Организация Объединенных Наций A/C.1/78/PV.20

Генеральная Ассамблея

Официальные отчеты

Семьдесят восьмая сессия

Первый комитет

20-е пленарное заседание

Вторник, 24 октября 2023 года, 10 ч 00 мин

Нью-Йорк

Председатель г-н Паулаускас . . . . . (Литва)

Заседание открывается в 10 ч 05 мин.

Тематическое обсуждение конкретных вопросов, а также внесение на рассмотрение и само рассмотрение всех проектов резолюций и решений, представленных по пунктам повестки дня, касающимся разоружения и международной безопасности

Председатель (*говорит по-английски*): Сейчас Комитет продолжит тематическое обсуждение блока вопросов «Обычные вооружения». Прежде чем предоставить слово желающим выступить, я хотел бы напомнить всем делегациям о необходимости соблюдать регламент выступлений в ходе тематических обсуждений.

Предоставляю слово наблюдателю от Святого Престола.

Архиепископ Качча (Святой Престол) (*говорит по-английски*): Прежде всего наша делегация напоминает, что все государства — участники Договора о нераспространении ядерного оружия поддерживают обязательство «добросовестно вести переговоры... по договору о всеобщем и полном разоружении». Подтверждение этой цели стало еще более актуальным в условиях стремительного глобального распространения вооружений.

Наибольшую озабоченность вызывает тот факт, что в ходе военных действий на территории Украины широко используется оружие неизбирательного действия, а именно противопехотные мины и кассетные боеприпасы. Святой Престол призывает к немедленному прекращению применения такого оружия, которое подвергает опасности гражданское население, особенно детей, и загрязняет наш общий дом. Как подчеркнул Папа Франциск, нельзя допускать, чтобы озабоченность моральными последствиями ядерной войны затмевала все более острые этические проблемы, возникающие в связи с применением в современных войнах так называемого обычного оружия, которое должно использоваться только в оборонительных целях и не должно быть направлено против гражданских объектов. Действительно, следы разрушений, оставленные обычным оружием, требуют принятия новых мер по ограничению его дальнейшего распространения, повышению прозрачности существующих запасов и обеспечению соответствия любого применения такого оружия нормам международного гуманитарного права.

При достижении таких целей международное сообщество должно всегда ставить во главу угла достоинство, присущее человеческой личности. В этой связи Святой Престол вновь заявляет о своей поддержке Программы действий Организации Объединенных Наций по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней, в которой государства выразили свою решимость «укреплять уважение к жизни», и

В настоящем отчете содержатся тексты выступлений на русском языке и тексты письменных переводов выступлений на других языках. Поправки должны представляться только к текстам выступлений на языке подлинника. Они должны включаться в один из экземпляров отчета и направляться за подписью одного из членов соответствующей делегации на имя начальника Службы стенографических отчетов, кабинет AB-0928 (verbatimrecords@un.org). Отчеты с внесенными в них поправками будут переизданы в электронной форме и размещены в Системе официальной документации Организации Объединенных Наций (http://documents.un.org).

рассчитывает на дальнейшие успехи в реализации программы в рамках четвертой Конференции Организации Объединенных Наций для обзора прогресса, достигнутого в осуществлении Программы действий, которая пройдет в следующем году. Наша делегация также поддерживает призыв Генерального секретаря к переговорам о заключении к 2026 году юридически обязательного документа, запрещающего смертоносные автономные системы вооружений, функционирующие без контроля или надзора со стороны человека. В то же время Святой Престол призывает все государства воздерживаться от разработки такого оружия, которое никогда не может быть субъектом моральной ответственности и нарушает веления общественной совести.

Поскольку вооруженные конфликты все чаще происходят в густонаселенных городах, применение взрывчатых веществ зачастую оказывается неизбирательным, что приводит к неприемлемым жертвам среди некомбатантов и разрушению инфраструктуры, имеющей решающее значение для выживания гражданского населения. В связи с этим Святой Престол высоко оценивает принятие в Дублине в ноябре прошлого года Политической декларации о гуманитарных последствиях применения оружия взрывного действия в населенных пунктах. Святой Престол выражает благодарность правительству Ирландии за его ведущую роль в этом начинании и надеется, что Декларация позволит перевести военные операции из парадигмы сопутствующего ущерба в парадигму предполагаемой защиты, тем самым сведя к минимуму человеческие жертвы.

В заключение позвольте мне процитировать фрагмент послания Папы Франциска, с которым он обратился к Совету Безопасности в июне:

> «С экономической точки зрения война часто более привлекательна, чем мир, поскольку более прибыльна. Но такая прибыль всегда достается очень узкой категории лиц, которые получают ее за счет благополучия всего населения. Поэтому деньги от продажи оружия испачканы кровью невинных. Отказ от легкой наживы ради сохранения мира требует большего мужества, чем продажа все более совершенного и мощного оружия. Для достижения мира нужно больше мужества, чем для ведения войны» (*S/PV.9346, с. 7*).

Председатель (*говорит по-английски*): Комитет заслушал последнего оратора в рамках тематической дискуссии по блоку вопросов «Обычные вооружения».

Сейчас Комитет начинает тематическое обсуждение по блоку вопросов «Другие меры в области разоружения и международная безопасность».

Г-н Сири (Индонезия) (*говорит по-английски*): Я рад возможности выступить от имени Движения неприсоединившихся стран (ДНП).

ДНП отмечает положительные преимущества информационно-коммуникационных технологий (ИКТ) и их вклад в развитие и также призывает государства соблюдать нормы, правила и принципы ответственного поведения государств, содействуя обсуждению механизмов реализации, поскольку это внесет вклад в повышение стабильности и безопасности в киберпространстве.

С другой стороны, ДНП решительно осуждает случаи злонамеренного использования новых ИКТ в целях, несовместимых с задачами поддержания международной стабильности и безопасности. ДНП призывает активизировать усилия, направленные на недопущение превращения киберпространства в арену конфликтов и на обеспечение его использования исключительно в мирных целях, поскольку это позволит в полной мере реализовать потенциал ИКТ на благо социально-экономического развития.

ДНП принимает к сведению выводы Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, которые содержатся в ее докладах за 2013, 2015 и 2021 годы и говорят о том, что международное право, в частности Устав Организации Объединенных Наций, применимо и имеет существенно важное значение для поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды.

ДНП напоминает, что Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 была учреждена резолюцией 75/240 и стала первым инклюзивным механизмом, созданным в рамках Организации Объ-

единенных Наций с участием всех государств-членов, действующих на основе консенсуса.

ДНП вновь заявляет о своей решимости содействовать успешной работе РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, которая была создана в соответствии с резолюцией 75/240 и в настоящее время является единственным инклюзивным механизмом, учитывающим проблемы и интересы всех государств, который действует на основе консенсуса и работает в рамках Организации Объединенных Наций при активном и равноправном участии всех государств. ДНП также обращает внимание на процесс принятия второго ежегодного доклада РГОС на основе консенсуса (см. A/78/265).

ДНП подчеркивает, что при разработке любой международно-правовой базы для решения проблем, связанных с использованием ИКТ и имеющих последствия для международного мира и безопасности, следует учитывать опасения и интересы всех государств и руководствоваться правилом консенсуса, и что этот процесс должен проходить в рамках Организации Объединенных Наций при активном и равноправном участии в нем всех государств. В этой связи ДНП выступает за создание в рамках Организации Объединенных Наций одновекторного постоянного механизма, возглавляемого государствами и подотчетного Первому комитету. ДНП поддерживает развитие открытого, инклюзивного, прозрачного, устойчивого и гибкого процесса, способного развиваться в соответствии с потребностями развивающихся стран и с учетом изменений ИКТ-среды. ДНП также подчеркивает, что такая законодательная основа вместе с многосторонней, инклюзивной институциональной платформой, посвященной международному сотрудничеству в области защиты мирного использования ИКТ, станет важным вкладом в укрепление стабильности и безопасности в киберпространстве путем предотвращения конфликтов, способствуя тем самым урегулированию международных споров мирными средствами и мирному использованию ИКТ. В то же время ДНП подчеркивает свою принципиальную позицию, что ни одно из положений этой законодательной базы не должно затрагивать неотъемлемые права государств на развитие и использование ИКТ в мирных целях.

ДНП отвергает любые односторонние меры, не соответствующие Уставу Организации Объединенных Наций и международному праву, которые препятствуют полному достижению экономического и социального развития населением затронутых стран и подрывают их благосостояние. ДНП осуждает неправомерное использование ИКТ, включая интернет и социальные сети, для подстрекательства к актам террора и их совершения. ДНП подчеркивает, что в деле повышения стабильности и безопасности киберпространства важное значение для государств-членов имеют меры по наращиванию организационно-кадрового потенциала и укреплению доверия.

ДНП также подчеркивает необходимость соблюдения экологических норм при разработке и осуществлении соглашений о разоружении и ограничении вооружений. Кроме того, ДНП подтверждает, что международные форумы по разоружению должны в полной мере учитывать соответствующие экологические нормы в ходе переговоров по договорам и соглашениям о разоружении и ограничении вооружений.

ДНП приветствует принятие без голосования резолюции 77/45 о взаимосвязи между разоружением и развитием. ДНП также подчеркивает важность сокращения военных расходов в соответствии с принципами ненанесения ущерба безопасности при самом низком уровне вооружений и настоятельно призывает все государства направить освободившиеся в результате этого ресурсы на решение новых задач, стоящих перед международным сообществом в области развития, искоренения бедности и ликвидации болезней, от которых страдает человечество.

По этому блоку вопросов ДНП представляет на рассмотрение следующие три проекта резолюций и будет признательно всем государствам за их поддержку: «Соблюдение экологических норм при разработке и осуществлении соглашений о разоружении и контроле над вооружениями» (A/C.1/78/L.6), «Содействие многосторонности в области разоружения и нераспространения» (A/C.1/78/L.7) и «Взаимосвязь между разоружением и развитием» (A/C.1/78/L.4).

Г-н Чиндавонгсе (Таиланд) (*говорит по-английски*): Я имею честь выступать с этим заявлением от имени Ассоциации государств Юго-Восточной Азии (АСЕАН).

АСЕАН присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран.

АСЕАН подтверждает свою приверженность созданию открытого, безопасного, надежного, стабильного, доступного, функционально совместимого, мирного и устойчивого киберпространства, которое является движущей силой экономического прогресса, расширения региональных связей и повышения уровня жизни для всех. В то же время АСЕАН признает широкое распространение киберугроз, которые постоянно развиваются и носят трансграничный характер. На фоне повсеместного перехода к цифровым технологиям в сфере экономики и распространения подключенных к интернету устройств в странах АСЕАН мы становимся все более уязвимыми для злонамеренных действий в киберпространстве, которые способны подорвать мир и безопасность. В этой связи АСЕАН считает, что государства должны работать сообща, чтобы эффективно реагировать на киберугрозы, минимизировать риск неправильного восприятия и просчетов путем укрепления доверия и уверенности, а также использовать преимущества технологий, признавая, что кибербезопасность — это междисциплинарный вопрос, который требует скоординированного опыта множества заинтересованных сторон в различных областях.

АСЕАН подчеркивает центральную роль Организации Объединенных Наций в обсуждении вопросов кибербезопасности. В этой связи АСЕАН подтверждает свою поддержку деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 в качестве меры укрепления доверия и в качестве форума для формирования и восстановления консенсуса по этому важному вопросу. В этой связи АСЕАН приветствует принятие консенсусом второго ежегодного доклада о проделанной работе РГОС в ходе ее пятой основной сессии, состоявшейся в июле 2023 года (см. A/78/265). АСЕАН гордится тем, что инициативы АСЕАН — в частности, реестр контактных пунктов Регионального форума АСЕАН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и матрица для Регионального плана действий АСЕАН по реализации норм ответственного поведения государств в киберпространстве — внесли значительный вклад в международное обсуждение вопросов, связанных с киберпространством, в рамках Организации Объединенных Наций. Мы надеемся на создание и введение в действие глобального межправительственного реестра контактных пунктов, а также на разработку дополнительных рекомендаций, включая контрольный перечень по выполнению норм, как указано в ежегодном докладе о проделанной работе.

АСЕАН выступает за то, чтобы РГОС оставалась центральной платформой для обсуждения вопросов кибербезопасности в Организации Объединенных Наций до окончания срока действия ее мандата, и надеется на дальнейший прогресс, в том числе на основе с таким трудом достигнутого консенсуса, которого мы добились в двух предыдущих ежегодных докладах. АСЕАН призывает государства-члены к сохранению и поддержанию консенсуса по такому важному вопросу, как кибербезопасность. Мы также должны избегать создания параллельных механизмов и/или дублирующих друг друга процессов, которые только еще больше ограничат и так ограниченные ресурсы Организации Объединенных Наций и ее государств-членов. В этой связи АСЕАН твердо убеждена в важности одновекторного процесса, который будет опираться на рекомендации РГОС по регулярному институциональному диалогу, принятые на основе консенсуса. АСЕАН по-прежнему готова к конструктивному взаимодействию со всеми партнерами в этом направлении.

В рамках АСЕАН сотрудничество в области кибербезопасности охватывает все основные направления деятельности и секторы и осуществляется в соответствии с Генеральным планом АСЕАН по развитию цифровых технологий на период до 2025 года и Стратегией сотрудничества АСЕАН в области кибербезопасности на период 2021–2025 годов, которые были приняты министрами цифровых технологий государств — членов АСЕАН в январе 2022 года. Государства — члены АСЕАН прилагают усилия для принятия расширенных мер кибербезопасности в соответствии со Стратегией 2021–2025 годов в связи с участившимися в последнее время глобальными кибератаками и угрозами кибербезопасности и в ответ на новые киберсобытия. В то же время АСЕАН в настоящее время работает над реализацией Азиатского регионального плана действий по выполнению решений Группы правительственных экспертов по поощрению ответствен-

ного поведения государств в киберпространстве в контексте международной безопасности, который был разработан для того, чтобы государства — члены АСЕАН определили области, нуждающиеся в дальнейшей поддержке для реализации этих норм, включая наращивание потенциала и международное сотрудничество.

Для укрепления потенциала АСЕАН по реагированию на инциденты в сфере кибербезопасности государства — члены АСЕАН договорились о создании Региональной группы реагирования на компьютерные инциденты АСЕАН, чтобы способствовать своевременному обмену информацией о киберугрозах и кибератаках между национальными группами реагирования на компьютерные инциденты государств — членов АСЕАН.

Поскольку кибербезопасность является междисциплинарной проблемой, для укрепления регионального сотрудничества и координации в области кибербезопасности был создан Координационный комитет АСЕАН по кибербезопасности. В состав Комитета входят представители соответствующих отраслевых органов для укрепления межсекторальной координации в области кибербезопасности с учетом сферы деятельности отраслевых органов.

АСЕАН подчеркивает важность расширения международного сотрудничества и наращивания организационно-кадрового потенциала в области ИКТ, поскольку это позволит государствам, особенно развивающимся странам, эффективно противостоять киберугрозам и применять при использовании ИКТ 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств. С этой целью АСЕАН инициировала реализацию проекта «Киберщит АСЕАН» на период с 2023 по 2026 год, чтобы дополнить предпринимаемые АСЕАН усилия по наращиванию потенциала, включая работу Центра передового опыта в области кибербезопасности АСЕАН — Сингапур и Центра по укреплению потенциала в области кибербезопасности АСЕАН — Япония в Таиланде, в поддержку общей цели по укреплению потенциала региона. АСЕАН рассчитывает работать в тандеме с Организацией Объединенных Наций в этом направлении, особенно в рамках Всестороннего партнерства между АСЕАН и Организацией Объединенных Наций.

Кроме того, АСЕАН работает с международными партнерами над укреплением международного сотрудничества в области безопасности ИКТ с помощью таких платформ, как Межсессионная встреча Регионального форума АСЕАН по безопасности и использованию информационно-коммуникационных технологий. АСЕАН также приветствует прогресс, достигнутый благодаря открытию Центра передового опыта в области кибербезопасности и информации в рамках Совещания министров обороны стран АСЕАН (СМОА) и Рабочей группы экспертов (РГЭ) по кибербезопасности в рамках Совещания министров обороны «АСЕАН плюс». Среди заметных достижений последних лет — создание реестра контактных пунктов и технического персонала АСЕАН, разработка глоссария кибертерминологии, проведение учений и создание портала РГЭ по кибербезопасности в рамках Совещания министров обороны «АСЕАН плюс».

В заключение АСЕАН подтверждает свое обязательство подготовиться к будущему, чтобы обеспечить экономический прогресс, улучшить качество жизни и гарантировать мир и безопасность для всех. Мы надеемся внести конструктивный вклад вместе с членами международного сообщества и соответствующими заинтересованными сторонами в достижение наших общих целей по созданию мирного, безопасного, функционально совместимого и устойчивого киберпространства.

Г-н Шэнь Цзянь (Китай) (*говорит по-английски*): Я имею честь выступить с этим совместным заявлением от имени Беларуси, Бурунди. Камбоджи, Камеруна, Кубы, Доминики, Экваториальной Гвинеи, Эритреи, Эфиопии, Гвинеи-Бисау, Гамбии, Казахстана, Киргизии, Лаосской Народно-Демократической Республики, Никарагуа, Пакистана, России, Сомали, Сирии, Вануату. Венесуэлы, Зимбабве и нашей страны, Китая.

По случаю второй годовщины принятия резолюции 76/234, озаглавленной «Поощрение международного сотрудничества в области мирного использования в контексте международной безопасности», мы, авторы резолюции, вновь заявляем, что неотъемлемым правом всех государств является участие в как можно более полном обмене оборудованием, материалами и научно-технической информацией в мирных целях. В условиях новой эпохи, учитывая потенциальное влияние научно-технического прогресса на глобальную безопасность, возрастает значение мирного использования для содействия экономическому и социальному развитию государств-членов, в особенности развивающихся

стран. Мы призываем международное сообщество принять конкретные меры для обеспечения эффективного выполнения этой резолюции.

