях других вопросов разоружения и международной безопасности. Наша делегация хотела бы воспользоваться возможностью и поделиться своим мнением по ряду вопросов, находящихся в повестке дня Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ на период 2021–2025 годов, включая осуществление норм международного права, мер укрепления доверия, деятельности по наращиванию потенциала и налаживание регулярного диалога под эгидой Организации Объединенных Наций.

Что касается осуществления норм международного права, то Сенегал отмечает, что все еще не решены некоторые вопросы, такие как принятие нового международного правового документа или сохранение позитивного международного права для регулирования киберпространства. В этой связи мы считаем необходимым продолжать обсуждения, с тем чтобы избежать недоразумений и содействовать более глубокому пониманию путей применения международного права к деятельности в киберпространстве. По мнению Сенегала, особого внимания заслуживают два вопроса.

Первый касается применения международного гуманитарного права. Необходимо отметить, что применение международного гуманитарного права следует рассматривать не как легитимизацию войны в киберпространстве, а как строгое соблюдение принципов целесообразности, избирательности, гуманности и соразмерности во всех видах деятельности в киберпространстве, осуществляемой в условиях вооруженного конфликта.

Второй вопрос затрагивает применение контрмер в ответ на кибератаки, включая коллективные контрмеры. В этой связи важно достичь четкого консенсуса в целях обеспечения баланса между признанием законности таких контрмер, в частности для защиты стран, которые не

имеют специалистов, обладающих техническими знаниями, и осуществлением контроля за их применением, с тем чтобы не допустить возникновения конфликтов в киберпространстве. В ходе данных обсуждений мы выступаем за обращение к услугам специалистов соответствующих учреждений, таких как Комиссия международного права.

Что касается мер укрепления доверия, то Сенегал приветствует предложение создать глобальный справочник национальных координаторов и поддерживает рекомендацию, содержащуюся в первом ежегодном докладе РГОС о проделанной работе, проводить более целенаправленные обсуждения вопроса о процессе составления этого справочника. В целях содействия обмену информацией было бы уместно заняться разработкой шаблона и унификацией материалов государств, включая материалы, предназначенные для подготовки доклада Генерального секретаря о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий (см. A/77/92) и размещения на Портале по киберполитике Института Организации Объединенных Наций по исследованию проблем разоружения. Такой шаблон мог бы предусматривать предоставление информации о стратегиях в сфере кибербезопасности, правовых рамках, административных структурах и киберугрозах, а также о конкретных потребностях в реагировании на киберугрозы.

Однако мы не должны забывать о технических трудностях, с которыми сталкивается ряд государств. Отсюда следует актуальность мер по наращиванию потенциала, что является серьезной задачей, особенно для развивающихся стран. Сенегал осознает это и принял в этой связи национальную стратегию в области кибербезопасности, в которой определены пять стратегических целей: укрепление правовой и институциональной базы кибербезопасности; защита критически важных информационных инфраструктур и государственных информационных систем; продвижение культуры кибербезопасности; наращивание потенциала и повышение уровня технических знаний в области кибербезопасности; а также участие в региональных и международных усилиях по вопросам кибербезопасности.

Наша страна стремится адаптировать правовую базу использования цифровых технологий и свою институциональную архитектуру, в частности путем создания центральной технической службы по обеспечению безопасности кодирования и информационных систем, специального подразделения по борьбе с киберпреступностью и комиссии по защите персональных данных. Те же самые меры принимаются и для повышения уровня подготовки в области компьютерной безопасности. В результате нашего сотрудничества с Францией было создано несколько учебных заведений, в частности Институт профессиональной подготовки в сфере информационной безопасности и Национальная школа кибербезопасности с региональным направлением в Дакаре.

При реализации этих усилий Сенегал строго следует положениям всех соответствующих правовых документов, включая Конвенцию Африканского союза об укреплении доверия и безопасности в киберпространстве, принятую в Малабо; Конвенцию Совета Европы о киберпреступности, подписанную в Будапеште; Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных; и директиву C/DIR/1/08/11 Экономического сообщества западноафриканских государств о борьбе против киберпреступности от 19 августа 2011 года.

Что касается налаживания регулярного диалога под эгидой Организации Объединенных Наций, то наша делегация приветствует принятие программы действий Организации Объединенных Наций по обеспечению кибербезопасности и проекта резолюции A/C.1/77/L.73 об ее осуществлении. С удовлетворением отмечаем тот факт, что в ходе консультаций по данному проекту резолюции были учтены такие вопросы, как признание РГОС в качестве основного механизма Организации Объединенных Наций по кибербезопасности и проведение обсуждений по программе действий в рамках РГОС, а также тот факт, что после начала реализации программы действий в рамках этого процесса будут учитываться утвержденные РГОС консенсусные итоги.

Наша делегация убеждена в том, что принимаемые в целях обеспечения кибербезопасности меры не должны приводить к сдерживанию цифрового развития или созданию препятствий на пути внедрения инноваций и реализации

предоставляемых ИКТ возможностей в сфере развития. Эти меры, являющиеся превентивным средством и инструментом противодействия вредоносному использованию киберпространства, должны приниматься с единственной целью — содействовать созданию доступной, безопасной, мирной и процветающей цифровой среды, в которой никто не будет оставлен позади, в соответствии с задачей 9.c целей в области устойчивого развития.

Сенегал вновь заявляет о своей решимости и готовности работать над решением всех этих вопросов в рамках Рабочей группы открытого состава, являющейся единственной площадкой для открытого и конструктивного обсуждения вопросов кибербезопасности.

Г-н Зленко (Украина) (*говорит по-английски*): Украина присоединяется к заявлению, с которым выступил наблюдатель от Европейского союза (см. A/C.1/77/PV.18), и хотела бы сделать следующее заявление в своем национальном качестве.

Стремительное развитие информационно-коммуникационных технологий (ИКТ) постепенно привело к переформатированию интернет-пространства. Сегодня это уже не удобная площадка для общения, а настоящее оружие, которое становится все более и более опасным в руках хакеров, преступников, а также некоторых государственных субъектов и их ставленников. К сожалению, несмотря на существующие правовые нормы и институциональные механизмы, созданные для борьбы с кибератаками на национальном, региональном и международном уровнях, предоставляемые современными цифровыми технологиями блага часто используются в неблаговидных целях, растет число совершаемых кибератак, которые превращаются в новый метод ведения войны.

Украина – государство, являющееся объектом кибератак, ставших одним из основных элементов предпринимаемых извне с 2014 года попыток подорвать наш суверенитет. В период с 2014 по 2021 годы Украина столкнулась с беспрецедентным количеством кибероперации против жизненно важных объектов нашей инфраструктуры, наиболее заметной из которых стала кибератака с применением вредоносного программного обеспечения NotPetya в июне 2017 года. В большинстве случаев эти атаки совершались группами хакеров, руководство деятельностью которых осуществлялось из Российской Федерации. После начала развязанной Россией против Украины 24 февраля 2022 года полномасштабной военной агрессии киберпреступниками были предприняты атаки на правительственные структуры и местные органы власти. В числе их основных целей также коммерческие организации и финансовые учреждения, объекты обеспечения безопасности и обороны, предприятия энергетического сектора и транспортной отрасли – то есть вся инфраструктура, которая служит обеспечению благосостояния населения. Фактически, Украина является первой страной в мире, ставшей участником полномасштабной кибервойны. Со времен Второй мировой войны человечество никогда не сталкивалось с такими серьезными проблемами, как после нападения России на нашу страну. Для киберпространства война является абсолютно новым вызовом. За восемь месяцев войны созданной правительством Украины группой реагирования на компьютерные инциденты зафиксировано более 1000 кибератак.

Несмотря на военную агрессию России, Украина продолжает укреплять свою систему обеспечения кибербезопасности при материальной и консультативной помощи своих западных партнеров. В соответствии со стратегией кибербезопасности Украины нами создана национальная система кибербезопасности, основными компонентами которой являются Министерство обороны, Государственная служба специальной связи и защиты информации, Служба безопасности Украины, Национальная полиция Украины и Национальный банк Украины. Эта система обеспечивает взаимодействие между всеми государственными учреждениями, местными органами власти, воинскими подразделениями, правоохранительными органами, научно-исследовательскими и образовательными учреждениями, гражданскими группами, предприятиями и другими заинтересованными субъектами. Целью текущей стратегии кибербезопасности Украины, разработанной на период 2021–2025 годов, является создание условий для безопасного функционирования киберпространства, его использования в интересах людей, общества и государства. В основе этого документа лежат принципы сдерживания, наращивания потенциала противодействия киберугрозам и взаимодействия.

Что касается деятельности на международном уровне, то хотим подчеркнуть необходимость

уделять особое внимание разработке единых стандартов борьбы с киберугрозами, обмену передовым опытом, укреплению взаимного доверия в области кибербезопасности, предотвращению использования киберпространства в политических, террористических и военных целях, а также оказанию странам финансовой и технической помощи в целях укрепления их потенциала в таких областях, как способность противостоять киберугрозам, уменьшение рисков и повышение устойчивости. Кроме того, особенно важное значение имеет вопрос о привлечении виновных к ответственности в случаях выявления конкретного государства или государственных субъектов, стоящих за подготовкой или осуществлением целенаправленного злонамеренного использования ИКТ или распространением лжи во враждебных целях. В конце концов международные усилия, предпринимаемые в этой области, утрачивают всякий смысл в условиях отсутствия надежных механизмов для выявления, наказания и привлечения к ответственности отдельных лиц и соответствующих государств, ответственных за координацию и финансирование незаконной деятельности в глобальном киберпространстве.

Как один из соавторов проекта резолюции A/C.1/77/L.73, всецело поддерживающий учреждение программы действий по поощрению ответственного поведения государств в киберпространстве, направленной на создание в рамках Организации Объединенных Наций постоянного, инклюзивного и ориентированного на принятие практических мер механизма, мы разделяем основные цели этой инициативы, заключающиеся в оказании государствам поддержки в реализации рамок ответственного поведения государств в киберпространстве и расширении диалога во взаимодействии с соответствующими заинтересованными сторонами. В этой связи наша делегация решительно поддерживает представленный Францией проект резолюции A/C.1/77/L.73.

Г-н Халди (Алжир) (*говорит по-английски*): Сегодня как никогда очевидна насущная необходимость установления и поддержания международного мира, безопасности, сотрудничества и доверия между государствами в информационно-коммуникационной (ИКТ) среде. На самом деле, меняющиеся угрозы, возникающие в результате злонамеренного использования информационно-коммуникационных технологий, а также увеличение числа кибератак на объекты критической инфраструктуры государств вызывают глубокую обеспокоенность и требуют принятия коллективных ответных мер. В этой связи Алжир не может не подчеркнуть чрезвычайную важность обеспечения того, чтобы использование ИКК в полной мере соответствовало целям и принципам Устава Организации Объединенных Наций и нормам международного права — прежде всего принципам суверенитета, суверенного равенства, невмешательства во внутренние дела, отказа от угрозы силой или ее применения в международных отношениях, мирного урегулирования конфликтов и соблюдения норм права прав человека — и не противоречило принципу мирного сосуществования государств.

Алжир с удовлетворением отмечает достигнутый заметный прогресс, свидетельством которого является успешное завершение в 2021 году деятельности Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Принятие на основе консенсуса их итоговых докладов придало положительный импульс многосторонним усилиям в области ИКТ в контексте международной безопасности и обеспечило важную основу для проведения наших обсуждений в этой сфере. В этой связи Алжир поддержал и приветствовал начало деятельности под эгидой Организации Объединенных Наций и под председательством Сингапура новой Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, учрежденной в соответствии с резолюцией 75/240 в качестве единственного инклюзивного механизма, основанного на консенсусе и предусматривающего активное и равноправное участие в его работе всех государств. Поэтому Алжир убежден в том, что учреждение нынешней РГОС стало важной вехой в процессе международного сотрудничества на пути к созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Многое еще предстоит сделать, но новая РГОС, как и предыдущая, представляет собой уникальный форум, позволяющий не только глубже вникнуть в суть важнейших проблем, обусловленных нарастанием угроз вследствие злонамеренного использования

ИКТ, но и продолжить коллективную работу по их преодолению.

Мы вновь заявляем о своей решительной поддержке новой РГОС и намерении продолжать конструктивную работу со всеми государствами-членами в целях обеспечения ее успеха в 2025 году, а также приветствуем принятие в июле 2022 года первого ежегодного доклада о ходе работы РГОС (см. A/77/275). Мы искренне надеемся на то, что дух консенсуса будет сохраняться в ходе оставшихся сессий РГОС, которые служат важной мерой укрепления доверия.

Мы также надеемся на то, что региональные и субрегиональные организации продолжат играть важную роль в деле продвижения вперед этого процесса.

Способность международного сообщества предотвращать вредоносную деятельность в области ИКТ или смягчать ее последствия зависит от возможностей каждого государства в плане обеспечения готовности и реагирования. Поэтому создание и укрепление потенциала стран в этой сфере является настоятельной необходимостью.

В этой связи Алжир считает, что нынешняя РГОС должна до окончания своего мандата определить соответствующие механизмы по оказанию государствами и представителями частного сектора развивающимся странам по их просьбе помощи и содействия. Такая помощь должна предусматривать, в том числе, выделение финансовых ресурсов, осуществление программ по наращиванию потенциала и передачу технологий в области ИКТ с учетом конкретных потребностей и особенностей каждого государства-получателя.

В то же время нынешняя РГОС остается оптимальной площадкой для обсуждения и согласования государствами-членами всех соответствующих инициатив, направленных на поддержание мира и безопасности в киберпространстве.

В заключение наша делегация присоединяется к заявлениям, сделанным ранее по данному блоку вопросов от имени Движения неприсоединившихся стран и Группы арабских государства (см. A/C.1/77/PV.18).

Г-жа Пейдж (Соединенное Королевство) (*говорит по-английски*): Соединенное Королевство привержено делу поощрения ответственного поведения государств в свободном, открытом, мирном и безопасном киберпространстве.

На протяжении многих лет государства регулярно выражают обеспокоенность в связи с тем, что ИКТ могут быть использованы в целях, несовместимых с задачами поддержания международного мира и безопасности, и что использование информационно-коммуникационных технологий (ИКТ) в будущих конфликтах между государствами становится все более вероятным.

