# Совет Безопасности

Семьдесят девятый год

*Предварительный отчет*

## 9662-е заседание

Четверг, 20 июня 2024 года, 15 ч 00 мин
Нью-Йорк

| | | |
|---|---|---|
| *Председатель*: | г-н Хён У Чо | (Республика Корея) |
| *Члены*: | Алжир | г-н Луафи |
| | Китай | г-н Ван Чжэнь Цзян |
| | Эквадор | г-н Дуран Медина |
| | Франция | г-н Стрехайано |
| | Гайана | г-жа Парманand |
| | Япония | г-н Судзуки |
| | Мальта | г-н Чискальди |
| | Мозамбик | г-н Ирашанди Говея |
| | Российская Федерация | г-н Дергачев |
| | Сьерра-Леоне | г-н Шенкс |
| | Словения | г-н Буркельйц |
| | Швейцария | г-н Штритт |
| | Соединенное Королевство Великобритании и Северной Ирландии | г-жа Пейдж |
| | Соединенные Штаты Америки | г-жа У |

## 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)



24-17610 (R)

*Заседание возобновляется в 15 ч 05 мин.*

**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 Кубы.

**Г-н Гала Лопес** (Куба) (*говорит по-испански*): Информационно-коммуникационные технологии должны и далее использоваться исключительно в мирных целях, с тем чтобы способствовать сотрудничеству между народами и их развитию.

Куба решительно выступает против милитаризации киберпространства и всякого использования информационно-коммуникационных технологий в качестве инструментов для осуществления угрозы силой или применения такой силы, а также для совершения действий в целях вмешательства во внутренние дела государств. Статья 51 Устава Организации Объединенных Наций не применяется в отношении киберпространства и не может быть использована в этом контексте. Поэтому вызывает беспокойство тот факт, что некоторые государства включают в свои национальные стратегии обеспечения безопасности использование кибероружия и возможность совершения кибератак — как утверждается, для сдерживания противника.

Необходимо принять все необходимые меры для предотвращения неправомерного использования информационно-коммуникационных технологий и медиаплатформ, в том числе социальных сетей, сетей радиовещания и электронных систем передачи информации, в качестве инструментов для пропаганды языка ненависти, подстрекательства к насилию, деструктивной деятельности, дестабилизации ситуации, распространения фальшивых новостей и искажения действительности в целях ведения подрывной деятельности и вмешательства в дела других государств в нарушение норм международного права. Кроме того, неприемлемым является тайное и незаконное использование национальных информационных систем отдельными лицами, организациями и государствами для совершения кибератак на третьи страны.

Куба выступает за проведение переговоров в рамках Организации Объединенных Наций и скорейшее принятие юридически обязательного международного документа, который позволит восполнить существенные правовые пробелы в области обеспечения кибербезопасности и эффективно противодействовать растущим вызовам и угрозам в этой сфере, в том числе на основе международного сотрудничества. Необходимо преодолеть колоссальный технологический разрыв и препятствия, стоящие перед развивающимися странами в том, что касается инвестиций в обеспечение безопасности их инфраструктуры ИКТ, и ограничивающие способность этих стран противодействовать угрозам.

Рабочая группа открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, учрежденная Первым комитетом Генеральной Ассамблеи, представляет собой надлежащий механизм для обмена мнениями и достижения договоренностей по вопросам угроз и вызовов, с которыми мы сталкиваемся как государства в связи со злонамеренным использованием информационно-коммуникационных технологий. Данная группа представляет собой инклюзивный, демократический и транспарентный форум, в рамках которого все государства-члены могут на равноправной основе вносить свой вклад в разработку пользующихся консенсусом соответствующих решений в этой сфере.

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

**Г-жа Салман** (Бахрейн) (*говорит по-арабски*): Прежде всего я хотела бы приветствовать министра иностранных дел Республики Корея Его Превосходительство г-на Чхо Дэ Юля, председательствовавшего на сегодняшней утренней сессии открытых прений, и поблагодарить Постоянное представительство Республики Корея при Организации Объединенных Наций за организацию этого заседания по теме, которая, учитывая большие достижения в области киберпространства, становится все более важной. Я также хотела бы поблагодарить Генерального секретаря Организации Объединенных Наций Его Превосходительство г-на Антониу Гутерриша и других докладчиков за их ценные заявления.

Растущие риски, связанные со злонамеренными действиями в киберпространстве, такими как атаки с использованием вирусов-вымогателей, кража криптовалюты и похищение конфиденциальной информации и активов, не только ставят под угрозу безопасность критически важных объектов инфраструктуры, но и усугубляют существующие вызовы глобальной стабильности. Такие действия многократно усиливают существующие угрозы, усугубляя традиционные проблемы в области безопасности и создавая новые факторы уязвимости. Взаимосвязь цифровых систем означает, что киберинциденты могут быстро перерастать в международные кризисы и подрывать стабильность и доверие в отношениях между государствами.

Королевство Бахрейн подчеркивает важность применения многоаспектного подхода, предусматривающего использование существующих и инновационных инструментов, платформ, рамок и стратегий для снижения рисков, связанных с киберугрозами, а также обеспечение участия всех заинтересованных сторон, поскольку киберинструменты и кибертехнологии больше не являются исключительной прерогативой правительств. Королевство Бахрейн также подчеркивает важность наращивания потенциала и обмена технологиями, знаниями и передовым опытом для расширения возможностей государств по предотвращению киберинцидентов и реагированию на них.

В этой связи Королевство Бахрейн поддерживает различные инициативы Генеральной Ассамблеи по укреплению сотрудничества в деле обеспечения кибербезопасности, включая группы правительственных экспертов, Рабочую группу открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, а также программу действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности.

