Организация Объединенных Наций **S**/PV.9662

Совет Безопасности

Предварительный отчет

Семьдесят девятый год

9662-е заседание

Четверг, 20 июня 2024 года, 10 ч 00 мин
Нью-Йорк

Председатель:	г-н Чхо Дэ Юль/г-н Хван	(Республика Корея)
Члены:	Алжир	г-н Бенджама
	Китай	г-н Фу Цун
	Эквадор	г-н де ла Гаска
	Франция	г-н де Ривьер
	Гайана	г-н Персауд
	Япония	г-н Ямадзаки
	Мальта	г-жа Фрейзьер
	Мозамбик	г-н Афонсу
	Российская Федерация	г-н Небензя
	Сьерра-Леоне	г-н Кану
	Словения	г-н Жбогар
	Швейцария	г-жа Чанда
	Соединенное Королевство Великобритании и Северной Ирландии	дама Барбара Вудворд
	Соединенные Штаты Америки	г-жа Томас-Гринфилд

Повестка дня

Поддержание международного мира и безопасности

Противодействие меняющимся угрозам в киберпространстве

Письмо Постоянного представителя Республики Корея при Организации Объединенных Наций от 7 июня 2024 года на имя Председателя Совета Безопасности (S/2024/446)

24-17604 (R)

Заседание открывается в 10 ч 00 мин.

Утверждение повестки дня

Повестка дня утверждается.

Поддержание международного мира и безопасности

Противодействие меняющимся угрозам в киберпространстве

Письмо Постоянного представителя Республики Корея при Организации Объединенных Наций от 7 июня 2024 года на имя Председателя Совета Безопасности (S/2024/446)

Председатель (*говорит по-английски*): Я хотел бы тепло приветствовать Генерального секретаря, а также уважаемых министров и других высокопоставленных представителей, присутствующих в этом зале. Их участие в сегодняшнем заседании подчеркивает важность обсуждаемой темы.

На основании правила 37 временных правил процедуры Совета я приглашаю принять участие в этом заседании представителей Албании, Аргентины, Австралии, Австрии, Бахрейна, Бангладеш, Бельгии, Бразилии, Болгарии, Камбоджи, Чили, Коста-Рики, Хорватии, Кубы, Чехии, Египта, Сальвадора, Эстонии, Гамбии, Грузии, Германии, Ганы, Греции, Гватемалы, Индии, Индонезии, Исламской Республики Иран, Израиля, Италии, Казахстана, Кирибати, Латвии, Лихтенштейна, Марокко, Непала, Норвегии, Пакистана, Панамы, Филиппин, Польши, Португалии, Румынии, Саудовской Аравии, Сингапура, Испании, Турции, Украины, Объединенных Арабских Эмиратов, Уругвая и Вьетнама.

На основании правила 39 временных правил процедуры Совета я приглашаю принять участие в этом заседании следующих докладчиков: главного административного сотрудника Института «Кибермир» г-на Стефана Дюгена и профессора права и технологий Лидсского университета им. Беккета г-жу Нненну Ифеани-Аджуфо.

На основании правила 39 временных правил процедуры Совета я приглашаю принять участие в этом заседании следующих докладчиков: временного поверенного в делах делегации Европейского союза при Организации Объединенных Наций Ее Превосходительство г-жу Хедду Самсон, Специального представителя Интерпола при Организации Объединенных Наций г-жу Рорайму Ану Андриани и постоянного наблюдателя и главу делегации Международного комитета Красного Креста при Организации Объединенных Наций г-жу Летицию Куртуа.

Совет Безопасности приступает к рассмотрению пункта своей повестки дня.

Я хотел бы привлечь внимание членов Совета к документу S/2024/446, в котором содержится письмо Постоянного представителя Республики Корея при Организации Объединенных Наций от 7 июня 2024 года на имя Председателя Совета Безопасности, препровождающее концептуальную записку по рассматриваемому вопросу.

Сейчас я предоставляю слово Генеральному секретарю Его Превосходительству г-ну Антониу Гутерришу.

Генеральный секретарь (*говорит по-английски*): Я благодарю Республику Корея за созыв этих прений высокого уровня по вопросу, который затрагивает всех нас, — по вопросу мира и безопасности в киберпространстве.

Развитие цифровых технологий идет с невероятной скоростью и охватывает такие сферы, как информационно-коммуникационные технологии, облачные вычисления, блокчейн, сети 5G, квантовые технологии и многие другие области. Цифровой прогресс кардинально меняет экономику и общество. Цифровые технологии объединяют людей; они позволяют получать информацию, новости, знания и образование одним касанием экрана или щелчком мыши; они предоставляют гражданам доступ к государственным услугам и учреждениям; они стимулируют экономическую деятельность, торговлю и охват финансовыми услугами.

Однако по самой своей природе беспрепятственная, мгновенная связанность, позволяющая получить огромные блага в киберпространстве, может также повысить уязвимость людей, учреждений и целых стран. А риски того, что цифровые технологии будут использованы в качестве оружия, растут с каждым годом. Киберпространство представляет собой широко распахнутую дверь. Любой желающий может войти в нее, и многие так и дела-

ют. Вредоносной деятельностью в киберпространстве занимаются все больше государственных и негосударственных субъектов, а также откровенных преступников.

Тревожит то, насколько обыденными стали серьезные инциденты в сфере кибербезопасности. Происходит нарушение работы важнейших государственных служб, таких как центры здравоохранения, банковские учреждения и телекоммуникационные службы; непрерывно ведется незаконная деятельность, в том числе преступными организациями и так называемыми кибернаемниками; целые полчища ненавистников используют наше информационное пространство, чтобы вселить в людей страх и посеять раскол; киберпространство все более часто используется в качестве нового оружия в текущих вооруженных конфликтах, когда в игру вступают так называемые гражданские «хактивисты», в результате чего во многих случаях стирается грань между комбатантами и гражданскими лицами. А растущая интеграция цифровых средств с системами вооружений, включая автономные системы, создает новые уязвимости.

В то же время злонамеренное использование цифровых технологий становится все более изощренным и незаметным. Все более распространенными становятся вредоносные программы, программы, злонамеренно удаляющие программы и данные, и троянские вирусы. Кибероперации с применением искусственного интеллекта (ИИ) кратно увеличивают угрозу, а квантовые вычисления способны выводить из строя целые системы благодаря своей способности преодолевать методы шифрования. Злоумышленники используют уязвимости в программном обеспечении, а программы для взлома информационных систем продаются даже в Интернете. Производственно-сбытовые цепочки компаний активно подвергаются хакерским атакам, которые приводят к серьезным, разрушительным и каскадным последствиям. В качестве печально известного примера можно привести вирусы-вымогатели, представляющие огромную угрозу для государственных и частных учреждений и критически важной инфраструктуры, от которой зависят люди. По некоторым оценкам, в 2023 году объем платежей вымогателям достиг в общей сложности 1,1 миллиарда долларов США.

Помимо финансовых расходов, речь идет еще и о поддержании нашего общего мира, безопасности и стабильности как внутри стран, так и между ними. Злонамеренные действия, подрывающие государственные институты, избирательные процессы и добросовестность в Интернете, ослабляют доверие, нагнетают напряженность и даже сеют семена насилия и конфликтов.

Цифровые технологии открывают невероятные возможности для создания более справедливого, равноправного, устойчивого и мирного будущего для всех. Однако достижения прогресса должны преследовать благие цели. В Новой повестке дня для мира в качестве центрального элемента всех мирных усилий признается предотвращение. В этом документе содержится призыв к разработке надежной базы на основе международного права, прав человека и Устава Организации Объединенных Наций, а также к тому, чтобы все государства прилагали целенаправленные усилия для предотвращения распространения и эскалации конфликтов в киберпространстве и посредством его использования. Как констатируется в «Новой концепции верховенства права», верховенство права должно распространяться на цифровую сферу в той же мере, в какой оно применяется в физическом мире.

Я приветствую также приверженность Генеральной Ассамблеи действиям в этой области. В частности, я хотел бы упомянуть специально созданную Ассамблеей Рабочую группу открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. Государства руководствуются общепризнанной нормативной базой ответственного поведения государств в киберпространстве и активно рассматривают вопрос о применимости международного права к деятельности государств в этой сфере. Под эгидой Генеральной Ассамблеи государства-члены стремятся в ближайшие месяцы достичь консенсуса по новому договору о киберпреступности, который призван углубить сотрудничество и защитить права человека в Интернете. Вместе с тем с учетом четких и все более выраженных связей между киберпространством и глобальным миром и безопасностью Совет также может играть в этой связи ключевую роль, если будет рассматривать киберпроблематику в контексте его текущих рабочих процессов и резолюций.

Совет Безопасности проводит официальное заседание по этому вопросу всего лишь второй раз. Однако киберпространство влияет на очень многие вопросы, рассматриваемые за этим столом, и связано с ними, включая защиту гражданских лиц в вооруженных конфликтах, операции в пользу мира, борьбу с терроризмом и гуманитарные операции. Рассмотрение этой проблематики в рамках обсуждений в Совете было бы полезным способом заложить основу для принятия более эффективных ответных мер в отношении этой важной проблемы.

(*говорит по-французски*)

Чтобы гарантировать мир и безопасность в физическом мире, нам нужны новые подходы к обеспечению мира и безопасности в цифровом мире. Сентябрьский Саммит будущего предоставит жизненно важную возможность укрепить сотрудничество в решении важнейших глобальных проблем и вдохнуть новую жизнь в многостороннюю систему. Пакт, который будет согласован по итогам саммита, представляет собой уникальный шанс поддержать международный мир и безопасность в киберпространстве. Среди прочих приоритетов глава 2 Пакта направлена на подтверждение глобального консенсуса по защите критически важной инфраструктуры от вредоносных действий в сфере цифровых технологий и обеспечению повышенной ответственности в технологиях, основанных на данных, включая технологии искусственного интеллекта. В то же время мой Консультативный орган высокого уровня по искусственному интеллекту завершает работу над заключительным докладом о том, как мы можем управлять искусственным интеллектом в интересах человечества, одновременно устраняя связанные с ним факторы риска и неопределенности. Я рассчитываю на сотрудничество с Советом, Генеральной Ассамблеей и всеми государствами-членами, чтобы обеспечить надлежащее использование технологий для достижения прогресса и безопасности всех людей и планеты, общей для всех нас.

Председатель (*говорит по-английски*): Благодарю Генерального секретаря за его сообщение.

Я предоставляю слово г-ну Дюгену.

Г-н Дюген (*говорит по-английски*): Для меня большая честь выступать сегодня в Совете Безопасности по вопросу исключительной важности: как противостоять эволюционирующим угрозам в киберпространстве. Как главный исполнительный сотрудник Института «КиберМир», независимой и нейтральной неправительственной организации, базирующейся в Швейцарии, я выступаю по этой теме с опорой на собственный опыт, поскольку институт предлагает бесплатные услуги в области кибербезопасности наиболее уязвимым структурам, а именно некоммерческим организациям, следит за представляющими угрозу субъектами, обеспечивает обнаружение и анализ угроз и выступает за соблюдение законов и норм в киберпространстве.

Анализируя эволюцию угроз, я хотел бы остановиться на кумулятивном эффекте серьезных факторов дестабилизации существующего спектра угроз, которые в совокупности оказывают непосредственное влияние на поддержание международного мира и безопасности. Я затрону различные темы: появление все большего количества представляющих угрозу субъектов и то, как это увеличивает вероятность нападений на объекты критической инфраструктуры; изменение характера существующих в настоящее время угроз, в частности совмещение кибератак с распространением дезинформации и использование кибератак для обхода международных санкций; и эволюция угроз завтрашнего дня с учетом уникального риска, который представляет для кибербезопасности искусственный интеллект (ИИ). Эти изменения создают уникальные проблемы для международного мира и безопасности, в частности препятствуя атрибуции тех или иных действий, то есть процессу выявления исполнителя или источника кибератак или иных операций.

Начну с увеличения количества представляющих угрозу субъектов. С момента вторжения Российской Федерации на Украину в 2022 году Институт «КиберМир» фиксирует рост числа представляющих угрозу субъектов, поддерживающих обе воюющие стороны. Ведение войны более не является прерогативой только государств. В кибератаках и иных операциях в контексте вооруженных конфликтов участвует целый ряд негосударственных субъектов — преступные группировки, группы хакеров-активистов, движимых геополитическими мотивами, и другие гражданские лица. Они преследуют четыре цели: разрушение инфраструктуры, нарушение нормального функционирования основных служб, синхронное распространение дезинформации и проведение кибератак, а также кража

и использование данных путем внедрения и шпионажа. В этой связи мы, Институт «КиберМир», отследили более 3000 кампаний кибератак, совершенных 127 представляющими угрозу субъектами, которые затронули 56 стран и были направлены на 24 сектора критической инфраструктуры. Ущерб от этих кибератак ощущается далеко за пределами воюющих стран: около 70 процентов всех кибератак затрагивают организации в странах, не являющихся воюющими сторонами. Эти показатели находятся в свободном доступе на нашей платформе «Кибератаки во время конфликтов». Такое распространение кибератак ставит вопрос о деэскалации в контексте потенциального прекращения боевых действий. Как в таких условиях заставить 127 представляющих угрозу субъектов прекратить или обуздать свою вредоносную деятельность?

Такое увеличение их числа напрямую влияет на безопасность критической инфраструктуры. Я хотел бы привести два примера. В феврале 2022 года кибератака с использованием вредоносного программного обеспечения AcidRain, удаляющего пользовательские данные, была направлена на широкополосный спутниковый доступ в Интернет на Украине. Ее последствия ощущались и за пределами Украины. Она повлияла на работу ветряных турбин по всей Европе: одна из крупнейших немецких энергетических компаний потеряла доступ к удаленному мониторингу состояния более чем 5800 таких турбин; пострадали также тысячи абонентов спутникового Интернета в Германии, Франции, Венгрии, Греции, Италии и Польше. Такие последствия ощущаются не только во время вооруженных конфликтов. Во время пандемии коронавирусной инфекции (COVID-19) Институт «КиберМир» отслеживал 500 кибератак на медицинские учреждения, осуществленных в течение двух лет пандемии. Пятьсот кибератак — это даже не вершина айсберга, а кубик льда на его вершине. Только эти 500 атак нарушили работу здравоохранения в 43 странах, привели к краже данных 20 миллионов пациентов и к случаям нарушения доступа к медицинскому обслуживанию, совокупная продолжительность которых составила пять лет. Это означает пять лет направленных по неправильному адресу машин скорой помощи, отмененных приемов и ограниченного доступа пациентов к медицинскому обслуживанию.

Еще одним аспектом эволюционирующей угрозы является использование кибератак для обхода международных санкций и финансирования незаконной деятельности. Так, несколько представителей гражданского общества, организаций по вопросам кибербезопасности и государств проанализировали деятельность двух предполагаемых преступных групп, Kimsuky и Lazarus Group, тактика, инструменты, процессы и намерения которых были атрибутированы как связанные с Корейской Народно-Демократической Республикой. Эти преступные группировки координируют глобальные кибератаки всех типов: удары по цепочкам поставок, операции с использованием вирусов-вымогателей, атаки на криптовалютные биржи и финансовые учреждения. Помимо значительного прямого или основного вреда от этих атак, они предоставляют способ обхода международных санкций. По последним оценкам, Lazarus Group и Kimsuky получили от таких атак более 3 млрд долл. США. Такая эскалация наносит огромный ущерб. Кибератака с использованием вредоносного программного обеспечения WannaCry в мае 2017 года, которая менее чем за сутки поразила более четверти миллиона компьютеров в более чем 150 странах, вызвала значительные сбои и оказала масштабное влияние на здравоохранение, финансовый и транспортный секторы.

Завершая тему об эволюции угроз, важно предусматривать возникновение новых рисков, таких как риск квантовых вычислений для криптографии, о котором говорилось ранее, и риск генеративного ИИ с точки зрения моделей действий злоумышленников. С момента появления генеративного ИИ и больших языковых моделей искусственный интеллект используется злоумышленниками лишь в целях расширения своих возможностей. На сегодняшний день искусственный интеллект используется для масштабирования существующих процессов в так называемой «цепочке кибердудара» — стандартной последовательности действий, посредством которой злоумышленники совершают кибератаки. Так, использование ИИ позволяет сэкономить время, уходящее на выявление целей, автоматизировать поиск уязвимостей и повысить результативности фишинга. И это только первый шаг, поскольку различные группы уже экспериментируют с использованием генеративного ИИ для автоматизации различных элементов кибератаки. Это представляет собой неприемлемый риск. Успех

этих экспериментов несет в себе риск достижения настолько высокого уровня автоматизации всей «цепочки киберуничтожения», что злоумышленник может добровольно или случайно спровоцировать автономную кибератаку.

Учитывая объединение нескольких совокупных факторов дестабилизации, — увеличение количества угроз, новые специфические методы атаки на критически важные объекты инфраструктуры или обхода санкций, а также то, что произойдет из-за новых технологий искусственного интеллекта, — трудно выработать согласованную стратегию реагирования. Тем не менее можно предпринять несколько шагов, и в заключение я скажу следующее. Мы можем ввести в действие законы, нормативные акты и санкции, в частности путем прозрачного документирования нарушений и применения упреждающего подхода к предотвращению злонамеренного использования киберпространства, включая неправомерное использование ИИ или квантовых вычислений.

Важно устанавливать нарушителей, применять санкции и принимать соответствующие и надлежащие меры. Деэскалация невозможна без установления нарушителей, поскольку это крайне важно для принятия решений о необходимых мерах и способах защиты. Установление нарушителей может служить сдерживающим фактором, поскольку привлечение нарушителей к ответственности может способствовать принятию правовых и дипломатических мер реагирования и активизации усилий по разработке политики.

Наконец, очень важно иметь возможность всесторонне и количественно измерить ущерб, наносимый кибератаками. Институт «Кибермир» в настоящее время разрабатывает методы измерения ущерба от кибератак, поскольку до сих пор зачастую оценивался только материальный ущерб в виде потери денежных средств или утраты потенциала, в то время как ущерб, наносимый населению и социальным структурам, также важен.

Все это имеет решающее значение для поддержания международного мира и безопасности.

Председатель (*говорит по-английски*): Благодарю г-на Дюгена за его выступление.

Слово предоставляется г-же Ифеани-Аджуфо.

Г-жа Ифеани-Аджуфо (*говорит по-английски*): Для меня большая честь получить приглашение выступить перед членами этого органа с сообщением по вопросам поддержания международного мира и безопасности и противодействия меняющимся угрозам в киберпространстве, в частности с региональной точки зрения и в контексте ситуации в Африке.

При обсуждении вопросов поддержания мира и безопасности в киберпространстве необходимо оценивать безопасность киберпространства с учетом региональной специфики и мнений региональных субъектов. Следует признать, что эффективное обеспечение кибербезопасности часто затруднено в связи с реалиями развивающихся государств, особенно стран Африканского региона, которые попрежнему находятся по другую сторону цифрового разрыва и не имеют достаточных возможностей, навыков и инфраструктуры для эффективного обеспечения мира и безопасности на уровне ожидаемых стандартов. Поэтому, признавая общие характеристики кибербезопасности, мы должны также признать существующие различия между регионами и различные проблемы, с которыми они сталкиваются, и рассматривать киберугрозы в контексте реалий конкретных стран и регионов.