Таково реальное положение дел. Сегодня мы видим, как Россия, постоянный член Совета Безопасности, задействуя свой мощный киберпотенциал, организует информационные войны с целью подрыва международного мира и безопасности. Также появляются примеры использования государствами своего киберпотенциала в рамках других конфликтов по всему миру.

Соединенное Королевство приветствует включение в текст первого принятого на основе консенсуса ежегодного доклада о ходе работы Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий четкой, основывающейся на прошлом опыте ссылки на применимость международного гуманитарного права. Мир должен выступить единым фронтом в поддержку применения и соблюдения норм международного гуманитарного права как в реальном, так и виртуальном мире.

Считаем правильным принятое Председателем Рабочей группы открытого состава решение выступить с предложением, предусматривающим возможность принятия ежегодного доклада РГОС о ходе работы на основе консенсуса. Призываем все государства поддержать этот подход и не снижать качества и темпов работы, которые мы совместно продемонстрировали в первый год деятельности РГОС.

Вместе с тем, поддерживая результаты усилий нынешней РГОС, мы не можем забывать о проблемах, с которыми мы сталкиваемся в нашей совместной работе по достижению прогресса. Соединенное Королевство является ответственной кибердержавой, стремящейся обеспечить соблюдение согласованных нами рамок ответственного

поведения государств в киберпространстве посредством позитивных действий.

Во-первых, когда то или иное государство нарушает указанные рамки, мы откровенно говорим об этом. Так, в последние восемь месяцев мы неоднократно указывали на причастность российского государства к совершению целого ряда разрушительных атак на объекты критически важной национальной инфраструктуры Украины, а также отмечаем безрассудную киберактивность со стороны Корейской Народно-Демократической Республики, Ирана и Китая. Подобные действия чреваты реальными последствиями. Их кумулятивное воздействие на объекты критически важной инфраструктуры может развиваться по нарастающей и приводить к разрушительным последствиям с точки зрения положения в области безопасности, а также в экономической, социальной и гуманитарной сферах.

В ходе недавних протестов в Иране также наблюдались случаи политически мотивированного отключения или введения ограничений на использование Интернета, а также перебои в мобильной связи. Ограничение доступа населения к Интернету подрывает возможность осуществления людьми своих прав человека, включая свободу выражения мнений и свободу объединений, и их способность привлекать правительство к ответу. Обращаемся ко всем ответственным государственным субъектам с призывом положить конец подобной злонамеренной деятельности.

Во-вторых, в тех случаях, когда нам будет представляться возможность оказать содействие в обеспечении соблюдения упомянутых выше рамок и защитить все государства от злонамеренных действий в киберпространстве, мы также будем ею пользоваться. Мы с удовлетворением отмечаем предпринятый РГОС важный шаг в направлении содействия достижению общей цели государств-членов по обеспечению ответственного поведения государств в киберпространстве — разработку глобального справочника координаторов.

Наконец, Соединенное Королевство продолжит, как это делают и другие страны, вырабатывать собственное понимание рамок и делиться им; в последний раз мы делали это в мае в нашем дополнительном заявлении о порядке применения существующих норм международного права к деятельности государств в киберпространстве. Такие действия являются еще одной важной основой нашей будущей совместной работы.

Наличие столь большого числа нерешенных вопросов однозначно указывает на необходимость налаживания регулярного институционального диалога по данной теме. Этот диалог будет с течением времени развиваться, но при этом исходные консенсусные рамки должны оставаться его надежной основой. В этой связи мы приветствуем представленный Францией проект-резолюции (A/C.1/77/L.73), предусматривающий для государств-членов четкий и транспарентный путь продолжения обсуждения возможной будущей киберпрограммы действий посредством участия в работе в рамках РГОС и предоставления материалов для подготовки доклада Генерального секретаря.

В рамках такого диалога должен обеспечиваться баланс между предоставлением государствам-членам помощи, необходимой им для соблюдения рамок, и устранением угроз международному миру и безопасности, которые являются реальными и становятся все более серьезными. Мы не можем игнорировать новые и назревающие вызовы миру и безопасности в киберпространстве.

Соединенное Королевство намерено углублять обсуждения со всеми заинтересованными сторонами в целях нахождения труднодостижимого консенсуса по сложным вопросам. Нам предстоит проделать большую работу. Посредством принятия конструктивных практических мер мы можем содействовать преодолению разрыва между реальными действиями государств и их обязательствами по соблюдению рамок ответственного поведения государств и устранить угрозы международного миру и безопасности в киберпространстве.

В заключение я хотела бы сказать несколько слов по поводу режимов контроля за ракетной технологией, представляющих собой исключительно важный компонент системы нераспространения. Помимо того, что эти режимы содействуют поддержанию международной безопасности, они обеспечивают определенные гарантии в отношении конечного использования, что является залогом уверенности государств при передаче технологии и способствует тем самым облегчению экспорта по всему миру. Соединенное Королевство обеспокоено продолжающимися попытками некоторых

государств подорвать и дискредитировать такие важные режимы.

Г-н аль-Баи (Ирак) (*говорит по-арабски*): Прежде всего делегация Ирака хотела бы присоединиться к заявлению, сделанному от имени Группы арабских государств, и заявлению, сделанному представителем Индонезии от имени государств-членов Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Делегация Ирака подчеркивает тот факт, что содействие приданию универсального характера конвенциям и договорам в области разоружения, в том числе относящимся к оружию массового уничтожения, важнейшим видом которого является ядерное оружие, служит единственной гарантией недопущения применения или угрозы применения такого оружия и тем самым предотвращения катастрофических последствий, которые могут возникнуть в результате применения такого смертоносного оружия, способного погубить и человечество, и окружающую среду.

Согласованные международные решения, изложенные в многостороннем механизме, являются единственным надежным залогом решения проблем в области разоружения и международной безопасности. В этой связи необходимо вновь подтвердить индивидуальные и коллективные обязательства в рамках международной многосторонней системы, а также обеспечить их выполнение. Необходимо также, чтобы Организация Объединенных Наций играла ключевую роль в области разоружения и нераспространения.

Ирак выражает свою растущую обеспокоенность по поводу отмечаемого в настоящее время на международной арене резкого обострения региональной и международной напряженности. Эта тенденция способствует расширению использования информационно-коммуникационных технологий (ИКТ) в деятельности, создающей угрозу для регионального и международного мира и безопасности. Поэтому Организация Объединенных Наций должна продолжать разработку обязательных правил, которые обеспечивали бы регулирование поведения государств в этой сфере, что является задачей первостепенной важности. В своей деятельности по разработке механизмов регулирования в этой области Организация Объединенных Наций также должна неизменно принимать во внимание стремительные темпы развития событий в данной сфере.

Кроме того, необходимо продолжать международное сотрудничество при сохранении центральной роли Организации Объединенных Наций в таких усилиях. В этой связи Ирак приветствует принятие на основе консенсуса первого доклада Рабочей группы открытого состава, учрежденной в соответствии с резолюцией 75/240 от 2020 года.

Ирак полностью поддерживает усилия по обеспечению успеха четвертой и пятой сессий, проведение которых запланировано на следующий год, с тем чтобы содействовать принятию рекомендаций по поддержке развивающихся стран, сталкивающихся с вызовами и опасностями, обусловленными применением ИКТ, а также с обострившимися угрозами в этой области, и заявляет о своей готовности делать все возможное в этой связи.

Г-н Гунаратна (Шри-Ланка) (*говорит по-английски*): Шри-Ланка присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

В этой взаимосвязанной сфере Интернета мы все, несмотря на неодинаковость наших возможностей, в одинаковой степени защищены и одинаково уязвимы. Говорят, что технология — полезный слуга, но опасный хозяин. Во время пандемии коронавирусного заболевания информационно-коммуникационные технологии (ИКТ) доказали, что они являются важными партнерами по процессу развития во многих сферах. В этой связи необходимо особо отметить стремительную трансформацию процесса предоставления образования в плане недопущения какого бы то ни было серьезного обесценивания достигнутых в этом секторе успехов.

Глобальная пандемия также изменила традиционное функционирование правительственных структур и организаций, которым пришлось перейти к дистанционному предоставлению услуг. Это, увы, привело к появлению в сфере критической цифровой инфраструктуры различного рода уязвимостей, одной из самых серьезных среди которых является их подверженность кибератакам, в результате которых происходят сбои в предоставлении основных услуг, совершаются кражи персональных данных и осуществляются разные мошеннические схемы.

Шри-Ланка вновь заявляет о важности принятия всеми государствами-членами совместных мер по обеспечению кибербезопасности в качестве непременного условия реализации странами в полной мере связанных с использованием ИКТ возможностей и преимуществ. Необходимо активизировать глобальные усилия по принятию международных стандартов и внедрению механизмов управления рисками в области кибербезопасности в целях обеспечения благого управления и формирования нормативно-правовой базы в сфере киберпространства. В этой связи Шри-Ланка с удовлетворением отмечает деятельность Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. На национальном уровне Шри-Ланка приступила к реализации своей первой стратегии в области информации и кибербезопасности, в которой подчеркивается важность выработки партнерского подхода к решению вопросов обеспечения кибербезопасности. Шри-Ланка продолжает укреплять свою правовую базу в области защиты пользователей компьютеров, важнейших объектов национальной инфраструктуры и киберпространства, чему способствовало, в том числе, принятие закона о преступлениях с использованием компьютера, закона о мошенничестве с использованием платежных устройств, законодательства о защите данных и закона об электронных транзакциях. В настоящее время в стране завершается разработка законопроекта о кибербезопасности.

Неправомерное использование ИКТ какими бы то ни было субъектами в каких бы то ни было целях заслуживает осуждения. В век информации неправомерное использование этого ресурса в злонамеренных целях наносит ущерб всем структурам – социальным, экономическим и политическим – и становится, скорее, средством раскола, а не мостом, объединяющим мир и наши народы. Поэтому следование нормам, правилам и принципам ответственного поведения и выполнение положений договоров и соглашений, обязанностей и обязательств в этой области является непременным условием обеспечения безопасного и защищенного киберпространства и содействия международному миру и безопасности.

Вследствие ухудшения обстановки в плане безопасности в мире сокращаются масштабы основанного на консенсусе сотрудничества и количество направлений будущих «дорожных карт» в этой сфере, что вызывает сожаление и наносит вред интересам всех государств. Эта тенденция будет способствовать лишь увеличению числа случаев неправомерного использования киберпространства террористами, проповедующими насильственные методы экстремистами и другими злоумышленниками в их стремлении подорвать безопасность пользователей этого пространства и поставить под угрозу международный мир и стабильность.

В этой связи Шри-Ланка подчеркивает важность дальнейшего сотрудничества, обмена передовым опытом и ресурсами между странами в целях эффективного решения проблем в области кибербезопасности, устранения цифрового разрыва и обеспечения беспрепятственного экономического и социального прогресса. Давайте не допустим, чтобы по причине нашей коллективной неспособности объединить усилия оказались воплощенными в жизнь сказанные еще до начала эпохи Интернета слова Альберта Эйнштейна о том, что стало чудовищно очевидно, что наши технологии превзошли нашу человечность.

Г-н Ованнисян (Армения) (*говорит по-английски*): Армения стремится поддерживать усилия международного сообщества в деле смягчения рисков и борьбы с угрозами, исходящими от использования информационно-коммуникационных технологий (ИКТ).

Вызванный пандемией коронавирусного заболевания кризис выявил растущий потенциал ИКТ в плане обеспечения надлежащего и бесперебойного функционирования правительств стран и предоставления государственных и социальных услуг. Вместе с тем ИКТ также использовались в качестве инструмента подстрекательства к дискриминации и разжиганию ненависти по признаку принадлежности к определенной группе, распространения экстремистских идеологий и побуждения к совершению насильственных действий. Все более широкое использование социальных сетей в целях распространения вражды, поощрения преступлений на почве ненависти по этническому и религиозному признаку и прославления их исполнителей, в особенности когда это происходит на государственном уровне, представляет собой опасную тенденцию, которая, если не принять меры,

может привести к серьезным нарушениям международного гуманитарного права и международного права прав человека.

В рамках четвертого Глобального форума «Против преступления геноцида», который пройдет 12 и 13 декабря в Армении под лозунгом «Предотвращение геноцида в век новых технологий», основное внимание будет уделяться потенциалу инновационных технологий в деле предупреждения зверских преступлений и угроз, порождаемых их использованием в качестве оружия, а также применению цифровых инструментов и платформ в качестве механизмов раннего предупреждения для предотвращения насилия и конфликтов.

Мы хотели бы вновь заявить о том, что принципы и нормы международного права во всей их полноте должны стать основой для ответственного поведения государств в киберпространстве.

Региональным организациям отводится важная роль в претворении в жизнь рамок ответственного поведения государств при использовании ИКТ. В этой связи Армения высоко ценит предпринимаемые в рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) на постоянной основе усилия, направленные на повышение транспарентности, предсказуемости и стабильности в использовании ИКТ, а также полное осуществление мер ОБСЕ по укреплению доверия для уменьшения рисков, возникающих в результате злонамеренного использования ИКТ.

Мы подчеркиваем важность соблюдения прав человека и основных свобод в контексте использования информационно-коммуникационных технологий. Анализируя существующие и возможные угрозы в сфере обеспечения информационной безопасности важно не упускать из виду последствия злонамеренного использования ИКТ для осуществления прав человека, в частности права искать, получать и распространять идеи независимо от государственных границ.

Армения поддерживает деятельность Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий в качестве инклюзивной и транспарентной платформы для развития диалога между государствами-членами и другими заинтересованными сторонами по вопросу применения правил, норм и принципов ответственного поведения государств. В задачу РГОС входит рассмотрение вопроса о применимости международного права в сфере ИКТ, определение путей предупреждения угроз в сфере информационной безопасности и борьбы с ними и поощрение мер, направленных на укрепление доверия и наращивание потенциала. Ежегодный доклад о ходе работы РГОС представляет собой хорошую основу для продолжения и углубления дискуссий между государствами-членами. Надеемся на конструктивные и ориентированные на результат обсуждения в ходе ее четвертой основной сессии, которая пройдет в марте 2023 года.