На национальном уровне Королевство Бахрейн придает огромное значение кибербезопасности: мы разработали понятную систему управления кибербезопасностью, подкрепленную комплексной национальной стратегией. Мы также создали Национальный центр кибербезопасности для обеспечения безопасности киберпространства Королевства Бахрейн путем установления эффективных стандартов управления, предоставления средств защиты от электронных атак, их мониторинга и реагирования на них, а также повышения осведомленности отдельных лиц и учреждений.

Национальная стратегия обеспечения кибербезопасности предусматривает укрепление региональных и международных партнерств. В этой стратегии определены пять основополагающих элементов, и каждый из них является важным и необходимым компонентом усилий по реализации разработанной в Королевстве Бахрейн концепции кибербезопасности. В совокупности они образуют всеобъемлющую и целостную структуру, позволяющую обеспечивать безопасность и устойчивость киберпространства. Этими элементами являются, во-первых, надежная и устойчивая киберзащита; во-вторых, эффективное управление и стандарты в области кибербезопасности; в-третьих, повышение осведомленности общественности о кибербезопасности; в-четвертых, усиление защиты путем развития партнерских отношений и сотрудничества; в-пятых, подготовка национальных кадров.

В заключение отмечу, что, учитывая быстро меняющийся характер угроз, возникающих в связи с развитием информационно-коммуникационных технологий, Королевство Бахрейн рассчитывает на дальнейший плодотворный диалог по вопросам кибербезопасности в рамках Организации Объединенных Наций, в частности в Совете Безопасности.

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

**Г-н Щерский** (Польша) (*говорит по-английски*): Распространение цифровых технологий по всему миру, включая разработку и внедрение системы электронного управления государством и объектами критически важной инфраструктуры, приводит к растущей зависимости от киберпространства. Это создает серьезные угрозы для безопасности и суверенитета государств. Число злонамеренных атак, совершаемых в киберпространстве как негосударственными, так и государственными субъектами и направленных против стабильности и безопасности стран и обществ, растет каждый день.

В качестве первого шага по обеспечению международного мира и безопасности Польша на национальном уровне заняла конкретную пози-

цию относительно применимости международного права в киберпространстве. В этой связи огромное значение для нашей страны имеют два момента. Во-первых, при определенных обстоятельствах действия в киберпространстве могут представлять собой нарушение запрета на применение силы. Во-вторых, кибератака может быть квалифицирована как вооруженное нападение. В этой связи считаем, что право на самооборону действует и в киберпространстве.

Проблема, с которой мы зачастую сталкиваемся, связана с установлением ответственности за кибератаки. Мы, несмотря ни на что, не оставим усилий по привлечению ответственных государств и киберпреступников к суду. Важно признать, что, вместо того чтобы бороться с киберпреступниками, действующими на их территории, некоторые государства обхаживают и защищают их ради политической или экономической выгоды. Тем самым они подрывают стабильность и безопасность других. Они пытаются размыть границы между спонсируемыми государством и действующими с преступным умыслом субъектами и ввести в заблуждение объектов атак, когда те пытаются защитить себя и привлечь виновных к ответственности.

В то же время существует большая группа государств, у которых есть политическая воля к выполнению норм международного права и добровольных норм, но которые могут не иметь для этого необходимых возможностей. В наших общих интересах тесно сотрудничать с ними, чтобы оказать им помощь и содействовать им в наращивании потенциала в этой области в соответствующих объемах. Это не может произойти в одночасье. Поэтому нам нужна постоянная платформа для такого сотрудничества в рамках Организации Объединенных Наций. В этой связи в соответствии с заявлением, сделанным от имени Европейского союза, Польша решительно поддерживает разработку соответствующей программы действий. Призываем всех членов Организации Объединенных Наций также ее поддержать и активно содействовать ее введению в действие.

Кибератаки и злонамеренные действия направлены на подрыв международного мира и безопасности. Поэтому мы призываем Совет Безопасности активизировать усилия по пресечению и предотвращению злонамеренной деятельности в киберпространстве. Мы также хотели бы призвать одно из государств — членов Совета — Российскую Федерацию — уважать международное право и прекратить незаконную агрессию против Украины и других своих соседей не только «на земле», но и в киберпространстве.

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

**Г-н Феруцэ** (Румыния) (*говорит по-английски*): Прежде всего я хотел бы поблагодарить Республику Корея за организацию прений по столь важной теме.

Я хотел бы высказать несколько соображений в дополнение к заявлению, сделанному от имени Европейского союза.

Угрозы в киберпространстве носят устойчивый и сложный характер, приводят к разрушительным последствиям и возникают все более часто. Румыния встревожена количеством злонамеренных кибератак, направленных против государственных учреждений и демократических процессов. Речь идет о серьезной угрозе: кибероперации, зачастую осуществляемые в сочетании с кампаниями по распространению дезинформации, могут подорвать целостность демократических процессов и жизнестойкость наших обществ в целом.

Нас также беспокоят кибератаки на критически важную инфраструктуру и основные службы, которые могут иметь разрушительные и опустошительные последствия. Решительно осуждаем злонамеренную активность с использованием киберсредств, направленную на подрыв наших демократических институтов, национальной безопасности и свободного общества. Безответственное поведение в киберпространстве создает угрозу международному миру и безопасности, и с ним нельзя мириться. Совет Безопасности имеет право заниматься такими вопросами и содействовать более эффективному привлечению виновных к ответственности.