Вопросы поддержания мира и безопасности в киберпространстве приобрели ключевое значение для многих регионов. Например, в ноябре 2022 года Совет мира и безопасности Африканского союза впервые рассмотрел вопрос о мире и безопасности в киберпространстве с точки зрения его регулирования в рамках норм международного права. После этого Африканский союз утвердил стратегию в отношении кибербезопасности в качестве флагманской программы Повестки дня Африканского союза на период до 2063 года и в сквозной темы разработанной Африканским союзом Стратегии цифровых преобразований для Африки (2020–2030 годы). Важно отметить, что в июне 2023 года вступила в силу Конвенция Африканского союза о кибербезопасности и защите персональных данных, которая обеспечивает единую нормативную базу для уменьшения киберугроз и защиты инфраструктуры информационно-коммуникационных технологий (ИКТ). В январе этого года Африканский союз также принял общую позицию африканских государств по применению норм международного права к использованию информационно-коммуникацион-

ных технологий в киберпространстве. Следует добавить, что позиция африканских стран — это первый документ о применении норм международного права в киберпространстве, в котором есть раздел, посвященный укреплению потенциала. Африка также стала первым регионом, разработавшим общую региональную позицию.

Мы также должны признать, что регионы сталкиваются с различными трудностями в их усилиях по поддержанию мира, безопасности и стабильности в киберпространстве. Например, с прошлого года мы стали свидетелями кибератак на штаб-квартиру Комиссии Африканского союза, которые нарушили работу систем электронной почты. Управление связи Кении объявило, что только в 2023 году в Кении было зарегистрировано 860 миллионов кибератак, причем тщательно спланированные атаки были направлены на важнейшие объекты информационной инфраструктуры страны. В частности, в июле 2023 года Кения подверглась резонансной кибератаке на очень важную платформу «eCitizen», которая лишила граждан страны доступа к более чем 5000 государственных услуг, предоставляемых министерствами, местными органами власти и различными учреждениями. Группа, называющая себя «Анонимный Судан», взяла на себя ответственность за эти кибератаки в Кении и других частях Африки. Несколько месяцев назад организованные кибератаки вынудили правительство Малави приостановить выдачу паспортов после кибератаки на компьютерную сеть Иммиграционной службы, которая была сочтена серьезным нарушением национальной безопасности.

В связи с этим возникают серьезные вопросы, в том числе касающиеся размытых границ ответственности государственных и негосударственных субъектов и того, как эти возникающие киберугрозы обостряют уже существующие конфликты. Мы видим, как деятельность организованных террористических и экстремистских групп еще больше активизируется из-за конфликтов в таких регионах, как Африка. Мы наблюдаем не только то, как преступная деятельность в киберпространстве усугубляет существующие вызовы и угрозы международному миру и безопасности в регионе, но и как государства нарушают международные права человека под предлогом обеспечения кибербезопасности, закрывая доступ в Интернет, особенно во время вооруженных конфликтов. Эти действия не только ущемляют права граждан на коммуникацию и свободу информации, но и препятствуют эффективной гуманитарной деятельности во время конфликтов в Африке и, конечно, в других местах. Мы также видим, как распространение дезинформации и ложных сведений в киберпространстве все чаще используется в качестве инструмента подрыва мира и безопасности в некоторых частях региона. Это еще более усугубляется применением искусственного интеллекта в подобных обстоятельствах.

Однако мы считаем, что Совет Безопасности может внести значительный вклад в укрепление мира и безопасности в киберпространстве, особенно с региональной точки зрения. Действительно, существующие факторы неравенства требуют сложного взаимодействия для того, чтобы определить мандат Совета Безопасности по поддержанию мира и безопасности в киберпространстве. Эти различия в инфраструктуре кибербезопасности и цифровом потенциале являются одной из ключевых проблем, наряду с постоянными политическими конфликтами в таких регионах, как Африка. Также очевидна недостаточная информированность об обязательствах, связанных с невмешательством, должной осмотрительностью и мирным урегулированием споров в контексте киберпространства.

Поэтому, пока Совет Безопасности формулирует свой мандат по поддержанию мира и безопасности в киберпространстве, важно рассмотреть совместные меры, которые могут быть эффективно использованы для противодействия существующим угрозам и наращивания потенциала. Необходимо создать и укрепить возможности региональных субъектов. Однако следует отметить, что это не только вопрос правового, технического и оперативного потенциала, но речь идет и о социальных, экономических и политических реалиях. Учитывая различия в уровнях развитости кибербезопасности и местных условиях, необходимо стратегическое наращивание регионального потенциала. Необходимо учитывать специфику различных регионов, поскольку в разных регионах могут быть разные пробелы в потенциале. К попыткам развития и передачи киберпотенциала между регионами необходимо подходить целенаправленно, а также разрабатывать стратегии на основе конкретных механизмов подотчетности.

В таких регионах, как Африка, приоритетными областями, в которых необходимо наращивать потенциал для борьбы с киберугрозами, являются управление, разработка стратегий, технические средства и инфраструктура, а также научные исследования. Необходимо наращивать потенциал для защиты критически важной инфраструктуры. Важно обеспечить создание групп реагирования на инциденты в сфере кибербезопасности на уровне регионов там, где они еще не созданы, и обязать создать региональные круглосуточные контактные центры. Также важно разработать и внедрить механизмы регионального и международного сотрудничества между этими группами.

Для укрепления доверия и безопасности в киберпространстве необходимо сосредоточиться на реализации разработанных Организацией Объединенных Наций норм ответственного поведения государств в киберпространстве во всех регионах. Много вопросов возникает по поводу добровольного характера применения существующих норм и необходимости в более подотчетных подходах к поддержанию мира и безопасности в киберпространстве, в частности в четком определении руководящих принципов применения силы, вооруженных нападений и самообороны в киберпространстве. Кроме того, создание и поддержка форумов для разработки мер укрепления доверия позволит уменьшить недоверие между государствами-членами и будет способствовать мирному урегулированию споров в киберпространстве.

Совету Безопасности также важно разработать механизмы для понимания характера киберугроз в различных регионах. Это позволит принимать обоснованные решения для обеспечения безопасности и стабильности. Можно также создать рабочую группу по вопросам мира и безопасности в киберпространстве — в первую очередь для рассмотрения рекомендаций в отношении конфликтов и укрепления мира и стабильности в киберпространстве. Достижению этих целей также будет способствовать создание специализированных региональных центров кибербезопасности для расширения трансграничного сотрудничества и обмена информацией. Следует также уделить внимание укреплению потенциала в деле разработки и реализации комплексных региональных и национальных стратегий в области кибербезопасности, а также развитию культуры лидерства в области кибербезопасности.

Ключевая роль в формулировании стратегий и налаживании взаимодействия с государствами того или иного региона в деле достижения результатов в области мира и безопасности отводится региональным организациям. В этой связи сотрудничество между Организацией Объединенных Наций и региональными и субрегиональными организациями в поддержании международного мира и безопасности должно охватывать вопросы кибербезопасности. Наконец, Совет Безопасности должен способствовать созданию платформы, которая позволит наладить эффективный диалог, направленный на поощрение каждого региона к разработке рамочных программ по обеспечению мира и безопасности в киберпространстве.

В заключение добавлю, что Совету Безопасности важно обеспечить, чтобы его повестка дня носила комплексный характер и наглядно показывала, что вопрос обеспечения верховенства права в киберпространстве связан с вопросами мира и безопасности. В этой связи также необходимо установить определенные принципы и стандарты в области управления киберпространством, которые позволят обеспечить, чтобы каждый регион и каждое правительство несло ответственность за обеспечение мира и стабильности. Поскольку мы становимся все более взаимосвязанными и все больше подвержены влиянию подрывающих привычный уклад жизни технологий, таких как искусственный интеллект, мы также становимся более уязвимыми. Поэтому крайне важно укреплять наш человеческий и институциональный потенциал для обеспечения безопасности киберпространства путем укрепления доверия к использованию кибертехнологий.

Председатель (*говорит по-английски*): Сейчас я сделаю заявление в своем качестве министра иностранных дел Республики Корея.

Прежде всего я хотел бы вновь поблагодарить Генерального секретаря Гутерриша за его участие в этом заседании и за его сегодняшнее сообщение. Позвольте мне также поблагодарить представителя Института «Кибермир» г-на Стефана Дюгена и представителя Университета им. Беккета в Лидсе профессора Нненну Ифеани-Аджуфо за то, что они поделились своими знаниями и опытом. Я также выражаю глубокую признательность всем представителям государств-членов за участие в этих открытых прениях высокого уровня.

Сегодняшнее заседание — лишь второй случай в истории Организации Объединенных Наций, когда Совет Безопасности проводит официальное заседание для обсуждения угроз международному миру и безопасности, исходящих от киберпространства. Совет провел первые в истории открытые прения по этой теме три года назад, в июне 2021 года (см. S/2021/621). Конечно, за пределами Совета Безопасности в этой связи уже были достигнуты значительные успехи. Структуры, созданные Генеральной Ассамблеей, разработали нормы ответственного поведения государств в киберпространстве. Также был проведен ряд заседаний по формуле Аррии по вопросам кибербезопасности, последним из которых стала апрельская встреча, организованная Республикой Корея совместно с Соединенными Штатами и Японией.

Генеральный секретарь также продемонстрировал сильные лидерские качества, призвав принять меры по снижению рисков, связанных с кибербезопасностью, и создав Консультативный орган высокого уровня по искусственному интеллекту, в состав которого входит и Корея. Однако события, произошедшие после первого заседания Совета Безопасности три года назад, наглядно демонстрируют, почему сейчас Совет должен как никогда активно предпринимать упреждающие действия по борьбе с угрозами, исходящими от киберпространства. Помимо многочисленных трансграничных кибератак, мир сталкивается со вспышкой крупных вооруженных конфликтов, в ходе которых нападения совершаются не только на традиционном поле боя, но и в киберпространстве.

Мир также становится свидетелем того, как бурное развитие искусственного интеллекта значительно расширяет возможности злоумышленников, которые теперь могут, совершая нарушения в киберпространстве, сеять еще больший хаос. Мир убедился в том, что злонамеренная активность с использованием киберсредств может приводить к реальным последствиям и подрывать уверенность в беспристрастности политических выборов, безопасность объектов критически важной инфраструктуры, а также основы мира и безопасности. Так, в одном из государств — членов даже пришлось объявить чрезвычайное положение после того, как оно подверглось атакам с использованием разработанных в другой стране вирусов-вымогателей.

Киберсредства по своей сути имеют двойное назначение: любой злоумышленник может с их помощью создать новые угрозы либо активировать, расширить или усилить существующие. Как однажды заметил известный футурист Элвин Тоффлер, «наши технологические возможности растут, но вместе с ними усиливаются и их побочные эффекты и увеличиваются связанные с ними потенциальные опасности».

Республике Корея не чужды угрозы, создаваемые злонамеренной активностью с использованием киберсредств, и их влияние на безопасность, поскольку за счет такой деятельности в значительной степени финансируется разработка угрожающего Корее оружия массового уничтожения. В последнем докладе Группы экспертов, учрежденной резолюцией 1718 (2006) (S/2024/215), говорится о том, что 40 процентов программ Корейской Народно-Демократической Республики по созданию оружия массового уничтожения финансируются за счет незаконных киберсредств. В период с 2017 по 2023 год Группа проводила расследование около 60 предполагаемых кибератак на криптовалютные компании, совершенных Корейской Народно-Демократической Республикой. К сожалению, по известным всем нам причинам Группа в настоящее время уже не функционирует.

Используя цифровые средства, Корейская Народно-Демократическая Республика систематически обходит введенные Советом санкции и бросает вызов международному режиму нераспространения, который является неотъемлемой частью работы Совета. Сейчас, когда мир и безопасность в физическом и кибернетическом мире все больше переплетаются, Совет Безопасности не должен зарывать голову в песок. Он должен по крайней мере идти в ногу с тенденциями за пределами Совета и расширять свое участие в борьбе с реально существующими угрозами, исходящими от киберпространства. Подобно тому как Совет Безопасности и Генеральная Ассамблея работают сообща, когда речь идет об обсуждении стрелкового оружия, терроризма и нераспространения, они также могут дополнять роли друг друга при рассмотрении вопросов кибербезопасности.

Несмотря на то что пока авторитетного подхода к дальнейшим действиям в этой связи выработано не было, Республика Корея хотела бы представить на рассмотрение Совета Безопасности следующие три предложения.

Во-первых, Совету необходимо провести четкую оценку текущей ситуации. Для этого Совет Безопасности может регулярно запрашивать доклады, чтобы иметь возможность рассматривать вопрос о том, как киберугрозы пересекаются с мандатом Совета и какое воздействие развивающиеся киберугрозы оказывают на международный мир и безопасность.

Во-вторых, предлагаемые в этой связи рекомендации должны охватывать весь спектр рассматриваемых Советом досье. Кибербезопасность может быть включена в повестку дня Совета по аналогии с другими сквозными вопросами, такими как женщины и мир и безопасность, а также молодежь и изменение климата. Как отметили многие государства-члены на заседании по формуле Аррии в апреле, существует прямая связь между злонамеренным использованием информационно-коммуникационных технологий и различными вопросами, входящими в сферу компетенции Совета Безопасности, включая санкции, нераспространение и терроризм. В этой связи Совет может рассматривать кибербезопасность как важный сквозной компонент всех обсуждаемых им региональных и тематических досье или вопросов.

В-третьих, в среднесрочной и долгосрочной перспективе Совет Безопасности должен быть в состоянии выработать соответствующий способ преодоления этого вызова. Совет может организовывать заседания, посвященные злонамеренной активности с использованием киберсредств, нарушающей международное право и наносящей ущерб миру и безопасности. Более того, он мог бы призвать все соответствующие стороны использовать кибертехнологии ответственным образом и добиваться привлечения злоумышленников к ответственности с помощью имеющихся в его распоряжении инструментов. Само собой разумеется, что Совет Безопасности должен разработать программу работы по кибербезопасности таким образом, чтобы она дополняла текущие обсуждения в Генеральной Ассамблее.

Совет Безопасности уже не раз изменял свою повестку дня с учетом новых вызовов в области безопасности. Составители Устава Организации Объединенных Наций и представить себе не могли, что Совет Безопасности будет обсуждать вопросы об изменении климата, нарушениях прав человека и пандемии. Для того чтобы Совет Безопасности оставался актуальным и гибким в решении одной из самых острых проблем в области безопасности нашего времени, ему необходимо вплотную заняться вопросами кибербезопасности. Я искренне надеюсь на то, что сегодняшние открытые прения дадут толчок к тому, чтобы это произошло.

Прежде чем завершить свое выступление, я хотел бы добавить еще одно замечание. Поскольку киберпространство не имеет границ, неблагоприятные последствия злонамеренной активности с использованием киберсредств могут испытывать на себе все страны — как страны, находящиеся на высоком уровне развития цифровых технологий, так и уязвимые в этой связи государства. Прочность системы международной безопасности в киберпространстве определяется прочностью ее самого слабого звена. Поэтому связь между гуманитарной помощью, развитием и миром не менее реальна и в кибермире. Киберпространство, свободное от злонамеренной активности с использованием киберсредств, будет способствовать цифровому развитию и раскрытию цифровых возможностей, что в конечном итоге поможет в достижении целей в области устойчивого развития. Открытое, безопасное, доступное и мирное киберпространство, в котором можно эффективно противостоять киберугрозам, будет также содействовать защите свободы и прав человека в Интернете.

Теперь я возвращаюсь к исполнению своих обязанностей Председателя Совета.

Я предоставляю слово Постоянному представителю Соединенных Штатов и члену кабинета президента Байдена Ее Превосходительству г-же Линде Томас-Гринфилд.

Г-жа Томас-Гринфилд (Соединенные Штаты Америки) (*говорит по-английски*): Прежде всего я хочу поблагодарить Республику Корея за то, что она вновь собрала нас для обсуждения этой важнейшей проблемы и вопроса мира и безопасности. Г-н Председатель, хотела бы приветствовать Вас в Совете Безопасности и выразить Вам свою глубокую признательность. Я имела честь познакомиться с Вами в Сеуле в ходе моего визита несколько месяцев назад и очень рада видеть Вас в этом зале. Благодарю Генерального секретаря и докладчиков за их сообщения и приветствую всех других министров, которые почтили нас сегодня своим присутствием.

Со времени нашего предыдущего заседания, состоявшегося в апреле, мы продолжаем убеждаться в настоятельной необходимости обеспечения надежной системы обеспечения безопасности киберпространства и, следовательно, необходимости обсуждения этой темы в Совете. Обеспечение кибербезопасности позволяет функционировать нашим самым основным системам — нашей экономике, нашим демократическим институтам и, да, даже самой Организации Объединенных Наций. Соединенные Штаты привержены сотрудничеству со всеми ответственными сторонами в целях защиты преимуществ киберпространства, формирования цифровой солидарности и использования технологий для достижения целей в области устойчивого развития. И все же слишком многие государственные и негосударственные субъекты выбирают совершенно иной путь. В разных странах мира они используют цифровую связь для целей вымогательства, кражи денег и идей у правительств и частных организаций, преследования журналистов и правозащитников, подготовки к будущим конфликтам и создания угроз для нашей критически важной инфраструктуры, в том числе здесь, в Организации Объединенных Наций.

Как члены Совета мы должны работать сообща в интересах противодействия киберугрозам, исходящим от негосударственных и государственных субъектов, укрепления норм ответственного поведения государств, привлечения стран к ответственности в случае их безответственного поведения в киберпространстве и поддержки жертв, пострадавших от такого поведения, а также разрушения сетей преступников, стоящих за опасными кибератаками, совершаемыми по всему миру. Для этого уже существует определенная основа. Рамки ответственного поведения государств в киберпространстве, которые были приняты неоднократно и на основе консенсуса, четко предусматривают, что международное право распространяется и на киберпространство и что от государств ожидается соблюдение добровольно принятых на себя норм поведения государств в мирное время. В числе этих норм — ожидание, что государства будут расследовать случаи злонамеренной активности с использованием киберсредств, которая осуществляется с их территории и направлена против критически важной инфраструктуры другой страны, и смягчать последствия такой активности. И все же некоторые из тех, кто поддержал эти рамки, предпочитают игнорировать — или, что еще хуже, поддерживать — злоумышленников.

Как было отмечено на проведенном в апреле заседании по формуле Аррии по вопросам кибербезопасности, к такой активности относятся вредоносные кибероперации Корейской Народно-Демократической Республики, которые используются последней для финансирования своих программ по созданию оружия массового уничтожения и баллистических ракет. А еще к ней относится деятельность России в киберпространстве на Украине, в Германии, Чехии, Литве, Польше, Словакии и Швеции, где, среди прочего, Главное разведывательное управление Генерального штаба России совершает атаки на политические партии и демократические институты. Кроме того, российское правительство предоставляет убежище лицам, стоящим за программами-вымогателями и за последние годы причинившим убытки в размере миллиардов долларов США, а также значительный ущерб больницам и другим объектам критически важной инфраструктуры.