Г-жа Субхашини (Индия) (*говорит по-английски*): Прежде всего я хотела бы передать всем сердечные поздравления по случаю празднования Дивали. Индия имеет честь представить в рамках рассматриваемого тематического блока проект резолюции A/C.1/77/L.59, озаглавленный «Роль науки и техники в контексте международной безопасности и разоружения», в котором затрагивается тема остро ощущаемой государствами потребности в расширении международного сотрудничества в области использования науки и техники в мирных целях.

В проекте резолюции признается, что научно-технические достижения могут применяться как в гражданских, так и в военных целях и что необходимо поддерживать и далее поощрять прогресс в области науки и техники для использования его достижений в гражданских целях. В нем учитывается необходимость регулирования передачи технологий в мирных целях согласно соответствующим международным обязательствам в целях устранения риска распространения государствами и негосударственными субъектами.

В нем подчеркивается важность продолжения усилий государств-членов по применению достижений в области науки и техники в целях, связанных с разоружением, а также взаимодействия с экспертами и соответствующими сторонами из числа представителей промышленности, научных кругов и гражданского общества для эффективного решения соответствующих проблем.

Индия признательна Генеральному секретарю за представление в соответствии с резолюцией 76/24 от 2021 года обновленного доклада A/77/188. Мы с удовлетворением отмечаем, что в прошлом году эта резолюция была принята консенсусом и

получила поддержку почти 40 государств-членов в качестве авторов и соавторов.

Как развивающаяся страна, Индия выступает за расширение международного сотрудничества в области применения достижений науки и техники в мирных целях и поощрение таких усилий посредством задействования соответствующих механизмов, включая передачу технологий и обмен информацией, оборудованием и материалами. В то же время Индия считает настоятельно необходимым добиваться действенного регулирования международной передачи товаров и технологий двойного назначения и передовых технологий военного применения при обеспечении должного учета законных потребностей в области обороны всех государств и соображений нераспространения.

Стремительное развитие различных отраслей, включая биологические науки, материаловедение, искусственный интеллект и применение данных в новых и новейших технологиях, приносит человечеству значительные блага, но при этом может также создавать проблемы с точки зрения поддержания мира и безопасности. Индия признает необходимость опоры на междисциплинарный подход для понимания последствий этого процесса, а также выработки соответствующих мер по смягчению его негативного воздействия.

Индия поддерживает обсуждение проблематики новых технологий в рамках различных многосторонних форумов Организации Объединенных Наций и специализированных учреждений, а также в контексте международных договоров, участником которых она является, и принимает активное участие в этих обсуждениях.

Индия преисполнена решимости содействовать созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Злонамеренное использование киберпространства террористами и преступниками, а также взаимосвязанность сферы ИКТ обуславливают необходимость выработки совместного, основанного на правилах подхода и мобилизации усилий, направленных на обеспечение ее открытости, стабильности и безопасности.

В этой связи Индия поддерживает прикладной характер деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий, функции председателя в которой возложены на Сингапур. Приветствуем консенсусное принятие ежегодного доклада о ходе работы Группы за 2022 год, который представляет собой хороший задел для работы Группы в следующем году.

РГОС в течение срока ее работы должна оставаться основной площадкой для всех межправительственных обсуждений по вопросам ИКТ, относящимся к сфере ее ведения. Настоятельно рекомендуем воздерживаться от учреждения официальных параллельных процессов до завершения работы РГОС.

Осознавая неравный уровень готовности государств-членов к противодействию различным киберугрозам и необходимость повышения их потенциала, Индия выступила с предложением, предусматривающим создание глобального портала сотрудничества по кибербезопасности на базе Организации Объединенных Наций, который мог бы стать глобальной платформой для наращивания потенциала и международного сотрудничества между государствами-членами. Надеемся на продуктивное обсуждение по этому вопросу в следующем году в рамках РГОС и принятие соответствующего решения.

Актуальность и важность этой темы обусловливают настоятельную необходимость мобилизации государствами коллективных усилий для решения стоящих перед ними в этой области сложных проблем. Индия рассчитывает на неизменную поддержку всеми государствами-членами представленного нами в этом году проекта резолюции о роли науки и техники в контексте международной безопасности и разоружения и его принятие консенсусом. Призываем государства-члены также стать соавторами проекта резолюции и присоединиться к нам под эгидой этого коллективного стремления внести значимый вклад в обеспечение мира и безопасности во всем мире.

Г-жа Родригес Акоста (Сальвадор) (*говорит по-испански*): Растущее взаимопроникновение информационно-коммуникационных технологий (ИКТ) и усиление нашей зависимости от их функционирования во всех сферах жизни диктуют необходимость уделения всеми государствами более пристального внимания анализу достижений в области информационной безопасности и их изучению с учетом важности предотвращения

любых случаев злонамеренного использования ИКТ.

В силу этих причин наша страна относит кибербезопасность к числу основополагающих элементов международной безопасности. С обеспокоенностью отмечаем, что недавние инциденты, связанные с использованием вирусов-вымогателей и других видов кибератак с целью выведения из строя или замедления работы систем предоставления государственных услуг, привели к серьезным последствиям для международной безопасности, указав на настоятельную необходимость укрепления киберустойчивости для защиты от таких глобальных угроз. Эту задачу государствам не по силам решить в одиночку. Необходимым условием успешного преодоления этих проблем является активное взаимодействие всех членов международного сообщества.

В связи с этим приветствуем принятие в этом году консенсусом первого доклада по результатам работы Рабочей группы открытого состава Организации Объединенных Наций по вопросам безопасности в сфере использования ИКТ и самих ИКТ, в которой мы активно участвовали. Как наша делегация отметила в своем заявлении, включенном в сборник разъяснений позиций, опубликованный после принятия доклада, этот доклад не претендует на роль исчерпывающего резюме работы Группы, а, скорее, призван обрисовать проделанную на сегодняшний день работу и задать рамки будущих дискуссий.

Приветствуем также достигнутый прогресс в деле создания глобального справочника контактных лиц, как наша делегация уже отмечала на заключительных заседаниях Группы. Мы считаем, что эта призванная содействовать укреплению доверия инициатива может стать ценным источником обмена информацией об угрозах, уязвимостях и инцидентах в сфере кибербезопасности в режиме реального времени. В этой связи мы предложили изучить возможность создания такого справочника на техническом и оперативном уровнях, включив в него контактных лиц из национальных ведомств по кибербезопасности и координаторов по вопросам кибердипломатии.

Надеемся представить наши национальные данные к открытию четвертой сессии Рабочей группы. Принимаем также к сведению представление проекта резолюции A/C.1/77/L.73 о разработке программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Сальвадор с самого начала поддержал эту инициативу. Считаем, что она дополнит усилия нынешней Рабочей группы и позволит в будущем создать прикладной постоянный дискуссионный механизм для государств-членов.

Наша страна продолжает прилагать усилия с целью содействовать организации многосторонних дискуссий на тему укрепления основ ответственного поведения государств в киберпространстве и сама принимает в них участие, как и в обсуждении существующих реальных и потенциальных угроз в области безопасности и информации. В связи с этим подтверждаем важность достижения прогресса в рамках усилий по согласованию обязательного правового механизма, который позволял бы обеспечить защиту критически важной инфраструктуры и объектов информационной инфраструктуры, подверженных критическим киберугрозам, а также выявлять уязвимые места в целях защиты стратегических национальных активов.

Сальвадор намерен продолжать осуществление своей программы цифровизации, уделяя особое внимание защите персональных данных и критически важной инфраструктуры с целью повысить уровень доверия людей к предоставляемым цифровым услугам на национальном уровне. В этой связи мы с удовлетворением сообщаем о завершении процесса консультаций с общественностью по закону о кибербезопасности, который курировал Секретариат по инновациям при аппарате нашего президента. Важно и впредь в этом же ключе поощрять разработку мер укрепления доверия, которые позволяют снижать напряженность и добиваться деэскалации конфликтов в киберпространстве.

Мы решительно подчеркиваем важность широкого участия других заинтересованных сторон в этих процессах. Вызовы в киберпространстве требуют активного сотрудничества со стороны гражданского общества, неправительственных организаций, региональных организаций и научных кругов.

Наконец, наша делегация неоднократно указывала на то, что опора на сквозной гендерный подход может помочь нам понять превалирующие тенденции в условиях вооруженного насилия и конфликтов, по-разному влияющие на мужчин и

женщин. Мы должны решительно браться за устранение этих проблем. Гендерные аспекты сохраняют свою актуальность и в контексте международной кибербезопасности.

Полный текст моего заявления будет размещен на портале eStatements.

Г-жа Ли (Республика Корея) (*говорит по-английски*): За последние несколько десятилетий человечество стало свидетелем небывалого прогресса в области цифровых технологий. Это развитие повлекло за собой беспрецедентные экономические и социальные выгоды, однако, поскольку с начала глобальной пандемии Интернетом начали пользоваться еще больше людей, повысилась наша уязвимость для злонамеренной активности с использованием киберсредств. Поведение государственных и негосударственных субъектов в киберпространстве лишь усложняет ситуацию в плане международной безопасности.

Несмотря на сложность стоящих перед нами задач, международное сообщество должно совместно работать над созданием открытого, безопасного, стабильного, доступного и мирного киберпространства. В связи с этим Республика Корея поддерживает центральную роль Организации Объединенных Наций в нынешних обсуждениях того, как решать стоящие перед нами задачи и поощрять ответственное поведение государств в киберпространстве. Хочу отдельно остановиться на следующих моментах.

Во-первых, Республика Корея с удовлетворением отмечает ежегодный доклад Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих информационно-коммуникационных технологий о проделанной работе за 2022 год, и приветствуем также решение Председателя одобрить этот доклад. Республика Корея продолжит конструктивное взаимодействие с РГОС, опираясь на этот принятый консенсусом доклад о ходе работы.

В качестве соавтора представленного Францией проекта резолюции A/C.1/77/L.73, озаглавленного «Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности», мы хотели бы подчеркнуть необходимость создания в рамках Организации Объединенных Наций постоянного механизма, например программы действий, для активизации применения норм на практике и содействия обмену передовым опытом и наращиванию потенциала.

Во-вторых, по мнению Республики Корея, консенсусные решения РГОС и предыдущих Групп правительственных экспертов (ГПЭ) отражают прогресс, достигнутый применительно к кумулятивной и эволюционирующей основе ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ). Соответственно, поскольку в киберпространстве не должно оставаться неохваченных правовыми нормами областей, к киберпространству должно в равной степени применяться международное право, включая Устав Организации Объединенных Наций, во всей его полноте. Кроме того, государства должны добросовестно соблюдать и выполнять добровольные, необязательные нормы, изложенные в консенсусных докладах ГПЭ и РГОС. В частности, наша делегация считает, что важнейшую роль в обеспечении кибербезопасности играет принцип должной предусмотрительности, и хотела бы тесно сотрудничать с другими государствами-членами в дальнейшей разработке и внедрении соответствующих норм.

В-третьих, Республика Корея является решительным сторонником мер укрепления доверия (МУД) и наращивания потенциала. МУД могут снизить риск возникновения конфликта в результате недопонимания и просчетов. Республика Корея будет также стремиться устранить пробелы в возможностях киберзащиты. Активно участвуем в соответствующей деятельности на таких региональных площадках, как Ассоциация государств Юго-Восточной Азии (АСЕАН) и Региональный форум АСЕАН.

Наша делегация считает, что взаимодействие с молодым поколением, расширение его возможностей и его просвещение могут внести ценный вклад в поддержание глобального режима нераспространения. С 2019 года государства-члены консенсусом поддерживают принимаемую раз в два года резолюцию «Молодежь, разоружение и нераспространение». Кроме того, в проекте заключительного документа последней Конференции участников Договора о нераспространении ядерного оружия по рассмотрению действия Договора

признается важность учета разнообразных мнений и приверженность расширению прав и возможностей молодежи и обеспечению ее участия в деятельности в области разоружения и нераспространения. Поддерживая реализацию действия 38, обозначенного в документе Генерального секретаря «Обеспечение нашего общего будущего: повестка дня в области разоружения», Республика Корея будет и впредь играть ведущую роль в осуществлении этой повестки дня и обязуется продолжать такую работу.

В заключение наша делегация хотела бы отметить, что Республика Корея уважает право всех государств-членов на доступ к оборудованию, материалам и научно-технической информации для использования в мирных целях и в этой связи твердо убеждена, что существующие режимы экспортного контроля способствуют выполнению этой задачи, поскольку в них вместо того, чтобы предоставлять странам-экспортерам свободу действий для введения произвольных ограничений или необоснованного лицензирования, проводится разграничение между тем, что можно и что нельзя экспортировать.

Г-н Айдиль (Турция) (*говорит по-английски*): Сегодня использование информационно-коммуникационных технологий (ИКТ) оказывает все большее влияние на глобальную ситуацию в плане мира, безопасности, прав человека и экономического развития.

Турция по-прежнему обеспокоена злонамеренным использованием таких технологий и ростом числа кибератак во всем мире, носящих все более серьезный характер. Жизнь наших граждан подвергается серьезному влиянию кибератак, которые направлены против такой критически важной инфраструктуры, как электронные коммуникации, энергетика, финансы, транспорт, водопользование и другие важнейшие сектора государственных услуг.

Для формирования открытого, свободного, стабильного и безопасного киберпространства на глобальном уровне необходимо устранить такие угрозы и риски в киберпространстве.

В отношении ответственного поведения государств в киберпространстве уже проделана большая работа. Подчеркиваем ключевую роль Организации Объединенных Наций в этом процессе. На наш взгляд, обсуждение связанных с киберпространством вопросов под эгидой Организации Объединенных Наций вышло на довольно высокий уровень. Поэтому нам необходимо приступить к обсуждению того, как содействовать внедрению существующей нормативной базы.

В заключительном докладе предыдущей Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ указано, что повышается вероятность применения ИКТ в будущих конфликтах между государствами. Война на Украине подтвердила обоснованность такой обеспокоенности, что обусловило неотложность выполнения поставленной задачи.