Международное право имеет силу и в киберпространстве. Государства обязаны действовать в киберпространстве ответственно, в соответствии с нормами международного права, включая Устав Организации Объединенных Наций, и мы призываем Совет Безопасности осудить злонамеренное поведение в киберпространстве. Любое использование государствами информационно-коммуникационных технологий (ИКТ) в нарушение норм между-

народного права и их обязательств по документам Организации Объединенных Наций, касающимся ответственного поведения государств при использовании ИКТ, подрывает международный мир и безопасность.

Усиление роли Совета Безопасности в борьбе с киберугрозами в дополнение к другим процессам Организации Объединенных Наций в области ИКТ является своевременным и крайне важным шагом, необходимым для поддержания международного мира и безопасности в киберпространстве. Эти открытые прения и предыдущие заседания по формуле Аррии в мае 2023 года и апреле 2024 года подтверждают важный вклад, который может внести в этой связи Совет Безопасности.

Румыния уделяет большое внимание необходимости укрепления потенциала противодействия в киберпространстве. На фоне попыток злонамеренных субъектов серьезно нарушить функционирование наших обществ нам необходимо усилить защиту объектов критически важной национальной инфраструктуры. Мы по-прежнему привержены Международной инициативе по борьбе с использованием вирусов-вымогателей и с нетерпением ждем ее укрепления в качестве скоординированного международного ответа на этот комплекс угроз. Более того, сама природа киберпространства требует обсуждения перспективного потенциала технологий искусственного интеллекта с точки зрения увеличения масштабов и сложности кибератак, но в то же время их предотвращения, более быстрого принятия мер противодействия и даже смягчения их последствий.

В заключение мы призываем все государства выполнять свои международные обязанности и обязательства по соблюдению международного права и действовать в соответствии с согласованными рамками ответственного поведения государств в киберпространстве. Мы действительно должны сохранять верность нашим основным ценностям и принципам и действовать ответственно.

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

**Г-н Преттерхофер** (Австрия) (*говорит по-английски*): Австрия хотела бы поблагодарить Республику Корея за своевременный созыв этих открытых прений.

Австрия присоединяется к заявлению, с которым выступил наблюдатель от Европейского союза. Позвольте мне добавить следующие моменты в нашем национальном качестве.

Отвечая на Ваши наводящие вопросы о роли Совета Безопасности, г-н Председатель, мы считаем, что можно добиться большей концептуальной ясности, если подходить к этим прениям с опорой на общий язык, в отношении которого мы все достигли согласия: язык международного права. Все государства-члены консенсусом согласились с тем, что международное право, и в частности Устав Организации Объединенных Наций, в полной мере применяется к кибердеятельности. В Уставе четко сказано: он наделяет Совет Безопасности мандатом реагировать на угрозы международному миру и безопасности. Для выполнения мандата Совета Безопасности необходимо, чтобы он продолжал реагировать на современные угрозы международному миру и безопасности. Не менее важно подчеркнуть роль Совета Безопасности в мирном урегулировании споров, как это предусмотрено в главе VI Устава. Кибердеятельность происходит не в отдельном виртуальном киберпространстве, а в реальном мире. Таким образом, кибердеятельность не является новой областью, требующей своих собственных новых правил или особого применения международного права. В конечном счете Совет рассматривает поведение государства. Вполне логично, что Совет не уклоняется от рассмотрения одной из форм поведения государств - кибердеятельности - всякий раз, когда это становится актуальным для его мандата. Например, что касается санкций, то все действия, направленные на нарушение принятых Советом обязательных санкций, включая кибердеятельность, заслуживают его внимания. В этой связи включение вопросов кибербезопасности в документы Совета Безопасности имеет решающее значение.

Австрия привержена принципу верховенства права как в киберпространстве, так и за его пределами и недавно опубликовала документ с изложением своей позиции по вопросам кибердеятельности и международного права. Австрия приветствует сегодняшние прения, которые подчеркивают важную роль Совета Безопасности в рамках выполнения его мандата, установленного Уставом Организации Объединенных Наций, по устранению угроз международному миру и безопасности.

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

**Г-н Умаров** (Казахстан) (*говорит по-английски*): Я хотел бы выразить нашу признательность Республике Корея за организацию сегодняшней очень важной встречи.

Темпы цифровизации опережают любые другие инновации в истории человечества. Всего за два десятилетия цифровые технологии изменили общество и затронули около 50 процентов населения развивающихся стран. Использование технологий для улучшения связи и доступа к финансовым, деловым и государственным услугам может значительно уменьшить неравенство населения. В сфере здравоохранения передовые технологии, использующие искусственный интеллект, применяются для спасения жизней, диагностики заболеваний и увеличения продолжительности жизни. В образовании доступность виртуальных учебных средств и дистанционного обучения позволяет студентам участвовать в программах, которые раньше были недостижимы.

В то же время информационно-коммуникационные технологии (ИКТ) используются многочисленными негосударственными субъектами, включая преступные группы и террористов, для похищения личных данных, мошенничества и кибератак. Они также используются для того, чтобы сеять раздор и распространять дезинформацию, что может дестабилизировать ситуацию в государствах и подорвать доверие между странами. Злонамеренные действия в киберпространстве могут нарушить работу важнейшей инфраструктуры, в том числе энергетической инфраструктуры, транспорта и связи, и поэтому могут стать фактором, усиливающим угрозу в существующих конфликтах, что потребует участия Совета Безопасности. Это подтверждает тенденцию, в рамках которой киберугрозы становятся геополитическим вызовом. В этой связи Казахстан поддерживает глобальный и ответственный подход к использованию ИКТ и искусственного интеллекта путем разработки общепринятых стандартов их использования.