Со своей стороны, в феврале Соединенные Штаты и Соединенное Королевство объявили о проведении операций по уничтожению группы лиц, которая стоит за программой-вымогателем LockBit, — жертвами ее действий стали 2000 человек, а общая сумма затребованных ею в качестве выкупа денег составляет сотни миллионов долларов США, более 120 миллионов из которых были выплачены. В последние месяцы мы обнародовали обвинительное заключение, в соответствии с которым граждане России Артур Сунгатов и Иван Кондратьев, также известные под ником Bassterlord, обвиняются в использовании программного обеспечения LockBit против множества лиц в Соединенных Штатах и других странах мира. Эта работа дополняет усилия, предпринимаемые нами в рамках Международной инициативы по борьбе с программами-вымогателями, которую мы создали в 2021 году и которая сейчас представляет собой крупнейшее в мире партнерство по борьбе с киберугрозами. Как отдельные государства, действующие в рамках этого партнерства, а также на многосторонних площадках, включая Организацию Объединенных Наций, мы призываем все государства вносить свой вклад в осуществление указанных рамок и содействие миру и стабильности в киберпространстве. И мы призы-

ваем Совет проследить за тем, чтобы обеспечение кибербезопасности являлось сквозной приоритетной задачей, которая учитывалась бы в рамках каждого аспекта нашего мандата. Независимо от того, нужно ли обсудить вопрос о том, как операции по поддержанию мира могут способствовать соблюдению надлежащей кибергигиены для ограничения возможных рисков, или добиться более четкого понимания того, как обеспечение кибербезопасности может поддержать усилия в области нераспространения, Совет должен продолжать рассматривать такие проблемы через призму кибербезопасности.

Мы в состоянии защитить нашу критически важную инфраструктуру и всех тех, кто на нее полагается. И мы располагаем возможностями для сохранения преимуществ киберпространства в интересах всех. Поэтому, руководствуясь рамками ответственного поведения государств в киберпространстве, давайте еще раз подтвердим, что международное право применимо к поведению государств, которое направлено против других государств. Давайте поощрять соблюдение добровольных норм ответственного поведения государств в мирное время и способствовать уменьшению риска возникновения конфликтов в результате киберинцидентов. И давайте поддерживать основанный на правилах международный порядок и следить за тем, чтобы цифровой мир оказывал на физический мир благотворное влияние.

Я еще раз благодарю Вас, г-н Председатель, за возможность собраться в этом зале для обсуждения этого важного вопроса.

Г-н Персауд (Гайана) (*говорит по-английски*): Я благодарю министра иностранных дел Его Превосходительство г-на Чхо Дэ Юля и председательствующую в Совете делегацию Республики Корея за организацию сегодняшних открытых прений по противодействию меняющимся угрозам в киберпространстве. Также выражаю признательность Генеральному секретарю и докладчикам за их глубокий вклад в это обсуждение.

Стремительный технологический прогресс создает мир безграничных возможностей, характеризующийся огромными экономическими, социальными и геополитическими благами. Однако в случае использования злоумышленниками цифровые технологии, которые все больше совершенствуются, представляют собой беспрецедентные риски как для безопасности людей, так и для национальной безопасности. Злонамеренное использование цифровых технологий также демонстрирует, что существует потенциальная угроза нарушения работы институтов и возникновения связанных с управлением трудностей в области нормативного регулирования и политики. Кроме того, транснациональный характер киберугроз приводит к тому, что традиционные понятия национальной безопасности и обороны уже устарели.

Угрозы кибербезопасности, с которыми мы в настоящее время сталкиваемся, могут разрушительным образом сказываться на здоровье и безопасности наших граждан и функционировании основных служб. По мере того, как современные угрозы кибербезопасности становятся все более изощренными и многогранными и начинают охватывать, среди прочего, спонсируемый государствами кибершпионаж, вмешательство в демократические процессы, нарушения прав человека, атаки на критически важную инфраструктуру и распространение ложной информации, дезинформации и ненавистнических высказываний, такими же должны становиться и наши меры реагирования на них.

В этой связи я хотел бы предложить рассмотреть три момента.

Во-первых, в целях защиты от кибератак необходимо создать механизмы подотчетности и надзора. В этой связи мы принимаем к сведению недавние дискуссии о том, могут ли кибератаки на объекты критически важной инфраструктуры, такие как медицинские учреждения или электростанции, сопряженные с серьезными последствиями для жизни людей, быть приравнены к военным преступлениям, преступлениям против человечности, геноциду и/или преступлению агрессии. Этот вопрос должен быть тщательно изучен и интегрирован в глобальную правовую основу, которая также должна обеспечивать разработку и использование цифровых инструментов и технологий с учетом соображений морали и необходимости уважения прав человека. В этой связи Гайана признает важность завершения работы Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и необходимость принятия конвенции, которая была бы ратифицирована значительным числом государств.

Во-вторых, мы должны уделять приоритетное внимание сотрудничеству, взаимодействию и партнерским связям в целях укрепления потенциала в области обеспечения кибербезопасности и устойчивости к киберугрозам, а также в интересах расследования киберпреступлений, в какой бы стране и каком бы регионе они ни совершались, и осуществления преследования за них. Что касается партнерства, то мы должны стремиться укреплять доверие и расширять региональное и международное сотрудничество, с тем чтобы способствовать обмену знаниями и информацией и передаче технологий. Мы должны также стремиться обеспечивать совместимость между нашими национальными, региональными и международными системами, которые занимаются отслеживанием и мониторингом угроз кибербезопасности. Чтобы действовать эффективно, необходимо разработать глобальную систему для обмена информацией о возникающих угрозах кибербезопасности между государствами и соответствующими заинтересованными сторонами. Несмотря на то что ведущиеся под эгидой Организации Объединенных Наций и региональных механизмов дискуссии вносят позитивный вклад в эти усилия, в том числе в рамках представленной Генеральным секретарем Дорожной карты по цифровому сотрудничеству и Программы ускоренного достижения целей в области устойчивого развития с помощью цифровых технологий, еще многое предстоит сделать. Мы должны также использовать возможности в киберсфере, чтобы привлечь к противодействию киберугрозам и укреплению кибербезопасности все наше общество.

Новые технологии, такие как системы искусственного интеллекта, могут помочь выявить и смягчить подобные угрозы. В этой связи мы как правительства должны активизировать наши усилия по сотрудничеству с технологическими компаниями и частным сектором для разработки более эффективных инструментов и мер безопасности и для расширения обмена информацией при анализе данных об угрозах. Кроме того, у многих развивающихся стран, таких как Гайана, отсутствуют необходимые ресурсы и опыт для борьбы с киберугрозами и повышения устойчивости к ним. Развитие технического потенциала в таких странах должно рассматриваться в контексте укрепления нашей коллективной безопасности, что поможет устранить существующее неравенство и дисбаланс в возможностях обеспечения кибербезопасности. С учетом этого мы как мировое сообщество могли бы рассмотреть возможность создания глобального фонда, по линии которого будет осуществляться обучение и наращивание потенциала, а также разработка программного и аппаратного обеспечения.

Более того, Гайана призывает развитые страны, обладающие современными технологиями, предоставить техническую помощь и финансирование для укрепления инфраструктуры обеспечения кибербезопасности и потенциала реагирования в развивающихся странах. Необходимо всеми силами стремиться к тому, чтобы ни одна страна или организация не могли монополизировать технологические средства и возможности, поскольку это может еще больше усугубить уязвимость развивающихся стран, например путем введения законов и правил с экстерриториальным действием.

В-третьих, невзирая на процессы, осуществляющиеся на других форумах Организации Объединенных Наций, Совет Безопасности также должен участвовать в диалоге по вопросам кибербезопасности с учетом угрозы, которую представляет собой злонамеренная кибердеятельность для поддержания международного мира и безопасности. Поэтому Совет должен активизировать обсуждение этого вопроса в рамках его заседаний по формуле Аррии и открытых прений, таких как нынешние прения, для того чтобы повысить осведомленность о возникающих угрозах, создаваемых новыми технологиями, и коллективно изучить эффективные меры, которые могут быть приняты против злонамеренного использования таких технологий.

В заключение я хотел бы заметить, что проблемы, возникающие в связи с угрозами кибербезопасности, являются сложными, но не непреодолимыми. Посредством коллективных усилий и воли, а также согласованных действий мы сможем построить прочный и безопасный цифровой мир, который будет способствовать укреплению доверия, внедрению инноваций и всеобщему процветанию. Давайте воспользуемся этим моментом, чтобы не просто преодолеть стоящие перед нами угрозы, но и принять активные меры для построения такого будущего, в котором никто не останется забыт. Гайана готова сотрудничать со всеми государствами-членами в достижении этой цели.

Г-н Небензя (Российская Федерация): Рады видеть Вас в кресле Председателя Совета Безопасности.

Благодарим Генерального секретаря за его доклад. Внимательно выслушали докладчиков.

Российская Федерация стояла у истоков обсуждения вопросов международной информационной безопасности в Организации Объединенных Наций. Еще в 1998 году, 26 лет назад, мы впервые подняли эту тему в Генеральной Ассамблее, внеся первый профильный проект резолюции (резолюция 53/70 Генеральной Ассамблеи), которая с тех пор стала ежегодной и получает поддержку подавляющего большинства государств-членов.

По нашей инициативе для обсуждения вопросов безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) была создана соответствующая Группа правительственных экспертов (ГПЭ) Организации Объединенных Наций, которая впоследствии переросла в инклюзивный формат — Рабочую группу открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Именно Рабочая группа открытого состава является уникальной единой переговорной площадкой под эгидой всемирной Организации для обсуждения всех вопросов международной информационной безопасности.

За время своей деятельности Рабочая группа открытого состава доказала свою эффективность и востребованность. Среди прикладных результатов — запуск в мае 2024 года предложенного Россией реестра контактных пунктов для обмена информацией о компьютерных атаках/инцидентах. Проводится подробное рассмотрение существующих и потенциальных угроз в сфере международной информационной безопасности. Предпринимаются конкретные шаги на направлении наращивания цифрового потенциала государств — в прошлом году согласованы универсальные принципы оказания содействия в этой области.

Убеждены, что усилия международного сообщества должны быть сосредоточены на продолжении укрепления межгосударственного взаимодействия в рамках Рабочей группы открытого состава в целях достижения конкретных, практических результатов в деле обеспечения международной информационной безопасности. Считаем принципиально важным закреплять и развивать достигнутые Рабочей группой открытого состава результаты — как в рамках нынешнего мандата Группы, так и будущего переговорного формата. Россия уже представила свое видение постоянно действующего инклюзивного механизма в данной области. Считаем целесообразным сохранить наше общее достояние путем создания после 2025 года постоянной Рабочей группы открытого состава с функцией принятия решений.

Данные факты наглядно демонстрируют, что в Организации Объединенных Наций уже давно ведется последовательная, эшелонированная работа по международной информационной безопасности. Поэтому необходимость вовлекать в нее в Совете Безопасности вызывает большие вопросы. Данная тема имеет свою специфику и должна обсуждаться на профильных площадках, где есть соответствующая экспертиза. Принципиально важно удерживать ее в профессиональном, конструктивном русле, избегая политизации. Дублирование усилий международного сообщества и «растаскивание» данной темы по различным ооновским площадкам контрпродуктивны и могут свести на нет все наработанные за десятилетия под эгидой Генеральной Ассамблеи результаты.

Не менее важно и то, что дискуссия в Рабочей группе открытого состава носит инклюзивный характер. В ней участвуют все без исключения члены Организации Объединенных Наций, причем на равноправной основе, так как Группа принимает решения консенсусом. Перенос этого сюжета на площадку Совета Безопасности автоматически отсечет от участия в принятии решений все государства, которые не входят в состав Совета. Те из них, кто сегодня поддержал призыв председательства сделать международную информационную безопасность частью повестки дня Совета Безопасности, должны это четко осознавать.

Наконец, в любом разговоре о потенциальных рисках необходимо иметь в виду технологические особенности информационного пространства. В отличие от физического мира угрозы в нем крайне сложно идентифицировать, не говоря уже об установлении источника атаки (так называемой атрибуции). Зачастую о том, что атака имела место, становится известно спустя значительное время, да и то по косвенным признакам. В связи с этим на данный

момент отсутствует даже самое базовое понимание, какие случаи злонамеренного использования ИКТ можно было бы с уверенностью отнести к прямым угрозам международному миру и безопасности.

Пока не решена проблема атрибуции, равно как и не выработано единого подхода по другим сложным аспектам этой многогранной и специфической проблематики, включая правовые, любая дискуссия в Совете Безопасности может превратиться в очередной обмен бездоказательными обвинениями, привести к углублению раскола в международном сообществе. Все это подрывает авторитет Совета Безопасности и никак не поможет выработать конструктивные решения.

Все государства, которые выступили и еще выступят сегодня, являются участниками Рабочей группы открытого состава, а предложенные к обсуждению вопросы аналогичны тем, которые обсуждаются в Группе. В мае состоялся глобальный «круглый стол» министерского уровня по тематике наращивания потенциала в сфере международной информационной безопасности, в июле предстоит 8-я сессия Рабочей группы открытого состава. По сути, дискуссия по этой теме и так идет непрерывно, а ее ход и результаты доступны для всех.

Поэтому не поддерживаем призыв «повышать осведомленность» международного сообщества по вопросам международной информационной безопасности посредством созыва на регулярной основе заседаний Совета Безопасности. Мандат Совета Безопасности предполагает оперативное реагирование на реальные угрозы международному миру и безопасности, а не философский обмен мнениями по популярным в общественном пространстве темам. Для этого существуют другие площадки и форматы.

Вызывают самую серьезную озабоченность попытки западных коллег использовать обвинения в злонамеренной деятельности с использованием ИКТ в качестве рычага давления на «неугодные» государства. Хоть сколь-нибудь убедительных доказательств в подтверждение этих слов не приводится.

Инструментом в этой нечистоплотной игре неоднократно становилась Группа экспертов Комитета Совета Безопасности 1718 по Корейской Народно-Демократической Республике, которая по наводке «одного государства» обращалась к российской стороне по поводу приписываемых Пхеньяну компьютерных атак. Когда мы просили предоставить точные данные, необходимые для расследования предполагаемых инцидентов, эксперты отвечали, что не получали от своего «источника» дополнительную информацию. Впрочем, отсутствие какой-либо конкретики не мешает западным коллегам голословно, в своем излюбленном стиле «highly likely» («с большей долей вероятности»), обвинять «во всех кибергрехах» не согласные с их действиями страны. Подобные бездоказательные инсинуации неприемлемы. Атрибуция ответственности требует профессионального подхода и предоставления исчерпывающих технических доказательств.

Категорически отвергаем любые рассуждения на тему того, что Россия якобы поощряет злонамеренные действия в информационном пространстве. Мы на протяжении четверти века выступаем за предотвращение его милитаризации и начали предлагать конкретные шаги в этом направлении задолго до того, как страны Запада вообще признали существование такого риска.

Для нашей страны приоритетом является формирование универсальных юридически обязывающих инструментов в области информационной безопасности, что будет способствовать предотвращению межгосударственных конфликтов в этой сфере. В этих целях Россия в 2023 году представила в Генеральной Ассамблее прообраз профильного международного договора — концепцию конвенции об обеспечении международной информационной безопасности. Принятие такой универсальной договоренности позволило бы не только юридически оформить права и обязанности стран, связанные с их деятельностью в сфере ИКТ, но и урегулировать в международных отношениях проблему политической атрибуции компьютерных атак. Это также помогло бы обеспечить неукоснительное соблюдение в информпространстве принципа суверенного равенства государств, который на нынешнем этапе открыто игнорируется многими технологически развитыми странами. Приглашаем все государства-члены к предметной дискуссии на основе нашего предложения на площадке Генеральной Ассамблеи.

К сожалению, западные страны, прежде всего Соединенные Штаты, эту идею отвергают, стремясь сохранить максимальную «свободу рук».

Особенно ярко это проявляется на фоне признания высокопоставленными лицами Соединенных Штатов фактов проведения против России наступательных операций с использованием ИКТ, а также закрепления в доктринальных установках Вашингтона и НАТО «наступательных» — а по сути, агрессивных — подходов.

Наш сегодняшний докладчик и выступавшие рассказывали нам о кибератаках. Только они забыли упомянуть, что против России ведется беспрецедентная дезинформационная война. Координируется вся эта зловредная деятельность из Соединенного Королевства, организациями, базирующимися в Лондоне. Это «Public Relations and Communications Association» и «PR Network», также неустанно трудятся на ниве дезинформации «IT Army of Ukraine». С помощью этих IT-ресурсов в эфир изливаются ушаты дезинформации и лжи в отношении России и российской специальной военной операции.

Тревожат и попытки размывания глобальной дискуссии по вопросам противодействия использованию ИКТ в преступных целях. Ярким примером является «инициатива по противодействию вирусам-вымогателям». Подобные «клубы для избранных», не особо скрывающие свою политизированную направленность, подрывают усилия государств — членов Организации Объединенных Наций по выработке универсальных механизмов борьбы с использованием ИКТ в преступных целях — в частности, по линии профильного Специального комитета Организации Объединенных Наций.

Российская Федерация уже более 26 лет продвигает конструктивную повестку дня в области международной информационной безопасности, внося свой вклад в поддержание мира и стабильности как в реальном, так и в виртуальном мире. Продолжим отстаивать принципы формирования мирной и безопасной среды ИКТ в глобальном масштабе.

Председатель (*говорит по-английски*): Я хотел бы напомнить всем ораторам о необходимости ограничивать продолжительность своих выступлений тремя минутами, с тем чтобы Совет мог оперативно завершить свою работу.

По истечении трех минут на ободке микрофона оратора начнет мигать световой сигнал, указывающий на необходимость завершить выступление.

Г-н Афонсу (Мозамбик) (*говорит по-английски*): Г-н Председатель, Мозамбик хотел бы выразить признательность Вам и Республике Корея за своевременный выбор этой важной темы в качестве знакового мероприятия в рамках председательства Вашей страны в Совете Безопасности в июне. Мы глубоко благодарны Генеральному секретарю за его чрезвычайно продуманный подход к этой теме — подход, который так хорошо и четко согласуется с Уставом Организации Объединенных Наций. Мы пристально следили за высказанными главой Института «Кибермир» г-ном Стефаном Дюгеном и профессором права и технологий Нненной Ифеани-Аджуфо важными мнениями.

Приветствуем министров и высокопоставленных лиц, которые присутствуют сегодня в этом зале.

Все уже сделанные заявления свидетельствуют о том, что границы между киберпространством и физическим миром продолжают стремительно стираться. Вследствие этого практически все аспекты нашей современной жизни переведены в плоскость цифровых технологий и зависят от них. Таким образом, настоятельная необходимость участия Совета подкрепляется тем фактом, что многие страны — как большие, так и малые — всерьез рассматривают киберпространство, которое не имеет границ, как сферу, где может вестись конфликт, наряду с землей, морем, воздухом и космическим пространством.

На самом деле, мы можем считать, что отправной точкой стал 2013 год, когда Генеральная Ассамблея согласилась с тем, что международное право, в том числе Устав Организации Объединенных Наций, действительно является применимым в отношении киберпространства. Тем не менее в глобальном дипломатическом дискурсе обсуждение правил ведения конфликта в киберпространстве пока что продвигается медленнее. В этой связи дискуссии, ведущиеся под эгидой Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, пока не принесли результатов.

Панорама и масштабы киберугроз стремительно меняются ввиду быстрого развития искусственного интеллекта и появления серьезных угроз, порождающих новые вызовы для мира, безопасности

и стабильности на национальном и международном уровнях. В условиях роста киберугроз не проходит и дня без сообщения о совершении атаки на государственную или частную организацию с использованием программы-вымогателя, о распространении генерируемых искусственным интеллектом «дипфейков», которые выглядят очень даже реально, или о попытке совершения атаки типа «отказ в обслуживании» на какой-либо район той или иной страны либо ее основные системы, такие как финансы, здравоохранение, электросеть, электронное правительство и иная критически важная инфраструктура. Поскольку инструменты, созданные для обеспечения возможности жить современной жизнью, используются не по назначению и превращаются в оружие, киберпреступность стала одной из наиболее значительных факторов увеличения угроз, в результате чего подрывается доверие общества к институтам и усиливается политическая и социальная напряженность.