Для более эффективного внедрения существующей кумулятивной основы хорошим шагом вперед стала бы разработка программы действий по вопросам кибербезопасности. Поддерживаем представленный Францией проект резолюции A/C.1/77/L.73 по этому вопросу и надеемся на продолжение наших обсуждений в будущем в рамках программы действий, служащей постоянным, инклюзивным и ориентированным на действия механизмом. Целесообразно также опираться на программу действий в целях развития диалога и сотрудничества по вопросам наращивания потенциала, которые имеют ключевое значение для обеспечения потенциала противодействия киберугрозам. Эта инициатива не направлена на дублирование работы действующей РГОС по вопросам безопасности ИКТ или конкуренцию с ней. В рамках такой инициативы принимаются во внимание выводы РГОС, и она способствует их реализации.

Турция принимает активное участие в работе нынешней РГОС. Приветствуем консенсусное принятие ежегодного доклада о ходе работы в этом году. Мы согласны с оценкой, в соответствии с которой Рабочая группа, имеющая универсальный членский состав, является уникальной площадкой и сама ее работа представляет собой меру укрепления доверия.

Характер киберугроз обуславливает необходимость осуществления согласованных действий. Хотелось бы, чтобы в этом году — так же, как и в прошлом — в Первом комитете удалось достичь консенсуса. Еще раз призываем к сотрудничеству в этом отношении.

Г-н Огасавара (Япония) (*говорит по-английски*): Киберпространство стало незаменимой экономической и социальной инфраструктурой для всех видов деятельности и поэтому является общественным пространством, открытым для всех граждан. Такие экономические и социальные преобразования также повысили нашу уязвимость для кибератак, которые представляют собой серьезную угрозу всеобщей безопасности. В плане национальной безопасности мы особенно обеспокоены злонамеренной активностью с использованием киберсредств, исходящей из других государств и наносящей ущерб критически важной инфраструктуре, независимо от того, поддерживается она самими государствами или нет.

В одиночку странам будет сложно справиться с такими угрозами кибербезопасности. Первостепенное значение для защиты и укрепления свободного, открытого и безопасного киберпространства имеет сотрудничество и взаимодействие между государствами.

По вопросу применения международного права в отношении кибероперациий позиция Японии однозначна: существующие нормы международного права применимы ко всем таким операциям. Кроме того, мы решительно поддерживаем разработку добровольных норм ответственного поведения государств. Огромное значение для стабилизации отношений между странами и мирного урегулирования споров имеет обеспечение уважения членами международного сообщества принципа верховенства права.

Япония считает важным продвигать принцип верховенства права и в киберпространстве. В связи с необходимостью такой работы и создания свободного, справедливого и безопасного киберпространства Япония приветствует ежегодный доклад о ходе работы, принятый консенсусом в Рабочей группе открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ в период 2021–2025 годов. Поскольку речь идет об ориентированном на действия процессе, важно, чтобы РГОС достигла конкретных результатов с учетом итогов обсуждений прошлых годов, отраженных в докладах Группы правительственных экспертов и РГОС. В связи с этим мы решительно поддерживаем решение председателя РГОС одобрить ежегодный доклад о ходе работы.

Поддерживаем также представленный Францией проект резолюции A/C.1/77/L.73 о программе действий по поощрению ответственного поведения государств в киберпространстве.

Кроме того, хотелось бы затронуть тему образования по вопросам разоружения и нераспространения, которую поддерживает Япония, поскольку такое образование служит полезным и эффективным средством построения мира, свободного от ядерного оружия.

В этой связи для нас крайне важно повышать осведомленность общественности о катастрофических гуманитарных последствиях любого применения ядерного оружия, об угрозе разнообразных рисков, связанных с распространением ядерного оружия, а также о мерах, необходимых для решения этих проблем.

В основе процесса просвещения общественности и повышения ее осведомленности относительно вопросов разоружения и нераспространения должен лежать инклюзивный подход, предполагающий совместные усилия. Различные субъекты, включая образовательные и исследовательские учреждения, аналитические центры, научное сообщество, гражданское общество, частный сектор, СМИ, местные муниципалитеты, международные организации и правительства, должны учиться друг у друга и дополнять усилия друг друга для содействия просветительным инициативам.

Именно исходя из этого Япония предлагает упомянуть некоторые конкретные инициативы в этом направлении в пункте 11 постановляющей части проекта резолюции A/C.1/77/L.61, озаглавленного «Шаги на пути к формированию общей дорожной карты в целях построения мира, свободного от ядерного оружия», который Япония представила на рассмотрение Комитета в этом году.

Япония активно участвует в различных мероприятиях, направленных на информирование общественности по вопросам разоружения и нераспространения. В частности, на состоявшейся в августе Конференции участников Договора о нераспространении ядерного оружия по рассмотрению действия Договора премьер-министр Кисида объявил о создании Фонда молодежных лидеров за построение мира, свободного от ядерного оружия. На Конференции Япония также возглавила работу

над совместным заявлением по вопросам образования в области разоружения и нераспространения, которое было поддержано 89 государствами-участниками ДНЯО.

Япония твердо верит в силу образования по вопросам разоружения и нераспространения и способность будущих поколений достичь нашей общей цели – построения мира без ядерного оружия.

Полный текст моего выступления будет размещен в Журнале Организации Объединенных Наций.

Г-жа Ромеро Лопес (Куба) (*говорит по-испански*): Мы присоединяемся к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Мы подтверждаем приверженность Кубы всеобщему и полному разоружению, которое позволит нам построить мир, в котором нет места оружию массового уничтожения, на благо нынешнего и будущих поколений. Призываем к принятию дальнейших мер в области разоружения и обеспечения международной безопасности, которые позволят нам продвинуться к установлению мира во всем мире.

Мы должны как можно скорее максимально сократить значительные объемы ресурсов, которые в настоящее время выделяются на военные цели. Те же ресурсы, которые сегодня используются для финансирования военно-промышленного комплекса и разработки, производства и совершенствования все более смертоносного высокотехнологичного оружия, а также научно-технический прогресс, которые служит таким же целям, принесли бы человечеству огромную пользу, если бы были перенаправлены на цели достижения устойчивого развития.

Государства-члены должны продолжать работу с целью сохранения многостороннего подхода в качестве основного принципа проведения переговоров по вопросам разоружения и контроля над вооружениями. Напомним, что в ходе таких переговоров необходимо соблюдать действующие международные экологические нормы.

Мы призываем к согласованию на основе переговоров имеющих обязательную юридическую силу инициатив, направленных на недопущение милитаризации космического пространства и киберпространства и создания смертоносного автономного оружия. Мы должны достичь соглашения касательно правил применения оружия, которое лишь частично контролируется человеком, и ударных беспилотных летательных аппаратов.

Мы подтверждаем нашу приверженность деятельности учрежденной на период 2021–2025 годов Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, касающейся вопросов безопасности и использования информационных технологий. Мы поддерживаем проведение обсуждений в таком формате, обеспечивающем участие всех государств на равных условиях.

Информационно-коммуникационные технологии недопустимо использовать в качестве средства ведения войны, ибо они предназначены исключительно для мирных целей. Мы выступаем против враждебного использования телекоммуникационных средств для достижения заявленных или тайных целей, заключающихся в подрыве правопорядка и политического строя государств, совершении или поощрении актов терроризма.

Мы считаем неприемлемым допущение применения силы в качестве законной меры реагирования на кибератаку. Мы вновь выражаем свою озабоченность по поводу утвержденной Соединенными Штатами киберстратегии, в рамках которой допускается применение наступательного кибероружия и проведение кибероборонительных операций, в том числе нанесение упреждающих кибердаров для сдерживания противника.

Мы отвергаем нетрадиционные методы войны, которые правительство Соединенных Штатов продолжает использовать против Кубы, задействуя в интересах достижения этой цели огромные ресурсы. Мы осуждаем использование новых информационных технологий и других цифровых платформ в стремлении дестабилизировать положение в нашей стране, содействовать распространению фальшивых новостей и добиться смены режима на Кубе. Мы считаем недопустимой деятельность целевой группы по вопросам интернета на Кубе, которая противоречит согласованным на международном уровне нормам в этой области. Мы призываем Соединенные Штаты немедленно

положить конец экономической, торговой и финансовой блокаде, введенной против Кубы, которая существенно ограничивает доступ к информационно-коммуникационным технологиям и возможности их использования и применения на благо кубинского народа.

Мы убеждены, что всеобщее и полное разоружение необходимо и возможно. Куба будет и впредь выступать за принятие эффективных мер, которые позволили бы нам достичь этой благородной цели.

Г-н Салмин (Кувейт) (*говорит по-арабски*): Делегация нашей страны присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Группы арабских государств (см. A/C.1/77/PV.18).

Кибербезопасность является одной из новых проблем, с которыми сталкивается мир, и в настоящее время многие страны страдают от ее негативных последствий, включая Государство Кувейт, которое в последние годы многократно подвергалось кибератакам, а также актам киберпиратства, представлявшим собой либо акты отдельных субъектов, либо спонсируемые террористическими и иностранными преступными группами диверсии. Это объясняется двойным назначением киберпространства и использованием микротехнологий и ресурсов для разработки новых оружейных систем, что ведет к усилению сомнений и недоверия в отношениях между государствами.

В этой связи наша страна подчеркивает необходимость установления стандартов в области безопасности и обеспечения защиты от кибератак и намеренных нарушений. Мы призываем все страны сотрудничать и координировать свои действия на региональном и международном уровнях.

Государство Кувейт придает большое значение обеспечению кибербезопасности, рассматривая ее в качестве важнейшего элемента обороны, тем более что киберпреступность не только причиняет вред отдельным лицам и учреждениям, но и ставит под угрозу национальную безопасность, а также объекты и экономику государства. Именно поэтому Государством Кувейт была разработана и реализуется национальная стратегия в области кибербезопасности на 2017-2020 годы, призванная содействовать укреплению культуры кибербезопасности и справедливому и безопасному использованию кувейтского киберпространства, а также обеспечению защиты критически важной национальной информационной инфраструктуры, в том числе путем укрепления механизмов обмена информацией между различными заинтересованными сторонами, как на местном, так и на международном уровне. Хотим подчеркнуть, что наша стратегия соответствует строгим требованиям в области безопасности и глобальным критериям, которые обеспечивают защиту информации от всех видов взлома и гарантируют безопасность киберпространства в Кувейте и его устойчивое использование.

В этой связи, осознание политическим руководством Государства Кувейт масштабов проблем в области киберпространства и приверженность нашей страны цифровой трансформации в качестве инструмента содействия нашему национальному развитию в рамках новой программы «Кувейт 2035» побудили Государство Кувейт создать национальный центр кибербезопасности, включающий оперативный центр кибербезопасности, а также группу реагирования на чрезвычайные ситуации в киберпространстве, с целью разработки всеобъемлющей национальной стратегии кибербезопасности. Это позволит обеспечить защиту наших информационных и телекоммуникационных сетей, а также осуществлять сбор информации и обмен ею с помощью любых электронных устройств в партнерстве со всеми национальными заинтересованными сторонами.

Мы переживаем технологическую революцию и демонстрирующую беспрецедентные темпы цифровую трансформацию, неуклонно расширяя при этом сферу использования Интернета и современных средств коммуникации. Сегодня мир взаимосвязан как никогда, что повышает риск кибератак, включая кражу информации и нарушения конфиденциальности. Также отмечается высокая доля изъянов в современном оружии, зависящем от современных технологий. В этом контексте у Государства Кувейт вызывают обеспокоенность развитие систем автономного оружия и использование в сфере телекоммуникации аддитивных технологий, получивших широкое распространение в производственных процессах по всему миру. Это представляет собой новую угрозу международному миру и стабильности — если эти технологии попадут в руки террористических групп или организованных преступных группировок или будут использоваться незаконно, это, безусловно,

повлечет катастрофические последствия для соответствующей инфраструктуры и потока товаров, производимых с использованием безопасных технологий. В этой связи наша страна подтверждает неизменный характер нашей позиции по вопросам разоружения и международной безопасности. Мы считаем, что потоки оружия и его распространение никак не способствуют достижению нашей заветной цели — обеспечению мира и стабильности во всем мире.

Поэтому мы призываем все государства направить усилия на разработку имеющего обязательную силу и пользующегося консенсусной поддержкой международного документа, который бы регулировал использование киберпространства, и на создание надлежащих механизмов для обмена информацией между государствами-участниками. Такой документ должен обеспечивать, помимо прочего, уважение суверенитета государств в контексте использования беспилотников, которые широко применяются в качестве нового средства ведения войны, направленного против гражданского населения и объектов государственной инфраструктуры. Государство Кувейт считает заслуживающими особого осуждения любые кибер- и электронные атаки с использованием беспилотников, поскольку они влекут за собой серьезные последствия для безопасности на региональном и международном уровнях. В этом контексте мы призываем государства придерживаться принципов Устава, в частности таких, как поддержание добрососедских отношений, уважение суверенитета государств и невмешательство в их внутренние дела.

Государство Кувейт приветствует две программы действий по кибербезопасности, инициированные Генеральным секретарем Антониу Гутеррешем в рамках предложенной им в 2018 году повестки дня по разоружению.

В заключение хочу сказать, что мы высоко ценим все международные усилия, связанные с вопросом кибербезопасности, и призываем не политизировать их и продвигать принцип прозрачности в этом отношении. Мы подчеркиваем нашу неизменную поддержку всех международных мер, способствующих укреплению доверия и наращиванию потенциала противодействия угрозам международному миру и безопасности.

Г-н Йоттеран (Швейцария) (*говорит по-французски*): У Швейцарии вызывает обеспокоенность все более широкое использование в рамках вооруженного конфликта на Украине кибероперациий, особенно в тех случаях, когда их целью являются объекты критически важной инфраструктуры. Это повышает вероятность непроизвольных последствий и различного рода эксцессов. Швейцария призывает все стороны вооруженного конфликта соблюдать международное гуманитарное право, а также международное право в области прав человека. Это касается и киберпространства.