Мы приветствуя политические обязательства и конкретные усилия государств-членов по поощрению международного сотрудничества в области мирного использования, а также прогресс, достигнутый в рамках многосторонних структур и по двусторонним каналам. В то же время сохраняются неоправданные ограничения на экспорт в развивающиеся страны материалов, оборудования и технологии для использования в мирных целях. Мы вновь подтверждаем важность развития международного сотрудничества в мирных целях и необходимость дальнейшего обсуждения этой важной темы в рамках Организации Объединенных Наций открытым и всеохватным образом и с использованием актуальных существующих международных, региональных и двусторонних механизмов и договоренностей в соответствии с резолюцией. Мы призываем государства-члены продолжать диалог по вопросам поощрения мирного использования и соответствующего международного сотрудничества, в том числе путем выявления пробелов и проблем, а также поиска новых идей и возможностей для укрепления сотрудничества и изучения возможных путей продвижения вперед.

Мы представим Генеральной Ассамблее на ее семьдесят девятой сессии в 2024 году проект резолюции, озаглавленный «Поощрение международного сотрудничества в области мирного использования в контексте международной безопасности». Мы приветствуем активное участие всех государств в процессе последующей деятельности.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Европейского союза в его качестве наблюдателя.

Г-н Карчмаж (Европейский союз) (*говорит по-английски*): Я имею честь выступать от имени Европейского союза (ЕС). К этому заявлению присоединяются страны-кандидаты Северная Македония, Черногория, Сербия, Албания, Украина, Республика Молдова и Босния и Герцеговина, потенциальная страна-кандидат Грузия и страны — члены Европейской ассоциации свободной торговли Исландия и Норвегия, входящие в Европейскую экономическую зону, а также Монако и Сан-Марино.

За последние десять лет международное сообщество ясно дало понять, что на поведение государств в киберпространстве распространяется основанный на правилах международный порядок. Все члены Генеральной Ассамблеи неоднократно подтверждали значение эволюционирующих нормативных рамок ответственного поведения государств в киберпространстве, основанных на признании того, что в киберпространстве действует международное право, на соблюдении добровольных необязательных норм поведения государств, наращивании потенциала и укреплении практических мер доверия для снижения риска возникновения конфликта. Широкий международный консенсус по этим четырем направлениям — главное достижение кибердипломатии за последнее десятилетие.

Развязанная Россией незаконная, неспровоцированная и неоправданная агрессивная война бросила серьезный вызов основанному на правилах международному порядку, в том числе в киберпространстве. Разрушительные кибератаки против Украины, часто в сочетании с ракетными ударами, являются беспрецедентными, оказывая побочное воздействие в том числе и на страны ЕС. За последний год Украина не только пострадала от большего, чем любая другая страна, количества вредоносных программ, уничтожающих данные, но и успешно предотвратила многие из таких атак благодаря своей исключительной системе киберзащиты и устойчивости.

Появление новых угроз в Европе, вызванное агрессией России против Украины, а также другие растущие и развивающиеся угрозы со стороны государств и негосударственных субъектов повлияли на то, как мы, ЕС, оцениваем вредоносные кибероперации. Мы подтверждаем нашу приверженность работе по дальнейшему пересмотру и постоянному повышению киберустойчивости в ЕС, а также разработке дальнейших стратегий по противодействию киберугрозам, исходящим от всех злоумышленников.

Признавая, что основную ответственность за обеспечение международного мира и безопасности несут государства, следует отметить, что роль других заинтересованных сторон в этой области также важна. Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, созданная в соответствии с резо-

люцией 75/240, дает международному сообществу возможность на открытой, всеохватной и транспарентной основе обмениваться мнениями об ответственном использовании государствами информационно-коммуникационных технологий в соответствии с нормами международного права.

Мы приветствуем консенсус, достигнутый в 2023 году по ежегодному докладу РГОС о проделанной работе (см. A/78/265), и подчеркиваем необходимость того, чтобы международное сообщество продолжало двигаться по пути дальнейшего укрепления безопасности и стабильности в киберпространстве. Несмотря на наличие потенциала для развития положений доклада о проделанной работе, в нем изложены многочисленные решения и последующие шаги, которые можно рассматривать как конкретные и реальные варианты практических действий для укрепления рамок ответственного поведения государств Организации Объединенных Наций и системы международного права.

Гораздо больше еще только предстоит сделать, особенно в плане поддержки практического претворения в жизнь результатов этих обсуждений. ЕС и его государства-члены рассчитывают на продолжение сотрудничества с государствами и другими заинтересованными сторонами в целях продвижения этих усилий, в частности, в рамках всестороннего диалога по разработке программы действий Организации Объединенных Наций, опираясь на консенсусные итоговые документы, подготовленные рядом групп правительственных экспертов Организации Объединенных Наций и рабочих групп открытого состава, а также на работу нынешней РГОС и доклад Генерального секретаря.

Широкая поддержка резолюции 77/37 на прошлогодней сессии Первого комитета, за которую проголосовало 157 членов и соавторами которой стала межрегиональная группа из 74 стран, подтвердила приверженность государств внедрению согласованной нормативной базы с помощью постоянного, инклюзивного и ориентированного на действия механизма. Это наглядно демонстрирует общее стремление подавляющего большинства государств к укреплению мира, безопасности и стабильности в киберпространстве с помощью постоянной платформы сотрудничества, которая способствует обмену знаниями и передовым опытом, позволяет избежать дублирования усилий и помогает в осуществлении национальных и региональных мероприятий. Более 40 государств, представляющих все региональные группы, представили свои письменные материалы, и Генеральный секретарь опубликовал доклад (A/76/77), в котором содержатся ценные материалы и рекомендации для дальнейшего всестороннего обсуждения программы действий.

Как указано в прошлогодней резолюции 77/37, это предложение направлено на предоставление государствам гибкости в решении вопросов, которые выиграют от обсуждения на политическом уровне, обмена информацией и практической реализации. Работа будет вестись под руководством государств и будет направлена на расширение участия многих заинтересованных сторон, предусматривая проведение регулярных консультаций с соответствующими заинтересованными сторонами, включая представителей частного сектора, научных кругов и гражданского общества, для рассмотрения и представления их уникальных точек зрения. Многие негосударственные заинтересованные стороны уже выступают с инициативами, направленными на укрепление доверия между государствами и негосударственными субъектами, и их привлечение приведет к более эффективным результатам, способствуя прозрачности, надежности и устойчивости реализации рамочной программы.

Самое главное, что создание постоянной платформы позволило бы международному сообществу сосредоточиться на обсуждении вопросов существа и укрепления сотрудничества и доверия между государствами, а не на постоянных дебатах о будущих процессах. Мы не должны упустить эту возможность продолжить нашу работу в стабильной обстановке, и Европейский союз и его государства-члены полностью поддерживают соответствующую резолюцию, представленную Генеральной Ассамблее с этой целью. Чтобы сохранить одновекторный процесс в Организации Объединенных Наций, нам необходимо создать постоянный механизм после завершения работы нынешней РГОС 2021–2025, при этом его сфера охвата, структура и содержание должны быть основаны на результатах обсуждений в рамках РГОС в 2024 и 2025 годах.

Учитывая эскалацию международных киберугроз, сейчас как никогда важно углублять наше сотрудничество с международными партнерами в области кибербезопасности и способствовать общему пониманию того, как применяется международное право и как дальше устанавливать рамки ответствен-

ного поведения государств, предложенные Организацией Объединенных Наций. По этой причине ЕС поддерживает представленный Францией проект резолюции A/C.1/78/L.60 о создании соответствующего механизма под эгидой Организации Объединенных Наций в качестве гибкой площадки, где государства — члены Организации Объединенных Наций смогут участвовать в практических дискуссиях о том, как наилучшим образом обеспечить безопасность киберпространства для всех. Мы сможем обеспечить открытое, стабильное и безопасное киберпространство только в том случае, если будем сотрудничать, улучшать координацию и взаимодополняемость, преодолевать разобщенность и формировать новые, инновационные методы борьбы со злонамеренным киберповедением. В этом и заключается амбициозная задача ЕС.

Г-н Лагардьен (Южная Африка) (*говорит по-английски*): Южная Африка присоединяется к заявлению, сделанному от имени Движения неприсоединившихся стран.

Южная Африка приветствует принятие консенсусом второго ежегодного доклада (см. A/78/265) о проделанной работе Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Этот процесс сыграл важную роль в укреплении взаимного доверия и развитии мирного сотрудничества между государствами. Принимая во внимание многочисленные угрозы, с которыми сталкиваются государства, Южная Африка считает, что для противодействия угрозам, направленным на инфраструктуру информационно-коммуникационных технологий (ИКТ), необходимы совместные усилия.

Мы добросовестно участвуем в Рабочей группе открытого состава (РГОС) в стремлении обеспечить проведение диалога между государствами под эгидой Организации Объединенных Наций — универсального, многостороннего форума, нацеленного на мирное урегулирование споров. Южная Африка считает, что поддержание международного мира и безопасности в киберпространстве является коллективной обязанностью. Мы считаем, что государства должны использовать существующие 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств в их нынешнем виде, в то время как мы рассматриваем возможность создания более широких рамок для сотрудничества.

Во втором ежегодном докладе о проделанной работе нам представлены две всеобъемлющие меры по укреплению доверия: продолжающаяся работа по налаживанию регулярного институционального диалога и реестр контактных пунктов. Мы также рассматриваем РГОС и ее консенсусные итоговые результаты как меру укрепления доверия и высоко оцениваем усилия председателя РГОС посла Бурхана Гафура и его сотрудников, направленные на достижение ощутимых результатов, а также на то, чтобы процесс оставался ориентированным на действия. Обсуждение различных форматов обмена мнениями между государствами о потенциальных и возникающих угрозах показало нам, что международное сообщество может сохранять конструктивный подход в сложные политические времена. В этой связи Южная Африка поддерживает предложения о создании хранилища угроз и глобального портала сотрудничества в области кибербезопасности. Мы надеемся, что будущие сессии РГОС смогут развить эти идеи.

Хотя межправительственный процесс выиграл бы от брифингов соответствующих экспертов из региональных и субрегиональных организаций, деловых кругов, неправительственных организаций и академических кругов, с должным учетом справедливого географического представительства, мы считаем, что председатель РГОС использовал свои организационные полномочия для приглашения различных заинтересованных сторон поделиться своими взглядами на внедрение безопасности в сфере использования ИКТ. Таким образом, РГОС смогла привлечь к своей работе представителей самых различных взглядов.

Как развивающаяся страна, Южная Африка выигрывает от обмена мнениями между государствами в рамках РГОС, и мы поддерживаем председателя и предложенный им график, призванный облегчить процесс согласования наших будущих обсуждений в рамках международного сообщества. Южная Африка считает, что для нас жизненно важно охранять существующие процессы, такие как те, которые доказали свою успешность в трудные времена.

Г-н аль-Каиси (Иордания) (*говорит по-арабски*): Прежде всего я хотел бы от имени Группы арабских государств вновь заявить о необходимо-

сти положить конец войне и жестокой израильской агрессии против сектора Газа. Группа арабских государств самым решительным образом осуждает эту агрессию. Необходимо обеспечить безопасный и устойчивый доступ к необходимой гуманитарной и медицинской помощи, а также положить конец насильственному перемещению палестинцев.

Переходя к нашей сегодняшней тематической дискуссии, Группа арабских государств присоединяется к заявлению, сделанному от имени Движения неприсоединившихся стран.

Что касается вопроса о других мерах по разоружению, то Группа арабских государств подчеркивает, что решения, согласованные в контексте многосторонних отношений в соответствии с Уставом Организации Объединенных Наций, представляют собой единственный устойчивый путь к решению проблем разоружения и обеспечения международной безопасности. Группа призывает все государства-члены подтвердить и выполнить свои индивидуальные и коллективные обязательства в контексте международного многостороннего сотрудничества. Группа вновь подтверждает свою убежденность в том, что Организация Объединенных Наций играет ключевую роль в вопросах разоружения и нераспространения.

Группа арабских государств выражает свою обеспокоенность ростом напряженности и военных расходов во всем мире, значительная часть которых могла бы быть направлена на содействие устойчивому развитию и искоренение бедности во всем мире, особенно в развивающихся странах, включая арабские страны. Группа подтверждает важность выполнения программы работы, принятой на Международной конференции по взаимосвязи между разоружением и развитием в 1987 году, а также последствий роста военных расходов для достижения целей в области устойчивого развития в соответствии с Повесткой дня в области устойчивого развития на период до 2030 года.

Серьезную угрозу международному миру и безопасности, а также устойчивому развитию несут непрекращающиеся приобретение и модернизация ядерных арсеналов. В связи с этим Группа арабских государств подчеркивает необходимость того, чтобы международные форумы по разоружению принимали во внимание соответствующие стандарты при обсуждении договоров и конвенций по разоружению и контролю над вооружениями. Все государства должны вносить свой вклад в обеспечение полного соблюдения экологических стандартов при выполнении таких договоров и конвенций.

Обращаясь к теме кибербезопасности, Группа арабских государств выражает свою обеспокоенность расширением масштабов использования информационно-коммуникационных технологий (ИКТ) для осуществления деструктивной деятельности, нарушающей международный мир и безопасность, включая действия террористических и преступных организаций. Группа подчеркивает необходимость того, чтобы Организация Объединенных Наций продолжала разрабатывать обязательные правила, регулирующие ответственное поведение государств в этой жизненно важной области, соразмерно ее стремительному развитию. Необходимо, кроме того, продолжать международное сотрудничество и сохранять центральную роль Организации Объединенных Наций в этих усилиях.

Группа арабских государств подчеркивает важность дальнейшего международного сотрудничества в деле обеспечения безопасности ИКТ. Это расширит возможности государств по противодействию любым диверсионным атакам. В многочисленных докладах, подготовленных различными группами правительственных экспертов и рабочими группами открытого состава, подчеркиваются случаи таких атак. Группа арабских государств стремится обеспечить центральную роль Организации Объединенных Наций во внедрении международных стандартов, касающихся безопасности и защиты ИКТ, и продолжать сотрудничество с Организацией Объединенных Наций в этой области, которая оказывает влияние на все жизненно важные объекты различных государств. Она все чаще используется в диверсионной деятельности, угрожающей международной безопасности.

В заключение Группа арабских государств подчеркивает свою готовность активно участвовать в деятельности Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, созданной в соответствии с резолюцией 75/240. Группа приветствует принятие консенсусом второго ежегодного доклада о проделанной работе Рабочей группы открытого состава

(см. A/78/265) и надеется на проведение целенаправленных обсуждений различных соответствующих предложений по поддержке развивающихся стран в противодействии растущим угрозам, связанным с использованием ИКТ.

Г-н Сири (Индонезия) (*говорит по-английски*): Индонезия присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Ассоциации государств Юго-Восточной Азии. В связи с этим я хотел бы отметить несколько моментов в национальном качестве.

Мое первое замечание касается важности укрепления мер сотрудничества в области безопасности информационно-коммуникационных технологий (ИКТ). Технологии часто называют обоюдоострым мечом: это ценный инструмент, но при этом они создают значительные риски. Однако по мере того, как мы оказываемся все более взаимосвязанными, кибератаки становятся главной угрозой для цифровой инфраструктуры, вызывая сбои в работе сервисов, кражу данных и мошенничество. В связи с этим Индонезия подчеркивает необходимость совместных действий всех государств-членов для обеспечения безопасного, надежного и стабильного киберпространства.

Индонезия подтверждает свою поддержку деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, включая ее акцент на наращивании потенциала и укреплении доверия. Это поможет странам укрепить свой потенциал в области кибербезопасности. Со своей стороны, Индонезия недавно, в июле, представила свою Национальную стратегию кибербезопасности. Это еще больше расширит возможности недавно созданного Национального агентства кибербезопасности и дополнит законодательную базу по защите пользователей компьютеров, важнейших объектов национальной инфраструктуры и киберпространства с помощью таких законов, как Закон о конфиденциальности данных от 2022 года и Закон об информации и электронных операциях от 2008 года. Индонезия надеется на продолжение обсуждения вопроса о наращивании потенциала в области кибербезопасности в рамках РГОС.

Мое второе замечание касается укрепления многосторонних рамочных программ и норм в области использования ИКТ. В нынешней ситуации в сфере международной безопасности наблюдается значительный спад сотрудничества, основанного на консенсусе. Мы не должны допустить этого в сфере безопасности ИКТ. Такая тенденция позволит злоумышленникам нарушать безопасность киберпространства, угрожая международному миру и стабильности. Поэтому, учитывая нестабильность нашей международной обстановки, Индонезия приветствует усилия государств-членов по принятию второго ежегодного доклада о проделанной работе (см. A/78/265) на основе консенсуса. Благодаря своему инклюзивному и поэтапному подходу РГОС смогла стать платформой, способствующей сотрудничеству, прозрачности и мерам по укреплению доверия в вопросах безопасности ИКТ. Индонезия также приветствует и с нетерпением ожидает внедрения реестра контактных пунктов в качестве одного из конкретных и ощутимых результатов работы РГОС. Поэтому крайне важно, чтобы мы сохранили неприкосновенность РГОС как всеохватывающей структуры для управления киберрисками, содействия благому управлению и передовой практике в киберпространстве.