Эти проблемы усугубляются тем, что определяющим фактором в сфере кибербезопасности стало обострение геополитической конкуренции. Рост числа обвинений, попыток возложить ответственность, актов возмездия и эскалационных действий свидетельствует о том, что противники стремятся получить возможности для использования киберпространства в военных и разведывательных целях, провоцируя гонку кибервооружений. По мере того как кибербезопасность становится все более тесно связанной с геополитикой, все менее близкими или даже все менее возможными представляются перспективы прогресса на пути к заключению международного соглашения, в котором были бы прописаны более эффективные нормы кибербезопасности. Такая неспособность сдвинуться с одного места и добиться прогресса в решении столь важного для человечества вопроса может подорвать нашу коллективную безопасность.

В условиях стремительно изменяющегося ландшафта угроз и отсутствия согласованных правил взаимодействия Совет Безопасности должен в срочном порядке выполнить ряд функций и предпринять ряд действий, в том числе следующие.

Во-первых, он должен установить международные нормы и рамки ответственного поведения государств и частных структур в киберпространстве, основанные на глобальном сотрудничестве.

Во-вторых, в духе укрепления нашей коллективной безопасности Совет мог бы поддержать инициативы по наращиванию потенциала в целях укрепления возможностей государств-членов по киберзащите, особенно государств с ограниченными ресурсами.

В-третьих, Совет мог бы содействовать проведению брифингов для повышения ситуационной осведомленности и способствовать обмену информацией об угрозах и передовым опытом между странами в целях повышения нашей общей устойчивости в сфере кибербезопасности.

В-четвертых, киберугрозы должны быть неразрывно связаны с другими пунктами повестки дня Совета Безопасности, такими как борьба с терроризмом, вмешательство в выборы, защита критической инфраструктуры и обеспечение безопасности миротворческих операций и гуманитарной деятельности.

Мы считаем, что крайне важно обновить и расширить дискуссию о кибербезопасности. Не меньшего внимания заслуживают вопросы, связанные с кражей идей, данных, интеллектуальной собственности, с правами человека и с неприкосновенностью частной жизни, а также с параметрами важнейших потребительских товаров и услуг. Для таких стран, как Мозамбик, очень важно, чтобы в глобальной дискуссии по кибербезопасности были услышаны голоса и взгляды стран Юга. Разнообразие точек зрения за столом переговоров и отказ от универсальных подходов крайне важны для достижения глобального прогресса в создании более справедливой и устойчивой системы управления. Поощряя дискуссии, подобные той, которую мы проводим под председательством Республики Корея, Совет может сыграть ключевую роль в обеспечении международного мира и безопасности в цифровую эпоху. Мозамбик привержен дальнейшей работе в этой области.

Г-н Кану (Сьерра-Леоне) (*говорит по-английски*): Благодарю Вас, г-н Председатель, за организацию этих важных открытых прений. Я благодарю также Генерального секретаря Его Превосходительство г-на Антониу Гутерриша за его содержательное сообщение. Мы благодарим также г-на Стефана Дюгена и г-жу Нненну Ифеани-Аджуфо за предоставленную полезную информацию. Приветствуем участие в этом заседании высокопоставленных министров.

Сьерра-Леоне признательна за возможность выступить по важнейшему вопросу противодействия изменяющимся угрозам в киберпространстве, признавая при этом огромные преимущества и взаимосвязанные вызовы, которые информационно-коммуникационные технологии (ИКТ) представляют для международного мира и безопасности. Мы признаем также фундаментальную проблему развития, связанную с устранением глобального цифрового разрыва, и риск углубления этого разрыва в связи с распространением искусственного интеллекта (ИИ), особенно генеративного ИИ.

В настоящем заявлении Сьерра-Леоне конкретно затронет важнейшие проблемы в этой сфере. К основным возникающим и развивающимся тенденциям вредоносной деятельности в киберпространстве, представляющим угрозу международному миру и безопасности, относятся распространение вредоносных программ, маскирующихся программ-вымогателей, применение модели «программа-вымогатель как услуга» и кражи криптовалюты. Эта деятельность представляет значительную опасность для гражданского населения и оказывает разрушительное воздействие на национальную безопасность и общую стабильность наших стран, создавая значительные риски для международного мира.

Мы глубоко обеспокоены развитием тактики, применяемой в киберпространстве, которая не только подпитывает террористическую деятельность, но и ставит под угрозу бесперебойную работы финансовых систем и важнейших служб. Мы подчеркиваем, что все более широкое применение моделей «программа-вымогатель как услуга» и кражи криптовалюты для поддержки злонамеренной деятельности подчеркивает острую необходимость расширения сотрудничества и наращивания потенциала для эффективной борьбы с этими угрозами. Участившиеся в последнее время и ставшие более масштабными атаки против важнейших объектов инфраструктуры и основных государственных служб с использованием программ-вымогателей свидетельствуют о серьезном влиянии киберугроз на общественную безопасность и политическую стабильность и требуют не терять бдительности. Сьерра-Леоне глубоко обеспокоена последствиями киберугроз, включая использование киберпреступлений для финансирования незаконной деятельности и обхода международных санкций. Все эти последствия подчеркивают настоятельную необходимость расширения международного сотрудничества и наращивания потенциала для эффективной борьбы с этими угрозами. Мы призываем к расширению сотрудничества между государствами-членами для укрепления потенциала Совета Безопасности по эффективному реагированию на злонамеренную деятельность в киберпространстве, особенно угрожающую важнейшим объектам инфраструктуры, гуманитарным операциям и защите гражданского населения. Для поддержания мира и безопасности в цифровую эпоху крайне важен целостный подход.

Мы считаем, что злонамеренное использование ИКТ служит фактором, кратно усугубляющим текущие конфликты и проблемы. Все более широкое распространение злонамеренных действий в киберпространстве, направленных против важнейших объектов инфраструктуры, включая больницы и другие системы здравоохранения, финансовые услуги, энергетический сектор, спутники, транспорт и другие экстренные службы, подчеркивает настоятельную необходимость согласованных глобальных действий по защите наших цифровых сетей и систем и важность участия Совета Безопасности в решении этих вопросов, а также в регулировании и разрешении конфликтов, в которых задействованы киберэлементы.

Как мы уже слышали, несмотря на огромные преимущества, ИИ может быть использован в качестве оружия, которое позволяет увеличивать масштабы, скорость и изощренность кибератак. Автономные системы способны вести непрерывные атаки и адаптироваться с учетом факторов внешней среды, что позволяет им более эффективно использовать уязвимости. Такие атаки, осуществляемые под управлением искусственного интеллекта, могут быть направлены против объектов критически важной инфраструктуры, финансовых систем и даже частной жизни людей, что приводит к масштабным нарушениям и ущербу. Вместе с тем мы признаем, что использование искусственного интеллекта в целях киберзащиты может помочь нам действовать на опережение в отношении новых угроз. ИИ может помочь более эффективно обнаруживать угрозы, сократить время реагирования и лучше справляться с инцидентами. Развивая технологии защиты, основанные на искусственном интеллекте, мы сможем создать более устойчивую

киберинфраструктуру. Делая ставку на наращивание потенциала и передачу технологий, мы можем обеспечить развивающимся государствам более равные возможности. Сьерра-Леоне считает, что Совет Безопасности может играть ключевую роль в противодействии меняющимся киберугрозам и укреплении международного мира и безопасности путем всестороннего взаимодействия с соответствующими комитетами Генеральной Ассамблеи, специализированными учреждениями и органами.

За последнее десятилетие Совет Безопасности все больше внимания уделяет воздействию вопросов, связанных с киберпространством, на международный мир и безопасность. С 2016 года члены Совета провели несколько заседаний по формуле Аррии, в ходе которых государства рассматривали вопросы кибербезопасности в контексте различных взаимосвязей с такими темами, как защита критически важной инфраструктуры, защита гражданского населения и дезинформация и язык ненависти в киберпространстве.

В связи с этим Сьерра-Леоне выражает признательность Эстонии за созыв первых открытых прений высокого уровня по этой теме во время ее председательства в июне 2021 года. В свете растущего внимания Совета Безопасности к вопросам кибербезопасности мы поддерживаем предложение о проведении регулярных брифингов для оценки меняющегося спектра киберугроз с учетом мнений различных заинтересованных сторон, чтобы обеспечить всестороннее понимание возникающих проблем и опережать их. Мы подчеркиваем необходимость эффективной координации, сотрудничества и вовлечения Совета для комплексной борьбы с киберугрозами.

Мы подчеркиваем, что участие Совета Безопасности может приобретать формы, дополняющие собой другие текущие процессы в области ИКТ в Организации Объединенных Наций, включая соответствующие обсуждения норм ответственного поведения государств в сфере использования ИКТ и рамок ответственного поведения государств в киберпространстве Организации Объединенных Наций, принятых на основе консенсуса под эгидой Генеральной Ассамблеи.

Разработка оценок и стратегий в связи с меняющейся ситуацией в плане киберугроз на основе учета всеобъемлющей информации, получаемой от структур системы Организации Объединенных Наций, частного сектора, гражданского общества и научных кругов, позволит Совету Безопасности оставаться в курсе новых событий и их последствий для международного мира и безопасности.

Признавая взаимосвязь между киберугрозами и другими пунктами повестки дня Совета Безопасности, государства-члены должны изучить пути эффективного учета проблем, связанных с киберпространством и ИКТ, в существующей работе Совета. Сьерра-Леоне предлагает учитывать проблемы, связанные с киберпространством, при обсуждении Советом различных тематических досье, включая миротворческие миссии, санкционированные Советом санкции, а также усилия по нераспространению и борьбе с терроризмом.

Укрепление национального потенциала в области кибербезопасности и развитие международного сотрудничества являются жизненно важными компонентами такого подхода и также могут быть интегрированы в каждое из этих направлений деятельности. Включив в свою работу рассмотрение тем, касающихся киберпространства, Совет сможет более эффективно решать сложные проблемы, возникающие в связи с киберугрозами, на всеобъемлющей и целостной основе.

Со своей стороны, создание в Сьерра-Леоне Национального координационного центра по реагированию на инциденты, связанные с компьютерной безопасностью, привело к централизации мандата по решению всех вопросов в области кибербезопасности, включая реагирование на инциденты, связанные с кибербезопасностью в Сьерра-Леоне.

С момента своего создания Центр добился значительных успехов в повышении устойчивости национальной кибербезопасности благодаря многогранному подходу к наращиванию потенциала и сотрудничеству. Среди значимых мероприятий — инициативы по наращиванию потенциала в области кибербезопасности и борьбы с преступностью. Центр играет ключевую роль в повышении осведомленности и организации учебных программ для различных заинтересованных сторон, сотрудничая с региональными партнерами и партнерами по развитию в проведении специализированных курсов для сотрудников судебных и правоохранительных органов по вопросам киберпреступности и электронных доказательств, передачи знаний и

обмена передовым опытом в области кибербезопасности и расследования киберпреступлений. Такое сотрудничество повышает коллективный потенциал для эффективной борьбы с глобальными киберугрозами посредством укрепления национальных возможностей.

В заключение позвольте мне прежде всего с сожалением отметить все более дерзкие киберугрозы в отношении наших многосторонних, международных и судебных институтов. В этой связи Сьерра-Леоне безоговорочно осуждает нападения на Международный уголовный суд. Одно из таких нападений было охарактеризовано Судом как «целенаправленное и изощренное нападение с целью шпионажа, [которое] может быть истолковано поэтому как серьезная попытка подорвать мандат Суда». Как государство-участник Сьерра-Леоне подтверждает свое обязательство поддерживать и защищать принципы и ценности, закрепленные в Римском статуте, и защищать его целостность от любого вмешательства и давления в отношении Суда, его должностных лиц и тех, кто с ним сотрудничает.

Во-вторых, позвольте мне подтвердить приверженность Сьерра-Леоне делу обеспечения кибербезопасности как основополагающего аспекта международного мира и безопасности и совместной работе в рамках Совета Безопасности и более широкого международного сообщества по устранению сложных и эволюционирующих угроз в киберпространстве, создаваемых вредоносной деятельностью.

Г-н Бенджама (Алжир) (*говорит по-английски*): Я благодарю Вас, г-н Председатель, за организацию этих важных открытых прений о растущих рисках киберугроз для глобальной безопасности. Я также благодарю Генерального секретаря и докладчиков за их сообщения, посвященные вызывающему тревогу росту числа вредоносных актов в киберпространстве.

Атаки на критически важные объекты инфраструктуры с использованием вирусов-вымогателей и кража цифровых активов и данных ставят под угрозу общественную безопасность и политическую стабильность. Участие как правительственных, так и неправительственных организаций делает ситуацию еще более сложной и опасной. Распространение дезинформации на онлайн-платформах разжигает рознь, ненависть и нетерпимость, а в конечном счете — терроризм, ложная информация вносит помехи в государственные дела, препятствует сотрудничеству и в конечном счете угрожает миру и безопасности во всем мире.

Новые технологии, включая искусственный интеллект, делают киберугрозы еще более серьезными и усложняют борьбу с ними. Поэтому нам необходимо в срочном порядке решать эти проблемы на глобальном уровне. Учитывая ситуацию, я хочу подчеркнуть несколько ключевых моментов.

Во-первых, принципы Устава Организации Объединенных Наций должны в равной степени применяться к киберпространству. Информационно-коммуникационные технологии должны использоваться в соответствии с этими принципами.

Во-вторых, мы стремимся обеспечить открытое и безопасное киберпространство, что необходимо для достижения глобальных целей в области развития, предусмотренных Повесткой дня в области устойчивого развития на период до 2030 года. Поэтому нам нужна юридически обязывающая основа, созданная в рамках Организации Объединенных Наций.

В-третьих, мы должны помочь развивающимся странам создать защиту от киберугроз и ликвидировать цифровой разрыв. Развитие их потенциала необходимо для обеспечения безопасности киберпространства для всех стран и должно быть одним из основных приоритетов.

В-четвертых, международное сообщество должно совместно бороться с распространением ложной информации в Интернете. Правительства являются вовлеченными сторонами, и вовлеченные стороны должны сотрудничать в соответствии с международным правом. Международное сотрудничество является ключевым фактором в наших усилиях по эффективной борьбе с постоянно меняющимися киберугрозами.

В-пятых, нам необходимо укрепить правовую базу для предотвращения киберпреступлений и наказания за них. В этом отношении я хотел бы подчеркнуть, что наша страна играет активную роль в международных усилиях по борьбе с пагубным использованием технологий в преступной деятельности. Это особенно четко видно на примере осуществляемого Алжиром руководства работой Специального комитета Организации Объединенных Наций по разработке всеобъемлющей международ-

ной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Надеемся, что в ходе своей следующей сессии этим летом Комитету удастся добиться успешных результатов.

В заключение хочу сказать, что Алжир решительно поддерживает роль Организации Объединенных Наций в решении связанных с использованием информационно-коммуникационных технологий вопросов, оказывающих влияние на международный мир и безопасность. Рабочая группа открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и Генеральная Ассамблея являются важнейшими площадками для всестороннего обсуждения киберугроз. Они обеспечивают участие всех государств-членов в разработке глобальных мер реагирования на вызовы в области кибербезопасности, и мы подтверждаем нашу готовность поддерживать их неоценимый труд.

Г-н Жбогар (Словения) (*говорит по-английски*): Выражаю благодарность Республике Корея за организацию сегодняшних прений. Благодарю также Генерального секретаря за его сообщение и выражаю признательность нашим сегодняшним докладчикам за предоставленную ими информацию и вынесенные ими рекомендации.

Позвольте мне остановиться на двух моментах, которые имеют отношение к теме сегодняшних прений.

Во-первых, что касается эволюционирующих угроз в киберпространстве, то, на наш взгляд, четкое понимание постоянно меняющейся ситуации с киберугрозами, особенно в контексте стремительного развития новых технологий, таких как искусственный интеллект, имеет первостепенное значение для обсуждения мер сотрудничества, которые международное сообщество может принять в ответ на злонамеренную активность с использованием киберсредств. В этой связи высоко оцениваем текущую работу учрежденной Генеральной Ассамблеей специальной Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и при этом признаем необходимость изучения Советом дополнительных материалов, таких как выводы, содержащиеся в докладе Генерального секретаря о киберугрозах (A/77/92), для более углубленного рассмотрения этого вопроса. Злонамеренная активность с использованием киберсредств, в том числе атаки с использованием вирусов-вымогателей и атаки на объекты критически важной гражданской инфраструктуры, особенно трансграничные по своему характеру атаки, могут создавать новые проблемы и усугублять существующие угрозы международному миру и безопасности.

Это подводит меня к моему второму замечанию, а именно к вопросу о борьбе с эволюционирующими угрозами в киберпространстве. Совет несет главную ответственность за поддержание международного мира и безопасности. Для того чтобы выполнять свои обязанности в соответствии с мандатом, Совет должен играть решающую роль в деэскалации напряженности и содействии привлечению виновных к ответственности в тех случаях, когда злонамеренная активность с использованием киберсредств создает угрозу международному миру и безопасности. По нашему мнению, деятельность, способствующая развитию терроризма и распространению оружия массового уничтожения, как и деятельность, обостряющая существующие конфликты или направленная против критически важной гражданской инфраструктуры, представляет собой такую угрозу и, следовательно, требует ответных мер со стороны Совета. Кроме того, Совет должен вести борьбу с такой злонамеренной активностью с использованием киберсредств, как кампании по дезинформации, которые подстрекают к насилию против гражданского населения, причиняют человеческие страдания или нарушают работу гуманитарных организаций и миротворческих и миростроительных операций.

В эпоху, характеризующуюся растущей цифровизацией конфликтов, крайне важно подчеркнуть применимость международного права, включая международное гуманитарное право и международные стандарты в области прав человека, которые должны соблюдаться.

В заключение позвольте мне заверить Совет в нашей готовности сотрудничать с членами Совета и всеми членами Организации Объединенных Наций в организации дальнейших дискуссий о киберугрозах международному миру и безопасности. Мы также по-прежнему решительно настроены

осуществлять меры, направленные на снижение этих рисков, в том числе путем реализации существующих норм ответственного поведения государств в киберпространстве.

Г-жа Фрейзьер (Мальта) (*говорит по-английски*): Прежде всего позвольте поблагодарить Республику Корея за организацию этих открытых прений по столь актуальному и важному вопросу. Благодарю также Генерального секретаря и докладчиков за их содержательные сообщения.

Злонамеренная активность с использованием киберсредств представляет собой многогранную проблему, которая может иметь серьезные последствия для поддержания международного мира и безопасности. Речь идет, среди прочего, о применении вирусов-вымогателей против государственных учреждений, критически важной инфраструктуры и основных государственных служб, а также о получении несанкционированного доступа к хранящимся в электронном виде данным и их неправомерном использовании.