В нашем быстро меняющемся мире ширится использование киберпространства в гражданских и военных целях, что создает новые вызовы для международного мира и безопасности. Справиться с этими вызовами можно только посредством обеспечения соблюдения согласованных рамок ответственного поведения государств в киберпространстве. Как подтверждается в консенсусных докладах Группы правительственных экспертов и Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, эти рамки предусматривают, в числе прочего, применение международного права в киберпространстве, реализацию 11 добровольных норм и принятие мер, содействующих укреплению доверия и наращиванию потенциала.

С удовлетворением отмечаем принятие в июле на основе консенсуса ежегодного доклада о деятельности Рабочей группы открытого состава, который содержит, среди прочего, важные предложения, направленные на дальнейшее разъяснение условий применения в тех или иных конкретных случаях международного права, включая международное гуманитарное право, и реализацию добровольных норм ответственного поведения государств в киберпространстве.

Ведущаяся в настоящее время нынешней Рабочей группой исключительно важная работа предоставляет бесценную возможность для дальнейшего укрепления консенсуса в отношении применения международного права в киберпространстве. В стремлении содействовать достижению нашей общей цели — выработке общего понимания механизмов применения международного права к киберпространству, — Швейцария в 2021 году представила свою национальную позицию по этому важному вопросу.

Призываем все государства-члены Организации Объединенных Наций подумать о формулировании собственных национальных позиций. Мы также рассчитываем на продолжение обсуждений по всем элементам мандата нынешней Рабочей группы.

Приветствуем предложение Председателя РГОС о проведении межсессионных совещаний в 2023 и 2024 годах для содействия проведению обсуждений, продолжения работы на основе ежегодного доклада о проделанной работе и поддержки дальнейшей деятельности Группы. В этой связи мы благодарим Председателя РГОС за представление Комитету проекта решения (A/C.1/77/L.54), которым предусматривается как одобрение этого доклада, так и проведение упомянутых межсессионных консультаций. Швейцария полностью поддерживает проект решения и воплощенный в нем чисто процедурный и практический подход.

Считаем также необходимым подчеркнуть, что у нас имеются серьезные сомнения относительно представленного Российской Федерацией по этому вопросу проекта резолюции (A/C.1/77/L.23/Rev.1), который представляется нам ненужным и дублирует текст Председателя РГОС. Проект, представленный Россией, также вызывает вопросы по существу, в частности потому, что он не опирается на консенсусные формулировки и использует избирательный подход. Это чревато подрывом того значительного прогресса, которого удалось достичь к настоящему времени в рамках нынешней РГОС. В этих условиях Швейцария не может поддержать данный проект.

Идея создания платформы для регулярного институционального диалога по кибервопросам в рамках Организации Объединенных Наций также заслуживает нашего пристального внимания. Швейцария хотела бы подчеркнуть, что решения о будущем кибердискуссий в Организации Объединенных Наций должны основываться на всестороннем обсуждении, которое позволит всем государствам-членам представить свои мнения. Кроме того, с нашей точки зрения, любые будущие процессы под эгидой Организации Объединенных Наций должны быть направлены на поддержку государств-членов в их усилиях по реализации существующих рамок ответственного поведения государств в киберпространстве.

Важно развивать и сохранять то, что было достигнуто за последние несколько лет, и эффективно использовать согласованные рекомендации. Поэтому мы поддерживаем представленный Францией проект резолюции A/C.1/77/L.73 о программе действий для содействия ответственному поведению государств в сфере использования информационно-коммуникационных технологий в контексте международной безопасности, который призван помочь государствам-членам Организации Объединенных Наций добиться прогресса в этом обсуждении.

Г-жа Владеску (Румыния) (*говорит по-английски*): Румыния полностью присоединяется к заявлению, с которым выступил представитель Европейского союза (см. A/C.1/77/PV.18), и хотела бы высказать следующие соображения в своем национальном качестве.

Наша встреча проходит на фоне кардинально изменившейся обстановки в сфере безопасности, характеризующейся ростом напряженности и глобальными проблемами, которые по-прежнему ослабляют архитектуру контроля над вооружениями, разоружения и нераспространения. В результате незаконной, необоснованной и неспровоцированной военной агрессии Российской Федерации против соседнего государства, Украины, эскалация достигла беспрецедентного уровня.

С 24 февраля мы наблюдаем драматические последствия этой агрессии, в ходе которой Россия использует все виды обычных вооружений, прибегая также к дезинформации и кибератакам. Румыния решительно осуждает российскую агрессию и вновь заявляет о своей неизменной поддержке независимости, суверенитета и территориальной целостности Украины в ее международно признанных границах.

Безопасность киберпространства стала вопросом первостепенной важности, учитывая тот факт, что злонамеренная деятельность в сфере информационно-коммуникационных технологий (ИКТ) со стороны источников постоянных угроз, к числу которых относятся государства и другие субъекты, может представлять серьезную угрозу для международной безопасности и стабильности, социально-экономического развития, а также безопасности и благополучия людей.

Сейчас как никогда важно содействовать созданию открытого, безопасного, стабильного, доступного и мирного киберпространства, полностью

придерживаться разработанных Организацией Объединенных Наций рамок ответственного поведения государств в киберпространстве и продолжать содействовать обеспечению безопасности и стабильности в процессе использовании ИКТ государствами.

Румыния с удовлетворением отмечает, что в этом году удалось достичь консенсуса по ежегодному докладу о результатах деятельности Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий на период 2021–2025 годов, созданной в соответствии с резолюцией 75/240. Мы вновь заявляем, что полностью поддерживаем решение Председателя Рабочей группы открытого состава по данному вопросу и его призыв к принятию этого документа на основе консенсуса.

Мы призываем все государства-члены поддержать проект резолюции A/C.1/77/L.73 о программе действий по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности, одним из авторов которого является трансрегиональная группа государств и который пользуется полной поддержкой Румынии.

На фоне усиления напряженности и роста числа конфликтов становится все более очевидной необходимость усиления регулирования и повышения транспарентности, особенно в области военных расходов. В этой связи мы хотели бы обратить внимание на проект резолюции этого года, озаглавленный «Объективная информация по военным вопросам, включая транспарентность военных расходов» (A/C.1/77/L.63), который по традиции был представлен Румынией и Германией. Настоятельно призываем государства-члены Организации Объединенных Наций поддержать проект резолюции, в основе которого лежит основной принцип укрепления доверия между государствами.

За многие годы удалось достигнуть больших успехов в рамках работы системы стандартизированной отчетности Организации Объединенных Наций о военных расходах, которая должна оставаться одним из наших самых важных инструментов повышения транспарентности. Пользуясь этой возможностью, мы хотели бы еще раз подчеркнуть неизменную важность Отчета Организации Объединенных Наций о военных расходах, тем более с учетом нынешних обстоятельств, и призвать все государства активно участвовать в подготовке отчетности.

Поскольку со времени принятия в 2019 году предыдущей резолюции по этому вопросу, резолюции 74/24, не было внесено никаких существенных изменений в работу стандартизированной системы отчетности, в том числе из-за пандемии коронавируса, мы решили сохранить текст, ранее принятый Первым комитетом и Генеральной Ассамблеей, и выступить с предложением о техническом продлении, внеся в него лишь несколько незначительных технических обновлений. Эта резолюция стоит на повестке дня Первого комитета уже более двадцати лет и неизменно пользовалась поддержкой подавляющего большинства государств – членов Организации Объединенных Наций. Мы надеемся, что на этой сессии проект резолюции вызовет такой же позитивный отклик и что государства-члены вновь продемонстрируют свою поддержку, приняв проект резолюции без голосования, как это неоднократно происходило на предыдущих сессиях Первого комитета.

Г-н Видаль (Чили) (*говорит по-испански*): Чили присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Мы приветствуем документы, основанные на принципах гендерного равенства и справедливости и продвигающие права женщин, детей и групп людей с различной сексуальной ориентацией на многосторонних форумах и в международных организациях, а также документы, в которых основной акцент сделан на учете гендерной проблематики в ходе таких переговоров.

В этой связи мы приветствуем проект резолюции A/C.1/77/L.18, озаглавленный «Женщины, разоружение, нераспространение и контроль над вооружениями» и представленный Тринидадом и Тобаго в соавторстве с нашей страной. Настоятельно необходимо, чтобы в существующих мандатах Организации Объединенных Наций, особенно в области международной безопасности, был обеспечен учет гендерных вопросов. Гендерные вопросы необходимо рассматривать в рамках инклюзивного, справедливого и эффективного процесса.

Чили считает, что угрозы, исходящие от информационно-коммуникационных технологий (ИКТ), могут по-разному влиять на государства в зависимости от уровня цифровизации их ИКТ, потенциала, ситуации в плане безопасности и жизнестойкости, а также их инфраструктуры и степени развития. Подобные угрозы также могут по-разному влиять на различные группы и субъекты, особенно на женщин и девочек. Такие государства, как наше, сталкиваются с различными видами угроз и испытывают различные потребности, в связи с чем крайне важно укреплять наши возможности по созданию структур и разработке планов координации усилий не только на уровне правительства, но и путем развития эффективных партнерских отношений с гражданским обществом, частным сектором и научными кругами.

Чили считает, что международное право, в частности Устав Организации Объединенных Наций, обеспечивает применимую нормативную базу, которая должна регулировать поведение государств в киберпространстве, включая международное гуманитарное право, права человека и те законы, которые определяют международную ответственность государств, поскольку они жизненно важны для поддержания мира и стабильности, необходимых для создания открытой, безопасной, стабильной, доступной и мирной среды для развития информационно-коммуникационных технологий.

По всем этим причинам мы поддерживаем деятельность, осуществляемую Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий на период 2021–2025 годов под руководством Постоянного представителя Сингапура, и программу действий по поощрению ответственного поведения государств при использовании ИКТ в международном контексте. Наша страна, как и другие члены, всегда будет поддерживать документы, направленные на укрепление доверия. Мы поддерживаем все органы, в рамках которых государства могут обмениваться мнениями и обозначать свои приоритеты и потребности, тем самым укрепляя безопасность, повышая устойчивость ИКТ к потрясениям и содействуя их мирному использованию в целом.

Г-н Суарис Дамику (Бразилия) (*говорит по-английски*): В своем документе «Обеспечение нашего общего будущего: повестка дня в области разоружения» Генеральный секретарь подтвердил необходимость вновь сфокусировать внимание международного сообщества на взаимосвязи между разоружением и развитием.

Исходя из давно сформировавшегося среди развивающихся стран мнения, Бразилия разделяет очевидное предположение о существовании прямой зависимости между разоружением и развитием. Действительно, безопасность на национальном и международном уровнях является необходимым элементом экономического роста. Если бы финансовые и технологические ресурсы, используемые для расширения обычных и стратегических арсеналов, были перенаправлены на деятельность в важнейших сферах человеческой жизни, таких как образование, здравоохранение и охрана окружающей среды, нам жилось бы гораздо лучше. Таким образом, в центре наших усилий должна быть связь между разоружением и целями в области устойчивого развития.

Мы получали достаточно серьезные дивиденды мира. В 1960 году в среднем объем военных расходов составлял 6,3 процента от валового внутреннего продукта (ВВП). Спустя 60 лет этот показатель достиг самого низкого уровня – 2,4 процента. Это означает, что за 25 лет у нас будут накоплены ресурсы для повышения социального благосостояния, эквивалентные годовому ВВП.

Тем не менее нынешняя напряженная ситуация привела к резкому обращению вспять этой тенденции. Что еще хуже, это совпало с периодом беспрецедентного дефицита государственного бюджета в результате противодействия последствиям пандемии коронавирусной инфекции, причем в некоторых развитых странах такой дефицит достиг уровня, ранее наблюдавшегося только во время Второй мировой войны. Единственным утешением в сложившейся ситуации является то, что в недалеком будущем налогоплательщики будут вынуждены выбирать между маслом и оружием.

Разоружение, нераспространение и контроль над вооружениями больше не могут оставаться вопросами высокой политики. Они как никогда ранее отражают социальный выбор, учитывая их огромное влияние на повседневную жизнь миллионов людей повсеместно каждый день.

Наша нынешняя повестка дня в области разоружения включает в себя целый ряд новых тем, более близких к нашим реалиям, таких как гендерные аспекты, дискуссии по вопросу о беспрепятственном доступе к технологиям для мирного использования и аспекты безопасности информационно-коммуникационных технологий. Однако от того, что эти темы тесно связаны с нашей жизнью, они не перестают быть сложными для обсуждения. До сих пор сохраняются серьезные разногласия относительно того, как решать эти вопросы.

Бразилия считает, что обсуждения вопросов чувствительных и новых технологий занимают видное место в современных международных отношениях. Необходимо не только тщательно продумать вопросы безопасности, но и выступать за создание открытой, доступной, мирной и безопасной среды для развития таких технологий, обмена ими и их использования. Приоритетная задача состоит в том, чтобы найти хрупкий баланс при рассмотрении этой темы с целью защиты неоспоримых экономических и социальных благ, которые технологии приносят нашим народам, а также пресечения их злонамеренного использования как государствами, так и негосударственными субъектами. Такой подход защищает законное право всех государств иметь доступ к важнейшим технологиям для своего развития, поддерживая при этом законные цели нераспространения и международной безопасности.

Развитие информационно-коммуникационных технологий (ИКТ) стало центральной темой обсуждения на заседаниях нашего Первого комитета. С 1998 года было созвано шесть составов Групп правительственных экспертов, в двух из которых председательствовала Бразилия.

Это постоянное стремление членов Организации сохранить вопрос ИКТ в своей текущей повестке дня свидетельствует о его стратегическом характере и настоятельной необходимости надлежащего регулирования, направленного на сохранение киберпространства как открытой, мирной и доступной среды, а также недопущения превращения киберпространства в театр военных действий.

Для этого необходимо согласовать различные представления о роли киберпространства в нашем обществе и о том, чего мы хотим от него. По своей природе эта межправительственная деятельность выиграет от вклада гражданского общества, научных кругов и промышленности. Как бы то ни было, в основе этой дискуссии лежит применимость международного права, особенно Устава Организации Объединенных Наций, и бескомпромиссная защита прав человека.

Надеемся, что нынешняя Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, равно как и будущий механизм институционального диалога, который будет создан после нее, укрепят понятия ответственного поведения, транспарентности и мер укрепления доверия, а также наращивания потенциала, опираясь на работу, проделанную предыдущими группами правительственных экспертов и отраженную в докладах РГОС, принятых на основе консенсуса.