Поскольку мы находимся в середине срока действия мандата РГОС, я хотел бы поддержать заявления, сделанные делегациями по предложенному проекту резолюции, касающемуся будущего механизма для обсуждения вопросов безопасности в сфере использования ИКТ. Важно, чтобы мы оставались последовательными в отношении общих элементов будущего механизма, согласованных консенсусом во втором ежегодном докладе о проделанной работе. Мы должны избегать представления конкурирующих проектов резолюций по одному и тому же вопросу, что приведет к фрагментации в работе Первого комитета и параллельным процессам, подрывающим работу РГОС. Вместо этого мы продолжим использовать РГОС для обсуждения вопросов устойчивого сотрудничества, обмена передовым опытом и возможностями между странами для эффективного решения проблем кибербезопасности, сокращения цифрового разрыва и содействия беспрепятственному экономическому и социальному прогрессу.

Г-н Хегази (Египет) (*говорит по-английски*): Прежде всего позвольте мне выразить наше решительное осуждение продолжающихся нападений на палестинцев в Газе. Мы вновь призываем к срочному и безоговорочному прекращению огня, а также к тому, чтобы Израиль немедленно прекратил попытки насильственного перемещения более миллиона гражданских лиц на юге Газы. Израиль также дол-

жен обеспечить беспрепятственный доступ гуманитарной помощи, чтобы облегчить продолжающиеся страдания палестинского народа.

Египет присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Группы арабских государств, и хотел бы высказать следующие замечания.

Египет вновь заявляет, что наиболее эффективными мерами достижения устойчивого прогресса в области разоружения и международной безопасности являются недискриминационные, многосторонние, юридически обязательные документы. Постоянная приверженность всех государств ранее согласованным обязательствам и международному праву является необходимым условием для поддержания международного мира и безопасности и предотвращения хаоса — принимая во внимание стремительный научно-технический прогресс в нескольких стратегических областях, которые оказывают непосредственное влияние на международную безопасность и до сих пор не имеют четких согласованных на международном уровне правил, которые бы не дали им превратиться в арену для гонки вооружений и вооруженных конфликтов, — а также для обеспечения уверенного дальнейшего роста и вклада соответствующих технологий в развитие и благосостояние.

Яркими тому примерами являются киберпространство, космическое пространство и организация применения искусственного интеллекта, включая сферу создания смертоносного автономного оружия. Отсутствие прогресса в устранении ряда угроз безопасности, возникающих в таких областях, очевидно, объясняется не отсутствием технических знаний у международного сообщества, а сохраняющейся ошибочной верой некоторых государств в возможность сохранения абсолютного господства в таких областях. Тем самым эти государства противостоят любым усилиям, направленным на разработку справедливых правовых многосторонних режимов, запрещающих злонамеренное использование и таких технологий и их использование в военных целях, что приведет к гонке вооружений, которую никто не сможет выиграть.

Мы приветствуем успешное завершение второго годового цикла деятельности Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 и принятие ее второго ежегодного доклада о проделанной работе (см. A/78/265) и документа с изложением элементов позиций о введении в действие глобального реестра контактных пунктов, а также других перспективных рекомендаций, которые могут проложить путь к целенаправленному обсуждению нерешенных вопросов и предложений, относящихся к сфере деятельности РГОС.

РГОС было представлено множество креативных идей и конструктивных предложений, включая регулярный институциональный диалог под эгидой Организации Объединенных Наций, например, возможная программа действий Организации Объединенных Наций по использованию информационных и телекоммуникационных технологий в контексте международной безопасности, которую Египет запустил в 2020 году совместно с Францией и которая была разработана при поддержке межрегиональной группы государств с целью дополнить работу РГОС после завершения ее мандата после 2025 года.

В связи с этим Египет представил на веб-сайте РГОС свою национальную позицию по будущему процессу регулярного институционального диалога. Мы разделяем мнение о том, что любой будущий процесс по этой теме должен содержать отдельный компонент, посвященный внедрению согласованных рамок и наращиванию потенциала развивающихся стран в этой области. Такой механизм должен быть гибким, ориентированным на конкретные действия, одновекторным, постоянным и основанным на консенсусе под эгидой Организации Объединенных Наций, как это предусмотрено в пункте 55 консенсусного второго ежегодного доклада о проделанной работе РГОС. Он должен выявить возможные пробелы в существующей системе путем реализации консенсусных решений, укрепить международное сотрудничество и помощь, а также доработать существующую систему норм, правил и принципов в дополнение к имеющим юридическую силу обязательствам.

В этом контексте мы приветствуем растущую поддержку в пользу того, чтобы сосредоточиться на реализации существующих согласованных рамок и их дальнейшем развитии. Кроме того, мы считаем, что нам следует продолжать поддерживать нынешнюю РГОС в целях успешного завершения ее работы и направить наши усилия на выработку общей основы для создания будущего механизма, опираясь на результаты деятельности РГОС. В связи с этим мы призываем все делегации не предвосхищать резуль-

таты текущих переговоров и не навязывать преждевременное создание параллельных процессов не только в рамках блока вопросов 5, но и по всем другим направлениям. Такая тенденция приведет лишь к дальнейшему расколу и тупику.

Г-жа Гомес Сардинас (Куба) (*говорит по-испански*): Мы поддерживаем заявление, сделанное представителем Индонезии от имени Движения неприсоединившихся стран. Мы также поддерживаем заявление представителя Китая о международном сотрудничестве в мирных целях в контексте международной безопасности.

Мы подтверждаем приверженность Кубы всеобщему и полному разоружению, которое позволит нам построить мир, где нет места оружию массового уничтожения, на благо нынешнего и будущих поколений. Мы призываем к принятию других мер в области разоружения и международной безопасности, которые помогут нам как можно скорее построить мир во всем мире. Мы должны сократить огромные расходы на милитаризацию. Эти деньги, а также достижения научно-технического прогресса, которые сегодня нацелены на финансирование военно-промышленного комплекса, разработку, производство и обновление все более совершенного оружия, принесли бы человечеству бесчисленные блага, если бы были использованы для осуществления Повестки дня в области устойчивого развития на период до 2030 года и целей в области устойчивого развития.

Мы, государства-члены, должны продолжать работу с целью сохранения многостороннего подхода в качестве основного принципа проведения переговоров в сфере разоружения и контроля над вооружениями. Мы напоминаем, что такие переговоры должны соответствовать обязательным международным экологическим нормам. Мы поддерживаем переговоры об имеющих обязательную юридическую силу инициативах, направленных на недопущение милитаризации космического пространства и киберпространства и запрет смертоносных автономных систем вооружений.

Место Председателя занимает г-н Лагардьен (*Южная Африка*), *заместитель Председателя.*

Мы поддерживаем текущую работу Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, которая позволяет государствам-членам обсуждать вопросы на прозрачной, инклюзивной и равноправной основе. В качестве подтверждения нашей приверженности этому форуму мы одобряем принятие консенсусом его второго ежегодного доклада о проделанной работе (см. A/78/265), хотя мы возлагали более высокие ожидания, в частности, на прогресс в разработке дополнительных норм ответственного поведения государств в области безопасности информационно-коммуникационных технологий (ИКТ). Мы не должны ни предвосхищать результаты обсуждения будущего механизма для проведения регулярного институционального диалога, ни продвигать предложенную программу действий в ущерб другим национальным инициативам.

Информационно-коммуникационные технологии должны использоваться не для ведения войны, а исключительно в мирных целях. Мы отвергаем враждебное использование ИКТ, открытое или тайное, направленное на подрыв правового и политического порядка государств, а также для совершения актов терроризма или подстрекательства к ним. Мы выступаем против применения силы в качестве законной меры реагирования на кибератаки.

Мы отвергаем нетрадиционные методы ведения войны, которые правительство Соединенных Штатов продолжает использовать против Кубы, и огромные ресурсы, которые оно направляет на это. Мы осуждаем использование новых ИКТ и других цифровых платформ для дестабилизации ситуации в нашей стране, распространения фальшивых новостей и содействия смене режима. Мы выступаем против манипулирования кубинским интернетом в нарушение согласованных на международном уровне норм в этой области. Мы призываем Соединенные Штаты немедленно прекратить продолжающуюся финансовую и торговую блокаду Кубы, которая существенно ограничивает доступ к ИКТ и их использование на благо кубинского народа.

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

Г-н Пиерис (Шри-Ланка) (*говорит по-английски*): Шри-Ланка присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран. Я выступаю с этим заявлением в национальном качестве.

Третье десятилетие XXI века характеризуется стремительным развитием и революциями в области информационно-коммуникационных технологий (ИКТ). Мы действительно переживаем знаменательный момент эпохи цифровых технологий и живем в мире, пожинающем плоды информационно-коммуникационных технологий. Сегодня ИКТ неразрывно связаны с повседневной жизнью людей, как никогда раньше. Виртуальное пространство, в котором мы живем каждый день, свидетельствует о той важнейшей роли, которую ИКТ играют на всех уровнях — от государств до отдельных людей. Распространившись во всех сферах человеческой деятельности, ИКТ стали помощником во всех этих областях.

В нашей стране в мае была запущена программа под названием «DIGIECON Sri Lanka 2023–2030», что подчеркивает теснейшую взаимосвязь между ИКТ и экономическим прогрессом в Шри-Ланке, а также демонстрирует твердую решимость превратить Шри-Ланку в инклюзивную страну в плане использования цифровых технологий. Программа, включающая в себя генеральный план развития цифровых технологий и нормативно-правовую базу, а также серию ежегодных мероприятий, направлена на ускорение перехода экономики Шри-Ланки к инклюзивной цифровой экономике за счет использования передовых технологических решений.

Провозглашая эти рубежи и невзирая на все свои положительные черты, киберпространство, как и другие разновидности трансформационных технологий, в то же время стало пристанищем для различных субъектов, занимающихся преступной и террористической деятельностью, а также для тех, кто преследует корыстные цели, распространяя ненависть, нетерпимость и подстрекательство к насилию, особенно в социальных сетях. В последнее время наблюдается беспрецедентный уровень уязвимости с точки зрения кибератак и других злонамеренных действий, направленных на услуги ИКТ, в результате которых миллионы людей становятся жертвами буквально по нажатию нескольких кнопок.

В связи с этим Шри-Ланка поддерживает многосторонние обсуждения в Рабочей группе открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Это единственный инклюзивный механизм, действующий в рамках Организации Объединенных Наций при активном и равноправном участии всех государств. Мы приветствуем принятие второго ежегодного доклада о проделанной работе (см. A/78/265) и создание глобального межправительственного реестра контактных пунктов и надеемся на дальнейшие обсуждения в рамках РГОС. Мы также с интересом следим за текущими обсуждениями в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Мы подчеркиваем, что использование таких технологий должно соответствовать целям и принципам Устава Организации Объединенных Наций и нормам международного права, в первую очередь принципам суверенитета, суверенного равенства, невмешательства во внутренние дела, отказа от угрозы силой или ее применения в международных отношениях, мирного разрешения споров, уважения прав человека и соблюдения устоявшихся принципов мирного сосуществования государств. Поэтому принятие законов и мер по предотвращению незаконной и преступной деятельности, направленной против отдельных лиц, объектов промышленности или государственных учреждений, является главной обязанностью соответствующих государств, однако многие развивающиеся страны, в том числе и наша страна, сталкиваются с проблемой ограниченности возможностей.

Все мы знаем, насколько человек изобретателен. Знаем и его способность к саморазрушению, к которому ведет эта изобретательность и преследование собственных сиюминутных интересов, будь то злонамеренное использование существующих технологий или изобретение новых, таких как искусственный интеллект или смертоносные автономные системы вооружений. Мы не можем позволить себе опасные эксперименты, которые ставят под угрозу само наше существование.

Г-жа Липана (Филиппины) (*говорит по-английски*): Филиппины присоединяются к заявлениям, сделанным представителем Таиланда от имени Ассоциации государств Юго-Восточной Азии и представителем Индонезии от имени Движения неприсоединившихся стран (ДНП). Позвольте мне высказать следующие замечания в своем национальном качестве.

Мы решительно поддерживаем проект резолюции ДНП A/C.1/78/L.4 о взаимосвязи между разоружением и развитием, в котором подчеркивается

важность согласования разоружения с глобальными целями в области развития. Проект резолюции призывает сократить военные расходы и перенаправить ресурсы на экономическое и социальное развитие, чтобы сократить разрыв между развитыми и развивающимися странами. В нем подчеркивается взаимосвязь между разоружением и развитием, а также роль безопасности в достижении мира и процветания.

Филиппины полностью поддерживают проект резолюции ДНП A/C.1/78/L.6 об экологических нормах и разоружении, подчеркивая важнейшую связь между охраной окружающей среды и глобальной безопасностью, способствуя ответственному разоружению с упором на сохранение окружающей среды. Филиппины присоединяются к ДНП, подчеркивая важность многостороннего подхода в усилиях по разоружению и нераспространению, а также отмечая важность прозрачных переговоров и сотрудничества между государствами для сохранения глобального мира и безопасности.

Что касается безопасности и использования информационно-коммуникационных технологий (ИКТ), Филиппины полностью поддерживают Рабочую группу открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Мы подчеркиваем положительное влияние ИКТ на развитие и необходимость ответственного поведения государств для обеспечения стабильности и безопасности в киберпространстве. Филиппины осуждают злонамеренное использование ИКТ, нарушающее международное право, и призывают к коллективным усилиям по защите киберпространства и содействию его мирному использованию.

Мы одобряем второй ежегодный доклад о проделанной работе РГОС (см. A/78/265). Рабочая группа, действующая на основе консенсуса и с участием всех членов, добилась успеха в выработке ориентированных на конкретные действия результатов, направленных на укрепление доверия между странами в вопросах кибербезопасности. Филиппины полностью поддерживают дальнейшее успешное функционирование РГОС в качестве действующего механизма, учитывающего проблемы и интересы всех государств — членов Организации Объединенных Наций в области кибербезопасности. Мы поддерживаем создание в рамках Организации Объединенных Наций одновекторного постоянного механизма, возглавляемого государствами и подотчетного Первому комитету. Этот механизм должен быть открытым, инклюзивным, прозрачным, устойчивым и гибким, чтобы адаптироваться к меняющимся потребностям развивающихся стран в динамичной среде ИКТ. Мы надеемся, что нам удастся согласовать наши усилия в этом направлении, а также при обсуждении вопросов кибербезопасности в настоящее время и в будущем.

Как мы уже слышали в ходе неофициальных консультаций, конкурирующие проекты резолюций не приносят пользы. Они приводят к расколу. В этой связи, в соответствии с принципом «наведения мостов», мы были и остаемся готовы помочь найти золотую середину, поэтому Филиппины продолжат взаимодействовать со сторонниками такого подхода и заинтересованными делегациями по вопросам разработки будущего механизма, который мог бы получить самую широкую поддержку.

Что касается смертоносного автономного оружия, то Филиппины полностью поддерживают проект резолюции A/C.1/78/L.56 по этому вопросу. Мы отдаем должное международному сообществу за признание срочной необходимости решения проблем, возникающих в связи с автономными системами вооружений, которые порождают гуманитарные, правовые, технологические и этические вопросы. В условиях стремительного развития этих технологий крайне важно соблюдать нормы международного права и поддерживать высочайшие стандарты человечества. Всеохватность проекта резолюции, учитывающего различные точки зрения, обеспечивает комплексный подход к решению этого важнейшего вопроса. Поручение Секретариату подготовить всеобъемлющий доклад, в котором будут учтены технологические достижения и представлены различные заинтересованные стороны, демонстрирует приверженность международного сообщества соблюдению международного права и обеспечению мира и безопасности. Филиппины считают, что данный проект резолюции станет катализатором коллективных многосторонних усилий по решению проблем, связанных со смертоносными автономными системами вооружений. Мы надеемся на продолжение обсуждений и прогресс в этом вопросе в рамках Конвенции по конкретным видам обычного оружия.

В заключение я хотел бы подтвердить, что Филиппины твердо намерены строить будущее, основанное на безопасности, развитии и ответственном использовании технологий. Мы обязуемся неизменно поддерживать принципы разоружения и устойчивого развития, опираясь на преимущества многостороннего подхода. Кроме того, мы подчеркиваем необходимость защищать цифровую сферу, обеспечивая мирное использование ИКТ и поддерживая безопасность киберпространства.

Наконец, мы поддерживаем международные усилия по решению этических проблем и проблем безопасности, связанных со смертоносным автономным оружием. Вместе мы сможем решить эти сложные вопросы, соблюдая международное право и высочайшие стандарты человечества.

Г-н Сивамохан (Малайзия) (*говорит по-английски*): Малайзия присоединяется к заявлениям, сделанным представителем Индонезии от имени Движения неприсоединившихся стран и представителем Таиланда от имени Ассоциации государств Юго-Восточной Азии.

Беспрецедентная зависимость глобального общества от информационно-коммуникационных технологий (ИКТ) требует постоянного внимания к вопросам безопасности, которые выходят за рамки национальных границ, и в то же время расширение использования ИКТ открывает новые возможности для достижения общих целей. Необходимо эффективно бороться с рисками и проблемами, возникающими в результате злонамеренного использования ИКТ. В этой связи следует отметить следующее. Малайзия высоко оценивает постоянные усилия Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Мы приветствуем принятие в июле второго ежегодного доклада о проделанной работе РГОС (см. A/78/265), который закладывает прочную основу для работы Группы в предстоящем году.

Мы рады, что государства-члены достигли согласия по элементам разработки и введения в действие глобального межправительственного реестра контактных пунктов. Малайзия также надеется на проведение дополнительных целенаправленных обсуждений в рамках РГОС, в частности по вопросам угроз, которые представляют ИКТ для объектов критически важной инфраструктуры и критически важной информационной инфраструктуры, учета согласованных принципов создания потенциала ИКТ и применения норм международного права при использовании ИКТ.

Малайзия по-прежнему намерена активно участвовать в работе РГОС, которая зарекомендовала себя как ценный форум для обсуждения вопросов безопасности в сфере использования ИКТ между всеми государствами-членами при участии соответствующих заинтересованных сторон. Целостность, эффективность и авторитет РГОС также необходимо поддерживать и в процессе изучения перспективных форматов регулярного институционального диалога на период после 2025 года.