Эксперты из нашей страны принимают активное участие в работе Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ и Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Мы поддерживаем глобальный межправительственный реестр контактных пунктов, который был введен в действие в мае. Как и многие другие государства-члены, Казахстан в настоящее время находится в процессе назначения дипломатических и технических контактных лиц для этого реестра.

Наконец, я хотел бы подчеркнуть, что в условиях геополитической нестабильности важно избегать политизации этого вопроса и вместо этого искать точки соприкосновения. Совет Безопасности мог бы играть ключевую роль в координации международных усилий и реализации конкретных мер по противодействию киберугрозам, в том числе: поддерживать инициативы по наращиванию потенциала государств, особенно в развивающихся регионах, повышая их способность предотвращать киберинциденты и реагировать на них; привлекать негосударственных субъектов, включая технологические компании и организации гражданского общества, и укреплять коллективные усилия по борьбе с киберрисками; и, разумеется, повышать осведомленность о проблемах в сфере кибербезопасности и проводить регулярные обзоры меняющейся ситуации в плане киберугроз.

**Председатель** (*говорит по-английски*): Я предоставляю слово представителю Исламской Республики Иран.

**Г-н Иравани** (Исламская Республика Иран) (*говорит по-английски*): Г-н Председатель, позвольте поблагодарить Вас за созыв этих открытых прений.

Борьба с эволюционирующими угрозами в сфере информационно-коммуникационных технологий (ИКТ) требует многоаспектного подхода, включающего технологические и юридические стратегии и стратегии в области сотрудничества.

Иран является главной целью и главной жертвой многочисленных кибератак на его инфраструктуру, которые приводят к значительным сбоям в работе общественных служб и государственных ведомств. Яркими примерами этого являются атаки с использованием вирусов Stuxnet и Duqu на мирные ядерные объекты Ирана, а также кибератаки на важнейшие объекты промышленной инфраструктуры, такие как объекты сталелитейной и нефтехимической промышленности и газовые станции.

Эта злонамеренная деятельность показала, что ИКТ-средства могут быть использованы в качестве оружия для нанесения ущерба инфраструктуре государств.

Учитывая сложный характер управления ИКТ, я хотел бы остановиться на следующих моментах.

Во-первых, основная ответственность за поддержание надежных, безопасных и заслуживающих доверия ИКТ лежит на отдельных государствах. Необходимо усилить роль и обеспечить активное участие государств в управлении сферой ИКТ на глобальном уровне, особенно в разработке политики и принятии решений. Управление ИКТ должно развиваться таким образом, чтобы не причинять ущерб праву государств определять свое собственное направление развития, управленческие структуры и законодательство в отношении сферы ИКТ. Государства должны действовать ответственно и в соответствии с основополагающими принципами международного права, в частности целями и принципами Организации Объединенных Наций.

Во-вторых, проблемой остается отсутствие универсальных юридически обязывающих норм в сфере ИКТ. Действующее международное право зачастую отстает от стремительных темпов технологических изменений, создавая пробелы, которыми пользуются злоумышленники. Поэтому разработка и применение международных юридически обязательных норм, в которых учитывается специфика сферы ИКТ, имеет большое значение.

В-третьих, государства должны воздерживаться от использования достижений ИКТ в качестве инструментов для принятия экономических, политических или иных принудительных мер, включая меры по ограничению или блокированию деятельности других государств. Они также должны предотвращать злоупотребления связанными с ИКТ цепочками поставок, находящимися под их контролем и юрисдикцией, и не допускать их, обеспечивая, чтобы в этих цепочках поставок не появлялись уязвимые места, которые ставят под угрозу суверенитет и защиту данных других государств. Государства должны обеспечить принятие соответствующих мер в отношении компаний и платформ ИКТ, оказывающих экстерриториальное воздействие в рамках их юрисдикции, и привлекать их к ответственности за их поведение в сфере ИКТ, особенно если они нарушают национальный суверенитет, безопасность или общественный порядок других государств.

В-четвертых, мы твердо убеждены, что ИКТ должны использоваться исключительно в мирных целях. Для этого Организация Объединенных Наций должна продолжать играть центральную роль в рамках Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, чтобы сформулировать имеющие обязательную юридическую силу обязательства по предотвращению использования ИКТ в злонамеренных целях и обеспечению их исключительно мирного использования.

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

**Г-н Акрам** (Пакистан) (*говорит по-английски*): Мы благодарим делегацию Республики Корея за созыв этих важных прений по вопросу о противодействии меняющимся угрозам в киберпространстве. Я также хочу поблагодарить Генерального секретаря и других докладчиков за их содержательные выступления.

Технологии и применение информационно-коммуникационных технологий (ИКТ) внесли огромный вклад в социально-экономическое развитие. Однако эти технологии также расширили сферу конфликтов. Военные действия в киберпространстве стали новым и важным видом военных действий, включающим в себя как информационную войну, так и реальные кибератаки государственных и негосударственных субъектов. Пакистан признает серьезность меняющегося характера киберугроз и их влияние на международный мир и безопасность. Мы также признаем настоятельную необходимость борьбы с другими видами злонамеренных действий в киберпространстве, включая атаки с использованием вирусов-вымогателей и кражу конфиденциальной информации.