Нельзя не отметить работу, проделанную послом Сингапура Бурханом Гафуром в качестве Председателя РГОС по вопросам безопасности ИКТ. Мы приветствуем принятие ежегодного доклада на последней сессии. Это хорошая основа для продолжения нашей работы.

Г-н Санчес Кисслих (Мексика) (*говорит по-испански*): Междисциплинарные проблемы, связанные с международной безопасностью, требуют мер, которые носят комплексный характер и выходят за рамки традиционного понимания безопасности. Именно поэтому мы подчеркиваем важность всех мер, которые укрепляют существующие региональные и международные рамочные документы по вопросам обеспечения международной безопасности, контроля над вооружениями, разоружения и нераспространения.

Законное и мирное использование киберпространства, цифровая устойчивость и возможности, предоставляемые информационными технологиями в качестве инструмента устойчивого развития, могут быть сохранены и гарантированы только с помощью многосторонних средств. Постоянное повышенное внимание Первого комитета к этой теме ясно свидетельствует о нашем доверии к приоритетной роли Организации Объединенных Наций и многостороннего подхода. Здесь ожидания высоки, но угрозы и вызовы будут еще выше, если нам не удастся обеспечить создание архитектуры для цифровой среды будущего.

Наша делегация высоко оценивает прогресс, достигнутый в деле включения гендерной проблематики в различные резолюции Организации Объединенных Наций и многосторонние договоры, связанные с Первым комитетом. Как и другие делегации, мы считаем, что полноценное, равноправное и значимое участие женщин в усилиях по разоружению и нераспространению является залогом достижения устойчивого мира. Мы будем продолжать продвигать и поддерживать те инициативы, которые направлены на расширение участия женщин в процессах принятия решений в этой области. По этой причине в этом году, как и в прошлом, мы рады выступить соавторами проекта резолюции A/C.1/77/L.18, озаглавленного «Женщины, разоружение, нераспространение и контроль над вооружениями».

Кроме того, Мексика по-прежнему твердо привержена просвещению в области разоружения как средству предотвращения. Считаем, что эта стратегия способствует повышению осведомленности о влиянии использования любого вида оружия на общество и нашу окружающую среду. Она также помогает воспитывать молодые, заинтересованные поколения как новых проводников перемен в области разоружения и международной безопасности.

В этом году мы рады вновь представить двухгодичные проекты резолюций по Информационной программе Организации Объединенных Наций по разоружению (A/C.1/77/L.20) и исследованию Организации Объединенных Наций по вопросу о просвещении в области разоружения и нераспространения (A/C.1/77/L.15). Надеемся, что эти проекты получат поддержку со стороны всех делегаций.

Наконец, мы рады, что трое мексиканцев участвуют в инициативе #Leaders4Tomorrow, и надеемся, что эти вдохновляющие проекты охватят гораздо больше молодых людей, с тем чтобы они могли распространять информацию о важности разоружения в своих сообществах.

Г-н Тун (Мьянма) (*говорит по-английски*): Мьянма присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Ассоциации государств Юго-Восточной Азии (см. A/C.1/77/PV.18).

Нет никаких сомнений в том, что процесс развития в различных сферах нашей жизни зашел бы в тупик без информационно-коммуникационных технологий (ИКТ). Экспоненциальный рост ИКТ позволил нам воспользоваться беспрецедентными возможностями и социально-экономическим развитием, принося пользу всем во всем мире, включая даже тех, кто не имеет доступа к ИКТ или имеет весьма ограниченное представление о них.

В то же время киберпространство становится все более уязвимым перед лицом злоумышленников и негосударственных субъектов, чей комплекс возможностей растет такими же темпами, как и сами ИКТ. Всепроникающие киберугрозы, которые являются трансграничными, неуловимыми и развивающимися, имеют серьезные последствия для международного мира и безопасности и нашей повседневной жизни. Киберпространство уже стало площадкой для ведения войны, чему мы были свидетелями в течение последних двух десятилетий.

Поэтому всем нам необходимо использовать международные нормы и стандарты в качестве руководства для минимизации киберугроз и максимального использования преимуществ ИКТ. В этой связи Мьянма хотела бы подчеркнуть главную роль Организации Объединенных Наций и многосторонних усилий государств-членов в решении проблем кибербезопасности и в создании безопасной и стабильной обстановки в области безопасности. Соответственно, Мьянма вновь заявляет о своей поддержке деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий на период 2021–2025 годов и приветствует консенсусное принятие в июле 2022 года первого ежегодного доклада о проделанной работе.

Мы призываем все стороны сотрудничать добросовестно и с максимальной гибкостью в целях достижения дальнейшего прогресса в рамках РГОС. Мы также глубоко ценим важную работу Группы правительственных экспертов (ГПЭ), которая внесла ценный вклад в эту область.

Мы осуждаем использование ИКТ в качестве оружия для подавления основных прав и свободы слова. В нашей стране, Мьянме, обеспечить свободный, безопасный и открытый доступ к Интернету больше не представляется возможным, поскольку военная хунта осуществляет цифровую диктатуру. Прослушивание и совершение кибератак против

собственного народа, включая граждан Мьянмы, проживающих за рубежом, стали новой нормой. Хунта активно следит за деятельностью государственных служащих в социальных сетях. Хунта также пытается принять драконовский закон о кибербезопасности, который специально разработан только для того, чтобы устранить любое инакомыслие или выражение мнения против военной хунты. Мы настоятельно призываем международное сообщество и индустрию высоких технологий помочь положить конец злонамеренному использованию ИКТ хунтой, цепляющейся за власть.

Пользуясь случаем, я хотел бы обратить Ваше внимание, г-н Председатель, на недавние чудовищные преступления, совершенные фашистским военным режимом против этнических меньшинств в штате Качин. Вечером 23 октября военные истребители террористов нанесли авиаудары и совершили нападение во время музыкального концерта, проводившегося 9-й бригадой Армии независимости Качина в А Нанг Па, штат Качин, Мьянма, по случаю шестьдесят второй годовщины создания Организации независимости Качина, которая приходится на 25 октября. По имеющимся данным, в результате этого налета погибло около ста человек, в том числе артисты, женщины и дети, и еще большее число людей получило ранения.

Речь явно идет о преступлении против человечности и военном преступлении. Это явно представляет собой преступление против человечности и военное преступление. И это не единичный случай. За последние 20 месяцев террористы нанесли более 250 авиаударов по гражданскому населению по всей стране, в том числе по районам проживания этнических меньшинств, и совершили несколько массовых убийств. Пока военные сохраняют доступ к оружию и технологиям, они будут продолжать совершать жестокие и бесчеловечные злодеяния против людей, включая детей. Я хочу попросить те государства-члены, которые продают смертоносное оружие и технологии военным, немедленно прекратить это. Мы считаем, что это спасет жизни людей в Мьянме.

В заключение мы подтверждаем нашу приверженность построению безопасного и мирного киберпространства, где возможно предотвращать вредоносную деятельность, подрывающую международный мир и безопасность, и содействовать применению международного права и реализации основных свобод и прав человека.

Г-н Балуджи (Исламская Республика Иран) (*говорит по-английски*): Наша делегация присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран (см. A/C.1/77/PV.18).

Исламская Республика Иран вновь подтверждает свою последовательную позицию, согласно которой киберпространство и информационно-коммуникационная среда являются общим наследием человечества, и должны использоваться исключительно в мирных целях, а государства обязаны предпринимать совместные действия, полностью соблюдая применимые нормы международного права. С учетом этого Иран активно участвует в соответствующих межправительственных переговорных процессах под эгидой Организации Объединенных Наций в интересах обеспечения прав для всех и установления надлежащих обязанностей для всех. После принятия первого ежегодного доклада Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и сборника заявлений государств-членов с разъяснением позиций, который включает заявление Ирана, мы считаем, что дальнейший прогресс и повышение эффективности работы Группы будут зависеть от следующего.

Во-первых, в ходе будущих обсуждений необходимо рассмотреть неисчерпывающий перечень разнообразных предложений по разработке правил, норм и принципов ответственного поведения государств, представленный в резюме Председателя, которое содержится в докладе РГОС за 2021 год, и принять соответствующие решения.

Во-вторых, согласно мандату РГОС, необходимо наладить регулярный институциональный диалог под эгидой Организации Объединенных Наций при широком участии государств. В этой связи ко всем национальным инициативам следует относиться одинаково, принимая во внимание проблемы и интересы всех государств.

В-третьих, мы призываем государства продолжать принимать конструктивное участие

в переговорах в ходе дальнейшей деятельности Группы, в том числе в межсессионный период.

В-четвертых, мы призываем РГОС создать тематические подгруппы с опорой на ее мандат для выполнения поставленных перед ней задач и содействия обмену мнениями между государствами, а также составления последующих докладов путем проведения переговоров на основе текста. С другой стороны, учитывая положение дел на местах, важно отметить, что такие страны, как Соединенные Штаты, не только начали осуществлять милитаризацию киберпространства, но и их вооруженные силы стали совершать многочисленные кибератаки. Израильский режим также осуществил большое число кибератак на Иран.

Наша страна уже давно является основной целью и главной жертвой кибератак, которым подвергаются жизненно важные объекты ее инфраструктуры и которые нарушают функционирование общественных служб и государственных ведомств. В качестве нескольких примеров таких кибератак можно привести атаки с использованием компьютерных червей Stuxnet на мирные ядерные объекты Ирана, и недавние атаки на объекты промышленной инфраструктуры, включая сталелитейную и нефтехимическую промышленность, автозаправочные станции и муниципальные системы коммунального обслуживания. Израильский режим неоднократно признавал свою причастность к этим международно-противоправным деяниям с использованием ИКТ-среды, которые пользуются неизменной поддержкой Соединенных Штатов. Мы осуждаем все эти нападения и настоятельно призываем международное сообщество привлечь виновных в совершении этих нападений к ответственности.

К сожалению, недавно против Ирана были выдвинуты ложные и необоснованные обвинения в якобы имевшей место кибератаке. Мы отвергаем любые ложные заявления, основанные на вымыслах и неверных предположениях, выдвигаемых против нас в политических целях. Учитывая характер и технические особенности киберпространства и проблемы установления ответственности в ИКТ-среде, Иран предупреждает о негативных последствиях возложения ответственности на государства на основе фальсификаций и подделок. Если бы Соединенное Королевство действительно было обеспокоено возможным негативным влиянием на безопасность, экономические, социальные и гуманитарные условия, оно бы воздержалось от поспешных заявлений, которые могут привести к распространению ложной информации.

В заключение следует отметить, что, по мнению Исламской Республики Иран, наиболее эффективный способ обеспечить безопасность и устойчивость ИКТ-среды заключается в дальнейшей разработке международных правовых норм и правил, касающихся предотвращения использования ИКТ и киберпространства в злонамеренных целях, а также мирного урегулирования споров, в рамках юридически обязывающего документа.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово наблюдателю от Святого Престола.

Архиепископ Качча (Святой Престол) (*говорит по-английски*): Папа Франциск в своей энциклике Fratelli Tutti («Все братья») написал, что постоянно крепнущие взаимосвязи и растущее число коммуникаций в современном мире заставляет нас ясно осознать единство и общую судьбу народов. Однако этому единству угрожает растущее злонамеренное использование информационно-коммуникационных технологий (ИКТ) как государственными, так и негосударственными субъектами. Такое злонамеренное использование ИКТ отчасти объясняется тем, что наш огромный технологический рост не сопровождался воспитанием у людей чувства ответственности, понимания ценностей и повышения сознательности. В этой связи Святой Престол приветствует созыв Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, которая располагает прекрасными возможностями устранить этот дисбаланс. Наша делегация с большим интересом следила за этими встречами и в дальнейшем будет активно участвовать в соответствующих обсуждениях. Сеть взаимосвязанных систем, составляющих киберпространство, представляет собой общую среду, для продолжения функционирования которой всем нам необходимо перейти от парадигмы конкуренции к парадигме сотрудничества. Для осуществления таких изменений необходим набор общих принципов. Учитывая это, позвольте нашей делегации поделиться несколькими соображениями.

Во-первых, в ходе своей деятельности в киберпространстве государства должны уважать достоинство, присущее каждой человеческой личности. С этой целью государства должны поощрять и защищать свободу выражения мнений каждого человека в Интернете. Такая свобода, необходимая людям для поиска ими истины, также имеет свои границы, определяемые моральным порядком и общими интересами. Для защиты человеческого достоинства в киберпространстве государства также должны уважать право на неприкосновенность частной жизни, ограждая своих граждан от интрузивного наблюдения и позволяя им защищать персональные данные от несанкционированного доступа.

Во-вторых, государства должны обеспечить защиту тех людей, которые оказались в наиболее уязвимом положении, с тем чтобы не допустить причинения им вреда. Это означает не только защиту собственной критической инфраструктуры, такой как больницы, системы водоснабжения, электростанции и объекты, содержащие опасные силы, но и отказ от любых действий, с помощью которых можно намеренно нанести ущерб критическим объектам инфраструктуры другого государства.

В-третьих, в ходе своей деятельности в киберпространстве государства должны руководствоваться принципами справедливости, а это означает, что государства, имеющие такую возможность, должны эффективно содействовать усилиям по преодолению цифрового разрыва. Такой разрыв ведет не только к неравномерному развитию человеческого потенциала, но и к появлению уязвимости в сфере кибертехнологий, что представляет угрозу для всех стран. Святой Престол призывает предпринимать — в целях устранения этих факторов уязвимости — усилия по наращиванию потенциала для улучшения положения тех государств, которые не пользуются в равной мере благами цифровой революции. Такая деятельность по наращиванию потенциала должна и далее носить политически нейтральный и необусловленный характер.

Человечество вступило в новую эру, и достигнутый технический прогресс поставил нас перед выбором, который сопряжен как с большими перспективами, так и с существенными рисками. Для того чтобы новые достижения в сфере ИКТ способствовали комплексному развитию человеческого потенциала, мы должны непрерывно думать о том, как применять новые инструменты таким образом, чтобы при этом сохранить человеческое достоинство. Наша делегация надеется, что такие усилия, а также дальнейшая разработка Рабочей группой открытого состава кодекса ответственного поведения государств позволят нам насладиться плодами этого успеха и воодушевиться теми колоссальными возможностями, которые они продолжают открывать перед нами.