Отрадно отметить, что, как видно из второго ежегодного доклада о проделанной работе РГОС, государства-члены достигли принципиального согласия в отношении общих элементов, на которых будет основан будущий механизм регулярного институционального диалога. Эти элементы включают

> «одновекторный, возглавляемый государствами постоянный механизм под эгидой Организации Объединенных Наций, подотчетный Первому комитету» (*A/78/265, приложение, п. 55 a*)).

Государства-члены также

> «признали важность принципа консенсуса как в отношении учреждения самого будущего механизма, так и в отношении процессов принятия решений в рамках этого механизма» (*там же, п. 56*).

В этой связи Малайзия вновь заявляет, что в ключевых областях разоружения и международной безопасности следует избегать параллельных многосторонних процессов. Этот вопрос вызывает особую озабоченность у небольших делегаций из развивающихся стран, учитывая ограниченность их финансовых и людских ресурсов.

На фоне возобновившейся напряженности в отношениях между крупнейшими державами и преобладающего дефицита доверия РГОС добилась ощутимых результатов, действуя постепенно и на основе консенсуса. Это свидетельствует о добросовестности, с которой все делегации участвуют в данном процессе. Несмотря на расхождения во мнениях по конкретным вопросам, входящим в ее компетенцию, очевидно, что сама РГОС представляет собой жизненно важную меру по укреплению

доверия. Рассматривая различные предложения по дальнейшим действиям, давайте продолжим конструктивную работу, чтобы обеспечить полную реализацию потенциала РГОС в соответствии с ее мандатом. Наша делегация искренне надеется, что РГОС до конца своего срока будет оставаться одновекторной, открытой и инклюзивной платформой, способной гибко реагировать на потребности государств-членов в быстро развивающейся сфере безопасности ИКТ.

Г-н Ин ден Бош (Королевство Нидерландов) (*говорит по-английски*): В дополнение к заявлению, сделанному от имени Европейского союза, я хотел бы высказать следующие замечания в своем национальном качестве.

Информационно-коммуникационные технологии (ИКТ) являются важным фактором устойчивого развития и могут положительно влиять на жизнь людей. Однако риск неправомерного использования этих технологий государственными и негосударственными субъектами растет вместе с нашей зависимостью от них. Поэтому нам крайне важно не только поддерживать, но и укреплять правила и нормы, применимые к использованию ИКТ государствами. Мы должны использовать потенциал цифровых технологий для экономического и социального развития, обеспечивая при этом безопасность и благополучие общества в целом и отдельных людей.

Для решения этих проблем государства разработали кумулятивные и эволюционирующие нормативные рамки ответственного поведения государств при использовании ИКТ в контексте международной безопасности. Это значительное достижение. Эти рамки стали результатом длительных переговоров и усилий по укреплению доверия между государствами и поэтому пользуются поддержкой всех членов Организации Объединенных Наций. Ежегодный доклад за 2023 год о проделанной работе Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 (см. A/78/265) добавляет еще один важный компонент к этим рамкам, подтверждая применимость международного права к киберпространству и обеспечивая конкретный прогресс в создании реестра контактных пунктов. В докладе даются конкретные рекомендации по внедрению норм ответственного поведения государств, подтверждается необходимость учета гендерных аспектов в борьбе с угрозами в сфере ИКТ, а также поощряется создание потенциала с учетом гендерных аспектов. В связи с этим Нидерланды продолжат поддерживать участие женщин в Рабочей группе открытого состава в рамках программы стипендий «Женщины в киберпространстве».

Мы приветствуем результаты работы, изложенные в докладе, включая дальнейшее углубление общего понимания в вопросе о том, как конкретные принципы международного права применяются в киберпространстве. Мы также продолжаем поддерживать деятельность Рабочей группы открытого состава по наращиванию потенциала в целях содействия реализации консенсусных рамок. В целях закрепления шагов, предпринятых в ежегодном докладе о проделанной работе РГОС Нидерланды выражают надежду, что проект позиции Сингапура по одобрению доклада будет принят без голосования.

Нидерланды поддерживают инициативу по разработке программы действий, направленную на создание постоянного, инклюзивного и ориентированного на действия механизма после завершения работы нынешней Рабочей группы открытого состава в 2025 году. Программа действий должна содействовать достижению двух целей — во-первых, обеспечить дальнейший прогресс и развитие рамок ответственного поведения государств на основе консенсуса; и, во-вторых, содействовать международному сотрудничеству в деле внедрения этих эволюционирующих нормативных рамок. Эти две цели также упоминаются в заключении доклада Генерального секретаря о программе действий (A/78/76), в котором приветствуются ориентированные на конкретные действия предложения, способствующие внедрению нормативных рамок и укреплению потенциала государств в этой области.

В процессе подготовки доклада Генерального секретаря о программе действий Нидерланды предложили механизм, ориентированный на удовлетворение потребностей, для содействия наращиванию потенциала в рамках программы действий, который использовал бы существующие инициативы в системе Организации Объединенных Наций и за ее пределами. Это предложение находится в процессе разработки, и мы продолжим взаимодействовать по нему с другими государствами-членами.

Что касается поддержки инициативы по осуществлению программы действий, то Нидерланды решительно поддерживают проект резолюции A/C.1/78/L.60, представленный Францией. Проект резолюции устанавливает четкие сроки и цели создания будущего механизма для регулярного институционального диалога в 2026 году. Он придает импульс дальнейшему развитию механизма в рамках текущей Рабочей группы открытого состава и использует сбалансированный подход к возможной будущей потребности в дополнительных обязательствах, имеющих силу закона.

В заключение хочу отметить, что Нидерланды надеются на продолжение работы Рабочей группы открытого состава и на достижение ощутимого прогресса в создании более открытого, свободного, безопасного, совместимого и мирного киберпространства.

Г-н Фаусто Гонсалес (Мексика) (*говорит по-испански*): Мексика придает особое значение нашему подходу к ответственному и мирному использованию космического пространства. В нашу цифровую эпоху, когда большинство видов человеческой деятельности взаимосвязано через киберпространство, мы должны признать, что безответственное поведение в этой сфере может привести к кибератакам, геополитической напряженности и даже конфликтам.

Именно поэтому Мексика вновь заявляет о настоятельной необходимости сохранить киберпространство открытым, свободным, стабильным, безопасным, доступным и устойчивым для всех. Как мы видим, необходимость обеспечить соблюдение норм международного права, в том числе международного гуманитарного права, в киберпространстве не вызывает сомнений. Мы твердо привержены неукоснительному соблюдению норм и принципов, определяющих ответственное поведение государств в этой области. Работая в этом направлении, мы считаем необходимым соблюдать баланс между вопросами кибербезопасности, защитой прав человека и содействием развитию с помощью информационно-коммуникационных технологий (ИКТ).

Для развивающихся стран регулирование киберпространства — это не просто вопрос безопасности, а скорее необходимое условие для устойчивого использования киберпространства в широком смысле этого слова. Это инструмент, который при правильном использовании и регулировании может содействовать инновациям, гарантировать справедливый доступ к информации, укреплять нашу цифровую экономику и устранять факторы неравенства, существующие в нашем мире.

Как и многие другие государства, мы давно обеспокоены возможностью возникновения гонки за наступательным потенциалом в киберпространстве. Тревожно думать, что страны или просто частные организации могут разработать передовые наступательные мощности, которые потенциально могут привести к дестабилизирующим действиям. В связи с этим Мексика призывает к коллективным усилиям, направленным на то, чтобы киберпространство не превратилось в новое поле для соперничества.

Председатель возвращается на свое место.

Учитывая это, мы подтверждаем нашу веру в многосторонний подход. Мы считаем, что Организация Объединенных Наций, в частности Рабочая группа открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, является идеальным форматом для дальнейшей совместной работы по решению проблем, которые киберпространство и ИКТ представляют собой в контексте международной безопасности. Мы подчеркиваем значительный прогресс, достигнутый в ходе обсуждений в Группе, особенно в принятии двух ежегодных докладов о проделанной работе, создании и введении в действие глобального реестра контактных пунктов, включая другие меры по развитию сотрудничества и доверия в киберпространстве. Рабочей группе особенно важно продолжать содействовать взаимопониманию и диалогу и избегать дублирования усилий в ущерб интересам всех стран.

В заключение я призываю продолжать продуктивные и конструктивные обсуждения, которые приведут к созданию постоянного механизма для обсуждения вопросов, связанных с киберпространством. Механизм должен быть инклюзивным и предусматривать участие всех соответствующих сторон, а также международное сотрудничество, при этом он также должен обеспечивать наращивание потенциала с учетом различных региональных и субрегиональных потребностей. Обсуждение вопроса о создании постоянного институционального механизма по киберпространству, который бы предусматривал наращивание потенциала и включал нормы международного права, правила и принципы

ответственного поведения государств, а также меры по укреплению доверия, должно оставаться в числе приоритетных задач Рабочей группы. Мексика надеется, что на будущих основных сессиях Рабочей группы открытого состава мы сможем выработать еще больше рекомендаций, направленных на обеспечение мирного и справедливого киберпространства для всех.

Г-жа Лукабио (Австралия) (*говорит по-английски*): Открытое, безопасное, стабильное, доступное и мирное киберпространство приносит пользу всем нам. Ценность киберпространства, основанного на правилах, как никогда очевидна. Только киберпространство, основанное на правилах, может обеспечить стабильность и независимость, необходимые всем странам для определения своего цифрового будущего и экономического развития.

Однако киберпространство никогда еще не вызывало столько споров. В этом году мы продолжаем наблюдать неприемлемые примеры злонамеренной активности с использованием киберсредств в нашем Индо-Тихоокеанском регионе и за его пределами, в том числе нападение России на энергетическую инфраструктуру Украины. Вопросы, связанные с киберпространством, стали стратегическими вопросами внешней политики, которые остро волнуют все страны. Мы все несем ответственность за совместную работу с промышленностью, гражданским обществом и техническим сообществом над решением сложных международных проблем безопасности в киберпространстве, а также за то, чтобы направить наши усилия на укрепление мира и предотвращение конфликтов.

Австралия по-прежнему твердо привержена коллективным усилиям по решению этих проблем, в том числе усилиям, предпринимаемым в рамках Организации Объединенных Наций. Организация Объединенных Наций имеет богатый опыт в деле развития международного сотрудничества для понимания возникающих угроз и снижения рисков для международного мира и безопасности.

Мы вновь подтверждаем нашу приверженность действиям в соответствии с нормативными рамками Организации Объединенных Наций по ответственному поведению государств в киберпространстве, разработанными и согласованными на основе консенсусных докладов групп правительственных экспертов Организации Объединенных Наций и рабочих групп открытого состава. Австралия будет и впредь официально сообщать о том, как она выполняет, толкует и соблюдает эти рамки. Прозрачность ведет к подотчетности, предсказуемости и стабильности, и поэтому мы призываем все государства эффективно выполнять и добросовестно соблюдать свои обязательства в соответствии с этими рамками.

Австралия рада, что в ходе недавней пятой сессии Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 был отмечен высокий уровень участия женщин-представителей и вовлеченности заинтересованных сторон. Австралия приветствует ежегодный доклад о проделанной работе РГОС (см. A/78/265) и его недвусмысленное подтверждение рамочной программы. Мы призываем все государства серьезно отнестись к выполнению дальнейших шагов, рекомендованных в докладе, особенно к рекомендациям государствам продолжать целенаправленные обсуждения вопросов, связанных с применением международного права в киберпространстве.

Австралия придает большое значение достижению консенсуса по вопросам кибербезопасности в Организации Объединенных Наций, поскольку эти вопросы слишком важны, чтобы делить их между разными форумами. Австралия давно выступает за создание в рамках Организации Объединенных Наций постоянного механизма для содействия ответственному поведению государств в киберпространстве — механизма, который должен быть инклюзивным, прозрачным, демократическим и консенсусным.

Мы приветствуем инициативу Франции возглавить работу над проектом резолюции A/C.1/78/L.60 о разработке программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, что позволит нам эффективно противостоять возникающим угрозам международной безопасности. Австралия подчеркивает, что никакой новый постоянный механизм не станет конкурентом для своих предшественников. Режим и структура обсуждения связанных с киберпространством вопросов в рамках Организации Объединенных Наций претерпели значительные изменения со времени создания первой Группы правительственных экспертов в

2004 году, в которую входили 15 государственных экспертов, работавших в закрытом режиме, до создания в 2018 году специальных рабочих групп открытого состава, в работе которых могут участвовать все 193 государства — члена Организации Объединенных Наций. Программа действий представляет собой дальнейшую эволюцию в обсуждении вопросов киберпространства в рамках Организации Объединенных Наций, которая опирается на результаты предыдущей работы, и гарантирует, что в будущем этим вопросам будет уделяться необходимое внимание и они будут иметь то значение, которого они заслуживают.

Мы также должны работать сообща, чтобы обеспечить ответственную разработку, внедрение и использование искусственного интеллекта (ИИ) в военной сфере. Военное применение ИИ создает как новые возможности, так и потенциальные риски. Австралия будет продолжать активно участвовать в этой формирующейся международной повестке дня, в том числе в ходе саммита по ответственному использованию искусственного интеллекта в военной сфере, который пройдет в следующем году в Республике Корея. Мы высоко оцениваем ведущую роль Соединенных Штатов в принятии Политической декларации об ответственном использовании искусственного интеллекта в военных целях и его автономности. Австралия будет и впредь активно сотрудничать со всеми государствами-членами в достижении консенсуса по вопросам киберпространства и ИИ, основываясь на приверженности международному праву и нормам ответственного поведения государств.

Г-н Видаль Меркадо (Чили) (*говорит по-испански*): Чили поддерживает заявление, сделанное представителем Индонезии от имени Движения неприсоединившихся стран.

Мы считаем, что злонамеренное использование информационно-коммуникационных технологий (ИКТ) не только влияет на развитие и благосостояние государств, уровень их цифровизации, устойчивости и инфраструктуры, но и представляет собой угрозу международной безопасности. Аналогичным образом, кибератаки и злонамеренная деятельность в киберпространстве могут оказывать более сильное воздействие на определенные группы и субъекты, такие как пожилые люди, уязвимые лица, женщины и девочки. В связи с этим международное сообщество должно продолжать усилия по достижению консенсуса, гарантирующего, что наше киберпространство останется свободным, открытым, доступным, стабильным, безопасным и мирным. Чили полагает, что международное право, в частности Устав Организации Объединенных Наций, обеспечивает применимую нормативную базу для регулирования ответственного поведения государств в киберпространстве, включая международное гуманитарное право, международное право прав человека и выполнение 11 добровольных, не имеющих обязательной силы норм Организации Объединенных Наций.

Мы признаем прогресс, достигнутый Рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, особенно в отношении создания и наращивания потенциала и разработки мер по укреплению доверия. В этой связи я подчеркиваю необходимость создания в Организации Объединенных Наций глобального реестра контактных пунктов. Мы также особо отмечаем программу действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Мы должны быть в состоянии укреплять свой потенциал и создавать форумы для сотрудничества и обмена информацией, тем самым способствуя работе со всеми заинтересованными сторонами, такими как частный сектор, гражданское общество, академические круги и техническое сообщество и прочими. Мы также подчеркиваем важность более тесных региональных связей и работы с региональными организациями по внедрению рамок Рабочей группы открытого состава.

Нет никаких сомнений в том, что разоружение, нераспространение и контроль над вооружениями могут оказать положительное влияние на благосостояние людей, равенство и справедливость, и в частности на развитие во всех регионах мира, в особенности в наименее развитых странах, малых островных развивающихся государствах и развивающихся странах, не имеющих выхода к морю. Очевидно, что колоссальные военные расходы можно было бы использовать с гораздо большей пользой. Мы должны способствовать расширению представительства наименее развитых стран на многосторонних форумах, обсуждающих вопросы разоружения и международной безопасности.

Наконец, мы призываем всех членов поддержать три проекта резолюций, выдвинутых Движением неприсоединившихся стран по этому и другим тематическим блокам вопросов, и также хотели бы особо отметить проект резолюции A/C.1/78/L.19, посвященный молодежи, разоружению и нераспространению. Мы считаем, что должны способствовать повышению осведомленности нашей молодежи об этих насущных проблемах, чтобы наши лидеры и лица, которые будут принимать решения в будущем, были соответствующим образом информированы и подготовлены по этим очень непростым вопросам, что поможет нам жить в мире и строить лучший мир. Мы также выражаем благодарность гражданскому обществу, образовательным учреждениям и неправительственным организациям, занимающимся распространением информации о разоружении и международной безопасности.

Г-жа Ханлумьюанг (Таиланд) (*говорит по-английски*): Таиланд присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Ассоциации государств Юго-Восточной Азии (АСЕАН).

Кибербезопасность — один из самых важных вопросов в современном взаимосвязанном мире. Неправомерное использование информационно-коммуникационных технологий (ИКТ) все чаще становится серьезной угрозой для международного мира и безопасности, а также для всего человечества. Нам необходимо стремиться к открытому, безопасному, надежному, стабильному, доступному, совместимому, мирному и устойчивому киберпространству. Для достижения этой цели Таиланд хотел бы еще раз подчеркнуть следующие четыре важных момента.

Во-первых, Таиланд подтверждает важность основанного на правилах киберпространства для предотвращения злоумышленных деяний и конфликтов в киберпространстве. Мы подтверждаем нашу давнюю позицию, что международное право, в частности Устав Организации Объединенных Наций, применимо в контексте ИКТ. Дополняя международное право, 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств в киберпространстве служат очень прочной основой для укрепления доверия между государствами. Важно, чтобы государства продолжали формировать понимание того, как международное право применяется в контексте ИКТ, и выявлять существующие пробелы. Государства должны совместно разработать дополнительные рекомендации, включая контрольный список по внедрению норм.