Несколько стран, включая Пакистан, стали жертвами кампаний по распространению дезинформации. В своих докладах за 2019 и 2020 годы базирующаяся в Брюсселе организация «Дезинфолаб», действующая в Европейском союзе, раскрыла информацию об антипакистанской кампании по распространению пропаганды и дезинформации, а также о военных действиях против Пакистана в киберпространстве. В отчете за 2019 год приводят-

ся доказательства проводившихся на протяжении 15 лет масштабных операций против Пакистана, в которых участвовали более 10 так называемых неправительственных организаций, обманным путем аккредитованных при Совете по правам человека, более 750 поддельных СМИ и 550 поддельных вебсайтов, на которых даже использовались личности людей, которых уже нет в живых. Это была систематическая кампания, проводимая под руководством государства с целью распространения дезинформации и использования Организации Объединенных Наций, а также европейских институтов в своих целях, чтобы очернить Пакистан. Разоблачение этой дезинформационной кампании, проведенное организацией «Дезинфолаб» Европейского союза, требует внимания мирового сообщества. Мы должны разработать механизмы с целью предотвращения такого незаконного и вопиющего злонамеренного использования киберсредств для продвижения враждебно настроенными государствами их версий событий и достижения ими своих целей.

В декабре 2021 года Генеральная Ассамблея консенсусом приняла резолюцию 76/227 «Борьба с дезинформацией в целях поощрения и защиты прав человека и основных свобод», автором которой выступил Пакистан. В резолюции подтверждается ответственность государств за противодействие распространению дезинформации, которое подрывает усилия по укреплению мира и сотрудничества между государствами. Пакистан по-прежнему страдает от продолжающейся враждебной кампании по распространению пропаганды в киберпространстве и с помощью других средств и намерен и впредь бороться с вирусом дезинформации. Мы будем содействовать принятию мер с этой целью в рамках международного сотрудничества, в том числе в Совете Безопасности.

Признавая важную роль Совета Безопасности в борьбе с конкретными киберугрозами, бросающими вызов международному миру и безопасности, мы считаем, что Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ является наиболее подходящей площадкой для расширения международного сотрудничества и принятия основанных на консенсусе мер для реагирования на вызовы и возможности, создаваемые стремительным развитием ИКТ.

В Уставе Организации Объединенных Наций содержится однозначный призыв к всеобщему соблюдению принципов суверенитета, территориальной целостности, неприменения силы и невмешательства во внутренние дела государств. Мы должны руководствоваться этими принципами в регулировании киберпространства.

Однако простого утверждения о том, что нормы международного права применимы в киберпространство, недостаточно. Пакистан разделяет мнение о том, что необходимо разработать юридически обязательный международный документ с учетом уникальных особенностей ИКТ, чтобы создать нормативную базу и механизм управления, необходимые для обеспечения стабильности и безопасности киберпространства. При разработке таких правовых и институциональных рамок следует учитывать проблемы и интересы всех сторон и обсуждать их в рамках Организации Объединенных Наций при равном участии всех государств.

Соответствующие меры укрепления доверия, такие как добровольный обмен информацией и передовым опытом, могут способствовать повышению транспарентности и предсказуемости в киберпространстве, снижению вероятности недопонимания и, следовательно, уменьшению риска возникновения конфликтов. Опубликование в прошлом месяце глобального справочника контактных центров по вопросам безопасности в сфере ИКТ стало важным шагом в деле укрепления доверия и сотрудничества между государствами в области безопасности ИКТ. Мы должны развивать такие механизмы и сотрудничество, чтобы укрепить кибербезопасность и в полной мере использовать потенциал ИКТ для достижения экономического и социального развития.

**Председатель** (*говорит по-английски*): Слово имеет представитель Уругвая.

**Г-жа Гонсалес** (Уругвай) (*говорит по-испански*): Мы признательны Генеральному секретарю за участие в сегодняшнем утреннем заседании, а также благодарны за вклад в обсуждения главному административному сотруднику Института «Кибермир» и профессору права и технологий Лидсского университета им. Беккета и заместителю председателя Группы экспертов Африканского союза по кибербезопасности.

Считаем организацию этих открытых прений нынешним председателем Совета, Республикой Корея, весьма своевременным. Эти прения позволяют привлечь внимание к этой теме и обогатить диалог

и дискуссию по вопросу, который является ключевым для повестки дня в области международного мира и безопасности и имеет отношение ко многим другим вопросам, входящим в сферу компетенции Организации. Уругвай поддерживает эту и другие инициативы, целью которых является выработка позитивных мер реагирования на разрушительное воздействие злонамеренного использования информационно-коммуникационных технологий (ИКТ) на глобальный мир, безопасность и стабильность.

Ни один регион или страна не защищены от этой опасности, которая не знает границ. Большинство государств-членов сталкивались с атаками такого рода, что делает киберпространство небезопасным местом и еще больше усугубляет такие бедствия, от которых страдают наши общества, как терроризм, наркоторговля, торговля людьми и нападения на важнейшие объекты инфраструктуры, и это лишь некоторые из них.

Мы внимательно выслушали Генерального секретаря сегодня утром и согласны с тем, что опасность, связанная с использованием цифровых технологий в качестве оружия, возрастает. Мы также осуждаем использование искусственного интеллекта в качестве инструмента, усиливающего существующие угрозы в киберпространстве, а также аналогичное использование технологии квантовых вычислений, которые еще больше расширяют возможности причинения вреда.

Уругвай выступает за свободное, открытое и безопасное использование киберпространства, которое позволяет развивать позитивные аспекты технологий и использования Интернета — позитивный подход, позволяющий нам достигать целей в области устойчивого развития, развивать международную торговлю и продолжать научные и медицинские открытия, которые улучшают благосостояние нашего населения.

Для этого у нас должны быть конкретные инструменты и надежная нормативно-правовая база, обеспечивающая такую безопасность. Однако в действительности не все страны и регионы в одинаковой степени способны реагировать на эти киберугрозы или защищаться от них в силу разного уровня развития технологий, которые позволяют обеспечивать кибербезопасность.