Председатель (*говорит по-английски*): Комитет заслушал последнего оратора по блоку вопросов «Другие меры в области разоружения и международная безопасность».

Сейчас я предоставляю слово тем представителям, которые попросили слова в порядке осуществления права на ответ. В этой связи я хотел бы напомнить делегациям о необходимости ограничивать продолжительность выступлений и попросить их об этом не забывать.

Г-н Шин (Российская Федерация): Я хотел бы воспользоваться правом на ответ, поскольку в некоторых выступлениях, которые здесь прозвучали, мы услышали враждебную риторику.

Вы знаете, должен признаться, что меня несколько смущают выступления представителей Соединенных Штатов, Европейского союза, Соединенного Королевства, Австралии и ряда других государств, которые заявляют, что они поддерживают Рабочую группу открытого состава (РГОС) и говорят о положительных сторонах этого механизма. Я точно помню, что именно эти страны голосовали против создания РГОС — причем не один, а два раза. Означает ли это, что сейчас они говорят неправду? Чему мы должны верить — их словам или их действиям? Сейчас они напористо продвигают резолюцию по программе действий и говорят, что это делается в интересах РГОС. Я хотел бы уточнить, как именно? Чем больше мы слышим о программе действий, тем больше вопросов возникает.

Мы не понимаем, почему государствам — членам Организации Объединенных Наций предлагается сначала создать этот формат и лишь потом решать, чем и как он будет заниматься. Включая механизм принятия решений, а также финансирования этого процесса. Нам фактически предлагают поставить телегу впереди лошади. Почему бы сначала не обсудить данную инициативу в рамках

РГОС — в полном соответствии с ее мандатом и с ранее достигнутыми консенсусными договоренностями? Мы считаем, что срок в три года — до 2025 года — более чем достаточен для того, чтобы сообща выработать понимание о целесообразности создания такого формата, его возможной сфере охвата и модальностях его функционирования.

Честно говоря, действия Франции и ее партнеров выглядят как попытка создать механизм, который будет удобен только некоторым — преимущественно западным — государствам. В нем они будут принимать решения, а затем навязывать их широкому большинству. В таком виде данная инициатива выглядит, если честно, как манифест киберколониализма. Решение об участии негосударственных субъектов в РГОС является суверенным правом государств, вы все об этом знаете.

Заявки многих российских организаций также были отклонены без объяснения причин. Прежде чем говорить о допуске НПО к межгосударственному переговорному процессу, на наш взгляд, следовало бы обеспечить беспрепятственный доступ государств и их национальных делегаций к площадке Организации Объединенных Наций. В этой связи мы выражаем решительный протест властям Соединенных Штатов, которые, используя «визовое оружие», на системной основе нарушают возложенные на них обязательства страны, где располагаются Центральные учреждения Организации Объединенных Наций.

Дальше, мы продолжаем слышать абсолютно бездоказательные обвинения России в кибератаках, в том числе в контексте специальной военной операции на Украине. Вместо того чтобы использовать установленные каналы связи компетентных ведомств, наши коллеги на Западе взяли за правило бездоказательно клеймить неугодные им государства, отвлекая внимание мировой общественности от собственных действий. Цель их риторики — прикрыть беспрецедентную по масштабам кибератаку, развернутую против России и других государств. Есть многочисленные документальные свидетельства, подтверждающие осуществление системной агрессивной деятельности в информпространстве спецслужбами Соединенных Штатов и стран НАТО. Вспомните хотя бы откровения Эдварда Сноудена. А чего стоит недавний доклад, опубликованный нашими китайскими коллегами относительно кибератак против Северо-Западного политехнического университета, произведенных с прямым участием Агентства национальной безопасности Соединенных Штатов. Альянс не скрывает усилий по отработке методов ведения кибервойны, проводит учения, приглашает на них представителей не являющейся членом блока Украины. Глава киберкомандования Соединенных Штатов Пол Накасоне публично признает факт проведения наступательных кибероперации против России, в том числе — и прежде всего — руками созданной ими же, американцами, IT-армии Украины.

С начала этого года число атак на российские сетевые ресурсы возросло более чем в четыре раза по сравнению с аналогичным периодом прошлого года. Большинство нападений исходит с территории Соединенных Штатов и стран Евросоюза. Масштабы кибератаки подтверждают, что ведется она скоординированно властями западных стран с привлечением хакерского сообщества и частных компаний. К сожалению, временной регламент не позволяет мне в полной мере осветить данную тему. Важно понимать, что эскалация напряженности в информпространстве не отвечает интересам широкого международного сообщества, которое заинтересовано в предотвращении конфликтов и использовании ИКТ в мирных целях на благо развития.

Г-н Ким Сон (Корейская Народно-Демократическая Республика) (*говорит по-английски*): Наша делегация вынуждена взять слово в порядке осуществления права на ответ в связи с безрассудным замечанием, сделанным представителем Соединенного Королевства.

Мы категорически отвергаем необоснованные обвинения, выдвинутые Соединенным Королевством против Корейской Народно-Демократической Республики. Нам хорошо известно о пагубной привычке Соединенного Королевства безрассудно обвинять других без каких-либо конкретных доказательств. В то же время Соединенное Королевство принимает активное участие в различного рода злонамеренных действиях в киберпространстве посредством таких инициатив, как «Пять глаз», стремясь осуществлять вмешательство во внутренние дела суверенных государств. Представление Соединенным Королевством такого заявления напоминает ситуацию, когда виновная сторона первой подает иск.

Мы и не ожидаем ничего иного от Соединенного Королевства, которое слепо следует враждебной политике Соединенных Штатов в отношении Корейской Народно-Демократической Республики, направленной на демонизацию нашей страны на международной арене и принуждение к осуществлению так называемого международного сотрудничества в целях оказания давления на Корейскую Народно-Демократическую Республику. Голословное обвинение, выдвинутое Соединенным Королевством, наглядно свидетельствует о его крайней предвзятости и враждебности по отношению к Корейской Народно-Демократической Республике. Мы настоятельно призываем Соединенное Королевство опомниться и задуматься о своем безрассудном и возмутительном поведении.

Г-н Ли Сун (Китай) (*говорит по-китайски*): Китай принимает к сведению безосновательные обвинения, высказанные представителем Соединенного Королевства в отношении активности Китая в киберпространстве, и решительно выступает против этих обвинений.

Китай твердо привержен обеспечению кибербезопасности. Наша страна является также одной из главных жертв кибератак. Правительство Китая решительно выступает против всех форм кибератак и ведет борьбу с ними в соответствии с законом, что наглядно свидетельствует о нашем ответственном поведении в сфере кибербезопасности.

Китай хотел бы подчеркнуть, что обеспечение кибербезопасности — это общая задача всех стран. Все страны должны на основе взаимного уважения, равенства и взаимной выгоды продолжать диалог и сотрудничество, чтобы совместно реагировать на угрозы кибербезопасности. Мы настоятельно призываем соответствующие страны прекратить клевету и беспочвенные обвинения в адрес Китая по вопросу кибератак и действительно занять ответственную позицию, работая вместе со всеми сторонами для сохранения мира и безопасности в киберпространстве.

Г-н Бургель (Израиль) (*говорит по-английски*): Я вынужден взять слово в связи с упоминанием нашей страны представителем Исламской Республики Иран. Израиль отвергает эти ложные обвинения. Судя по поведению Ирана в киберпространстве, особенно в последнее время, когда была совершена опасная кибератака на инфраструктуру Албании, его высказывания по меньшей мере абсурдны.

В связи с этим позвольте мне также осудить две недавние кибератаки на операции Организации Объединенных Наций по поддержанию мира, обе из которых были осуществлены иранским режимом и его приспешниками. Как и во многих других вопросах, обсуждаемых Комитетом, Иран систематически действует вопреки интересам международного сообщества, провоцируя крах форумов по контролю над вооружениями. Подобно тому, как Иран спонсирует и поддерживает террористические группы, чтобы посеять страх среди государств всего региона, он пытается использовать вредоносные инструменты в сфере информационно-коммуникационных технологий, а также для того, чтобы посеять страх и разрушение среди государств всего мира.

Г-жа Макинтайр (Франция) (*говорит по-французски*): Я хотела бы воспользоваться правом нашей страны на ответ в связи с замечаниями делегации Российской Федерации по представленному нашей страной проекту резолюции A/C.1/77/L.73 о программе действий по поощрению ответственному поведению государств при использовании информационно-коммуникационных технологий в контексте международной безопасности.

Как известно членам Совета, Франция предложила всем государствам — членам Организации Объединенных Наций на прозрачной и открытой основе проект резолюции, направленный на создание программы действий по наращиванию потенциала в вопросах, касающимся киберпространства. Проект резолюции открыто и подробно обсуждался в ходе четырех раундов открытых консультаций, проведенных здесь, в Нью-Йорке, и ранее в Женеве. Проект резолюции был значительно улучшен в стремлении учесть многочисленные предложения, внесенные делегациями, за что мы им весьма признательны.

Проект резолюции основан на консультациях, проведенных ранее для создания Программы действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней. Я хотела бы напомнить членам Совета о процессе, соблюдавшемся в этой связи, который включал сначала доклад Генерального секретаря, а затем два года консультаций, направленных на учет предложений всех государств-членов в отношении

содержания Программы действий. Наконец, Программа действий была принята на международной конференции, состоявшейся по итогам процесса. Именно такой последовательности мы предлагаем придерживаться при рассмотрении проекта резолюции A/C.1/77/L.73, возложив на Генерального секретаря задачу представить в следующем году доклад с указанием условий и содержания будущей программы действий при полном соблюдении прерогатив Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021–2025, которая, разумеется, также должна будет обсудить условия программы действий, прежде чем государства-члены смогут приступить к ее принятию, если они того пожелают.

Поэтому я хотела бы напомнить, что применяемый в ходе нашей работы подход является открытым, транспарентным и инклюзивным и направлен на полное соблюдение процесса, согласованного государствами-членами, в том числе в рамках РГОС. Мы будем продолжать придерживаться этого транспарентного и инклюзивного подхода до завершения обсуждений.

Г-н Балуджи (Исламская Республика Иран) (*говорит по-английски*): Я вынужден взять слово, чтобы отвергнуть обвинения, выдвинутые против нашей страны представителем Израиля.

Нас не удивляет эта ложь, распространяемая представителем режима, поскольку он не уважает международное право. Он постоянно инициирует кибератаки против многих секторов Ирана, от мирных ядерных объектов до общественных служб, таких как служба экстренной помощи. Нам хорошо известно о деспотичном и апартеидном характере израильского режима, его мрачном послужном списке в отношении прав человека и его игнорировании международных призывов присоединиться, среди прочего, к Договору о нераспространении ядерного оружия, Конвенции по химическому оружию и Конвенции по биологическому оружию.

Израиль нарушил 29 резолюций Совета Безопасности, которые имеют обязательную юридическую силу для государств-членов в соответствии со статьей 25 Устава Организации Объединенных Наций, включая резолюции 54 (1948), 111 (1956), 233 (1967), 234 (1967), 236 (1967), 248 (1968), 250 (1968), 252 (1968), 256 (1968), 262 (1968), 267 (1969), 270 (1969), 280 (1970), 285 (1970), 298 (1971), 313 (1972), 316 (1972), 468 (1980), 476 (1980) и — не в последнюю очередь — резолюцию 2231 (2015), подорвать которую он стремится при любом удобном случае и прилагает для этого все возможные усилия. Такой режим не имеет морального основания говорить об уважении норм международного права и приверженности их соблюдению.

Когда речь идет о кибербезопасности, ситуация еще хуже. Сказанное нами не является голословным утверждением, поскольку все международные наблюдатели подтвердили безответственные действия Израиля, которые мы решительно осуждаем.

Председатель (*говорит по-английски*): Мы заслушали последнего оратора, выступившего в порядке осуществления права на ответ.

У нас есть немного свободного времени, поэтому давайте постараемся использовать эти несколько минут с максимальной пользой. Позвольте мне обратиться к блоку вопросов «Региональное разоружение и безопасность». У нас длинный список докладчиков по этому блоку вопросов, поэтому я призываю делегации к всестороннему содействию.

Г-жа Кристанти (Индонезия) (*говорит по-английски*): Я имею честь выступить от имени Движения неприсоединившихся стран (ДНП).

ДНП вновь заявляет о своей глубокой обеспокоенности по поводу все более широкого применения одностороннего подхода и в этой связи подчеркивает, что многосторонность и согласование решений на многосторонней основе в соответствии с Уставом Организации Объединенных Наций обеспечивают единственный надежный метод решения вопросов разоружения и международной безопасности. ДНП также подчеркивает свою принципиальную позицию относительно отказа от применения силы или угрозы ее применения против территориальной целостности любого государства.

Государства-члены ДНП, являющиеся участниками Договора о нераспространении ядерного оружия, глубоко обеспокоены стратегическими оборонными доктринами государств, обладающих ядерным оружием, и некоторых государств, не обладающих ядерным оружием, которые подписываются на расширенные гарантии ядерной безопасности, предоставляемые государствами, обладающими ядерным оружием. Они не только

обосновывают применение и угрозу применения ядерного оружия, но и поддерживают неоправданные концепции международной безопасности, основанные на поощрении и расширении военных союзов и политике ядерного сдерживания. Поэтому ДНП настоятельно призывает соответствующие государства полностью исключить применение или угрозу применения ядерного оружия из своих военных доктрин и доктрин безопасности.

ДНП вновь заявляет о своей полной поддержке создания на Ближнем Востоке зоны, свободной от ядерного оружия и всех других видов оружия массового уничтожения. В качестве приоритетного шага в этом направлении ДНП подтверждает необходимость скорейшего создания зоны, свободной от ядерного оружия, на Ближнем Востоке в соответствии с резолюцией 487 (1981) Совета Безопасности и пунктом 14 резолюции 687 (1991) Совета Безопасности, а также соответствующими резолюциями Генеральной Ассамблеи. ДНП призывает все заинтересованные стороны безотлагательно принять практические меры в целях осуществления предложения, выдвинутого Ираном в 1974 году, о создании такой зоны.