Во-вторых, регулярные институциональные диалоги, которые носят открытый, инклюзивный и прозрачный характер, служат необходимой платформой для обсуждения вышеупомянутых вопросов. Диалоги также могут стать площадкой для обмена передовым опытом и активизации усилий по наращиванию потенциала. Текущая Рабочая группа открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 остается важнейшей основой для такого обсуждения. Мы выражаем благодарность послу Сингапура Бурхану Гафуру за его достижения на посту председателя, результатом которых стало успешное принятие ежегодного доклада о проделанной работе (см. A/78/265) на основе консенсуса. Таиланд приветствует предложение о создании будущего механизма для содействия регулярному институциональному диалогу по этому вопросу, включая программу действий. Мы выступаем за создание постоянного одновекторного механизма под руководством государств и под эгидой Организации Объединенных Наций.

В-третьих, Таиланд подчеркивает важнейшую роль мер по укреплению доверия в упрочении доверия между государствами в киберпространстве на всех уровнях. Таиланд приветствует конкретные результаты работы РГОС по разработке и введению в действие глобального межправительственного реестра контактных пунктов, который мог бы способствовать обеспечению безопасной и прямой коммуникации между государствами для предотвращения и устранения серьезных инцидентов в сфере ИКТ и ослабления напряженности в кризисных ситуациях. Не менее важно повышать эффективность мер по укреплению доверия с помощью региональных усилий. Что касается стран АСЕАН, инициативы и механизмы, связанные с мерами укрепления доверия, включают Стратегию сотрудничества АСЕАН в области кибербезопасности на 2021–2025 годы, Координационный комитет АСЕАН по кибербезопасности и Межсессионную встречу Регионального форума АСЕАН по безопасности и использованию информационно-коммуникационных технологий.

Наконец, Таиланд признает необходимость программ по наращиванию потенциала для оказания помощи государствам в повышении их потенциала в области противодействия киберугрозам, а также в имплементации норм и международного права. Мы призываем государства, которые в состоянии сделать это, продолжать поддерживать такие программы, которые должны быть устойчивыми, политически нейтральными, прозрачными и ориентированными на спрос. В этой связи мы хотели бы поблагодарить Японию за постоянную поддержку Центра по укреплению потенциала в области кибербезопасности АСЕАН — Япония в Бангкоке с 2018 года.

В заключение я хочу сказать, что Таиланд намерен активно взаимодействовать со всеми сторонами для преодоления разногласий и формирования более безопасной, надежной и стабильной среды ИКТ.

Г-н Саади (Ирак) (*говорит по-арабски*): Прежде всего делегация Ирака хотела бы присоединиться к заявлениям, сделанным представителем Иордании от имени Группы арабских государств и представителем Индонезии от имени Движения неприсоединившихся стран.

Делегация Ирака присоединяется к призывам к израильскому образованию прекратить жестокие обстрелы безоружных гражданских лиц в секторе Газа. Мы подчеркиваем необходимость прекращения огня и доставки гуманитарной помощи, чтобы положить конец гуманитарным страданиям людей в Секторе и их систематическому принудительному перемещению,

Продолжающееся обладание военными арсеналами, их модернизация и наращивание, а также рост международной и региональной напряженности сопровождаются ускорением гонки вооружений и ростом глобальных военных расходов, что в совокупности представляет серьезную угрозу для международного и регионального мира и безопасности. По этой причине мы все должны принять срочные и реальные меры для снижения таких угроз и укрепления международного и регионального мира и безопасности, чтобы достичь целей в области устойчивого развития к 2030 году.

Делегация Ирака подчеркивает, что содействие всеобщему присоединению к конвенциям и договорам по разоружению, в том числе применительно к оружию массового уничтожения, особенно ядерного оружия, является единственной гарантией неприменения или угрозы применения такого оружия и предотвращения его катастрофических последствий. Это оружие смертельно опасно и разрушительно как для людей, так и для окружающей среды. Согласованные решения, достигнутые Организацией Объединенных Наций в контексте многосторонних отношений, являются единственной надежной гарантией решения проблем разоружения и международной безопасности. Следовательно, необходимо подтвердить и выполнить индивидуальные и коллективные обязательства, принятые на международном, многостороннем уровне. Необходимо также, чтобы Организация Объединенных Наций играла ключевую роль в области разоружения и нераспространения.

Делегация Ирака выражает растущую озабоченность в связи с усилением напряженности международной и региональной обстановки в плане безопасности. Это приводит к росту использования информационно-коммуникационных технологий (ИКТ) в деятельности, ставящей под угрозу региональный и международный мир и безопасность. В этой связи Ирак приветствует принятие второго ежегодного доклада о проделанной работе (см. A/78/265) Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, созданной в соответствии с резолюцией 75/240 от 2020 года, а также приветствует исключительные усилия, предпринятые Председателем Рабочей группы послом Бурханом Гафуром. Мы готовы полностью поддержать его и приложить все усилия для обеспечения успешной работы будущих сессий, чтобы принять рекомендации, которые поддержат все государства, особенно развивающиеся, и помогут им справляться с проблемами и рисками, возникающими при использовании ИКТ, на форе растущих угроз в этой области. Это поможет создать безопасное и надежное киберпространство, доступное для всех.

Г-н Ахмед (Пакистан) (*говорит по-английски*): Мы стоим на пороге монументального сдвига в технологической истории человечества, который ознаменовался появлением искусственного интеллекта (ИИ). Неотвратимое шествие ИИ от алгоритмов к оружию продолжается без надлежащих защитных механизмов, которые бы регулировали его проектирование, разработку и внедрение. Мы также стоим на пороге новой гонки вооружений, где алгоритмы

будут играть ведущую роль. По мере того как ИИ выходит на поле боя, вполне резонно задаться вопросом, будут ли люди по-прежнему контролировать его и «держать руку на тумблере», и если да, то в какой степени.

Эти новые военные средства и мощности, созданные с помощью технологий, в отсутствие человеческого контроля могут повысить ядерные риски, увеличить вероятность просчетов и аварий и спровоцировать асимметричные меры реагирования, тем самым снижая порог для применения силы и развязывания вооруженных конфликтов. В условиях кризиса низкий порог для применения силы будет иметь крайне дестабилизирующий эффект. Эти новые инструменты также способны изменить динамику конфликта, скорректировать стратегии сдерживания, усилить гонку вооружений, создать непредвиденные модели эскалации и повысить новые риски в и без того сложной ситуации в области международной безопасности.

Хотя некоторые государства подчеркивают преимущества использования ИИ в ходе военного конфликта, не менее важно обратить внимание на огромные риски и потенциально катастрофические последствия. Окно возможностей для принятия мер и создания защитных механизмов стремительно сокращается, поскольку мы стоим на пороге нового технологического прорыва. Если не принять меры по устранению этих серьезных рисков для мира и безопасности, то государства, оказавшись перед лицом существующих асимметричных угроз, будут вынуждены защищать себя с помощью имеющихся в их распоряжении мощностей. Отрадно видеть растущее число региональных инициатив и многосторонних усилий, направленных на устранение опасений, связанных с военным потенциалом ИИ. Мы также высоко оцениваем призыв Генерального секретаря к управлению ИИ.

Реакция многостороннего механизма была довольно скромной и недостаточной. Обсуждения в рамках Конвенции по конкретным видам обычного оружия (КОО) в основном сосредоточены на применении международного гуманитарного права и направлены на решение только тех проблем, которые связаны со смертоносными автономными системами вооружений (САС). В них не рассматривается ни более широкая проблематика развития ИИ во всех сферах его военного применения, включая интеграцию в существующие области, ни их влияние на безопасность и стабильность на глобальном и региональном уровнях.

В Первом комитете группой стран впервые был представлен новый проект резолюции (A/C.1/78/L.56) по САС. Мы считаем, что дискуссии по САС должны продолжаться в группах правительственных экспертов в рамках КОО с целью разработки международных правил на основе нового протокола. Параллельно с этим другие органы по разоружению могут и должны играть вспомогательную роль в решении более широкой проблемы использования ИИ в военных целях таким образом, чтобы обеспечить положительный синергетический эффект, избегая дублирования.

Масштаб проблем, возникающих в результате использования ИИ в военных целях, в том числе в системах вооружения, требует многопланового и целостного подхода к реагированию. В связи с этим Пакистан представил в этом году на Конференции по разоружению рабочий документ с предложениями включить в повестку дня пункт, посвященный обсуждению последствий применения ИИ в военных целях для безопасности и стабильности.

Использование информационно-коммуникационных технологий (ИКТ) и киберпространства в военных целях представляет собой огромную угрозу миру, безопасности и стабильности как на глобальном, так и на региональном уровне. Уникальные различия между физическим пространством и киберпространством, а также степень и сфера применимости существующего международного права и его толкование требуют ускоренного рассмотрения, разработки и развития соответствующих норм и правил, регулирующих порядок использования киберпространства. Текущие обсуждения в Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности могут помочь прийти к общему пониманию, которое станет основой для дальнейших нормотворческих усилий по недопущению превращения киберпространства в еще одну сферу конфликта.

Мы также рады быть участниками совместного заявления представителя Китая о развитии международного сотрудничества в области мирного использования в контексте международной безопасности. Право всех государств на использование науки и техники в мирных целях в соответствии с

их международными обязательствами должно быть гарантировано на недискриминационной основе без каких-либо необоснованных ограничений. Усилия по регулированию материалов и технологий двойного назначения должны предприниматься в рамках Организации Объединенных Наций и на инклюзивных многосторонних площадках.

Г-н Морико (Кот-д'Ивуар) (*говорит по-французски*): Наша делегация присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран, и в своем национальном качестве хотела бы высказать следующие соображения.

Хотя угрозы безопасности, связанные с цифровыми технологиями, появились сравнительно недавно, они, тем не менее, являются одними из самых сложных и настораживающих. Действительно, число случаев враждебного использования киберпространства государственными и негосударственными субъектами постоянно растет, причем формы, которые они принимают, быстро эволюционируют, порой оказывая серьезное влияние на все аспекты человеческой жизни. Это явление не имеет пространственных границ, что серьезно угрожает миру и стабильности во всем мире и требует принятия решительных мер.

Любой по-настоящему эффективный ответ на этот вызов, выходя за рамки национальных границ, должен также осуществляться на международном и многостороннем уровне. Среди прочего он должен сосредоточиться на защите критически важной инфраструктуры и критически важной информационной инфраструктуры, которые все чаще подвергаются изощренным атакам, вызывающим серьезные сбои в работе, наносящим финансовый ущерб и даже угрожающим жизни людей. Особое внимание следует уделить поощрению региональных усилий по обмену опытом и передовой практикой, таких как форум «Кибер-Африка», состоявшийся 24–25 апреля в Кот-д'Ивуаре и посвященный защите критически важной инфраструктуры от киберугроз.

Кроме того, важно вести работу по предотвращению использования киберпространства для пропаганды, планирования и логистики терроризма, в частности путем более эффективного выполнения Крайстчерчского призыва к действиям по ликвидации в интернете материалов, пропагандирующих терроризм и насильственный экстремизм, который наша страна подписала в сентябре 2019 года.

Важно также укреплять рамки ответственного поведения государств, созданные под эгидой Организации Объединенных Наций, подчеркивая нашу приверженность более глубокому анализу в рамках Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Результаты обсуждений в рамках Группы вызывают обоснованный оптимизм у нашей делегации, которая в этом году вновь присоединилась к консенсусу по второму ежегодному докладу о проделанной работе (см. A/78/265), основанному на динамичном и реалистичном подходе, в том числе в отношении последующих шагов.

Наша делегация приветствует, в частности, создание глобального межправительственного реестра контактных пунктов, цель которого — активизировать взаимодействие и сотрудничество государств для повышения прозрачности и предсказуемости, способствуя тем самым сохранению международного мира и безопасности. Наша страна также приветствует продолжающиеся обсуждения требований и условий для разработки программы действий по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности. Кот-д'Ивуар решительно поддерживает программу действий, которая, опираясь на деятельность Рабочей группы, будет служить инклюзивным и ориентированным на практические действия постоянным механизмом, реагирующем на потребности международного сообщества в процессе непрерывной адаптации к постоянно меняющимся вызовам в области безопасности.

В частности, наша страна поддерживает концепцию обновленного подхода к наращиванию потенциала государств, особенно наиболее уязвимых. Такой подход, безусловно, благоприятно скажется на способности государств реагировать на киберинциденты. Это необходимо для того, чтобы укрепить потенциал всех государств по внедрению рамок ответственного поведения с целью расширения их сферы действия и создания мирной, надежной и устойчивой цифровой среды. Поэтому наша делегация в прошлом и в этом году стала автором проекта резолюции, поддерживающего этот механизм, и настоятельно призывает к благоприятному завершению дискуссий о его создании.

Г-жа Гонсалес Лопес (Сальвадор) (*говорит по-испански*): Информационно-коммуникационные технологии (ИКТ) являются основополагающими инструментами в современном мире, однако их использование, не соответствующее правилам ответственного поведения государств в киберпространстве, и нарушение ими норм международного права, в частности Устава Организации Объединенных Наций, создают серьезные проблемы для международной безопасности.

Сальвадор в полной мере осознает, что киберсредства все чаще используются для создания угроз объектам критически важной инфраструктуры, критически важной информационной инфраструктуре и глобальным цепочкам поставок. Эти угрозы требуют серьезного обсуждения вопросов, связанных с регулированием ответственного поведения и международного права в киберпространстве, а также принятия мер по укреплению доверия и развитию потенциала и институционального диалога. Эти обсуждения проходят в Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в работе которой наша страна принимает конструктивное участие. Мы считаем, что Группа проводит важнейшую работу по выработке общего понимания и сближению позиций по вопросам, связанным с киберпространством.

Несмотря на прогресс, достигнутый Сальвадором в сфере кибер- и цифровых технологий, концептуально мы поддерживаем дальнейшее развитие этих дискуссий в постоянном и инклюзивном формате под эгидой Организации Объединенных Наций. По этой причине мы представили точку зрения нашей страны и приняли участие в консультациях, чтобы предложить элементы по охвату, структуре и содержанию будущей программы действий по ответственному поведению государств в киберпространстве.

В ходе этой сессии Первый комитет заслушал многих представителей, которые говорили о последствиях появления новых технологий, в частности искусственного интеллекта (ИИ), для международной безопасности. Наша страна на соответствующих форумах решительно заявляла о рисках, связанных, например, с генеративным искусственным интеллектом и машинным обучением, и в то же время мы видим значительные возможности для совершенствования наших систем кибербезопасности за счет использования ИИ. Мы призываем к тому, чтобы использовать подход к кибербезопасности с точки зрения ИИ, а не подход к ИИ с точки зрения кибербезопасности.

Мы настоятельно призываем регулировать и поощрять использование ИИ с учетом соответствующих рисков и проводить углубленные обсуждения о моделях управления этой технологией, а также постоянно анализировать потенциальные угрозы и вызовы, имеющие последствия для международной безопасности. Кроме того, необходимо подчеркнуть, что использование ИИ в сфере безопасности выходит за рамки автономных систем вооружения, распространяясь на новые направления, где основной упор делается на автоматизацию, а не только на автономность. Мы призываем к целостному рассмотрению ИИ, поскольку природа этой технологии, ее применение и использование затрагивают все аспекты человеческой жизни, включая те, которые не имеют прямого отношения к безопасности. Эта зависимость от технологий стремительно развивается и требует серьезного обсуждения.

В Первом комитете Сальвадор выступал за комплексный гендерный подход как важнейший инструмент для понимания различий в опыте женщин и мужчин в вопросах безопасности. Киберпространство не является исключением. Не вызывает сомнений, что гендерное насилие может усугубляться за счет использования ИКТ.

Наконец, Сальвадор придает большое значение участию многих сторон в этих процессах. Вызовы, связанные с киберпространством, требуют активного сотрудничества гражданского общества, неправительственных организаций, региональных организаций, академических кругов и промышленности. Поэтому мы настоятельно призываем государства-члены и впредь опираться на ценный вклад этих участников в наши обсуждения.

Г-н Мухитх (Бангладеш) (*говорит по-английски*): Бангладеш присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран. Позвольте мне изложить национальную позицию нашей страны.

Быстро меняющаяся ситуация в сфере глобальной безопасности, обусловленная стремительным развитием технологий, неоспоримо подчеркивает необходимость принятия разнообразных мер по разоружению, выходящих за рамки традиционных.

Бурное развитие технологий, особенно в области искусственного интеллекта (ИИ), автономных систем вооружений, биотехнологий и киберпотенциала, произвело революцию не только в нашей повседневной жизни, но и в сфере глобальной безопасности. Эти новые технологии открыли неограниченные возможности для развития человечества и экономического роста. Однако при этом они также принесли с собой новые риски, требующие принципиально новых решений в области разоружения.

Бангладеш глубоко обеспокоена развитием военного потенциала ИИ и появлением квантовых технологий, особенно связанных с системами вооружений, которые выявили недостаточность существующих систем управления. Наша первоочередная обязанность заключается в использовании ИИ для достижения мира, а не для продолжения конфликтов. Поэтому мы подчеркиваем настоятельную необходимость разработки комплексных рамочных механизмов для эффективного регулирования ИИ и новых технологий, чтобы обеспечить их ответственное, эффективное и этичное использование.