В этой связи мы обеспокоены отсутствием значительного прогресса в области наращивания потенциала и международного сотрудничества. Развивающиеся страны как никогда ранее нуждаются в передаче технологий, знаний, передового опыта и оборудования, необходимых для эффективного решения проблем, возникающих в результате злонамеренного использования ИКТ.

В условиях неблагоприятной ситуации, сложившейся в киберпространстве, Организация Объединенных Наций играет основополагающую роль в обеспечении международного мира и безопасности, что является одним из необходимых условий всякого процветания.

В этой связи мы обращаем внимание на роль Генеральной Ассамблеи, действующей через Первый комитет. Мы высоко оцениваем и поддерживаем деятельность Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, как это было в прошлом и с работой Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Деятельность Рабочей группы, в ходе которой были выработаны рекомендации и стандартизированные нормы ответственного поведения государств, позволившие создать общую основу для понимания ситуации, на которую можно ориентироваться, и сформирован главный форум для проведения дискуссий и обсуждений. Государства также несут ответственность за применение указанных норм и стандартов.

По мере развития технологий активную роль должны играть и организации. Они должны меняться и совершенствовать свою организационную структуру и систему управления с помощью постоянного механизма, который позволит им решать проблемы, возникающие в связи с этим постоянным развитием. Они должны избегать дублирования усилий и в конечном итоге добиться принятия обязательных правил для всех государств. Киберпространство не исключено из сферы действия международного права и иных международных норм, что обеспечивает правовую определенность.

Пользуясь возможностью, мы хотели бы упомянуть о важности предстоящей сессии Специального комитета по разработке всеобъемлющей международной конвенции о противодействии ис-

пользованию информационно-коммуникационных технологий в преступных целях, известной также как конвенция о киберпреступности. Мы надеемся, что она будет принята как можно скорее и что государства разработают соответствующие национальные стандарты. Считаем, что ее принятие станет шагом, благодаря которому Организации сможет начать двигаться в правильном направлении.

Наконец, я хотела бы еще раз подтвердить важность укрепления деятельности по противодействию киберугрозам и наращивания потенциала — этот общий знаменатель объединяет большинство членов Организации, в рамках которой региональные организации играют важную роль. Мы высоко оцениваем поддержку со стороны различных стран, которые осуществляют программы сотрудничества и содействуют подготовке технических специалистов и профессионалов, способных решать проблемы, возникающие в киберпространстве, благодарим их и призываем их продолжать следовать по этому пути, который, без сомнения, приведет к созданию экосистемы кибербезопасности, сопряженной с более многочисленными преимуществами для всех и основанной на международном сотрудничестве, а не на конфронтации, базирующейся на политизации этих вопросов.

Как и в других сферах, в рамках борьбы с киберугрозами решающее значение имеет взаимодействие между Советом Безопасности и Генеральной Ассамблеей. Проведение периодических брифингов и прений, подобных нынешним, является необходимым для выработки эффективных мер борьбы с неправомерным использованием технологий в рамках всей сферы международной безопасности, в том числе в ходе конфликтов, что будет также способствовать обеспечению защиты гражданского населения в контексте киберпространства.

Г-н Председатель, благодарю Вас за включение этого пункта в сегодняшнюю повестку дня.

**Г-жа Янина** (Албания) (*говорит по-английски*): В современном цифровом мире кибербезопасность становится важным вопросом для всех государств-членов. Мы хотели бы поблагодарить председательствующую делегацию Кореи за организацию в Совете Безопасности этой важной дискуссии, а докладчиков за их полезный вклад.

Многим из нас уже приходилось сталкиваться с кибератаками в той или иной форме. Мы видели, что эта злонамеренная деятельность не только сказывается на повседневной жизни наших граждан, но и в более широком смысле оказывает влияние на все международное сообщество и напрямую угрожает международному миру и безопасности. Рост числа кибератак имеет значительные последствия в виде снижения валового внутреннего продукта стран в различных регионах, причем в наиболее уязвимом положении находятся развивающиеся страны.

Поскольку киберугрозы становятся все более сложными и разнообразными, наши меры реагирования должны быть гибкими. Мы должны быть оснащены всем необходимым для разработки таких мер реагирования и смягчения киберугроз, с которыми мы сталкиваемся в индивидуальном порядке и на коллективной основе, путем содействия международному сотрудничеству и обмену информацией. Два года назад Албания подверглась беспрецедентно мощной кибератаке со стороны множества хакерских групп, связанных с Исламской Республикой Иран, — их явной целью было разрушить государственную инфраструктуру, парализовать работу государственных служб, посеять в стране хаос и создать небезопасную обстановку. Мы по-прежнему сталкиваемся с изощренными кибератаками.

В этой связи Албания инвестирует силы и средства в свой национальный потенциал противодействия киберугрозам, уделяя при этом значительное внимание региональным и международным подходам к обеспечению кибербезопасности. Наш регион, Западные Балканы, продолжает сталкиваться с растущим числом киберугроз, которые продолжают меняться. Мы работаем над созданием потенциала в области кибербезопасности в нашем регионе с помощью программ по обеспечению кибербезопасности, борьбе с киберпреступностью и поощрению кибердипломатии. Региональный саммит по вопросам кибербезопасности, который пройдет в июле в моей стране, Албании, будет направлен на повышение потенциала противодействия киберугрозам на Западных Балканах.

Мы твердо убеждены в том, что на международном уровне можно и нужно прилагать больше усилий.

В этой связи я хотела бы подчеркнуть три момента.

