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.