Мы твердо убеждены, что киберпространство необходимо рассматривать как глобальное общественное благо, которое должно служить в интересах всех людей во всем мире без какой-либо дискриминации. Для того, чтобы воспользоваться огромными преимуществами цифровых технологий, международное сообщество должно создать безопасную, защищенную, надежную и открытую среду информационно-коммуникационных технологий (ИКТ) на основе применимости международного права к киберпространству, четко определенных норм ответственного поведения государств, эффективных мер укрепления доверия и скоординированных усилий по наращиванию потенциала. Единственной возможностью обеспечить свободную, безопасную, стабильную, доступную и мирную среду ИКТ является многосторонний подход, и мы подчеркиваем, что Организация Объединенных Наций должна играть ведущую роль в разработке международных кибернорм.

В этой связи Бангладеш рассматривает Рабочую группу открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 в качестве центрального и всеобъемлющего механизма в рамках Организации Объединенных Наций. Мы вновь подтверждаем наше конструктивное участие в успешной работе РГОС и приветствуем принятие консенсусом двух ежегодных докладов о проделанной работе РГОС подряд. В соответствии со вторым ежегодным докладом о проделанной работе (см. A/78/265) мы поддерживаем идею создания в рамках Организации Объединенных Наций одновекторного постоянного механизма, возглавляемого государствами. Мы также поддерживаем создание открытого, инклюзивного, прозрачного, устойчивого и гибкого процесса, способного эффективно удовлетворять меняющиеся потребности развивающихся стран в условиях динамично меняющейся ситуации в области ИКТ.

Мы считаем, что в отсутствие общепринятой структуры норм принципы Устава Организации Объединенных Наций и соответствующего международного права должны применяться к киберпространству для поддержания мира и стабильности. В Бангладеш мы осуществляем инвестиции в развитие надлежащей культуры кибербезопасности в правительстве и обществе. Мы разработали необходимые механизмы, политику и стратегии, включая недавно принятый Закон о кибербезопасности 2023 года, и 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 внедрению и соблюдению соответствующих экологических норм в рамках международного правового режима, касающегося разоружения и контроля над вооружениями. Вопрос о применимости или актуальности таких правовых норм к разоружению на морском дне и в космическом пространстве должен стать предметом дальнейших обоснованных исследований и анализа. Образование является основополагающим фактором, способствующим пониманию гуманитарных и экономических последствий вооружения. Бангладеш подчеркивает важность образования в области разоружения и нераспространения. Мы высоко оцениваем важную работу, проводимую Институтом Организации Объединенных Наций по исследованию проблем разоружения, и подчеркиваем необходимость выделения дополнительных и прогнозируемых ресурсов для обеспечения деятельности Института по расширению и управлению его базой знаний на благо всех государств-членов.

В заключение хочу сказать, что в центре наших усилий по разоружению должны быть люди, и мы должны добиваться разоружения, которое спасает жизни сегодня и будет спасать их завтра. Давайте продолжать работать сообща в целях обеспечения более безопасного мира.

Г-н Эустатиу де лос Сантос (Уругвай) (*говорит по-испански*): Уругвай разделяет обеспокоенность многих государств-членов по поводу участившихся случаев злонамеренной деятельности в области информационно-коммуникационных технологий (ИКТ), особенно тех, которые влияют на уязвимость секторов, связанных с критически важной инфраструктурой, здравоохранением, безопасностью и обороной. Такая злонамеренная деятельность является реальной и растущей проблемой и требует более тесного сотрудничества между государствами, а также между государственным и частным секторами для защиты целостности, функций и доступности киберпространства.

В Уругвае мы работаем над укреплением нашего Национального центра реагирования на инциденты в сфере компьютерной безопасности, расширяя его деятельность по реагированию и мониторингу, чтобы свести к минимуму время, необходимое для обнаружения и реагирования на инциденты, снизить риски и добиться значительной экономии для страны. Уругвай считает, что для устранения этих реальных и потенциальных угроз нам необходимо продолжать работу по расширению сотрудничества и наращиванию потенциала, учитывая различия между странами в решении проблемы злонамеренного использования ИКТ. Мы полагаем, что наращивание потенциала в первую очередь призвано гарантировать безопасное, эффективное и значительное участие всех государств в киберпространстве, чтобы воспользоваться теми возможностями устойчивого развития, которые оно предоставляет. При этом механизмы сотрудничества, такие как традиционное сотрудничество по направлениям Север — Юг, Юг — Юг и трехстороннее сотрудничество, будут обеспечивать конкретные меры по оказанию технической помощи для наращивания потенциала, в том числе направленные на реализацию 11 норм Организации Объединенных Наций по обеспечению ответственного поведения государств в киберпространстве.

Уругвай подтверждает важность обмена передовым национальным опытом в области предотвращения цифровых угроз. Наша страна участвует в обмене опытом с рядом стран нашего региона через наше правительственное агентство по ИКТ. Мы также признаем ключевую роль Организации Объединенных Наций в осуществлении мер по укреплению доверия и содействии их реализации во всем мире, что было недавно подчеркнуто в докладах Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (A/76/135) и Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 (см. A/78/265).

Технологические разработки должны идти рука об руку с надежными институтами, системой, признающей права человека, и юридически защищенной и надежной средой. Как общество, мы имеем не только общие обязательства, но и права и возможности. Совместное внедрение нормативной базы должно осуществляться скоординированно, с учетом мнений всех членов и на основе ориентированного на человека подхода.

В связи с этим наша страна разработала комплексную программу, которую мы называем «Цифровая повестка Уругвая», в рамках которой мы рассматриваем нормативную базу и способствуем повышению осведомленности о ней в сотрудничестве со всеми заинтересованными сторонами. Для нас цифровая трансформация идет рука об руку с правовой определенностью. Поэтому мы содействуем нормативным изменениям, необходимым для учета технологического прогресса, уделяя первостепенное внимание совершенствованию административных процедур, механизмов обмена информацией между государственными и частными структурами, а также цифровому управлению бизнес-процессами.

Наша делегация считает, что при принятии нормативно-правовых актов мы должны уделять особое внимание вопросам доступности, авторского права, прав потребителей, честной конкуренции, защиты данных, безопасности, прозрачности и киберпространства, а также способствовать соблюдению соответствующих международных стандартов и конвенций.

Г-жа Муйгаи (Кения) (*говорит по-английски*): Кения присоединяется к заявлениям, сделанным представителями Нигерии и Индонезии от имени соответственно Группы африканских государств и

Движения неприсоединившихся стран. Я бы хотела озвучить несколько дополнительных замечаний в своем национальном качестве.

Мы выражаем благодарность Постоянному представителю Сингапура, Председателю Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, за брифинг, который он вскоре проведет. Мы высоко оцениваем значительный прогресс, достигнутый Рабочей группой открытого состава под его руководством, и ожидаем дальнейших ощутимых результатов в этой важнейшей области.

В нашу цифровую эпоху всепроникающее влияние технологий формирует наше глобальное общество, которое становится все более взаимосвязанным. Действительно, в эпоху стремительного развития цифровых технологий наше восприятие безопасности и наш образ жизни, в том числе в сфере дипломатии, подвергаются соответствующему переосмыслению. Обеспечить хрупкое равновесие между инновациями и предотвращением злонамеренных действий — задача первостепенная, но очень непростая. Более того, она требует коллективных глобальных усилий на основе многостороннего подхода.

В этой связи наша главная задача ясна — определить правила, нормы и принципы ответственного поведения государств в области нашей безопасности и использования информационно-коммуникационных технологий. Учитывая стремительный технологический прогресс, остро встает вопрос о создании среды ответственности, обеспечивающей кибербезопасность и ответственное развитие глобального цифрового сотрудничества. Решая эту всеобъемлющую задачу, мы должны учитывать инициативы государств, которые внедрили значительные инновации и стали первопроходцами в области цифровой безопасности. Мы призываем эти государства проявить великодушие и поделиться соответствующей информацией и передовым опытом, оказывая поддержку другим странам в развитии их собственной инфраструктуры кибербезопасности.

Организация Объединенных Наций также должна активно поддерживать страны в укреплении цифрового потенциала и решении проблем, связанных с последствиями цифровой революции, включая неправомерное использование искусственного интеллекта, больших данных и социальных сетей. В этой связи следует продолжать и укреплять сотрудничество и координацию в области наращивания потенциала, используя существующие специализированные многосторонние агентства и организации, такие как Глобальный форум по обмену опытом в области компьютерных технологий. Крайне важно также постоянно изучать и анализировать непрерывно меняющуюся ситуацию с киберугрозами. Имея понимание существующих и потенциальных угроз в сфере информационной безопасности, мы можем инвестировать в превентивные и упреждающие меры на основе сотрудничества, взаимодействия и координации.

Стремясь обеспечить безопасность своего цифрового пространства, Кения, в частности, создала Национальную кенийскую группу реагирования на компьютерные инциденты, внедрила национальную инфраструктуру открытых ключей и недавно открыла Национальный координационный комитет по компьютерным и киберпреступлениям, в состав которого входят представители соответствующих министерств и ведомств и который располагает полноценным секретариатом для обеспечения эффективного исполнения решений.

В заключение делегация Кении подчеркивает, что, как указано в нашем мандате, регулярный институциональный диалог имеет первостепенное значение не только для того, чтобы голос каждой страны был услышан, но и для того, чтобы мы коллективно учились, действовали и развивались сообща. Пусть нашей общей целью будет создание инклюзивного цифрового пространства, безопасного и надежного для нынешнего и будущих поколений.

Г-н Гужман ди Соза (Тимора-Лешти) (*говорит по-английски*): В качестве развивающегося государства Тимор-Лешти разделяет со многими государствами преимущества и угрозы, связанные с использованием информационно-коммуникационных технологий (ИКТ) в процессе государственного строительства и развития страны. Это включает в себя поддержание мира и безопасности на основе уважения национального суверенитета всех членов и в соответствии с правилами мирного использования ИКТ, изложенными в Уставе Организации Объединенных Наций.

Недавняя пандемия коронавирусной инфекции показала нам важность наличия мощных ресурсов в области безопасности ИКТ. Мы должны уделять особое внимание потребностям развивающихся

стран с точки зрения реализации существующих правил и их дальнейшего развития. Все более широкое развитие ИКТ, а также возникающие угрозы в киберпространстве могут нанести вред нашей жизни. Будучи небольшим государством, Тимор-Лешти убежден в важной роли этой многосторонней платформы, поскольку она обеспечивает более широкие возможности для диалога между всеми, помогая преодолеть разногласия между странами и убедиться в том, что все смогут воспользоваться преимуществами, которые принесут нам ИКТ.

В качестве страны, только начинающей процесс цифровизации государства, Тимор-Лешти по-прежнему обеспокоен растущей угрозой кибератак на объекты критически важной инфраструктуры и критически важную информационную инфраструктуру. Развивающиеся государства по-прежнему сталкиваются с различными проблемами при реагировании на киберугрозы. Поэтому Тимор-Лешти считает, что координация и сотрудничество, а также обмен передовым опытом в рамках двусторонних, региональных и многосторонних платформ будут способствовать поддержке и укреплению национальных структур. В этой связи мы полагаем, что предыдущие Группа правительственных экспертов и Рабочая группа открытого состава (РГОС) дополняли друг друга в своей работе и представляли собой динамичные платформы для укрепления сотрудничества и взаимодействия по вопросам кибербезопасности.

Пользуясь случаем, мы также хотели бы отметить работу Сингапура по руководству деятельностью нынешней Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 и подчеркнуть ее центральную роль в обсуждении вопросов ИКТ и обеспечения международного мира и безопасности под эгидой Организации Объединенных Наций. Мы приветствуем принятие ежегодного доклада о проделанной работе за 2023 год (см. A/78/265) и создание глобального реестра контактных пунктов; в настоящее время мы разрабатываем наши внутренние процедуры для этого процесса.

Что касается будущих механизмов регулярного институционального диалога, то Тимор-Лешти приветствует предложение о разработке будущей программы действий по кибербезопасности — мы рассматриваем ее в качестве возможной основы, которая является всеохватной, открытой, прозрачной и эффективной под эгидой Организации Объединенных Наций. Тем не менее, мы хотим подчеркнуть, что РГОС остается надлежащим форумом для разработки программы действий и ее утверждения, поскольку это инклюзивный механизм, отражающий интересы всех государств. Мы также считаем, что если мы хотим, чтобы программа действий была принята всеми, она должна быть направлена на меры по укреплению доверия, особенно в отношении развивающихся стран, чтобы удовлетворить их потребности, например в укреплении потенциала, чтобы предоставить всем возможность и расширить применение установленных норм, включая устранение правовых пробелов в применимости международного права к киберпространству. Соответственно, мы приветствуем дальнейшее обсуждение предложений, включая конкретные детали, такие как организационные вопросы, для целей нашей подготовки.

Мы хотели бы подчеркнуть необходимость укрепления многостороннего сотрудничества, чтобы держать руку на пульсе в том, что касается стремительно меняющейся обстановки в плане безопасности, включая события в киберпространстве. Мы считаем, что меры по повышению уровня доверия являются исключительно важным инструментом для создания атмосферы доверия и предотвращения конфликтов. В этой связи мы подтверждаем нашу приверженность созданию механизма разоружения и подчеркиваем необходимость равного участия женщин в работе такого механизма.

Мы также хотели бы присоединиться к заявлению, с которым выступил представитель Индонезии от имени Движения неприсоединения, и подчеркнуть важность обеспечения того, чтобы использование информации, связи и технологий полностью соответствовало целям и принципам Устава Организации Объединенных Наций и международного права. Тимор-Лешти придает большое значение поддержанию международного правового режима, касающегося разоружения и контроля над вооружениями. Его применимость к киберпространству важна для поддержания мира и стабильности. Наше правительство вкладывает значительные средства в процесс цифровизации, и в настоящее время мы разрабатываем необходимые механизмы, стратегию и политику в области киберпространства. В этой связи мы стремимся к сотрудничеству со всеми в процессе нашей деятельности, особенно в плане наращивания потенциала.

Наконец, мы считаем, что взаимодействие с соответствующими секторами, такими как частный сектор, поможет государствам, особенно развивающимся, понимать характер угроз, сотрудничать и надлежащим образом реагировать на них, что позволить повысить эффективность этого процесса.

Г-жа Родригес Мансия (Гватемала) (*говорит по-испански*): Международная обстановка характеризуется угрозами миру, часто совершаемыми актами, направленными против мировой безопасности, а также бедствиями, затрагивающими наиболее уязвимые слои нашего общества. Несмотря на это, развитие информационно-коммуникационных технологий (ИКТ) идет гигантскими шагами, требуя от нас более глубокого понимания и укрепления национального потенциала и сотрудничества в киберпространстве. Киберпространство стало критически важной областью для глобальной деятельности в силу того, что оно одновременно носит гражданский характер, и имеет двойное назначение. Оно также неоднократно использовалось преступными группировками и террористами. Поэтому его защита на основе ответственного поведения государств является важнейшим условием обеспечения международного мира и безопасности.

Особую тревогу вызывает тот факт, что ряд государств разрабатывает ИКТ для военных целей, что делает все более вероятным использование этих технологий в ходе будущих конфликтов между государствами. Такая деятельность представляет собой совокупность условий, требующих участия и сотрудничества всех секторов наших стран для разработки технической и правовой основы для укрепления киберпространства на глобальном и национальном уровнях. Поэтому наша страна полностью убеждена в необходимости продолжать содействовать работе по наращиванию потенциала как важнейшему компоненту сотрудничества между государствами в продвижении мер по укреплению доверия в области безопасности средств ИКТ. Я вновь заявляю о том, что необходимо обеспечивать полную прозрачность и поддерживать обмен информацией и распространение передового опыта на субрегиональном, региональном и международном уровнях.

Наша делегация подчеркивает особую важность применения международного права к поведению государств в киберпространстве, добровольных необязательных норм поведения государств в мирное время и осуществления мер по укреплению доверия, а также необходимость выявления пробелов между странами в области кибербезопасности и обороны. Наша страна особенно заинтересована в усилиях по наращиванию потенциала с целью создания более справедливого киберпространства, которое поможет сохранить баланс в контексте международной безопасности.

Гватемала приняла национальную стратегию кибербезопасности, основными целями которой являются укрепление потенциала нашей страны, создание среды и условий, необходимых для обеспечения участия, развития и осуществления прав человека в киберпространстве. Кроме того, за последний год Гватемала добилась значительного прогресса в разработке закона о кибербезопасности. Наша страна имеет честь быть наблюдателем Конвенции Совета Европы о киберпреступности, которая направлена на борьбу с цифровой и интернет-преступностью путем гармонизации законодательства между странами, совершенствования методов расследования и развития сотрудничества между государствами.

Поэтому мы приветствуем принятие второго ежегодного доклада (см. A/78/265) о проделанной работе Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. Мы подчеркиваем важность проекта резолюции A/C.1/78/L.60, направленного на содействие разработке программы действий по созданию постоянного механизма ответственного поведения государств в области использования ИКТ в контексте международной безопасности, который Гватемала поддерживает. В этой связи мы принимаем к сведению рекомендации Генерального секретаря, содержащиеся в Новой повестке дня для мира, в которых предлагается создать независимый многосторонний механизм подотчетности в отношении злонамеренного использования государствами киберпространства.

Наконец, мы напоминаем всем государствам, что ИКТ должны использоваться в мирных целях и для блага человечества, способствуя устойчивому развитию всех стран, независимо от уровня их научно-технического развития.

Г-н Варем (Эстония) (*говорит по-английски*): Эстония присоединяется к заявлению, с которым выступил наблюдатель от Европейского союза. Кроме того, мы хотели бы в нашем национальном качестве особо отметить следующие моменты.

Предотвращение и устранение угроз международному миру и безопасности, в том числе угроз, возникающих в результате злонамеренного использования киберпространства, имеет для Эстонии первостепенное значение. Угрозы, связанные с использованием информационно-коммуникационных технологий (ИКТ), развиваются и усугубляются, вызывая все большую озабоченность в отношении национальной и международной безопасности. Инциденты, связанные со злонамеренными действиями в киберпространстве, могут иметь разрушительные последствия для целей экономического и социального развития и критически важной инфраструктуры, а также оказывать непосредственное влияние на международную стабильность.