Государства — члены ДНП, являющиеся участниками ДНЯО, вновь выражают глубокое разочарование в связи с тем, что принятый в 2010 году План действий по созданию на Ближнем Востоке зоны, свободной от ядерного оружия и всех других видов оружия массового уничтожения, так и не был осуществлен. Они решительно отвергают утверждения о наличии препятствий, которые якобы стоят на пути осуществления Плана действий 2010 года по Ближнему Востоку и резолюции 1995 года по Ближнему Востоку. ДНП вновь подчеркивает, что на государствах — соавторах резолюции 1995 года по Ближнему Востоку лежит особая ответственность за ее осуществление. ДНП выражает обеспокоенность в связи с тем, что постоянное невыполнение резолюции 1995 года, вопреки решениям соответствующих конференций по рассмотрению действия ДНЯО, подрывает эффективность и авторитет ДНЯО и нарушает хрупкий баланс между его тремя элементами.

В этой связи ДНП с удовлетворением отмечает проведение в соответствии с решением 73/546 первой сессии Конференции по вопросу о создании на Ближнем Востоке зоны, свободной от ядерного оружия и других видов оружия массового уничтожения, под председательством Иорданского Хашимитского Королевства, а также принятие участниками Конференции политической декларации. ДНП приветствует также проведение второй сессии Конференции под председательством Государства Кувейт и ее итоги, включая, в частности, принятие правил процедуры и создание неофициального рабочего комитета. Кроме того, ДНП с нетерпением ждет проведения третьей сессии Конференции и по-прежнему призывает все без исключения государства региона принимать активное участие в работе этой конференции и вести в духе доброй воли и завершить переговоры о заключения юридически обязывающего договора о создании такой зоны.

По мнению ДНП, создание зон, свободных от ядерного оружия, в рамках договоров Тлателолко и Раротонга, Бангкокского и Пелиндабского договоров и Договора о зоне, свободной от ядерного оружия, в Центральной Азии, а также придание Монголии статуса государства, свободного от ядерного оружия, — это важные, конструктивные шаги, способствующие укреплению режима глобального ядерного разоружения и ядерного нераспространения. Что касается зон, свободных от ядерного оружия, то следует отметить необходимость предоставления государствами, обладающими ядерным оружием, всем государствам соответствующей зоны безусловных гарантий против применения или угрозы применения ядерного оружия при любых обстоятельствах. ДНП призывает все государства, обладающие ядерным оружием, ратифицировать соответствующие протоколы ко всем договорам о создании зон, свободных от ядерного оружия, отозвать любые оговорки или заявления о толковании, противоречащие целям и задачам этих документов, и уважать безъядерный статус этих зон. ДНП настоятельно призывает государства добровольно заключить соглашения между государствами соответствующего региона о создании в тех регионах, где их еще нет, новых зон, свободных от ядерного оружия.

В заключение ДНП хотело бы подчеркнуть большое значение прилагаемых Организацией Объединенных Наций на региональном уровне усилий по укреплению стабильности и безопасности ее государств-членов, чему могли бы существенным образом способствовать сохранение и активизация деятельности всех трех региональных центров по вопросам мира и разоружения.

Г-н Фуллер (Белиз) (*говорит по-английски*): Я имею честь выступать в ходе сегодняшнего обсуждения блока вопросов, касающихся регионального разоружения и безопасности, от имени 14 государств — членов Карибского сообщества (КАРИКОМ).

Государства — члены КАРИКОМ на региональном и субрегиональном уровнях применяют коллективный, скоординированный и практический подход в борьбе с возникающими в регионе различными угрозами безопасности. КАРИКОМ твердо намерено играть свою роль в глобальных усилиях, направленных на поддержание нашей коллективной безопасности на основе выполнения наших международных обязательств. В дополнение к нашей международной деятельности прилагаются серьезные усилия по региональному разоружению.

Безопасность входит в число неотъемлемых компонентов нашей региональной интеграции. КАРИКОМ создал региональную институциональную структуру для поддержки сотрудничества в рамках региона, в том числе Исполнительное агентство КАРИКОМ по борьбе с преступностью и обеспечению безопасности (КАРИКОМ ИМПАКС) под надзором Совета министров по вопросам национальной безопасности и охраны правопорядка, а также другие вспомогательные региональные учреждения, в том числе региональную систему обеспечения безопасности.

Незаконный транзит огнестрельного оружия и боеприпасов через страны региона остается серьезной проблемой и был признан угрозой первого уровня в соответствии со стратегией КАРИКОМ по обеспечению безопасности. Семь из десяти убийств в регионе совершаются с применением стрелкового оружия и легких вооружений. По оценкам, только в Гаити оборот нелегального огнестрельного оружия достигает более полумиллиона единиц. Нелегальное огнестрельное оружие играет ключевую роль во всех аспектах транснациональной организованной преступности и представляет собой инструмент поддержки преступного и девиантного поведения. Поэтому оборот этого оружия оказывает значительное воздействие на социально-экономическую обстановку и приводит к человеческим жертвам.

Ни одно государство — член КАРИКОМ не входит в число производителей или крупных импортеров огнестрельного оружия. Пресечение и предотвращение незаконного транзита огнестрельного оружия и боеприпасов через наши границы входит в число первостепенных задач для региона. Несмотря на наличие многочисленных инициатив и механизмов, нацеленных на борьбу с проблемой вооруженного насилия, в регионе сохраняется высокий уровень преступлений, совершенных с применением огнестрельного оружия.

В Стратегии КАРИКОМ по борьбе с преступностью и обеспечению безопасности отмечается, что, хотя на уровне региона уважается право государств принимать либеральные законы в отношении доступа к оружию, отрицательные последствия такой политики выходят за пределы государственных границ. Они имеют очень серьезные последствия для других стран, в том числе государств — членов КАРИКОМ. Поэтому предотвращение незаконного оборота оружия относится к обязанностям, которые должны выполнять не только государства КАРИКОМ, но и страны, из которых поступает это оружие. Во время сорок третьего очередного заседания, состоявшегося 3 июля 2022 года в Суринаме, главы правительств наших стран выразили также особую обеспокоенность в связи с притоком оружия из других стран за пределами региона.

В 2020 году главы стран КАРИКОМ приняли «дорожную карту» по реализации Поэтапной программы первоочередных и последовательных действий Карибского бассейна по борьбе с незаконным распространением огнестрельного оружия и боеприпасов в странах Карибского бассейна на период до 2030 года (Карибская поэтапная программа действий по огнестрельному оружию). Исполнительное агентство КАРИКОМ ИМПАКС принимает ряд конкретных мер по реализации этой «дорожной карты», включая оказание технической и консультативной помощи национальным органам, укрепление потенциала и подготовка персонала, обмен информацией и разведданными, пограничный и таможенный контроль, оказание поддержки по вопросам законодательства путем разработки типовых законов, предоставление оперативных средств и разработка международных, региональных и национальных нормативных рамок, подходов и стандартов.

Хотим отметить работу ИМПАКС в регионе при поддержке правительств и организаций-партнеров, в том числе подготовку совместного с организацией «Смол армз сервей» всестороннего, основанного на фактах исследования по вопросу о незаконных поставках оружия в регион Карибского

бассейна и обороте этого оружия внутри региона, а также о связанных с такими поставками социально-экономических издержках; создание Группы КАРИКОМ по сбору оперативной информации об используемом для совершения преступлений оружии с целью помочь государствам — членам КАРИКОМ в расследовании преступлений, связанных с огнестрельным оружием, и осуществлении судебного преследования за их совершение, причем Группа будет получать поддержку от таких ведомств правительства Соединенных Штатов, как Бюро по контролю за оборотом алкогольной и табачной продукции, огнестрельного оружия и взрывчатых веществ, Отдел расследований Министерства национальной безопасности и Бюро таможенного и пограничного контроля; оказание помощи государствам — членам КАРИКОМ в вопросах управления запасами огнестрельного оружия и боеприпасов; налаживание в целях оказания помощи в борьбе с преступлениями, совершаемыми с применением огнестрельного оружия, важнейших партнерских отношений с многочисленными международными учреждениями, включая Интерпол, Всемирную таможенную организацию (ВТамО), Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), Региональный центр Организации Объединенных Наций по вопросам мира, разоружения и развития в Латинской Америке и Карибском бассейне, «Смол армз сервей» и Консультативную группу по вопросам разминирования; взаимодействие с Интерполом и проведение в партнерстве с этой организацией совместных операций по борьбе с огнестрельным оружием во всем Карибском бассейне в период с 24 по 30 сентября 2022 года, в результате которых во всем регионе было изъято приблизительно 320 единиц оружия, 3300 патронов и рекордные партии наркотиков; организацию подготовки и содействие укреплению потенциала правоохранительных органов и органов безопасности, в том числе таможенных служб, в партнерстве с ВТамО; содействие государствам-членам в использовании Региональной объединенной пулегильзотеки; совершенствование и расширение использования в странах КАРИКОМ Системы предварительного сбора информации о пассажирах, которая представляет собой единственную в мире многостороннюю систему, позволяющую государствам эффективно проверять представляющих интерес лиц на борту самолета или судна в каждом порту прибытия в одно из государств-участников и таким образом гарантировано охватить все государства — члены КАРИКОМ и заинтересованные третьи государства; создание региональной системы предварительных уведомлений о передвижении грузов для оказания помощи ее участникам из числа государств — членов КАРИКОМ в повышении эффективности слежения за грузами; и разработку типового закона о Договоре о торговле оружием.

Региональный центр Организации Объединенных Наций по вопросам мира, разоружения и развития в Латинской Америке и Карибском бассейне остается одним из важных партнеров КАРИКОМ. Региональный центр вместе с ИМПАКС отвечают за реализацию Карибской поэтапной программы действий по огнестрельному оружию. Региональный центр Организации Объединенных Наций по вопросам мира, разоружения и развития в Латинской Америке и Карибском бассейне провел в регионе 54 мероприятия, способствующих осуществлению Поэтапной программы действий, в которых приняли участие 600 должностных лиц, в том числе 220 женщин. Центр оказал также помощь в разработке национальных планов по реализации Поэтапной программы действий, а также в мониторинге и оценке хода ее выполнения. На сегодняшний день 10 государств Карибского бассейна разработали свои национальные планы действий.

В регионе также был проведен ряд вебинаров и учебных занятий по различным вопросам, в том числе по темам передовой международной практики для следователей по уголовным делам, криминалистической экспертизы огнестрельного оружия, изготовленного кустарным способом, усовершенствования методов расследования инцидентов с применением огнестрельного оружия и проведения баллистической экспертизы.

КАРИКОМ поддерживает призыв Генерального секретаря к государствам-членам и другим партнерам об оказании Центру финансовой поддержки и помощи в натуральном выражении.

КАРИКОМ рассматривает Договор о торговле оружием (ДТО), Программу действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней, Международные документы по отслеживанию (МДО) и другие применимые резолюции Организации Объединенных Наций по стрелковому оружию и легким вооружениям в качестве важнейших инструментов в деле

предотвращения, контроля и искоренения незаконной торговли стрелковым оружием и легкими вооружениями и соответствующими боеприпасами во всех ее аспектах. КАРИКОМ призывает все государства в полной мере выполнять положения этих документов.

Одной из основных проблем, с которыми сталкиваются малые островные развивающиеся государства при реализации документов по стрелковому оружию и легким вооружениям, является отсутствие достаточных ресурсов и технического потенциала. Для полного и эффективного осуществления ДТО, Программы действий и МДО необходимо рассматривать международное сотрудничество и помощь как основанное на принципе национальной ответственности партнерство между развивающимися государствами, развитыми государствами и государствами-донорами. Поэтому мы подчеркиваем важность удовлетворения просьб развивающихся стран об оказании помощи на безусловной и недискриминационной основе в целях укрепления их потенциала для эффективного выполнения положений международных документов по разоружению.

Одной из основных проблем, с которыми сталкиваются развивающиеся государства, в том числе КАРИКОМ, при реализации ДТО, Программы действий и МДО, связана с отсутствием процесса передачи технологий и обмена опытом в сфере их реализации. Для усиления контроля над стрелковым оружием и легкими вооружениями и сокращения разрыва в уровне развития цифровых технологий между развитыми и развивающимися государствами крайне важно наращивать работу по устранению такого дисбаланса.

Признавая, что в настоящее время кибербезопасность является неотъемлемой частью региональной безопасности и что, если не принять срочных мер, проблемы в этой сфере могут серьезно затруднить социально-экономическое развитие наших Карибских государств, страны региона разработали План действий КАРИКОМ по обеспечению кибербезопасности и борьбе с киберпреступностью. План призван восполнить пробелы в плане кибербезопасности в каждой из стран-участниц региона Карибского бассейна и содействовать в разработке практического и унифицированного набора процедур, систем и экспертных ресурсов в области кибербезопасности, на которые каждая страна региона Карибского бассейна сможет опираться в краткосрочной и среднесрочной перспективе. В нем предусматривается также наращивание надлежащего потенциала и укрепление инфраструктуры с целью обеспечить своевременное выявление, расследование и судебное преследование киберпреступлений, а также изучение их возможных связей с другими формами преступной деятельности.

Хотя регион располагает ограниченными ресурсами для решения разнообразных сложных проблем в плане безопасности, обусловленных проницаемыми границами, протяженными морскими и сухопутными границами и ролью региона в качестве зоны транзита, мы наладили ряд партнерских отношений для содействия разоружению на региональном уровне посредством ряда практических мер.

Председатель (*говорит по-английски*): Мы исчерпали время, отведенное для этого заседания. Комитет вновь соберется завтра утром на заседание, в ходе которого мы сначала заслушаем выступление председателя Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий. После этого мы продолжим обсуждение в рамках блока вопросов «Разоружение и международная безопасность».

Я хотел бы напомнить членам Комитета, что завтра в конце утреннего заседания Комитет проведет традиционную церемонию вручения свидетельств выпускникам Стипендиальной программы в области разоружения.

Заседание закрывается в 18 ч 05 мин.