Во-первых, Совет Безопасности как главный орган по поддержанию международного мира и безопасности, может и должен играть более активную роль. Речь идет о ценной платформе для обсуждения киберугроз и способов их устранения. Обсуждения должны быть всеохватными и открытыми для разного рода участников. В этой связи мы считаем полезным сотрудничество между правительствами и частным сектором, направленное на усиление защиты от киберугроз.

Во-вторых, в рамках наших совместных усилий по созданию безопасного киберпространства необходимо уделять больше внимания процессу привлечения к ответственности недобросовестно действующих государственных и негосударственных субъектов. Это должно сопровождаться соблюдением международных норм ответственного поведения в киберпространстве.

В-третьих, необходимо активизировать работу по наращиванию потенциала. В то время как развитые страны занимают сильную и весомую позицию в киберпространстве, многие развивающиеся страны не имеют достаточных ресурсов и опыта для борьбы с киберугрозами. Это может привести к возникновению опасных рисков для критически важной инфраструктуры, кибератакам, кибершпионажу и другим деструктивным действиям.

В заключение позвольте мне еще раз повторить, что безопасное киберпространство может быть обеспечено только при условии объединения усилий на глобальном уровне, и проведение этого заседания — шаг в правильном направлении.

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

**Г-н Секерис** (Греция) (*говорит по-английски*): Прежде всего я хотел бы поблагодарить Республику Корея за организацию этой крайне важной дискуссии на высоком уровне, а наших докладчиков за их весьма интересные замечания.

Греция полностью присоединяется к заявлению, сделанному ранее представителем делегации Европейского союза, и хотела бы добавить следующие соображения в своем национальном качестве.

Происходящая в наше время цифровая эволюция становится катализатором человеческого прогресса посредством преобразования наших обществ и экономических систем и расширения возможностей для сотрудничества. Новые технологии открывают перед человечеством значительные возможности для экономического роста, а также устойчивого и инклюзивного развития, что оказывает влияние все три основных направления деятельности Организации: мир и безопасность, права человека и устойчивое развитие.

А поскольку наши экономические, демократические и общественные системы как никогда зависят от безопасных, надежных и все более взаимосвязанных сетей и информационных систем, кибербезопасность приобретает важнейшее значение для построения глобального, открытого, свободного, стабильного и безопасного киберпространства.

В то же время злонамеренное использование этих технологий порождает новые риски и трудности. Злонамеренные действия в киберпространстве в последние годы активизировались и привели, среди прочего, к резкому и постоянному росту числа кибератак, направленных на критически важную инфраструктуру, цепочки поставок и интеллектуальную собственность, а также увеличению числа атак на правительства, организации, предприятия и граждан, совершаемых с использованием программ-вымогателей.

Кроме того, еще большую тревогу вызывает тот факт, что кибератаки становятся неотъемлемой частью операций в ходе вооруженных конфликтов. Греция выражает глубокую обеспокоенность по поводу такого рода деятельности, которая подрывает международный мир и безопасность и может привести к дестабилизирующим и многоуровневым последствиям, сопряженным с повышенным риском возникновения конфликта.

Однако киберпространство не является областью беззакония. Согласно так называемым рамкам ответственного поведения государств в киберпространстве, все государства договорились, что существующее международное право и, в частности, Устав Организации Объединенных Наций являются применимыми и имеют существенно важное значение для поддержания мира и стабильности. В этой сфере международное право должно поддерживаться и соблюдаться точно так же, как и во всех других областях международных отношений.

Поскольку Совет Безопасности несет главную ответственность за поддержание международного мира и безопасности, мы надеемся, что в

будущем он будет играть более активную роль по вопросам, связанным с новыми и современными угрозами. Такая роль может включать в себя усилия по укреплению вышеупомянутых рамок ответственного поведения государств и реагированию на активность в киберпространстве, несовместимую с задачами обеспечения международного мира, безопасности и стабильности.

Будучи убежденными сторонниками приоритета норм международного права и мирного урегулирования споров, мы еще раз подтверждаем наше стремление к обеспечению мирного и безопасного киберпространства и нашу полную приверженность дальнейшему обсуждению этой крайне важной темы, в том числе во время нашего пребывания в Совете Безопасности в качестве его непостоянного члена в период 2025–2026 годов.

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

**Г-н Гомес Эрнандес** (Испания) (*говорит по-испански*): Я приветствую организацию этих открытых прений. Как убежденный сторонник и активный участник процесса поддержания международного мира и безопасности Испания подтверждает свою приверженность борьбе с киберугрозами и поощрению ответственного поведения государств в киберпространстве на основе регионального и международного сотрудничества и в соответствии с рамками ответственного поведения государств — членов Организации Объединенных Наций.

Хотя быстро меняющийся характер угроз заставляет нас адаптировать наши подходы и инструменты в целях их совместного и комплексного устранения, ключом к глобальной и национальной киберустойчивости остается внедрение большего числа более совершенных киберинструментов, обеспечивающих защиту критически важной инфраструктуры по всему миру.

Среди наиболее тревожных тенденций можно отметить распространение практики захвата данных, в частности данных об объектах критически важной инфраструктуры, манипулирование информацией и восприятием с помощью цифровых технологий, а также атаки на международные цепочки поставок, совершаемые субъектами, использующими в своих целях существующие факторы уязвимости, и приводящие к экономическим потерям.

С появлением гибридных стратегий, серых зон и асимметричных войн изменилась сама концепция конфликта. В некоторых случаях провести четкое различие между войной и миром больше невозможно. Злонамеренное использование информационно-коммуникационных технологий (ИКТ) сегодня является неотъемлемой частью сложной и меняющейся ситуации с инструментами, используемыми для получения преимуществ в конфликте. Необходимо срочно принять более широкий подход для комплексного урегулирования современных конфликтов.