В частности, незаконное и неспровоцированное вторжение России на Украину продемонстрировало, как кибероперации используются для содействия достижению военных целей и становятся частью военных операций. В ходе российской агрессии объектами нападения в киберпространстве стали украинские государственные органы, объекты критически важной инфраструктуры, местные органы власти, сектор безопасности и обороны, а также частные компании. Злонамеренные кибероперации также продемонстрировали опасный побочный эффект, подчеркивающий трансграничный характер киберугроз.

Эстония решительно осуждает подобные злонамеренные кибероперации. Мы подчеркиваем, 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. Государствам — членам Организации Объединенных Наций необходимо объединить усилия для укрепления основанного на правилах международного порядка и придерживаться его и в киберпространстве. Мы напоминаем, что любое использование государствами ИКТ в нарушение их обязательств в соответствии с рамками ответственного поведения государств подрывает международный мир и безопасность, а также стабильность и доверие между государствами-членами.

Эстония высоко оценивает деятельность Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 и приветствует согласование ежегодного доклада о проделанной работе (см. A/78/265) в июле. Несмотря на сложную геополитическую ситуацию, консенсусный доклад подчеркивает растущий интерес государств — членов Организации Объединенных Наций к более глубокому обсуждению рамок ответственного поведения государств. Эстония считает обсуждения по вопросам угроз, норм, международного права, наращивания потенциала и будущего институционального диалога очень полезными для прояснения национальных и региональных перспектив, а также для формирования глобальных обязательств в области обеспечения киберстабильности.

Государства — члены Организации Объединенных Наций неоднократно призывали к созданию постоянного механизма Организации Объединенных Наций по проблемам киберугроз в контексте международной безопасности. Эстония по-прежнему поддерживает разработку инклюзивной, одновекторной и ориентированной на конкретные действия программы действий после завершения работы нынешней РГОС в 2025 году, как указано в резолюции 77/37. Мы высоко ценим тот факт, что предстоящие заседания РГОС предоставят дополнительные возможности для коллективного формирования программы действий.

Наконец, мы хотели бы еще раз подчеркнуть важность использования опыта и знаний многостороннего сообщества заинтересованных сторон. Мы ценим возможности для значимого, регулярного и существенного участия представителей частного сектора, гражданского общества и академических кругов в сессиях РГОС. Эстония предлагает государствам и другим заинтересованным сторонам и впредь участвовать в конструктивном обмене мнениями, делиться опытом, выслушивать друг друга и работать над повышением глобального потенциала в области противодействия киберугрозам.

Г-жа Нам (Новая Зеландия) (*говорит по-английски*): Новая Зеландия привержена делу поощрения ответственного поведения государств в свободном, открытом, мирном и безопасном киберпространстве. Технологические разработки в киберпространстве могут сделать мир более безопасным, а также внести вклад в устойчивое развитие, процветание и экономический рост. В то же время киберпространство все чаще становится вектором для новых и возникающих

угроз, которые несовместимы с международным миром и безопасностью. Это и распространение вирусов-вымогателей, и атаки на объекты критически важной инфраструктуры, и злонамеренное использование кибероперации, которые сегодня все чаще происходят в контексте вооруженных конфликтов.

Новая Зеландия придает большое значение коллективной работе по решению этих проблем и поощрению ответственного поведения государств в интернете. В этой связи мы приветствуем достигнутый в июле консенсус по второму ежегодному докладу о проделанной работе (см. A/78/265) Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025.

Новая Зеландия отмечает, как уже отмечали ранее и мы, и многие другие страны, что киберпространство не является территорией беззакония, и что международное право применяется в интернете точно так же, как и вне его. Новая Зеландия с удовлетворением отмечает, что государства продолжают делиться своими национальными взглядами на применение международного права. К их числу относятся и государства, которые обмениваются мнениями о применимости международного гуманитарного права и международного права прав человека. Мы еще раз подчеркиваем нашу позицию, что Устав Организации Объединенных Наций во всей его полноте применим и необходим для поддержания мира, безопасности и стабильности в киберпространстве, и что государства могут и должны быть готовы нести ответственность за злонамеренную деятельность с использованием киберсредств, которая противоречит Уставу и международному праву.

Мы приветствуем предложение о разработке программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Мы продолжаем обеспечивать эффективную работу Рабочей группы открытого состава, и в ходе наших обсуждений был выявлен целый ряд вопросов, которые мы должны решать сообща. Мы считаем, что после завершения работы нынешней РГОС потребуется постоянный, инклюзивный, гибкий и адаптируемый механизм регулярного институционального диалога, чтобы продолжить внедрение рамок ответственного поведения государств и способствовать дальнейшей работе по целому ряду вопросов, опираясь на результаты работы последовательно сменявших друг друга групп правительственных экспертов и рабочих групп открытого состава.

Мы приветствуем и поддерживаем проект резолюции A/C.1/78/L.60, предложенный Францией, который обеспечивает четкий и прозрачный путь для всех государств-членов к рассмотрению вопроса о разработке сферы охвата, структуры, содержания и условий работы будущего механизма таким образом, чтобы это дополняло работу нынешней РГОС.

Наконец, мы также подтверждаем важность участия многих заинтересованных сторон, включая представителей промышленности, академических кругов и гражданского общества, в решении многочисленных проблем, возникающих в киберпространстве. Эти проблемы не могут быть решены только на уровне правительств. Неправительственные заинтересованные стороны по-прежнему являются источником важнейших идей и ценного опыта для международных дискуссий по кибербезопасности, и мы продолжаем приветствовать и поощрять диалог со всеми заинтересованными сторонами.

Г-н Огасавара (Япония) (*говорит по-английски*): Мы являемся свидетелями растущей угрозы в киберпространстве на фоне увеличения числа инцидентов, связанных со злонамеренным использованием информационно-коммуникационных технологий (ИКТ), таких как атаки вредоносных программ, кибероперации против объектов критически важной инфраструктуры и кража криптовалюты. В киберпространстве не существует границ. Именно поэтому международное сотрудничество является абсолютной необходимостью для всех нас.

В этом контексте Япония придает большое значение текущей Рабочей группе открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 в качестве инклюзивной платформы под эгидой Организации Объединенных Наций. Мы высоко оцениваем руководящую роль сингапурского Председателя и его сотрудников и приветствуем принятие в июле второго ежегодного доклада о проделанной работе (см. A/78/265), а также значительный прогресс, которого мы коллективно достигли, например создание глобального реестра контактных пунктов.

Мы должны содействовать верховенству права в киберпространстве. Киберпространство не является территорией беззакония. Нормы международного права, включая Устав Организации Объединенных Наций и международное гуманитарное право, применимы и в отношении киберпространства. Учитывая стремительно меняющийся характер среды ИКТ, нашей приоритетной задачей должно стать участие в дальнейших конкретных дискуссиях о том, как применяется существующее международное право. Мы надеемся на более конкретные и содержательные обсуждения этой важной темы, в том числе на межсессионных заседаниях РГОС.

Наращивание потенциала — еще одно приоритетное направление. Япония тесно сотрудничает с Ассоциацией государств Юго-Восточной Азии, Всемирным банком и другими международными партнерами в целях активизации региональных и глобальных усилий по наращиванию потенциала в области ИКТ. Глобальный круглый стол по вопросам укрепления потенциала в области безопасности ИКТ, запланированный на май 2024 года, предоставит всем государствам-членам прекрасную возможность обменяться мнениями о практических мерах по укреплению потенциала при широком участии соответствующих заинтересованных сторон.

Что касается регулярного институционального диалога, то мы благодарим основных межрегиональных авторов за представление проекта резолюции A/C.1/78/L.60 по программе действий, предложенной Францией. Япония считает, что это предложение о разработке гибкой, всеобъемлющей и одновекторной программы действий может обеспечить плавный переход к новому, ориентированному на практические действия, постоянному механизму после 2025 года, в рамках которого мы сможем и дальше развивать достижения РГОС. Мы искренне надеемся, что проект резолюции, ставший результатом наших коллективных усилий, будет принят при широкой поддержке государств-членов.

Будучи единственной страной, которая пострадала от применения атомных бомб в ходе военных действий, Япония придает первостепенное значение нашим усилиям в области разоружения и просвещения по вопросам нераспространения. На десятой Конференции участников Договора о запрещении ядерного оружия по рассмотрению действия Договора, состоявшейся в августе прошлого года, премьер-министр Фумио Кисида объявил о намерении Японии внести вклад в учреждение Фонда молодежных лидеров за построение мира, свободного от ядерного оружия, в рамках работы по выполнению Хиросимского плана действий, который премьер-министр Кисида также представил на Конференции. Главная цель программы — собрать в Японии будущих лидеров из государств, как обладающих, так и не обладающих ядерным оружием, чтобы они из первых рук получили информацию о реальных последствиях применения ядерного оружия. Еще одна его цель — создать глобальную сеть, объединяющую различные международные сообщества будущих лидеров и других ключевых участников, представляющих правительства, гражданское общество, академические и научные круги, средства массовой информации, промышленность и другие области.

Трагедия Хиросимы и Нагасаки никогда не должна повториться. Повышение осведомленности о том, что пережили жители Нагасаки и Хиросимы после применения ядерного оружия, должно лежать в основе наших коллективных усилий по построению мира, свободного от ядерного оружия. Япония считает своим долгом передать этот опыт будущим поколениям не только в Японии, но по всему миру.

Г-н Ван дер Хеген (Швейцария) (*говорит по-французски*): В последнее время наблюдается постоянный рост числа злонамеренных кибероперация со стороны государственных и негосударственных субъектов, как в мирное время, так и в условиях вооруженного конфликта. Война против Украины — один из примеров такого развития событий, но есть и другие. Число кибератак, совершаемых преступными группировками против компаний или частных лиц, против объектов критически важной инфраструктуры или непосредственно против государств, как показала атака на Коста-Рику, растет в геометрической прогрессии. Эти задачи могут быть решены только при соблюдении согласованных рамок ответственного поведения государств в киберпространстве, как это было подтверждено и вновь подтверждено в консенсусных докладах групп правительственных экспертов и рабочих групп открытого состава и одобрено всеми государствами на Генеральной Ассамблее.

Швейцария приветствует принятие второго ежегодного доклада о проделанной работе (см. A/78/265) Рабочей группы открытого состава

(РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, поскольку в нем заложена прочная основа для будущей работы Группы. Мы особенно приветствуем возможность продолжить дискуссию о применимости международного права, включая международное гуманитарное право, в киберпространстве. Мы также приветствуем то особое внимание, которое уделяется защите объектов критически важной инфраструктуры и критически важной информационной инфраструктуры от угроз в сфере ИКТ, а также рекомендации по проведению дальнейших целенаправленных обсуждений на эту тему. Недавние инциденты, связанные со злонамеренными действиями в киберпространстве, а также текущая геополитическая ситуация свидетельствуют о том, что защита критически важной инфраструктуры, в частности медицинских и здравоохранительных учреждений, имеет первостепенное значение. В этом контексте Швейцария считает, что РГОС в первую очередь должна направить усилия на то, чтобы обеспечить более глубокое понимание, пропаганду и внедрение существующих 11 добровольных норм, прежде чем разрабатывать новые.

Мы благодарим Председателя РГОС за представление проекта решения A/C.1/78/L.13, в котором особое внимание уделяется принятию ежегодного доклада о проделанной работе и расписанию заседаний. Швейцария полностью поддерживает проект решения и воплощенный в нем процедурный и практический подход. Мы также должны подчеркнуть, что у Швейцарии имеются серьезные оговорки в отношении проекта резолюции A/C.1/78/L.11, представленного Российской Федерацией по этому вопросу, поскольку он представляется излишним и дублирует текст, представленный председателем РГОС. Проект, представленный Российской Федерацией, также вызывает вопросы по существу, в частности, потому что он не опирается на консенсусные формулировки, использует избирательный подход, не ссылается на консенсусные рамки и пытается адаптировать мандат РГОС. Это может поставить под сомнение тот значительный прогресс, который был достигнут к настоящему времени в рамках нынешней РГОС. В таких обстоятельствах Швейцария не может поддержать данный проект.

Швейцария поддерживает текущие дискуссии о разработке программы действий Организации Объединенных Наций по кибербезопасности в рамках РГОС. Мы считаем, что эта программа действий лучше всего подходит для того, чтобы стать новым регулярным институциональным диалогом после того, как нынешняя РГОС завершит свою работу в 2025 году. Именно поэтому мы являемся одним из соавторов проекта резолюции A/C.1/78/L.60, представленного Колумбией, Сенегалом, Соединенными Штатами и Францией, который будет способствовать дальнейшему прогрессу в этих обсуждениях.

В заключение я хотел бы остановиться на многочисленных проблемах, с которыми мы сталкиваемся в свете стремительно развивающегося технического прогресса. Последствия применения искусственного интеллекта, а также других областей науки и техники, включая науки о жизни, занимают важное место в работе этой сессии Первого комитета. В дальнейшем эти события должны быть в центре внимания Комитета, и мы должны обеспечить принятие резолюции, в которой различные направления контроля над вооружениями и разоружения будут увязаны с новейшими технологиями, и в которой будет рассмотрен комплексный синергетический эффект науки и техники и их влияние на международный мир и безопасность.

Г-жа Пейдж (Соединенное Королевство) (*говорит по-английски*): Соединенное Королевство привержено делу создания свободного, открытого, мирного и безопасного киберпространства, укрепляющего коллективную безопасность и поддерживающего глобальное развитие. Это требует от всех государств соблюдения и выполнения существующих обязательств, согласованных в Организации Объединенных Наций, а именно: рамок ответственного поведения государств в киберпространстве и применимости существующего международного права к киберпространству, включая Устав Организации Объединенных Наций, во всей его полноте.

Несмотря на эти соглашения, некоторые государства продолжают действовать безответственно. Россия использует кибероперации в рамках длительной кампании враждебной и дестабилизирующей деятельности против Украины. Эти атаки имеют реальные последствия. Мы глубоко обеспокоены тем, что представленный Россией проект резолюции пытается переиначить эти консенсусные

договоренности в своих узкокорыстных интересах и тем самым подрывает рамки, которые мы коллективно создали здесь вместе.

Модели злонамеренной активности с использованием киберсредств продолжают развиваться. В Соединенном Королевстве участились случаи нападок на наши демократические институты, процессы и ценности. Мы будем жестко реагировать на враждебные действия против нашей критически важной национальной инфраструктуры, в том числе путем укрепления нашей обороны с помощью Целевой группы по защите демократии и применения новых полномочий в соответствии с Законом о национальной безопасности.

Воздействие вирусов-вымогателей на важнейшие объекты национальной инфраструктуры может подорвать международный мир и безопасность, поэтому мы приветствуем упоминание об этом во втором ежегодном докладе о проделанной работе (см. A/78/265) Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025. В этом году Соединенное Королевство в координации с международными партнерами наложило санкции на 18 субъектов киберпространства, использующих вирусы-вымогатели. Мы будем продолжать наказывать тех, кто причиняет нам вред, и привлекать злоумышленников к ответственности.

Кроме того, Соединенное Королевство особенно обеспокоено безответственным использованием коммерчески доступных передовых киберсредств. Этот растущий рынок охватывает широкий спектр продуктов и услуг, включая коммерческое шпионское ПО. В соответствии с положениями внутреннего и международного законодательства по защите прав человека коммерческие киберинструменты могут ответственно использоваться правоохранительными органами для предотвращения серьезных преступлений и актов терроризма. Однако их неправомерное использование может подорвать права человека и поставить под угрозу нашу коллективную безопасность и стабильность киберпространства. Это комплексная задача, и для ее решения необходимо привлекать целый ряд секторов. Соединенное Королевство и Франция тесно сотрудничают в разработке ответных мер с участием многих заинтересованных сторон, и мы надеемся на дальнейшее сотрудничество со всеми странами-членами в этом направлении.

Соединенное Королевство признает результаты работы РГОС, включая тщательно выверенный текст ее ежегодного доклада, который был принят консенсусом. Мы привержены выполнению своих обязательств по внедрению и поддержке ответственного поведения в киберпространстве. Это включает в себя финансирование мероприятий по наращиванию потенциала на общую сумму 32 млн фунтов стерлингов в этом году и участие в конструктивных обсуждениях, направленных на углубление общего понимания государствами того, как международное право, включая международное гуманитарное право, применяется к киберпространству.

Соединенное Королевство поддерживает проект резолюции A/C.1/78/L.60, представленный Францией, о создании постоянного, ориентированного на практические действия, всеохватного механизма после завершения работы РГОС в 2025 году, который будет основываться на консенсусных итоговых документах, включая те, которые были приняты в рамках РГОС. Такой механизм обеспечит непрерывность проводимых государствами обсуждений по вопросам применения информационно-коммуникационных технологий в контексте обеспечения международной безопасности, а также позволит внедрить и доработать разработанные Организацией Объединенных Наций рамки ответственного поведения государств в киберпространстве.

В заключение я бы хотела сказать несколько слов о многосторонних режимах экспортного контроля, которые являются важнейшей частью системы нераспространения. Помимо того, что эти режимы содействуют поддержанию международной безопасности, они обеспечивают определенные гарантии в отношении конечного использования, что является залогом доверия государств при передаче технологии и способствует тем самым облегчению экспорта по всему миру. Мы обеспокоены продолжающимися попытками некоторых государств подорвать и дискредитировать такие важные режимы.

Г-н Горбанпур Наджафабади (Исламская Республика Иран) (*говорит по-английски*): Исламская Республика Иран выражает свои искренние соболезнования стойкому народу Палестины и твердую солидарность с ним. Мы решительно осуждаем тяжкие злодеяния, совершенные недавно израильским режимом в Газе, которые на сегодняшний день привели к гибели более 5000 человек, из них более 60 процентов — дети и женщины. Необходимо не-

медленно положить конец этому кровопролитию и неизбирательным бомбардировкам, а также обеспечить беспрепятственную доставку гуманитарной помощи.