Мы встревожены злонамеренной активностью с использованием киберсредств, направленной против государственных учреждений и демократических процессов и зачастую имеющей своей непосредственной целью подрыв стабильности и безопасности и снижение доверия к результатам демократических выборов. Растущая зависимость женщин-правозащитников и других активистов от цифровых технологий повышает их риск подвергнуться преследованиям и нападениям в Интернете. Кроме того, права человека и основные свободы, включая свободу выражения мнений и собраний, все больше ограничиваются за счет строгого наблюдения, отключения Интернета и уменьшения пропускной способности. В то же время цифровые платформы часто используются для распространения дезинформации, ложной информации и ненавистнических высказываний, включая женоненавистнические, гомофобные и радикализирующие материалы.

Наши коллективные усилия по поощрению стабильности в этой сфере должны опираться на права человека как в Интернете, так и в реальной жизни. Для выявления и предотвращения вредного воздействия угроз в области цифровой безопасности, таких как гендерное насилие, которому способствует развитие технологий, в рамках стратегий по обеспечению кибербезопасности должны учитываться особые условия, связанные с конфликтами, возрастом и гендерной принадлежностью. Полноценное, равноправное, безопасное и значимое лидерство и участие женщин в принятии связанных с кибербезопасностью решений имеет огромное значение, особенно в условиях конфликта и в постконфликтных ситуациях.

Подтверждаем, что международное право, в частности Устав Организации Объединенных Наций, применимо к деятельности в киберпространстве, что признается и Генеральной Ассамблеей. Кроме того, правила ответственного поведения государств в киберпространстве представляют собой согласованные руководящие принципы для государств-членов. Эти правила должны соблюдаться всеми государствами-членами, и мы поддерживаем разработку программы действий для налаживания постоянного системного диалога. Мы также призываем все государства проявлять осмотрительность, принимать соответствующие меры с учетом норм ответственного поведения государств в киберпространстве и воздерживаться от участия в злонамеренной активности с использованием киберсредств, осуществляемой с их территории, и от содействия такой активности.

Спонсируемые государствами злоумышленники в киберпространстве используют вирусы-вымогатели и крадут цифровые данные для получения незаконных доходов. В частности, они совершают атаки на критически важную инфраструктуру, финансовые учреждения и криптовалютные компании. Кибератаки и киберпреступления не знают границ, и ни одна страна не застрахована от них. По оценкам специалистов, только в 2023 году злонамеренная активность с использованием киберсредств, осуществляемая хакерами, спонсируемыми Корейской Народно-Демократической Республикой, принесла доход, эквивалентный 1 млрд долл. США. Режим использует эти доходы для финансирования своей незаконной программы создания оружия массового уничтожения, которая угрожает миру и безопасности на полуострове и за его пределами. Эта деятельность подробна описана в докладах Группы экспертов Комитета, учрежденного резолюцией 1718 (2006), которая сыграла неоценимую роль в расследовании этих преступлений.

В заключение следует отметить, что Совет Безопасности может сыграть важную роль в решении вопроса кибербезопасности. Его усилия могут и должны дополнять другие форумы по кибербезопасности, действующие в Генеральной Ассамблее, включая ее Рабочую группу открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. Совет может стать мощной платформой для утверждения согласованных принципов и активизации дальнейших обсуждений. Он должен способствовать созданию открытого, безопасного, доступного и мирного киберпространства. Мы намерены и впредь поддерживать активизацию его работы по этому вопросу.

Г-н Ямадзаки (Япония) (*говорит по-английски*): Я искренне благодарю Вас, г-н Председатель, за Вашу руководящую роль в созыве этих важных и своевременных открытых прений, а также благодарю Генерального секретаря и докладчиков за их ценные идеи.

Прежде всего Япония хотела бы выразить свою приверженность содействию созданию свободного, справедливого и безопасного киберпространства. В последние годы мы наблюдаем тревожную тенденцию качественного и количественного роста кибероперaций, используемых во вредоносных целях, включая атаки с использованием вирусов-вымогателей, повреждение критической инфраструктуры, вмешательство в демократические выборы и кражу конфиденциальных данных. Тревожный рост краж криптовалюты также представляет собой явную и актуальную угрозу международному миру и безопасности, поскольку это может использоваться для финансирования незаконных программ вооружений. В частности, хорошо известно, что Северная Корея финансирует свои программы создания оружия массового уничтожения и баллистических ракет за счет вредоносных кибероперaций, и международное сообщество должно в срочном порядке бороться с такими угрозами, как об этом говорится в отчете Группы экспертов Комитета, учрежденного резолюцией 1718 (2006). Кроме того, распространение коммерческих средств кибервмешательства, таких как шпионские программы, вызывает глубокую озабоченность в связи с их влиянием на национальную безопасность, права человека и международный мир и безопасность. Ставки как никогда высоки.

Чтобы решить эти тревожные проблемы и обеспечить свободное, справедливое и безопасное киберпространство, мы должны поддерживать верховенство права в киберпространстве, поощряя конкретные дискуссии по применению существующего международного права и реализации согласованных норм, правил и принципов ответственного поведения государств. Мы также должны придавать большое значение обмену информацией о существующих потенциальных угрозах, обмену передовым опытом и содействию усилиям по наращиванию потенциала. Посредством диалога на всех уровнях мы должны стремиться к укреплению доверия, снижению угроз и, самое главное, уменьшению просчетов. В рамках Организации Объединенных Наций Япония продолжит конструктивное участие в работе нынешней Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Япония также считает, что программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, будучи ориентированной на действия рамочной программой, в будущем должна служить постоянной платформой для содействия осуществлению согласованных норм, правил и принципов ответственного поведения государств.

В то же время Япония полностью согласна с тем, что Совет Безопасности, несущий главную ответственность за поддержание мира и безопасности, должен играть более значительную и дополняющую роль в области кибербезопасности. Совет должен внимательно следить за серьезными инцидентами в киберпространстве, имеющими важные последствия для международного мира и безопасности, включая те, которые направлены против критической инфраструктуры. Регулярные брифинги в Совете были бы очень полезны для отслеживания меняющегося спектра угроз безопасности в сфере информационно-коммуникационных технологий (ИКТ). Кроме того, Совет должен рассматривать растущие киберугрозы для глобального режима контроля над вооружениями и нераспространения, включая риски распространения, потенциально создаваемые негосударственными субъектами.

В заключение Япония подтверждает свою непоколебимую приверженность защите свободного, справедливого и безопасного киберпространства.

Совет Безопасности должен сохранять повышенную бдительность в отношении возникающих рисков для безопасности, связанных с ИКТ. Мы надеемся на продолжение обсуждения дальнейших шагов Совета по эффективному решению этой важной проблемы на основе сегодняшних прений, которые были проведены по Вашей инициативе, г-н Председатель.

Дама Барбара Вудворд (Соединенное Королевство) (*говорит по-английски*): Я благодарю министра иностранных дел Республики Корея Чхо Дэ Юля за организацию этих прений и за то, что он представил Совету Безопасности несколько четких идей о том, как мы можем добиться прогресса в нашей работе в этой области. Я также благодарю Генерального секретаря и наших сегодняшних докладчиков за то, что они рассказали о том, как киберугрозы могут повлиять на международный мир и безопасность.

Я остановлюсь на трех тенденциях, имеющих важное значение для Соединенного Королевства.

Во-первых, как мы уже слышали, применение вирусов-вымогателей может нарушить работу правительства и предоставление жизненно важных государственных услуг. Когда это приобретает масштабный характер или сохраняется в течение длительного времени, складываются условия для возникновения нестабильности, что, как известно Совету, может повлиять на мир и безопасность. Любое государство может стать жертвой применения вирусов-вымогателей. Именно поэтому необходимо принять международные меры, чтобы ограничить способствующую этому экосистему и дать возможность всем государствам повысить свою устойчивость и способность к реагированию. Соединенное Королевство играет ведущую роль, будучи вместе с Сингапуром сопредседателями политического компонента Инициативы по борьбе с применением вирусов-вымогателей. Мы призываем других присоединиться к этой инициативе.

Во-вторых, поскольку использование систем искусственного интеллекта (ИИ) в наших обществах расширяется, мы должны понимать, как изменятся киберугрозы, и одновременно выявлять возможности использования ИИ для достижения наших целей в области кибербезопасности. Злоумышленники и безответственные субъекты могут использовать уязвимости в системах ИИ, чтобы вызвать у них определенное поведение или манипулировать процессом принятия решений. Для поддержания международного мира системы ИИ должны быть безопасными по своей конструкции. Именно поэтому в прошлом году во время нашего председательства Соединенное Королевство впервые провело в Совете прения по ИИ (см. S/PV.9381), и именно поэтому мы совместно с Соединенными Штатами и межрегиональной группой из 18 государств опубликовали руководство по безопасной разработке систем ИИ.

В-третьих, злоумышленники и безответственные субъекты также могут воспользоваться растущим рынком передовых средств кибервмешательства, что приведет к созданию более непредсказуемого спектра угроз для всех нас. Соединенное Королевство и Франция приглашают международных партнеров присоединиться к нам в рамках многостороннего Пэлл-Мэллского процесса, где мы рассматриваем подходы к решению этой общей проблемы.

В этом контексте мы должны продолжать повышать осведомленность о киберугрозах. Так, мы очень обеспокоены тем, что Корейская Народно-Демократическая Республика использует вредоносные действия в киберпространстве в целях получения криптовалюты для финансирования своей незаконной программы вооружений. Именно поэтому мы должны удвоить наши усилия по обеспечению эффективного соблюдения режима санкций в отношении Корейской Народно-Демократической Республики.

Наконец, киберугрозы также повышают риски дезинформации. Это, безусловно, серьезная проблема в нашей работе. То, что Россия обвиняет Соединенное Королевство в ведении дезинформационной войны, поражает, поскольку ее собственная машина дезинформации была так явно и четко разоблачена, в том числе здесь, в Организации Объединенных Наций. Не мы были той делегацией, которая принесла в этот зал и в Интернет теорию заговора об использовании летучих мышей и уток в качестве оружия.

Киберугрозы будут представлять все больший риск для международного мира и безопасности, и правительства должны эволюционировать, чтобы эффективно противостоять им. В рамках этой деятельности Соединенное Королевство по-прежнему привержено соблюдению рамок ответственного

поведения государств в киберпространстве Организации Объединенных Наций и сотрудничеству с другими странами путем наращивания потенциала и создания условий для партнерства между государственным и частным секторами.

Г-жа Чанда (Швейцария) (*говорит по-французски*): Я благодарю Республику Корея за организацию этих важных прений по угрозам в области кибербезопасности. Я также благодарю Генерального секретаря, профессора Нненну Ифеани-Аджуфо и г-на Стефана Дюгена, главного административного сотрудника Института «КиберМир» в Женеве, за их сообщения.

Швейцария является свидетелем двух переломных изменений в киберпространстве, которые вызывают у нас озабоченность. С одной стороны, растущая цифровизация конфликтов и использование кибероперации в вооруженных конфликтах меняют характер этих конфликтов. С другой стороны, серьезную озабоченность Швейцарии вызывает растущая интенсивность атак с применением программ-вымогателей и спонсируемых государством кибератак в отношении важнейших объектов инфраструктуры. Атаки с применением специальных программ для вымогательства денежных средств и криптовалют или атаки, направленные против критически важных объектов инфраструктуры, могут парализовать ключевые системы нашего общества. Поскольку развивающиеся страны особенно уязвимы в этой связи, соответствующие действия затрагивают также возможности международного сообщества в плане достижения целей в области устойчивого развития. Они могут представлять угрозу для международного мира и безопасности и поэтому являются прерогативой Совета.

В концептуальной записке, предложенной Республикой Корея (S/2024/446, приложение), ставится вопрос о том, какую роль может играть Совет в борьбе с угрозами, возникающими в результате злонамеренной деятельности в киберпространстве. Позвольте остановиться на некоторых связанных с этим аспектах.

Во-первых, Совет должен регулярно отслеживать текущие события и угрозы в сфере кибербезопасности. С учетом многогранных последствий и географического охвата проблемы было бы целесообразным проведение регулярных брифингов в Совете. В ходе таких брифингов могли бы выступать представители учреждений системы Организации Объединенных Наций, частного сектора, гражданского общества и научных кругов, а также других соответствующих структур. Такое повышение осведомленности позволило бы Совету принимать полностью обоснованные решения, в частности по конкретным географическим вопросам и в контексте операций по поддержанию мира.

Во-вторых, Совет должен подтвердить некоторые устоявшиеся принципы. Мы придаем особое значение вопросам применимости норм международного права к киберпространству, особенно применимости норм международного гуманитарного права к деятельности в киберпространстве в контексте вооруженного конфликта. Совет должен также подчеркнуть важность ответственности и должной осмотрительности государств и признать 11 норм ответственного поведения государств в киберпространстве. Эти элементы, дополняемые мерами по укреплению доверия и наращиванию потенциала, составляют рамки ответственного поведения государств в киберпространстве, которые были приняты всеми государствами-членами на основе консенсуса. Мы поддержали бы документ Совета, в котором подтверждалась бы эта основа, что тем самым способствовало бы восстановлению доверия.

Наконец, деятельность Совета должна дополнять деятельность других органов. В компетенцию Совета не входит разработка правил поведения или соглашений. Это прерогатива Генеральной Ассамблеи и уполномоченных ею экспертных процессов. Совет должен сосредоточить свое внимание на углублении понимания рисков и их смягчении, в том числе в конкретных случаях.

Несмотря на признанные риски в этой сфере, ответственное использование киберпространства открывает огромные возможности для решения задач будущего. В своей Новой повестке дня для мира Генеральный секретарь призывает нас найти новые способы защиты от этих новых угроз. Хотя переговоры в отношении Пакта во имя будущего дают нам возможность выработать общее понимание в этом вопросе, Совет также призван играть ключевую роль. Сегодняшние прения это подтверждают.

Г-н Фу Цун (Китай) (*говорит по-китайски*): Г-н Председатель, благодарю Вас за руководство сегодняшним заседанием. Благодарю Генерального секретаря Гутерриша за сообщение и благодарю также обоих экспертов за их выступления.

Сегодня мы живем в беспрецедентную цифровую эпоху, во время стремительной революции в сфере информационных технологий, бурного развития цифровой экономики и киберэкономики и ускоренного формирования на международном уровне сообщества с общим будущим, взаимосвязанными интересами, а также общими радостями и бедами. В то же время риски и проблемы в киберпространстве становятся все более серьезными. Не прекращаются кибератаки, кибершпионаж, киберпреступления и дезинформация. Глобальной общественной угрозой стал кибертерроризм. Повышается степень милитаризации, блоковый характер и идеологизированность киберпространства, а также продолжает расти цифровое неравенство между странами и регионами.

Хотя все страны пользуются общими возможностями и имеют общие интересы в киберпространстве, они также сталкиваются с общими проблемами и несут общую ответственность. Международное сообщество должно углублять обмены, укреплять взаимное доверие, действовать сообща, а также коллективно способствовать регулированию киберпространства и выработке международных правил в этой сфере. Китай хотел бы предложить следующее.

Во-первых, нам необходимо создать более мирное и безопасное киберпространство. Киберпространство глубоко интегрировано с физическим миром и является важной опорой для развития человеческого общества. Оно не должно никогда стать новым театром боевых действий. Есть одна страна, которая рассматривает киберпространство в качестве пространства для проведения военных операций, развивает наступательный военный кибер потенциал, создает военные кибер альянсы и добивается выработки правил ведения военных действий в киберпространстве. Такое поведение лишь подорвет взаимное доверие между странами, усилит риски трений и конфликтов в киберпространстве и поставит под угрозу международный мир и безопасность. Все стороны должны отказаться от действий в духе антагонизма и менталитета «холодной войны», придерживаться концепции общей, всеобъемлющей, совместной и устойчивой безопасности, твердо отстаивать мирный характер киберпространства, эффективно предотвращать милитаризацию и гонку вооружений в киберпространстве, устранять угрозы кибербезопасности посредством диалога и сотрудничества и сохранять приверженность обеспечению собственной безопасности посредством укрепления коллективной безопасности.

Во-вторых, нам необходимо добиваться того, чтобы киберпространство в большей степени несло всеобщее благо и процветание. Цифровая экономика и киберэкономика уже стали основными двигателями глобального экономического роста. Все страны должны проводить более активную, открытую, скоординированную и инклюзивную политику, способствовать применению и популяризации информационно-коммуникационных технологий (ИКТ) и обеспечивать открытость, стабильность и безопасность производственных цепочек в сфере ИКТ, для того чтобы больше стран и людей могли воспользоваться преимуществами Интернета. Развитые страны должны помогать развивающимся странам в обеспечении развития на основе цифровых, сетевых и «умных» технологий, укреплять их потенциал в части предотвращения рисков и реагирования на чрезвычайные ситуации, а также обеспечивать равноправный доступ к ключевым ресурсам, в том числе технологиям создания киберинфраструктуры и вычислительным мощностям, для того чтобы минимизировать цифровой разрыв и достичь целей в области устойчивого развития, сформулированных в Повестке дня в области устойчивого развития на период до 2030 года. Практика формирования узких группировок по идеологическому признаку, чрезмерное расширение концепции национальной безопасности, возведение железного занавеса в сфере цифровых технологий, стремление к технологическому доминированию и преимуществам, а также откровенное вмешательство и подавление экономического и технологического развития других стран будут лишь мешать усилиям международного сообщества по развитию системы регулирования киберпространства.

В-третьих, нам необходимо создать более равноправное и упорядоченное киберпространство. Разработка приемлемых для всех международных правил в киберпространстве является ключом к поддержанию прочного мира и стабильности в киберпространстве. Все стороны должны добросовестно соблюдать цели и принципы Устава Организации Объединенных Наций, в частности принципы суверенного равенства, невмешательства во

внутренние дела, неприменения силы или угрозы силой и мирного урегулирования споров, а также соблюдать и выполнять принятые Организацией Объединенных Наций рамки ответственного поведения государств в киберпространстве. В то же время все стороны должны неизменно поддерживать роль Организации Объединенных Наций в качестве главной площадки, а также на основе равноправного и широкого участия в рамках давно достигнутого на международном уровне консенсуса выработать юридически обязательные нормы поведения в киберпространстве. Предложенные Китаем конструктивные инициативы, такие как Глобальная инициатива по регулированию искусственного интеллекта и Глобальная инициатива по безопасности данных, могут стать основой для будущего нормотворчества в вопросах киберпространства.

В-четвертых, нам необходимо создать более равное и инклюзивное киберпространство. Многообразие — важнейшая особенность нашего мира и движущая сила человеческого прогресса. Интернет связывает все страны, народы и цивилизации способами, которые раньше невозможно было представить, и по понятным причинам должен стать для всего человечества важной платформой для демонстрации различных культур и содействия развитию и преемственности цивилизаций. Нам необходимо в полной мере использовать возможности ИКТ, активизировать онлайн-взаимодействие в рамках диалога, поощрять взаимопонимание и дружбу между народами всех стран, содействовать терпимости и сосуществованию различных цивилизаций и более активно пропагандировать общие ценности человечества. Следует настороженно отнестись к стремлению небольшого числа стран навязывать свои собственные ценности в качестве универсальных и даже вмешиваться во внутренние дела других стран, подрывая их развитие и стабильность. Мы должны решительно противостоять использованию киберпространства для распространения идей экстремизма и терроризма, дезинформации и языка ненависти.