Наша делегация присоединяется к заявлению, сделанному представителем Индонезии от имени Движения неприсоединившихся стран.

На фоне значительного роста числа кибератак, которые, по оценкам, выросли почти на 50 процентов в 2022 году, Исламская Республика Иран решительно заявляет о своей непоколебимой позиции в отношении использования киберпространства и среды информационно-коммуникационных технологий. Мы твердо убеждены, что эти бесценные активы, являющиеся общим достоянием человечества, должны использоваться исключительно в мирных целях, и государства должны сотрудничать друг с другом, тщательно соблюдая соответствующие нормы международного права.

В соответствии с этой принципиальной позицией Иран активно участвует в межправительственных переговорах под эгидой Организации Объединенных Наций. Наше участие обусловлено глубокой приверженностью защите прав всех вовлеченных сторон. В соответствии с основополагающей резолюцией 75/240 руководящим принципом рабочей методологии Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 является консенсус. Это подразумевает уважение позиции каждого отдельного государства-члена. Принцип консенсуса должен поддерживаться и продвигаться, поскольку он лежит в основе обсуждений в Группе.

После принятия второго ежегодного доклада РГОС (см. A/78/265), сопровождаемого обширной подборкой заявлений, разъясняющих позицию государств-членов, включая Иран, мы понимаем, что дальнейший прогресс и итоговый успешный результат работы РГОС в значительной степени зависят от достижения реального консенсуса. Как мы уже подчеркивали ранее, добровольное участие государств-членов в консенсусе или решение не препятствовать ему не должно восприниматься как нечто само собой разумеющееся. Следовательно, мы обязаны тщательно изучить и принять во внимание мнения и вклад всех государств-членов в итоговые документы РГОС.

В связи с этим нам необходимо проанализировать предыдущие документы РГОС, включая подготовленное Председателем резюме и ежегодный доклад о проделанной работе за 2021 год (см. A/77/275), в которых были изложены основные нерешенные вопросы. Эти документы должны послужить основой для конструктивных переговоров и сближения различных точек зрения. Мы хотели бы подчеркнуть, что, если мы хотим, чтобы РГОС эффективно функционировала в качестве меры укрепления доверия, мы должны внимательно относиться к проблемам и интересам всех государств-членов. В противном случае доверие, которым пользуется РГОС, будет подорвано. Эти качества бесценны для ее миссии.

В свете меняющихся реалий крайне важно признать, что некоторые государства, в частности Соединенные Штаты, не только участвуют в милитаризации киберпространства, но и проводят многочисленные кибератаки. Израильский режим, в частности, предпринял ряд кибератак против Ирана, ярким примером которых является применение пресловутого вируса Stuxnet. Мы безоговорочно осуждаем эти действия и призываем международное сообщество привлечь виновных к ответу за свои действия. К сожалению, недавно Иран был ложно и необоснованно обвинен в совершении предполагаемой кибератаки. Мы категорически отвергаем любые безосновательные обвинения, основанные на лживых домыслах, и предостерегаем от них.

Г-н Гетахун (Эфиопия) (*говорит по-английски*): Наша делегация присоединяется к заявлениям, сделанным от имени Движения неприсоединившихся стран и Группы африканских государств.

Информационно-коммуникационные технологии (ИКТ) вносят огромный вклад в обеспечение мира, роста и развития, и это не вызывает сомнений. Для того чтобы этот вклад имел положительный и долгосрочный эффект, крайне важно соблюдать принципы ответственного поведения государств при использовании ИКТ исключительно в мирных целях. Наряду с растущим применением ИКТ в промышленности, возрастают и угрозы, вытекающие из их использования в преступных целях. Мы считаем, что это наносит ущерб нашим коллективным усилиям по использованию этих технологий для обеспечения мира и стабильности, а также для осуществления наших стратегий, поэтому необходимо принимать соответствующие меры своевременно и оперативно.

Эфиопия совместно с другими странами вносит вклад в успешную работу Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, которая в настоящее время является единственным всеохватным механизмом. Равноправное участие всех государств в принятии консенсусных итоговых документов имеет решающее значение для обеспечения успешной деятельности. В этой связи Эфиопия поддерживает мнение о том, что оптимальным подходом является процесс, осуществляемый под руководством государств и подотчетный Первому комитету. Аналогичным образом, мы полагаем, что региональные платформы также важны для достижения необходимого консенсуса. Поэтому мы разделяем мнение о том, что изменения в использовании киберпространства в контексте международной безопасности можно обсуждать на основе индуктивного метода, начиная с субрегионального и континентального уровней и заканчивая глобальным, что поможет укрепить доверие на всех уровнях.

Мы подчеркиваем, что развивающимся странам необходимы программы наращивания потенциала по техническим, правовым и смежным аспектам ИКТ, имеющим отношение к мирному использованию киберпространства. В этой связи крайне важно, чтобы система Организации Объединенных Наций и региональные организации играли ключевую роль в оказании поддержки в наращивании потенциала, с тем чтобы развивающиеся страны могли укреплять свой потенциал на всех уровнях и получать выгоду от использования ИКТ для достижения своих целей в области развития. Такая поддержка в наращивании потенциала также важна для принятия мер по укреплению доверия с целью повышения стабильности и безопасности киберпространства.

Эфиопия интенсивно работает над использованием возможностей ИКТ для ускорения экономических и социальных изменений и построения более процветающего общества. Мы разработали политику и законодательство, направленные на продвижение и использование ИКТ, и добились прогресса в создании институционного потенциала для использования возможностей ИКТ и достижения наших задач в области развития. Эфиопия намерена внести свой вклад в реализацию программы глобального цифрового договора и извлечь из нее пользу для укрепления цифрового сотрудничества на основе открытого и инклюзивного процесса. Мы полностью поддерживаем идею внедрения цифровых решений через доступ к цифровым общественным благам и их использование для достижения целей в области устойчивого развития и преодоления цифрового разрыва.

В своих усилиях по развитию отрасли ИКТ и эффективному решению проблем, связанных с киберпространством, мы столкнулись с различными трудностями, включая нехватку финансовых ресурсов, низкий уровень цифровых навыков и умения принимать цифровые общественные блага. В нашем стремлении эффективно и устойчиво использовать ИКТ для решения наших многогранных проблем в области развития мы призываем международное сообщество оказать поддержку при необходимости, чтобы мы могли устранить узкие места, связанные с использованием ИКТ.

В заключение Эфиопия подчеркивает важность обеспечения мира, безопасности и стабильности среды информационно-коммуникационных технологий и подтверждает свою готовность сотрудничать со всеми для достижения этой цели.

Г-н Берар Кадье (Канада) (*говорит по-английски*): Канада хотела бы затронуть две темы, имеющие важное значение для международного мира и безопасности, а именно: ответственное поведение государств в киберпространстве и важность учета гендерных аспектов в вопросах разоружения, причем в качестве общего правила, а не в виде исключения.

Канада приветствует кумулятивные и эволюционирующие рамки ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ), разработанные в консенсусном докладе (см. A/76/135) Группы правительственных экспертов (ГПЭ) по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и в Рабочей группе открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025, а также в ее ежегодных докладах о проделанной работе за 2022 и 2023 годы (см. A/77/275 и A/78/265 соответственно).

Эти рамки играют важную роль в обеспечении мира и безопасности, а также в выработке общего понимания того, как государства должны вести себя в киберпространстве. Поэтому мы обеспокоены тем, что небольшая группа государств, в том

числе те, которые сыграли ключевую роль в его разработке, теперь ставят под сомнение надежность этих рамок. Мы напоминаем, что в докладах ГПЭ 2015 (см. A/70/174) и 2021 годов международное сообщество согласовало на основе консенсуса набор всеобъемлющих добровольных норм ответственного поведения государств в киберпространстве, и государства также согласились с тем, что в киберпространстве применяются нормы международного права. Эти нормы и международное право представляют собой надлежащие средства для определения того, что государства могут и чего не могут делать в киберпространстве. Мы приветствуем продолжающиеся в Рабочей группе открытого состава дискуссии об осуществлении норм и о том, как применяется международное право.

Практические меры укрепления доверия и меры по наращиванию потенциала — два других компонента рамок ответственного поведения государств в киберпространстве. С 2015 года Канада выделила более 30 млн долларов на проекты по созданию киберпотенциала по всему миру и сотрудничает с различными организациями в целях продвижения открытого и безопасного интернета. Мы признаем, что многое еще предстоит сделать, и надеемся на более глубокое обсуждение в ближайшие годы.

(*говорит по-французски*)

Канада считает, что членам Организации Объединенных Наций необходимо создать постоянный форум для проведения прагматичных, ориентированных на практические действия обсуждений по завершении нынешнего мандата РГОС. Поэтому Канада является одним из авторов предложения по программе действий на этой сессии Первого комитета. Программа действий — это лучший механизм для реального внедрения согласованной нормативной базы, в том числе посредством поддержки целевой деятельности по наращиванию потенциала. Программа действий также станет инклюзивным форумом для всех государств-членов, на котором они смогут обсудить эти и все другие вопросы, связанные с кибербезопасностью, опираясь на опыт частного сектора, гражданского общества и академических кругов.

Стремясь к инклюзивности, Канада подтверждает, что создание открытого интернета требует инвестиций в обеспечение гендерного равенства и понимания того, как гендерные аспекты влияют на проблемы в области кибербезопасности. Мы высоко оцениваем работу, проделанную РГОС по привлечению внимания к разнообразному вкладу женщин, размещение документации на портале РГОС и текущую программу стипендий «Женщины в киберпространстве». Мы рассчитываем развивать эту программу в ходе дальнейшей работы Организации Объединенных Наций в области киберпространства.

Гендерная проблематика важна не только в отношении киберпространства, но она также играет ключевую роль в нашей работе в рамках всего механизма разоружения. Учет гендерной проблематики помогает создавать эффективные и долговременные инициативы, способствующие устранению наиболее острых угроз безопасности в мире. Один из способов сделать это — собирать и распространять данные о воздействии оружия с разбивкой по возрасту и полу. Канада с удовлетворением отмечает рост гендерного представительства на площадках Организации Объединенных Наций, включая данный Комитет. Однако гендерный дисбаланс сохраняется, и поэтому нам не хватает важных голосов и точек зрения за столом переговоров — голосов и точек зрения, которые необходимы для выработки эффективной политики и программ в области нераспространения и разоружения.

В заключение следует отметить, что устранение гендерного разрыва является необходимым условием для создания более инклюзивного, мирного и процветающего мира. Поэтому Канада непоколебима в своем стремлении взаимодействовать со всеми заинтересованными сторонами для более широкого учета гендерной проблематики во всех аспектах международной безопасности.

Г-н Шэнь Цзянь (Китай) (*говорит по-китайски*): В настоящее время международная обстановка в киберпространстве сложна, тяжела и характеризуется формированием блоков, милитаризацией и фрагментацией. В этом году исполняется двадцать пять лет с того момента, как в Организации Объединенных Наций был запущен процесс обеспечения информационной безопасности. Начиная с групп правительственных экспертов и заканчивая Рабочей группой открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, работа по обеспечению информационной безопасности в Организации Объединенных Наций начиналась с нуля и росла в масштабах, и были достигнуты зна-

чительные успехи, включая признание принципов суверенитета в киберпространстве и поддержание мира в киберпространстве; разработку 11 норм ответственного поведения государств в киберпространстве; соблюдение и внедрение рамок ответственного поведения государств; а также недавно созданный глобальный межправительственный реестр контактных пунктов. Эти достигнутые с таким трудом успехи сыграли важную роль в поддержании мира и стабильности в киберпространстве.

Успешный опыт последних 25 лет показал, что единственный путь к решению проблем и обеспечению совместного развития и общего процветания — это поддержание мира, сотрудничества и инклюзивности при одновременном отказе от конфликтов, конфронтации и исключительности. Сохранение мирного характера киберпространства — наш единственный выход. Мы должны поставить мир и сотрудничество в центр нашей политики и продемонстрировать нашу готовность добиваться мира и развития посредством сотрудничества, отказаться от киберконфликтов и кибервойн и сделать так, чтобы киберпространство стало арсеналом цифровых возможностей, а не новым полем битвы в условиях противостоянии крупнейших держав.

Глобальное управление киберпространством требует равного участия и совместного принятия решений на уровне всех стран. Мы должны решительно отстаивать центральную роль Организации Объединенных Наций в вопросах информационной безопасности, уважать авторитет РГОС как единственного механизма по обеспечению информационной безопасности под эгидой Организации Объединенных Наций, и объединять усилия для принятия долгосрочных мер по созданию будущего института по вопросам информационной безопасности.

В цифровую эпоху нам необходимо взять на себя инициативу по решению возникающих проблем в области информационной безопасности и упорно работать над решением реальных и неотложных проблем, затрагивающими все страны. Во втором ежегодном докладе о проделанной работе РГОС признается, что

> «государства отметили возрастающую актуальность защиты данных и обеспечения их безопасности, учитывая увеличение объема и агрегирование данных, связанных с новыми и новейшими технологиями» (*A/78/265, приложение, п. 17*).

Китай предложил глобальную инициативу по безопасности данных, которая обеспечивает эффективное решение проблемы глобальной безопасности данных. Это может послужить основой для наших будущих обсуждений. Перед лицом рисков и вызовов в киберпространстве Китай хотел бы работать со всеми сторонами, поддерживать солидарность и сотрудничество и прилагать совместные усилия для создания сообщества с общим будущим в киберпространстве.

Искусственный интеллект (ИИ) — это новая область развития человечества, которая создает огромные возможности для социально-экономического развития, однако при этом она чревата непредсказуемыми рисками и проблемами. Управление искусственным интеллектом — общая задача, стоящая перед всеми странами мира и затрагивающая будущее человечества. Недавно Китай опубликовал Инициативу по глобальному управлению ИИ, призвав все страны активизировать обмен и сотрудничество и совместно работать над предотвращением рисков. Мы должны разработать систему управления ИИ на основе широкого консенсуса, чтобы сделать технологии ИИ более безопасными, надежными, контролируемыми и справедливыми. Ранее Китай также выпустил документ с изложением позиции по вопросам регулирования ИИ, применяемого в военных целях, и по вопросам этического управления ИИ.

Китай выступает за подход, ориентированный на людей, и такие концепции, как «Искусственный интеллект во благо», с акцентом на развитие и этику в первую очередь. Мы считаем, что ИИ всегда должен развиваться так, чтобы приносить пользу человеческой цивилизации. Мы должны работать сообща над предотвращением и пресечением злонамеренного использования и злоупотребления технологиями ИИ со стороны террористов, экстремистов и транснациональных организованных преступных группировок. Все страны, особенно крупные, должны разумно и ответственно подходить к исследованиям, разработкам и применению технологий ИИ в военной сфере, воздерживаясь от стремления к абсолютному военному преимуществу и подрыву глобального стратегического баланса и стабильности.

Китай выступает за внедрение многоуровневого регулирования по определенным категориям, с тем чтобы соответствующие системы вооружений всегда находились под контролем человека. В свете

двойного назначения технологий ИИ, наряду с ужесточением регулирования и управления, нам необходимо обеспечить права всех стран на их мирное использование. Китай выступает против проведения идеологических линий или создания эксклюзивных групп, препятствующих развитию ИИ в других странах. Мы также выступаем против создания препятствий и нарушения глобальной цепочки поставок ИИ посредством введения технологических монополий и односторонних принудительных мер.

Китай активно поддерживает дискуссии о создании международного института по управлению ИИ в рамках Организации Объединенных Наций и координации усилий по решению основных вопросов, касающихся развития, безопасности и управления ИИ.

Г-н Христоглу (Греция) (*говорит по-английски*): Греция присоединяется к заявлению, сделанному наблюдателем от Европейского союза, и хотела бы высказать несколько замечаний в своем национальном качестве.

Злонамеренные действия в киберпространстве в последние годы активизировались и привели, среди прочего, к резкому росту числа кибератак, направленных на объекты критически важной инфраструктуры, цепочки поставок и объекты интеллектуальной собственности, при этом также наблюдалось увеличение числа атак на предприятия, организации и граждан, совершаемых с использованием вирусов-вымогателей. Кибератаки превратились в средство вооруженных конфликтов, став одной из самых серьезных угроз миру и безопасности в наше время. Учитывая это, Греция решительно поддерживает работу, проделанную в Организации Объединенных Наций, которая, в частности, касается применения национального законодательства в киберпространстве. Она установила как нормы ответственного поведения, так и меры по укреплению доверия. Дальнейшая работа в этом направлении способствует укреплению мира и стабильности в киберпространстве и приносит пользу всем странам.

Греция также приветствует ежегодный доклад за 2023 год Рабочей группы открытого состава (РГОС) по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021-2025 (см. A/78/265), в котором, в частности, содержится рекомендация, призывающая государства принять участие в обсуждении сферы охвата, структуры и содержания программы действий по развитию ответственного поведения государств в киберпространстве. Мы твердо убеждены, что создание постоянного, инклюзивного и ориентированного на практические действия механизма послужит прочной основой для последующей работы над двумя наиболее важными аспектами нашей деятельности: внедрением и дальнейшим развитием рамок ответственного поведения государств в киберпространстве.

Греция всецело привержена идее дальнейшего обсуждения в Организации Объединенных Наций вопросов кибербезопасности, и мы подтверждаем свою готовность к позитивному взаимодействию в стремлении добиться конструктивного прогресса, о чем свидетельствует наше активное участие в недавно запущенном процессе РГОС с момента его создания.

Заседание закрывается в 12 ч 55 мин.