Китай наблюдает за развитием Интернета и пользуется его преимуществами. Сегодня в нашей стране проживает около 1,1 миллиарда пользователей Интернета. Мы создали крупнейшую в мире и самую передовую в технологическом отношении киберинфраструктуру и разработали надежную систему регулирования киберпространства. В последние годы Китай активно расширяет взаимодействие и обмен опытом со странами глобального Юга по вопросам политики; содействует практическому сотрудничеству с целью наращивания потенциала в таких областях, как инфраструктура, технологии, правоприменение и реагирование на чрезвычайные ситуации; активно участвует в процессах обсуждения вопросов кибербезопасности в рамках таких структур, как Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ; Группа двадцати, Форум Азиатско-Тихоокеанского экономического сотрудничества, группа Бразилии, России, Индии, Китая и Южной Африки, Шанхайская организация сотрудничества, Региональный форум Ассоциации государств Юго-Восточной Азии и другие, а также вносит важный вклад в развитие глобального управления киберпространством.

Информационная революция как главная тенденция нашего времени набирает обороты. Киберпространство дает человечеству безграничную надежду на светлое будущее. Китай готов вместе с другими членами международного сообщества работать над созданием более мирного, безопасного, открытого, основанного на сотрудничестве и регулируемого киберпространства и объединить усилия для создания сообщества с общим будущим в киберпространстве.

Г-н де ла Гаска (Эквадор) (*говорит по-испански*): Я хотел бы приветствовать присутствующего на этом заседании министра иностранных дел Республики Корея г-на Чхо Дэ Юля. Я также благодарю Генерального секретаря Антониу Гутерриша за предоставленную информацию и докладчиков, г-на Стефана Дюгена и г-жу Нненну Ифеани-Аджуфо, за их сообщения.

В мире, который становится все более взаимосвязанным и взаимозависимым, обеспечение кибербезопасности является глобальной задачей, требующей скоординированных и совместных действий всего международного сообщества.

Злонамеренное использование информационно-коммуникационных технологий (ИКТ) множит угрозы миру и безопасности, в том числе в следующих областях.

Во-первых, оно может повлиять на работу критически важной инфраструктуры, в частности на

системы здравоохранения, предоставление финансовых услуг и работу энергетических сетей, которые необходимы для функционирования общества.

Во-вторых, оно может быть инструментом распространения дезинформации и разжигания ненависти, усиливая поляризацию в обществе и обостряя конфликты.

В-третьих, он может использоваться для содействия террористической деятельности и финансирования незаконной деятельности государственных и негосударственных субъектов.

Учитывая эти вызовы, реагирование Совета Безопасности не должно отставать от темпов эволюции киберугроз, поскольку такие угрозы связаны с несколькими пунктами повестки дня Совета, включая нераспространение и борьбу с терроризмом. В этой связи Совету Безопасности следует рассмотреть возможность включения в свои документы положений, касающихся обеспечения кибербезопасности, в зависимости от потребностей каждой конкретной ситуации. Одним из примеров является укрепление стратегических коммуникаций в рамках миротворческих операций и специальных политических миссий.

Содействие созданию безопасного, открытого и мирного киберпространства требует соблюдения стандартов ответственного поведения при использовании ИКТ. Кроме того, развитие международного права в этой области должно сопровождаться наращиванием потенциала, особенно в странах, находящихся в конфликтной ситуации, поскольку они наиболее уязвимы к неправомерному использованию ИКТ. Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ добивается прогресса в этой области. Результаты ее работы могут послужить ориентиром для работы Совета.

В заключение я хотел бы напомнить о необходимости дальнейшего обеспечения и поощрения ответственного использования киберпространства, с тем чтобы гарантировать его стабильность и безопасность и тем самым снизить значительный риск, который оно представляет для государств.

Г-н де Ривьер (Франция) (*говорит по-французски*): Я благодарю Генерального секретаря, г-на Дюгена и г-жу Ифеани-Аджуфо за их брифинги и благодарю Вас, г-н Председатель, за созыв этих прений.

Развитие информационно-коммуникационных технологий способствует прогрессу и достижению целей в области устойчивого развития. Тем не менее оно также создает серьезные угрозы для нашей коллективной безопасности. В обществах, которые в значительной степени зависят от этих технологий, вредоносные кибератаки становятся все более частыми, серьезными и изощренными. Нарушители способны использовать многочисленные факторы уязвимости и применяют все более разнообразные методы, которые теперь доступны множеству субъектов. Используемые для таких атак инструменты и сервисы бесконтрольно распространяются на рынках, и их безответственное использование способствует росту числа киберугроз.

Кибератаки сами по себе могут представлять угрозу международному миру и безопасности из-за их воздействия на критически важную инфраструктуру и рисков эскалации, которые они влекут за собой. Кибератаки с целью получения выкупа, число которых, по данным французских властей, в 2023 году увеличилось на 30 процентов, могут затронуть такие важные отрасли, как энергетический сектор, дестабилизировать экономику стран и даже нарушить работу государственных учреждений. Кибератаки теперь также осуществляются в контексте вооруженных конфликтов, как мы видели на примере атак, совершенных Россией против спутниковой сети «Viasat» в первые часы ее незаконного вторжения на Украину.

Злонамеренная деятельность с использованием киберсредств может также усиливать другие угрозы международному миру и безопасности, включая распространение. В последнем докладе Группы экспертов Комитета, учрежденного резолюцией 1718 (2006) (S/2024/215), отмечается, что незаконные программы северокорейского режима по созданию оружия массового уничтожения на 40 процентов финансировались за счет средств, полученных в результате незаконных действий в киберпространстве, таких как вымогательство или кража криптовалюты.

Тем не менее Организация Объединенных Наций и Совет Безопасности, выполняя свой мандат, располагают возможностями для скоординированного реагирования на эти угрозы. Прежде всего следует помнить о том, что киберпространство — это не Дикий Запад, и в нем не существует нормативно-

го вакуума. Международное право, включая Устав Организации Объединенных Наций, международное гуманитарное право и международное право прав человека, полностью применимо в киберпространстве. Кроме того, на основе консенсуса были разработаны нормы ответственного поведения государств в целях развития сотрудничества, предотвращения конфликтов и укрепления стабильности в киберпространстве.

Франция поддерживает работу Первого комитета Генеральной Ассамблеи по дальнейшему развитию этой нормативной базы. Для поддержки ее применения Франция предложила структуру будущего амбициозного механизма программы действий для киберпространства. Совет Безопасности должен сделать соблюдение нормативных рамок ответственного поведения государств в киберпространстве главным элементом своей работы по борьбе с киберугрозами и призвать государства выполнять свои обязательства по содействию обеспечению безопасности и стабильности киберпространства.

Кроме того, Совет Безопасности должен продолжать свои усилия по включению проблематики киберпространства в различные аспекты своего мандата. Очень важно, чтобы Совет регулярно информировали эксперты об эволюции киберугроз и их последствиях для международного мира и безопасности. Сегодняшние прения являются ценным примером таких усилий.

Совет также должен продолжать уделять внимание использованию киберсредств для обхода режимов санкций. Злонамеренная деятельность с использованием киберсредств, осуществляемая северокорейским режимом для финансирования своих программ по созданию оружия массового уничтожения, заслуживает постоянного внимания в этой связи. Франция будет продолжать активно добиваться того, чтобы несмотря на то, что мандат Группы экспертов Комитета 1718 не был продлен, Совет продолжал бдительно следить за нарушениями своих резолюций в этой области.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово министру иностранных дел, международного сотрудничества и по делам гамбийцев за рубежом Республики Гамбия Его Превосходительству г-ну Мамаду Тангаре.

Г-н Тангара (Гамбия) (*говорит по-английски*): Прежде всего я хотел бы поблагодарить докладчиков за их познавательные замечания и поздравить Республику Корея с организацией этих прений.

Сегодня мы стоим на перепутье. Цифровая эпоха сплела паутину связей, возможностей и прогресса. Однако внутри этой паутины скрывается растущая тьма, угрожающая международному миру и безопасности. Постоянно растущая угроза киберпреступности — это не просто вопрос финансовой выгоды или украденных данных. Новая волна киберугроз бросает прямой вызов международному миру и безопасности, требуя нашего неотложного внимания. В этой связи мы благодарим Республику Корея за привлечение нашего внимания к еще одному новаторскому мероприятию Совета Безопасности с целью обмена мнениями по существу пункта повестки дня «Поддержание международного мира и безопасности: противодействие меняющимся угрозам в киберпространстве». Как орган, которому поручено поддерживать международный мир и безопасность, Совет Безопасности не может позволить себе молчать, и мы воздаем ему должное за его постоянные усилия, направленные на то, чтобы бить тревогу по этому важному и общему вопросу. Нам нужен комплексный подход к решению этой эволюционирующей угрозы.

В этой связи я хотел бы предложить следующие три направления действий, которые будут содействовать нашим совместным усилиям по борьбе с киберугрозами международному миру и безопасности.

Во-первых, Совет Безопасности должен стать поборником образцового следования нормам ответственного поведения государств в киберпространстве, и мы можем добиться этого, регулярно повышая уровень осведомленности, чтобы стимулировать соответствующие дискуссии по вопросам кибербезопасности с целью активизации работы киберфорумов Генеральной Ассамблеи, и работая с государствами-членами над воплощением этих норм в жизнь, содействуя наращиванию потенциала и обмену информацией для сдерживания вредоносной деятельности.

Во-вторых, Совет Безопасности может усилить ответственность за угрозы в области кибербезопасности, выступая за повышение потенциала

государств-членов в киберпространстве, чтобы выявлять злонамеренных субъектов и создать единый фронт борьбы с безнаказанностью.

В-третьих, Совет Безопасности может использовать опыт учреждений Организации Объединенных Наций, таких как Управление по вопросам разоружения и Контртеррористическое управление, для адекватного противодействия угрозе подрыва устойчивого международного мира, безопасности и демократии. Сотрудничество с этими учреждениями также может способствовать координации деятельности, чтобы избежать дублирования и обеспечить комплексный подход, отвечающий поставленным целям.

Эти действия, предпринимаемые в рамках мандата Совета, будут не только способствовать международному миру и безопасности, но и укреплять предпринимаемые усилия, повышая осведомленность, поощряя подотчетность и способствуя эффективному сотрудничеству между государствами и соответствующими международными учреждениями. Поэтому Совет Безопасности имеет все возможности для того, чтобы стать лидером в создании более безопасного и стабильного киберпространства для всех.

Мы должны поднять это обсуждение на более высокий уровень и регулярно включать вопрос о киберугрозах в наши дискуссии по региональным конфликтам и тематическим вопросам. Это расширяет работу форумов Генеральной Ассамблеи, посвященных нормам деятельности в киберпространстве. Мы также должны побудить государства-члены воплотить эти нормы в конкретные действия. Это включает наращивание потенциала для кибербезопасности, содействие обмену информацией и сдерживание вредоносной деятельности.

В заключение я должен еще раз поблагодарить Республику Корея за эту похвальную инициативу, которая дает государствам-членам возможность принять участие в этих очень важных и актуальных прениях по вопросу, представляющему общий интерес. Совет Безопасности занимает центральное место в деятельности по оказанию столь необходимой критической поддержки, требуемой для смягчения и устранения киберугроз, связанных с международным миром и безопасностью.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Германии.

Г-н Линднер (Германия) (*говорит по-английски*): Германия благодарит Республику Корея за ее ведущую роль в привлечении внимания Совета Безопасности к вопросам кибербезопасности, и я хотел бы также поблагодарить Генерального секретаря и докладчиков за их познавательный вклад.

Международное сообщество сталкивается со все большим числом инцидентов, связанных с вредоносной деятельностью в киберпространстве и осуществляемых как государствами, так и частными компаниями. Эти инциденты оказывают серьезное влияние на поддержание международного мира и безопасности. Серьезные атаки киберпреступников, включая атаки с использованием вирусов-вымогателей, показали, что подобные действия могут угрожать стабильности государственных институтов. Они затрагивают целые общества.

Недавняя тенденция — появление на театре международных конфликтов групп хакеров-активистов, которые атакуют ключевые объекты критической инфраструктуры. Это подорвало доверие к оказанию государственных услуг и посеяло страх среди гражданского населения. Растущее сотрудничество ряда государственных субъектов с частными компаниями, работающими в сфере информационных технологий, группами хакеров-активистов и киберпреступниками еще больше усугубляет существующие риски. Все эти тенденции усиливают угрозы, учитывая, что киберпространство расширяет границы обычного поле боя, включая в него значительные гражданские пространства.

В свете этих резко эволюционирующих угроз Германия привлекает внимание к следующим четырем областям, в которых Совету Безопасности следует проявить активность.

Во-первых, мы видим важную роль Совета Безопасности в оценке угрозы, как в соответствии со статьей 34 Устава Организации Объединенных Наций, которая уполномочивает Совет Безопасности расследовать любую ситуацию, которая может привести к международным трениям или вызвать спор, так и в более общем плане, учитывая, что Совет должен углубленно рассматривать и анализировать риски для международного мира и безопасности, исходящие от кибератак.

Во-вторых, Совет Безопасности играет важную роль в разрешении споров, основываясь на полной применимости Устава Организации Объединенных Наций к киберпространству.

В-третьих, мы считаем, что Совет Безопасности может играть важную роль в укреплении доверия и нормотворчестве. Включая международные киберконфликты в свою повестку дня, расследуя ситуации киберконфликта или содействуя их мирному урегулированию, Совет будет способствовать формированию эволюционирующих рамок ответственного поведения государств в киберпространстве. Это должно основываться на международном праве и дополняться добровольными нормами Организации Объединенных Наций и мерами укрепления доверия.

Наконец, Германия приветствовала бы усилия Совета Безопасности по включению угроз в области кибербезопасности в свою повестку дня. Это должно включать в себя защиту от вредоносных кибератак Организации Объединенных Наций, включая ее присутствие на местах, такое как миротворческие операции.

В заключение я хотел бы подчеркнуть, что Германия будет и впредь вносить свой вклад в международную дискуссию по этому важному вопросу. Вот лишь один пример: в прошлом году мы запустили формат глобального диалога по теме «Киберпространство в ситуации конфликта». Его цель — рассмотреть повышенные риски для гражданского населения, связанные с использованием киберсредств в международных конфликтах, повысить осведомленность и разработать варианты смягчения последствий. Следующее мероприятие из этой серии пройдет здесь, в Нью-Йорке, в Постоянном представительстве Германии 8 июля и будет организовано в сотрудничестве с Японией, Сенегалом и Международным Комитетом Красного Креста.

Председатель (*говорит по-английски*): Слово имеет представитель Объединенных Арабских Эмиратов.

Г-н Шараф (Объединенные Арабские Эмираты) (*говорит по-английски*): Я благодарю министра иностранных дел Его Превосходительство г-на Чо Дэ Юля за исполнение обязанностей Председателя в ходе этих открытых прений и выражаю признательность Республике Корея за ее руководство работой Совета Безопасности в этом месяце. Я также благодарю Генерального секретаря и других наших докладчиков за их содержательный вклад.

Как мы услышали сегодня, угрозы киберпространству быстро эволюционируют. Вредоносные киберсредства и методы, такие как вирусы-вымогатели, фишинг и атаки типа «отказ в обслуживании», используются для атак на правительственные и частные сети, угрожая важнейшим объектам инфраструктуры и общественной безопасности. Это особенно тревожно, поскольку наши страны, включая Объединенные Арабские Эмираты, переживают цифровую трансформацию, в результате которой мы все больше полагаемся на надежные онлайн-системы. Образовательные учреждения также подвергаются риску: их цифровая инфраструктура и ценные информационные активы становятся мишенью для злоумышленников. Кроме того, злонамеренное использование информационно-коммуникационных технологий, включая, в частности, появляющиеся технологии искусственного интеллекта (ИИ), становится фактором увеличения угрозы в существующих конфликтах.

В 2020 году Объединенные Арабские Эмираты как глобальный центр в сфере технологий и инноваций создали Совет по кибербезопасности. Цель этого совета — добиться более безопасного процесса цифровых преобразований и повысить уровень кибербезопасности во всех целевых секторах страны. Мы привержены делу укрепления потенциала и обмена информацией с нашими партнерами, а также содействия применению ответственного подхода к разработке технологий и применению во благо искусственного интеллекта в целях борьбы с распространением и более частым использованием языка ненависти, ложной информации и дезинформации. В соответствии с этим обязательством совместно с Албанией мы провели в декабре 2023 года заседание по формуле Аррии для обсуждения этих трудностей.

В этой связи я хотел бы предложить рассмотреть четыре момента.

Во-первых, использование кибертехнологий должно осуществляться в соответствии с международным правом. Устав Организации Объединенных Наций, суверенитет, невмешательство во внутренние дела государств, ответственность государств и право вооруженных конфликтов

должны соблюдаться, как и сформулированные Организацией Объединенных Наций нормы ответственного поведения государств в киберпространстве. Устранение пробелов в нормативно-правовой сфере требует постоянного сближения позиций по поводу того, каким образом обеспечивать соблюдение и защиту норм международного права в киберпространстве.

Во-вторых, Объединенные Арабские Эмираты поддерживают идею учета проблем, связанных с наличием киберпространства, в работе Совета по обеспечению международного мира и безопасности. Это может включать более регулярное упоминание проблем, тенденций и событий, связанных с киберпространством, в рамках сообщений, заявлений и обсуждений приоритетных вопросов, а также в связи с ситуациями в конкретных странах и другими тематическими досье. Например, в резолюции 2341 (2017) признается необходимость защиты критически важных объектов инфраструктуры от террористических нападений, в том числе обеспечения безопасности в кибернетическом пространстве, и подчеркивается необходимость более эффективного противодействия широкому спектру киберугроз, которые возникают в связи с оцифровкой и киберпространством.

В-третьих, Совету следует рассмотреть возможность проведения ежегодного брифинга, посвященного новым технологическим угрозам и их последствиям для международного мира и безопасности. Кроме того, опубликование Генеральным секретарем ежегодного доклада по вопросам кибербезопасности позволило бы получить всеобъемлющую оценку общемировой ситуации с киберугрозами и рекомендации по укреплению соответствующего международного сотрудничества. Такой доклад также должен включать гендерный анализ, который позволит более эффективно реагировать на угрозы в киберпространстве, направленные против женщин и девочек.

В-четвертых, укрепление партнерских отношений между государственным и частным секторами имеет решающее значение для использования соответствующих опыта и ресурсов в целях эффективного противодействия киберугрозам. Объединенные Арабские Эмираты привержены делу сотрудничества с частным сектором в целях разработки надежных инструментов обеспечения кибербезопасности и наращивания национального и международного потенциала, а также поддержке частного сектора в обеспечении безопасной и ответственной разработки соответствующих решений.

Использование кибертехнологий имеет решающее значение для нашего будущего, однако необходимо проявлять бдительность в том, что касается связанных с ними рисков. Международное сотрудничество и укрепление потенциала играют жизненно важную роль в обеспечении устойчивости глобальной безопасности. Объединенные Арабские Эмираты будут и впредь поощрять ответственное поведение в киберпространстве и следить за тем, чтобы оно отражало наши коллективные устремления к обеспечению мира и безопасности.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Латвии.

Г-жа Мелбарде (Латвия) (*говорит по-английски*): Латвия хотела бы выразить признательность Республике Корея за организацию этих открытых прений высокого уровня в Совете Безопасности. Мы также хотели бы поблагодарить Генерального секретаря и докладчиков из Института «КиберМир» и Лидского университета им. Беккета за их содержательные выступления.

Использование цифровых технологий и зависимость от них значительно возросли с тех пор, как более 20 лет назад в повестку дня Организации Объединенных Наций были впервые включены вопросы, связанные с обеспечением кибербезопасности. Сегодня киберсфера стала соединительной тканью в процессе глобального экономического и социального развития. Расширение киберпространства пусть и открывает широкие возможности для прогресса, но в то же время сопряжено со все более серьезными рисками и проблемами. В последние годы мы сталкиваемся с рядом негативных тенденций в контексте международного мира и безопасности. Растет число случаев, когда кибератакам подвергается критически важная инфраструктура, в том числе критически важная информационная инфраструктура, что грозит катастрофическими последствиями в реальном мире. Кроме того, мы видели, что кибератаки стали неотъемлемой частью полномасштабной агрессии России против Украины.

Киберугрозы зачастую сопровождаются другими враждебными действиями, такими как распространение ложной информации и дезинформации и злонамеренное использование искусственного интеллекта и других новых технологий. Кроме того, широко распространена киберпреступность: в 2023 году объем платежей, сделанных в результате использования программ-вымогателей, достигло рекордного уровня. Эти события влияют на глобальный мир и безопасность. Мировое сообщество должно координировать свои меры реагирования, и Совет Безопасности должен играть в этой деятельности свою роль в соответствии со своим мандатом.

Таким образом, Латвия считает, что существующие в киберпространстве угрозы и вызовы заслуживают того, чтобы их регулярно обсуждали в Совете. Такие обсуждения могли бы опираться на периодические доклады Генерального секретаря. Более пристальное внимание Совета к вопросу о кибербезопасности также могло бы способствовать интеграции связанных с киберпространством аспектов в другие тематические мандаты, такие как поддержание мира и женщины и мир и безопасность. Кроме того, Совету следует рассмотреть вопрос об укреплении собственной способности реагировать на крупномасштабные кибератаки, имеющие потенциальные последствия для международной безопасности.

Очевидно, что более активная роль Совета в решении вопросов кибербезопасности не может сформироваться в одночасье. Это поэтапная работа, и заседания, подобные сегодняшнему, играют важнейшую роль в содействии этому процессу. Также очевидно, что Совету не следует подменять своей деятельностью работу, которая уже выполняется в рамках других форматов Организации Объединенных Наций под эгидой Генеральной Ассамблеи. Напротив, Совету следует укреплять договоренности, достигнутые в рамках этих форматов, в частности касательно применимости к киберпространству международного права во всей его полноте. Кроме того, предстоит еще много совместной работы по осуществлению рамок ответственного поведения государств в киберпространстве. До создания постоянного механизма Организации Объединенных Наций по обеспечению кибербезопасности, известного как программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, мы считаем возможным наладить новые формы взаимодействия Совета и Генеральной Ассамблеи в этой сфере.

В заключение я хотела бы подчеркнуть приверженность Латвии делу дальнейшей поддержки предпринимаемых в рамках Организации Объединенных Наций усилий по борьбе с растущими угрозами и вызовами в области кибербезопасности. Мы активно участвуем в обсуждении этой темы в комитетах Генеральной Ассамблеи, а также будем и впредь выступать за усиление роли Совета.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Египта.

Г-жа Ризк (Египет) (*говорит по-английски*): Египет придает большое значение аспектам обеспечения международной безопасности в связи с использованием информационно-коммуникационных технологий (ИКТ) и решительно призывает Организацию Объединенных Наций играть центральную и ведущую роль в продвижении и разработке правил и принципов использования ИКТ государствами на основе всеохватного и справедливого процесса, осуществляемого с участием всех государств.

Ряд государств занимаются наращиванием потенциала в сфере ИКТ для их потенциально злонамеренного использования и в целях их применения в наступательных военных операциях. Использование ИКТ в ходе будущих конфликтов между государствами становится одной из современных реалий, при этом риск совершения с использованием ИКТ вредоносных атак на критически важные объекты инфраструктуры является вполне реальным и серьезным. Эта новая гонка вооружений имеет далеко идущие последствия для международного мира, безопасности и стабильности, особенно в условиях продолжающегося стирания границ между обычными и иными вооружениями.

Кроме того, соответствующие технологии, разработанные государствами, передаются, копируются и воспроизводятся террористами и преступниками. Злонамеренное использование ИКТ террористическими и преступными организациями представляет собой серьезную угрозу для международного мира и безопасности, особенно в свете проблем, связанных с установлением ответственности. Согласно международному праву и Уставу

Организации Объединенных Наций, все государства-члены должны воздерживаться от любых сознательных или намеренных действий, которые наносят ущерб критически важной инфраструктуре других государств, иным образом затрудняют ее использование и функционирование или представляют собой вмешательство в их внутренние дела. Нет никаких сомнений в том, что аспекты обеспечения международной безопасности в связи с использованием ИКТ приобретают слишком важное и стратегическое значение, чтобы обойтись без четких обязательных правил, принятых на международном уровне. Всеохватный процесс под эгидой системы Организации Объединенных Наций является наилучшим и наиболее эффективным способом создания справедливых, всеобъемлющих и эффективных механизмов в этой области.

Организация Объединенных Наций уже предприняла некоторые шаги по созданию нормативной базы, дополняющей принципы международного права. Приняв консенсусом два ежегодных доклада о ходе работы Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, созданной на основании резолюции 75/240 Генеральной Ассамблеи, и другие консенсусные доклады, подготовленные в рамках связанных с Организацией Объединенных Наций процессов, Организация Объединенных Наций уже заложила первоначальные элементы рамочной основы предотвращения конфликтов и обеспечения стабильности в киберпространстве.

Генеральная Ассамблея призвала государства-члены руководствоваться при использовании ИКТ общими рамками ответственного поведения государств в киберпространстве, которые находятся в процессе развития и сформулированы в ряде последовательных докладов групп правительственных экспертов Первого комитета. Вместе с тем, ввиду их добровольного характера и отсутствия какого-либо механизма контроля за их выполнением, реализация этих норм остается в лучшем случае минимальной.

Признавая прогресс, который был достигнут Рабочей группой открытого состава, созданной в соответствии с резолюцией 75/240 Генеральной Ассамблеи, в отношении различных аспектов ее мандата, мы считаем важным, чтобы Группа заложила основу для будущей разработки под эгидой Организации Объединенных Наций механизма, который был бы ориентирован на действия, предполагал бы работу на единой площадке, был бы основан на принципе консенсуса и носил бы инклюзивный характер. Он должен основываться на согласованных решениях процессов, связанных с Организацией Объединенных Наций, и должен быть направлен на выполнение согласованных решений, включая рамки ответственного поведения государств в киберпространстве, дальнейшее ее развитие и содействие международному сотрудничеству с развивающимися странами и оказанию им помощи.

Наиболее эффективным каналом для выработки справедливых, всеобъемлющих и эффективных механизмов в этой области являются инклюзивные процессы, осуществляемые в рамках Организации Объединенных Наций, в первую очередь под эгидой Генеральной Ассамблеи. Со своей стороны, Совету Безопасности рекомендуется учитывать возможности, открывающиеся благодаря новым технологиям, при рассмотрении таких тем, как поддержание мира и борьба с терроризмом. При этом Совет не следует использовать в качестве нормотворческого органа, который пытается от имени государств — членов Организации Объединенных Наций устанавливать нормы и правила по вопросам, которые в обязательном порядке должны обсуждаться в рамках инклюзивных и транспарентных процессов.

Рекомендации, одобренные Генеральной Ассамблеей на основе консенсуса, могут быть использованы в качестве основы для разработки политически или юридически обязательных правил, особенно если учесть, что соответствующие рекомендации вытекают из принципов международного права и Устава Организации Объединенных Наций. Хотя мы исходим из того, что международное право и принципы Устава Организации Объединенных Наций применимы ко всем областям, включая киберпространство, мы полагаем также, что существует острая необходимость в определении конкретных обязательств, которые позволили бы обеспечить соответствие поведения государств в киберпространстве нормам международного права, а также целям и принципам Устава Организации Объединенных Наций.

В мире, который становится все более взаимосвязанным, любой международный режим кибербезопасности будет надежен настолько, насколь-

ко надежным будет его наиболее слабое звено. К счастью, всеми признается необходимость более активно и решительно заниматься наращиванием возможностей в плане предотвращения возможных атак в отношении объектов критически важной инфраструктуры, а также развивать потенциал и технические навыки, необходимые развивающимся странам. Организация Объединенных Наций должна возглавить скоординированные усилия, направленные на оказание необходимой помощи развивающимся странам.

В заключение следует отметить, что ИКТ открывают широкие возможности и бросают серьезные вызовы, и мы подчеркиваем, что настоятельно необходимо определить и разработать правила ответственного поведения государств, с тем чтобы повысить стабильность и безопасность глобальной информационно-коммуникационной среды и не допускать превращения киберпространства в еще одну арену для конфликтов и гонки вооружений.

Председатель (*говорит по-английски*): Хочу напомнить всем ораторам о необходимости ограничивать продолжительность своих выступлений тремя минутами, с тем чтобы Совет мог оперативно завершить свою работу. По истечении трех минут на ободке микрофона оратора начнет мигать световой сигнал, указывающий на необходимость завершить выступление.

Сейчас я предоставляю слово представителю Украины.

Г-жа Гайовишин (Украина) (*говорит по-английски*): Мы благодарим председательствующую в Совете Безопасности Республику Корея за созыв этих открытых прений высокого уровня. Благодарим также Генерального секретаря и других докладчиков за их замечания.

Украина присоединяется к заявлению, которое будет сделано от имени Европейского союза и в дополнение к которому мы хотели бы высказать следующие соображения от имени нашей собственной страны.

Мы твердо убеждены, что Совет Безопасности играет важную роль в устранении угроз международному миру и безопасности, в том числе в киберпространстве. Ландшафт киберугроз продолжает развиваться и становится как никогда сложным. Все более распространенными становятся программы-вымогатели, представляющие серьезный риск для правительств, предприятий и частных лиц. Кроме того, мы наблюдаем увеличение числа злонамеренных кибероперации, направленных против критически важных объектов инфраструктуры и критически важной информационной инфраструктуры, включая энергетическую отрасль, государственные службы и избирательные процессы. Осуществляя злонамеренную деятельность в киберпространстве, некоторые государственные субъекты продолжают подрывать международный порядок, основанный на правилах, и базовые правила ответственного поведения государств в киберпространстве.

В этой связи Корейская Народно-Демократическая Республика занимается кибершпионажем и кражей криптовалюты с целью дальнейшего развития ее ядерных программ и программ создания оружия массового уничтожения в нарушение соответствующих резолюций Совета Безопасности. Недавно российская кибершпионская группа «APT28» совершила кибератаки против ряда государств — членов ЕС.

Украина подвергается агрессии со стороны России, в том числе в киберпространстве. С начала войны Россия проводила все более изощренные кибератаки против государственных и силовых структур, предприятий и финансовых учреждений. Московские киберпреступники проводят фишинговые атаки, занимаются кибершпионажем и совершают атаки против объектов критически важной инфраструктуры, а также занимаются дезинформацией и распространяют пропаганду.

Для эффективного предотвращения и нейтрализации киберугроз и смягчения их последствий Украина активно сотрудничает с международными партнерами в целях создания эффективного киберпотенциала, что имеет основополагающее значение для осуществления права на самооборону в киберпространстве. Кроме того, в рамках расследований и уголовных процессов Украина начала рассматривать кибератаки в качестве военных преступления.

Государства должны соблюдать свои международные обязательства и обязанности, в том числе в контексте безопасности использования ИКТ. Как мы вновь заявляли здесь, в Организации Объединенных Наций, международное право, включая Устав Организации Объединенных Наций, при-

менимо к киберпространству. Поэтому все государственные субъекты, которые действуют вразрез с согласованными рамками, должны нести ответственность.

В заключение мы призываем государства — члены Организации Объединенных Наций продолжать совместную работу в целях укрепления и осуществления рамок ответственного поведения государств в киберпространстве, повышения осведомленности и обмена передовым опытом противодействия имеющимся и возникающим угрозам в киберпространстве.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Эстонии.

Г-н Таммсаар (Эстония) (*говорит по-английски*): Мы приветствуем сегодняшний обмен мнениями и благодарим докладчиков, особенно Генерального секретаря, за их исключительно ценные соображения.

Эстония присоединяется к заявлению, с которым выступит представитель Европейского союза. Позвольте мне высказать несколько соображений в национальном качестве.

Мы не можем игнорировать то, что злонамеренные киберинциденты, совершаемые как государственными, так и негосударственными субъектами, становятся все более изощренными и причиняют все больший ущерб. Кибератаки, направленные против стратегически значимых целей, таких как объекты критически важной инфраструктуры, финансовые учреждения и демократические процессы, обладающие трансграничным характером и осуществляющиеся с задействованием все более существенных ресурсов, способны причинять все более серьезный ущерб. Поэтому обеспечение кибербезопасности, безусловно, является одним из национальных и международных вызовов безопасности, а предотвращение и смягчение таких угроз является нашей общей первоочередной задачей.

Российская агрессия против Украины показала, как кибероперации переплетаются с активными боевыми действиями. Мы стали свидетелями того, как в нарушение международного гуманитарного права Россия атаковала критически важную инфраструктуру Украины. Действия России подчеркнули необходимость подходить к обеспечению национальной обороны и внутренней безопасности комплексно. Чтобы повысить готовность Украины к кибератакам и ее способность противостоять им, Эстония активно поддерживает Украину в киберсфере по двусторонним каналам, а также по линии Таллиннского механизма и «IT-коалиции».

Мы глубоко обеспокоены также последней информацией из Пхеньяна о дальнейшем наращивании военного сотрудничества Корейской Народно-Демократической Республики с Россией, что является грубым нарушением соответствующих резолюций Совета Безопасности. Эстония решительно осуждает продолжающуюся злонамеренную деятельность Корейской Народно-Демократической Республики в киберпространстве, которая направлена на подпитку программы вооружений Корейской Народно-Демократической Республики, дестабилизирует региональную безопасность и угрожает миру на планете.

Система ответственного поведения государств в киберпространстве была разработана Организацией Объединенных Наций на основе действующих норм международного права. Международное право, в частности Устав Организации Объединенных Наций, правовые нормы об ответственности государств, международное право прав человека и международное гуманитарное право, в полной мере применимо к кибероперациям. Мы должны вместе отстаивать международное право и добиваться его соблюдения в киберпространстве. В интересах содействия соблюдению правил ответственного поведения государств в киберпространстве Эстония выступает за разработку инклюзивной и обладающей практической направленностью программы действий в качестве единой постоянной структуры после завершения в 2025 году деятельности нынешней Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

Нельзя воспринимать открытую, безопасную, стабильную, доступную и мирную среду информационно-коммуникационных технологий как нечто само собой разумеющееся и отделенное от физического мира. Агрессия России против Украины продемонстрировала взаимосвязанный характер кибератак и реальных военных действий, и мы считаем, что эта модель будет использоваться и в ходе будущих конфликтов. Поэтому Совету Безопасности отводится значительная роль в качестве

форума для обмена информацией о существующих и будущих киберугрозах, а также для повышения осведомленности о стратегических последствиях таких угроз для кибербезопасности, что Эстония уже подчеркивала во время нашего пребывания в Совете Безопасности.

В заключение хочу отметить в этой связи, что Эстония благодарит Республику Корея за проведение нынешней дискуссии в зале Совета, где ей и место. Открытые обсуждения вопросов кибербезопасности, подобные этим, будут иметь ключевое значение для укрепления внутреннего, регионального и глобального потенциала противодействия киберугрозам, способствуя предотвращению киберконфликтов и смягчению их последствий.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Чехии.

Г-н Кульганек (Чехия) (*говорит по-английски*): Прежде всего я хотел бы поблагодарить Республику Корея за организацию этих весьма актуальных открытых прений. Приветствуем сегодняшнюю дискуссию о роли Совета Безопасности в области кибербезопасности, особенно в отношении реализации согласованных рамок ответственного поведения государств в киберпространстве.

Разумеется, мы разделяем многие опасения и предостережения, высказанные сегодня в этом зале. Особую обеспокоенность у нас вызывают атаки на критически важную инфраструктуру, кибершпионаж, атаки на государственные и частные учреждения, включая учреждения системы здравоохранения, с использованием вирусов-вымогателей, кража криптовалюты и попытки получить постоянный доступ к критически важным промышленным системам, причем не только в целях шпионажа и кражи интеллектуальной собственности, но и для обретения возможности осуществлять над ними контроль, открыто демонстрируя свои враждебные намерения. Все более широкое использование информационно-коммуникационных технологий (ИКТ) в ходе вооруженных конфликтов и их пагубное воздействие на гражданское население вызывают тревогу. Такие безответственные действия ставят под угрозу международный мир и безопасность, ответственность за которые несет Совет Безопасности. Кроме того, киберпространство все чаще используется для распространения дезинформации, обострения существующих социальных конфликтов и даже подстрекательства к террористическим актам. Наряду с соответствующими форумами Организации Объединенных Наций и другими международными организациями, занимающимися вопросами киберпространства, Совет должен активизировать свои усилия по поиску эффективных способов борьбы с этими менее очевидными видами вредоносной деятельности в киберпространстве. Он также должен заниматься повышением осведомленности об истинных масштабах этих угроз и содействовать проведению мероприятий, способствующих укреплению потенциала противодействия.

В мае Чехия в координации с Германией и другими государствами публично осудила деятельность подконтрольного российскому государству субъекта «APT28», который проводил долгосрочную кампанию кибершпионажа в европейских странах и совершал атаки на чешские правительственные учреждения. Такая деятельность идет вразрез с разработанными Организацией Объединенных Наций нормами ответственного поведения государств в киберпространстве. Мы намерены и далее вести решительную борьбу с такой деятельностью вместе с нашими партнерами и в соответствии с нашими международными обязательствами.

Чехия всецело одобряет основанный на международном праве международный порядок, который способствует созданию открытой, безопасной, стабильной, доступной и мирной среды ИКТ. Мы вновь заявляем о нашей поддержке идеи создания — по завершении работы нынешней Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий в 2025 году — постоянного, одновекторного, инклюзивного и ориентированного на конкретные действия механизма под эгидой Организации Объединенных Наций. Считаем, что таким механизмом могла бы служить программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности.

Наконец, я хотел бы подтвердить, что наша страна по-прежнему решительно настроена принимать участие в развитии поистине глобального партнерства для борьбы с существующими и будущими угрозами в области кибербезопасности. Для

этого нам потребуется подход, основанный на совместных усилиях всех сторон. Мы уже ведем подробные обсуждения с рядом стран в Африке, Индо-Тихоокеанском регионе и Латинской Америке, чтобы оценить меняющуюся ситуацию с угрозами и усилить наши совместные ответные меры. Так, в конце апреля Чехия организовала в Боготе семинар, посвященный современным вызовам в области преступной деятельности в киберпространстве. Мы благодарны экспертам из Колумбии, Коста-Рики, Доминиканской Республики, Эквадора, Сальвадора, Гватемалы, Гондураса и Панамы за то, что они посетили это мероприятие и поделились с нами своими ценными идеями.

Я еще раз благодарю Вас, г-н Председатель, за возможность поделиться мнением нашей страны по этому важному вопросу.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово г-же Самсон.

Г-жа Самсон (*говорит по-английски*): Я имею честь выступать от имени Европейского союза (ЕС) и его государств-членов. К этому заявлению присоединяются страны-кандидаты Северная Македония, Черногория, Албания, Украина, Республика Молдова, Босния и Герцеговина и Грузия, а также Андорра.

Благодарю Вас, г-н Председатель, за организацию этих открытых прений высокого уровня. ЕС приветствует сегодняшнюю дискуссию, проводимую в целях обмена мнениями об изменении ситуации, связанной с киберугрозами, и ее последствиях для поддержания международного мира и безопасности.

В только что сделанных заявлениях отражен широкий спектр возникающих и развивающихся угроз — от незначительных DDoS-атак до крупномасштабных кибероперациий и атак на критически важные объекты инфраструктуры. Мы также обеспокоены потенциальными трансграничными последствиями злонамеренной активности с использованием киберсредств. Отмечаем также размытость границ между преступной деятельностью и спонсируемыми государством атаками с использованием наемных киберпреступников, что делает и без того непростую задачу установления ответственности еще более сложной. Необходимо совместными усилиями расширять наш инструментарий, предназначенный для укрепления коллективного потенциала противодействия, и мы благодарим делегации, которые делятся своими соображениями и своим опытом в этой связи.

ЕС и его государства-члены встревожены количеством, изощренностью и масштабами злонамеренных кибератак, направленных против государственных учреждений и демократических процессов. В прошлом месяце Германия сообщила о том, что связанная с Россией группа «APT28», занимающаяся кибершпионажем, взломала электронные почтовые ящики членов Социал-демократической партии Германии. Государственные учреждения, агентства и организации в странах — членах ЕС, в том числе в Чехии, Польше, Литве, Словакии и Швеции, уже подвергались атакам со стороны одного и того же представляющего угрозу субъекта. Такой злонамеренной деятельности необходимо положить конец.

Разработанные Организацией Объединенных Наций нормы ответственного поведения государств в киберпространстве должны послужить руководством в этом отношении. Основные принципы такого поведения просты: в киберпространстве действует международное право; от государств ожидается соблюдение добровольно принятых на себя норм поведения; государства должны предотвращать неправомерное использование киберпространства на своей территории; для снижения риска эскалации и конфликтов, возникающих в результате киберинцидентов, необходимо принимать практические меры по укреплению доверия. По мнению ЕС, направление усилий на разработку и внедрение согласованных рамок ответственного поведения государств в киберпространстве имеет решающее значение для выполнения нашей общей ответственности в соответствии с нашими общими интересами и защиты всех государств от рисков злонамеренной активности с использованием киберсредств. Государства могут добиться значимого прогресса путем разъяснения вопроса о применении действующих норм международного права и обсуждения внедрения и соблюдения существующих норм ответственного поведения. Для того чтобы согласованные рамки ответственного поведения государства были эффективными, мы все должны их придерживаться. В этой связи важно под эгидой Организации Объединенных Наций создать постоянный, инклюзивный и ориентированный

на действия механизм. Поэтому мы поддерживаем разработку программы действий по содействию ответственному поведению государств при использовании информационно-коммуникационных технологий в контексте международной безопасности и надеемся согласовать ее условия этим летом.

С нетерпением ожидаем дальнейшего развития дискуссий по этой важной теме и приветствуем усилия, подобные тем, которые мы прилагаем сегодня, и направленные на то, чтобы подчеркнуть важную роль Совета Безопасности в выполнении его определенного Уставом Организации Объединенных Наций мандата по устранению угроз международному миру и безопасности путем выделения уникальных и конкретных международных угроз, возникающих в киберпространстве. Мы также рассчитываем на дальнейшее изучение вопроса о том, как будущая работа Совета может эффективно дополнять другие соответствующие процессы Организации Объединенных Наций в этой области.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Филиппин.

Г-н Лагдамео (Филиппины) (*говорит по-английски*): Филиппины хотели бы воспользоваться этой возможностью, чтобы еще раз подчеркнуть исключительную важность устранения угроз, связанных с информационно-коммуникационными технологиями (ИКТ), для международной безопасности. Стремительное развитие цифровых технологий создает новые вызовы, требующие немедленных и согласованных действий. В связи с этим мы хотели бы выделить три ключевых момента: тенденции, касающиеся угроз в сфере ИКТ, влияние киберугроз на международный мир и безопасность и кибератаки как фактор, усиливающий существующие угрозы.

Во-первых, что касается тенденций в области ИКТ-угроз, то рост числа автоматических звонков с использованием искусственного интеллекта (ИИ) для целей мошенничества, распространение дипфейков и ложных сведений, а также атаки с использованием вирусов-вымогателей представляют собой значительные риски и сложные проблемы. Для противодействия этим сложным угрозам необходимы комплексные стратегии. Злонамеренное использование ИИ в киберпространстве создает серьезные риски. Мы должны уделять первоочередное внимание оценке этих угроз, с тем чтобы разработать эффективные стратегии обеспечения кибербезопасности и обеспечить безопасное внедрение технологий ИИ.

Во-вторых, что касается влияния киберугроз на национальный мир и безопасность, Филиппины на собственном опыте убедились в разрушительном воздействии кибератак на национальную безопасность и доверие общественности. Недавние инциденты, такие как взлом и изменение содержания правительственных веб-сайтов, несанкционированный доступ к данным важнейших учреждений и кража большого объема личных данных, подчеркивают настоятельную необходимость усиления мер кибербезопасности. Кибератаки могут привести к сбоям в оказании основных услуг, подорвать доверие к институтам и иметь далеко идущие социально-экономические последствия. Мы также особенно обеспокоены злонамеренной деятельностью в сфере ИКТ, направленной на вмешательство во внутренние дела государств. Мы видим, что государства все чаще злонамеренно используют скрытые информационные кампании, проводимые с применением ИКТ, чтобы влиять на процессы, системы и общую стабильность других государств. Такие действия подрывают доверие, могут потенциально привести к эскалации ситуации и создать угрозу международному миру и безопасности. Еще одним вызывающим тревогу фактором является доступность этих сложных ИКТ-технологий для негосударственных субъектов и способность последних злонамеренно использовать эти технологии для получения коммерческой выгоды и ухода от ответственности.

В-третьих, что касается того, что кибератаки усиливают другие угрозы, то преступная деятельность в киберпространстве усугубляет существующие вызовы международному миру и безопасности. Филиппины стали свидетелями того, как кибератаки могут стать значительным фактором усиления угроз, затрудняя усилия по поддержанию мира и стабильности. Транснациональный характер киберпространства означает, что ни одно государство не застраховано от этих угроз, а наша коллективная безопасность прочна лишь настолько, насколько прочно ее самое слабое звено. Учитывая серьезную опасность, которую представляют киберугрозы, Филиппины подчеркивают ключевую роль Совета Безопасности в борьбе с этими угрозами. Хотя текущие обсуждения в рамках Рабочей группы от-

крытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ крайне полезны, Совету Безопасности также необходимо продолжать участвовать в формировании глобальной повестки дня в области кибербезопасности.

В этой связи Филиппины поддерживают принятие Советом следующих коллективных мер по противодействию киберугрозам, которые обсуждались на состоявшемся в апреле заседании по формуле Аррии, посвященном теме кибербезопасности: во-первых, укрепление согласованных нормативных рамок ответственного поведения государств в киберпространстве; во-вторых, ежегодный созыв совещаний для обсуждения и анализа угроз в сфере ИКТ и в этой связи поручение Генеральному секретарю подготовить ежегодный доклад о тенденциях для информирования государств-членов о ходе обсуждений; и, в-третьих, руководство сбором информации или изучением конкретных угроз или инцидентов для предоставления государствам-членам руководящих принципов и справочных материалов.

Филиппины подтверждают свою приверженность укреплению потенциала противодействия киберугрозам и поощрению ответственного поведения в киберпространстве. Мы призываем к продолжению сотрудничества, наращиванию потенциала и созданию механизмов оказания поддержки, в том числе постоянного целевого фонда для оказания помощи развивающимся странам в борьбе с киберугрозами. Мы рассчитываем на партнерскую поддержку и передачу технологий, которые помогут нам сократить цифровой разрыв и укрепить нашу киберзащиту.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Индонезии.

Г-н Насир (Индонезия) (*говорит по-английски*): Индонезия благодарит Республику Корея за организацию этого важного заседания. Благодарю также Генерального секретаря и докладчиков за их выступления.

Угрозы в киберпространстве стали реальной и настоящей опасностью для национального и международного мира и безопасности. Мы все чаще сталкиваемся с угрозами, создаваемыми новыми и быстро развивающимися технологиями. Только приняв скоординированные меры реагирования и разработав надежную правовую базу, международное сообщество сможет укрепить потенциал противодействия киберугрозам и эффективно снизить эти риски.

В этой связи хотел бы высказать следующие соображения.

Во-первых, мы должны уделять первоочередное внимание смягчению гуманитарных последствий кибератак, направленных на объекты критически важной инфраструктуры, для населения. Мы должны обеспечить защиту киберпространства как сферы, свободной от конфликтов, и не допустить его превращения в арену противостояния. Хотя достижения в области искусственного интеллекта (ИИ), включая генеративный ИИ и машинное обучение, могут принести пользу человечеству, они также могут использоваться для злонамеренных действий и совершения кибератак, приводя таким образом к значительным негативным последствиям для людей во всем мире. Поэтому очень важно обеспечить защиту критически важной инфраструктуры в рамках наших усилий по предотвращению значительного ущерба, наносимого действиями злоумышленников и безответственных государств в киберпространстве.

Во-вторых, необходимо обеспечить взаимодополняемость и слаженность действий в рамках системы Организации Объединенных Наций в области кибербезопасности, информационно-коммуникационных технологий (ИКТ) и обеспечения международного мира и безопасности. В то время как Совет Безопасности обладает важным мандатом по поддержанию международного мира и безопасности, другие органы Организации Объединенных Наций имеют не менее важные мандаты по рассмотрению вопросов цифровой безопасности и безопасности в области ИКТ, а также кибербезопасности. Важно, чтобы Совет Безопасности определил параметры и механизмы, которые помогут ему развивать сотрудничество и взаимодополняемость усилий и лучше понять риски, которые киберугрозы представляют для международного мира и безопасности. Поэтому Индонезия подтверждает свою приверженность поддержке деятельности Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ и других процессов, осуществляемых в этой области, в том числе подготовки к Саммиту будущего.

В-третьих, следует повысить глобальную кибербезопасность путем укрепления регионального сотрудничества. Сотрудничество с региональными организациями необходимо, поскольку они играют важную роль в разработке действенного и всеобъемлющего подхода к обеспечению кибербезопасности. В нашем регионе Ассоциация государств Юго-Восточной Азии (АСЕАН) играет важную роль в создании механизмов и инициатив, в том числе в рамках Регионального форума АСЕАН, для повышения регионального потенциала противодействия киберугрозам. Использование такого опыта и знаний региональных организаций действительно может быть полезным и способствовать повышению слаженности международных усилий.

Наконец, необходимо преодолеть разрыв в уровне технического развития, чтобы укрепить потенциал противодействия киберугрозам. Недостаточные возможности для обеспечения кибербезопасности являются серьезной проблемой для развивающихся стран и делают их уязвимыми перед лицом усиливающихся угроз, подрывая их стабильность. Принятие коллективных мер на всех уровнях, в том числе с соответствующими заинтересованными сторонами из частного сектора, имеет решающее значение для укрепления стабильности в киберпространстве, особенно путем наращивания потенциала, оказания технической помощи и передачи технологий. Только объединив усилия, мы сможем создать безопасное киберпространство, которое будет способствовать обеспечению мира и стабильности во всем мире.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Сингапура.

Г-н Сих (Сингапур) (*говорит по-английски*): Мы благодарим Республику Корея за созыв сегодняшнего заседания по этому важному вопросу.

Со времени первых открытых прений Совета Безопасности по кибербезопасности, которые состоялись в июне 2021 года (см. S/2021/621), спектр и характер киберугроз продолжает меняться тревожными темпами. Поэтому международное сотрудничество в рамках Организации Объединенных Наций является крайне важным и необходимым для борьбы с киберугрозами глобального и трансграничного характера. В этой связи необходимо, чтобы Генеральная Ассамблея и Совет Безопасности совместно работали над укреплением нормативных рамок ответственного поведения государств в киберпространстве, основанных на применении норм международного права и соблюдении принципов, закрепленных в Уставе Организации Объединенных Наций. Будучи небольшим государством, Сингапур всегда поддерживал многостороннюю систему, основанную на верховенстве права. Мы придерживаемся этого подхода и в вопросах, касающихся кибербезопасности, которая имеет исключительно важное значение для многих малых и развивающихся государств. Сингапур твердо убежден в важности Организации Объединенных Наций как ключевой платформы для обсуждения вопросов разработки и реализации правил, норм и принципов ответственного поведения государств, регулирующих киберпространство.

Сингапур удостоен чести быть с 2021 года председателем Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Эта рабочая группа открытого состава опирается на результаты более чем двух десятилетий работы в рамках Организации Объединенных Наций, в результате которой были выработаны кумулятивные и эволюционирующие рамки ответственного поведения государств в киберпространстве, одобренные всеми государствами-членами. Отрадно отметить, что за последние три года Рабочая группа открытого состава добилась значительного прогресса в дальнейшем укреплении нормативных рамок ответственного поведения государств в киберпространстве.

Рабочая группа открытого состава также сама по себе является ценной мерой укрепления доверия. Помимо общих договоренностей, достигнутых в двух ежегодных докладах Рабочей группы открытого состава о проделанной работе, согласованных на основе консенсуса в июле 2022 года (см. A/77/275) и июле 2023 года (см. A/78/265) соответственно, Рабочая группа открытого состава возглавила разработку и реализацию ориентированных на конкретные действия инициатив, призванных сыграть важную роль в укреплении международного мира и безопасности в киберпространстве; в первую очередь был составлен глобальный реестр контактных пунктов, официально введенный в работу 9 мая. Также в мае Рабочая группа открытого состава провела успешное и содержательное совещание на уровне министров по вопросам укрепления потенциала в области безопасности информационно-ком-

муникационных технологий. Основное послание по итогам этой встречи заключалось в том, что необходимо срочно наращивать потенциал, чтобы помочь многим малым и развивающимся странам получить возможность противодействовать киберугрозам. Не менее важно и широкое признание того, что наращивание потенциала может быть важным средством укрепления доверия между государствами.

В своих вводных вопросах, г-н Председатель, вы спросили, как киберугрозы связаны с другими пунктами повестки дня Совета Безопасности и какую конкретную роль может играть Совет Безопасности в решении проблем для международного мира и безопасности, исходящих из киберпространства. Учитывая текущую работу, проводимую в Генеральной Ассамблее, Совету Безопасности важно избегать дублирования усилий, которые уже прикладываются в рамках других процессов. В то же время мы должны признать, что Совет Безопасности имеет четкий мандат на обсуждение вопросов, связанных с поддержанием международного мира и безопасности. Нельзя исключать возможность того, что тот или иной киберинцидент может вызвать недопонимание между государствами и привести к эскалации и, возможно, к конфликту, тем самым создав угрозу международному миру и безопасности. Поэтому мы не можем исключать того, что Совет Безопасности будет играть определенную роль в рамках возложенной на него Уставом ответственности за поддержание международного мира и безопасности.

Поэтому Совет должен придерживаться инклюзивного подхода при определении того, что представляет собой угрозу международному миру и безопасности, и действовать с осознанием того, что киберугрозы могут иметь физические и реальные последствия. В этой связи мы готовы поддержать идею о том, чтобы Совет Безопасности продолжал проводить открытые прения, подобные сегодняшним, в целях обмена информацией и укрепления взаимопонимания между государствами-членами. Обсуждения в Совете могут помочь в работе Генеральной Ассамблеи, в том числе в плане укрепления потенциала и доверия, а также способствовать укреплению рамок ответственного поведения государств в киберпространстве, в том числе при рассмотрении вопроса о том, как лучше всего применять правила, нормы и принципы к существующим и потенциальным киберугрозам.

В заключение позвольте мне подчеркнуть необходимость расширения международного сотрудничества для укрепления нашего коллективного потенциала противодействия киберугрозам. Содействие расширению сотрудничества между Советом Безопасности и Генеральной Ассамблеей по вопросам международного мира и безопасности и совместная работа на устойчивой, комплексной и взаимодополняющей основе позволит международному сообществу лучше поддерживать международный мир и безопасность в киберпространстве. Сингапур готов сотрудничать со всеми государствами-членами в достижении этой цели.

Председатель (*говорит по-английски*): Сейчас я предоставляю слово представителю Коста-Рики.

Г-жа Чан Вальверде (Коста-Рика) (*говорит по-испански*): Коста-Рика хотела бы поблагодарить Республику Корея за организацию сегодняшних открытых прений.

Два года назад Коста-Рика стала жертвой масштабных атак с использованием вирусов-вымогателей. Мы до сих пор ощущаем последствия сбоев в работе системы здравоохранения, социального обеспечения, финансов и других важнейших секторов.

В связи с этим Коста-Рика хотела бы сделать сегодня три замечания.

Во-первых, Коста-Рика твердо убеждена в том, что повестка дня по вопросу о защите гражданских лиц должна быть расширена таким образом, чтобы охватывать деятельность в киберпространстве, которая затрагивает гражданское население во время вооруженных конфликтов. Государства должны присоединиться к растущему консенсусу о том, что данные, касающиеся гражданского населения, пользуются такой же защитой согласно международному гуманитарному праву, как и все другие гражданские объекты, и что операции в киберпространстве, выводящие из строя гражданские системы или препятствующие их функционированию, запрещены по международному гуманитарному праву. Государства также должны воздерживаться от вовлечения гражданских лиц в военную деятельность в киберпространстве, поскольку это может подвергнуть их опасности.

Во-вторых, Коста-Рика считает, что настало время обновить повестку дня по вопросу о женщинах и мире и безопасности, включив в нее вопросы

цифровой безопасности женщин. Коста-Рика призывает членов Совета Безопасности рассмотреть возможность принятия нового проекта резолюции, предусматривающего меры по защите женщин и девочек от насилия, надругательств и эксплуатации в Интернете, особенно в условиях конфликта и в постконфликтных ситуациях. Проблематика цифровой безопасности также должна быть систематически интегрирована во все новые мандаты, цели и инициативы, относящиеся к этой повестке дня.

В-третьих, все государства, независимо от того, являются они членами Совета или нет, несут ответственность за укрепление международного верховенства права в киберпространстве. Коста-Рика является гордым членом растущей группы государств, обнародовавших свои национальные документы с изложением позиции в отношении применения международного права в киберпространстве. Эти документы с изложением позиции опираются на глобальный консенсус в отношении того, что международное право, включая международное гуманитарное право и международное право прав человека, применимо к использованию государствами информационно-коммуникационных технологий и имеет важное значение для поддержания мира и стабильности. Мы призываем другие государства разработать такие документы с изложением позиции и высоко оцениваем существующие ресурсы по наращиванию правового потенциала, такие как Инструментарий по киберправу, которыми можно руководствоваться в своих усилиях в этой области.

Поскольку наши общества становятся все более уязвимыми перед кибер- и цифровыми угрозами, Коста-Рика настоятельно призывает Совет учитывать эти проблемы в своей работе и делать это таким образом, чтобы укреплять уважение к международному праву как в мирное время, так и во время вооруженных конфликтов.

Председатель (*говорит по-английски*): В моем списке остается еще ряд ораторов, записавшихся для выступления на этом заседании. С согласия членов Совета я намерен прервать это заседание и возобновить его сегодня во второй половине дня в 15 ч 00 мин.

Заседание прерывается в 13 ч 10 мин.