В этой связи любые международные механизмы или обязательства, связанные с информационно-коммуникационными технологиями, должны основываться на консенсусных соглашениях о рамках ответственного поведения государств в отношении ИКТ и разрабатываться в ходе открытого, инклюзивного и транспарентного процесса.

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

**Г-н Виньяш** (Португалия) (*говорит по-английски*): Я хотел бы поблагодарить Республику Корея за проведение сегодняшних прений и присоединиться к заявлению, сделанному ранее сегодня представителем Европейского союза.

Будучи гарантом международного мира и безопасности, Совет Безопасности должен быть способен противостоять существующим, возникающим и будущим угрозам. Тот факт, что мы обсуждаем вопрос об угрозах в киберпространстве, показывает, что при необходимости Совет может адаптироваться к новым вызовам.

Враждебные действия и операции в киберпространстве оказались самым серьезным вызовом процветанию, которое принесла цифровая трансформация. Они также стали серьезным вызовом для целостности наших институтов и доверия к ним со стороны граждан наших стран. Еще бóльшую тревогу вызывает влияние кибербезопасности на физический мир, которое нельзя недооценивать.

Растущий наступательный потенциал киберзлоумышленников приводит к увеличению расходов на предотвращение совершаемых ими атак и восстановление после них. Ситуация с киберугрозами усложняется, в частности в связи с ролью киберпреступных групп. После разрушительных

атак, совершенных в 2022 году предположительно с использованием вирусов-вымогателей, Португалия присоединилась к Международной инициативе по борьбе с вирусами-вымогателями. Стоит отметить, что вирусы-вымогатели также все чаще используются спонсируемыми государством субъектами в качестве прикрытия для достижения стратегических целей.

Искусственный интеллект в значительной степени выровнял возможности различных представляющих угрозу субъектов, что позволяет неопытным игрокам выходить на новый уровень и потенциально увеличивает масштабы совершаемых атак. На фоне сложившейся ситуации с угрозами мы надеемся на скорейшее завершение процесса разработки будущей конвенции Организации Объединенных Наций по борьбе с киберпреступностью, которая будет содействовать налаживанию международного сотрудничества правоохранительных органов. Такое сотрудничество в борьбе с киберпреступлениями, совершаемыми спонсируемыми государством субъектами, в свою очередь будет способствовать реализации ряда разработанных Организацией Объединенных Наций законов, норм и мер укрепления доверия в отношении ответственного поведения государств в киберпространстве.

Важную роль играет также наращивание потенциала, и Португалия в партнерстве с Университетом Организации Объединенных Наций намерена приступить к реализации ежегодной программы по расширению цифрового потенциала в развивающихся странах. Ожидается, что будущий постоянный институциональный механизм, или программа действий, которая будет осуществляться с 2026 года, также будет способствовать преодолению цифрового разрыва.

Совет должен играть важную вспомогательную роль, сохраняя при этом роль Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ как главной платформы для углубления нашего понимания угроз, норм и законов, а также для содействия наращиванию потенциала и укреплению доверия между государствами.

Во-первых, Совет Безопасности мог бы вновь утвердить свод норм ответственного поведения государств, согласованных на основе консенсуса в Рабочей группе открытого состава, например опубликовав соответствующее заявление Председателя. Одна эта мера стала бы важным признанием того, что киберугрозы могут оказывать влияние на международный мир и безопасность.

Наконец, во-вторых, Совет Безопасности мог бы также по необходимости пытаться включать связанные с ИКТ проблемы в свои соответствующие мандаты. Укрепление устойчивости критической инфраструктуры к враждебным кибератакам может в определенных условиях внести решающий вклад в укрепление стабильности в долгосрочной перспективе.

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

**Г-жа Гонсалес Лопес** (Сальвадор) (*говорит по-испански*): Я хотела бы поблагодарить Республику Корея за организацию этих актуальных прений по вопросу о эволюционирующих угрозах, с которыми мы сталкиваемся в киберпространстве.

Как уже неоднократно отмечала наша делегация, масштабы и серьезность угроз, связанных с использованием информационно-коммуникационных технологий (ИКТ) в контексте международной безопасности, продолжают расти. Эти угрозы, возникающие в результате неправомерного использования новых технологий, таких как искусственный интеллект или квантовые вычисления, могут породить новые методы совершения атак, что приведет к использованию злоумышленниками в своих целях недостатков систем ИКТ. Расширение возможностей сетевого подключения цифровой инфраструктуры во всех сферах управления — социальной, экономической и политической — может оказать многоуровневое воздействие, последствия которого трудно предсказать.

Злонамеренная деятельность в сфере ИКТ может иметь разрушительные последствия, выходящие за пределы международного мира и безопасности. Кроме того, она может причинять прямой вред гражданскому населению, особенно в случаях, когда объектом атак становится критически важная инфраструктура, необходимая для функционирования общества, в том числе система здравоохранения или основные службы, например система водо- и энергоснабжения и транспортная система, или когда такие атаки подрывают или ухудшают функциональность и доступность Интернета.

Наша страна считает, что этот орган, Совет Безопасности, должен принимать более систематические упреждающие меры по борьбе с киберугрозами миру и безопасности в рамках своего мандата и обязательства по поддержанию международного мира и безопасности. Для этого можно, среди прочего, проводить тематические обсуждения, способствующие достижению конкретных результатов в деле защиты критически важной инфраструктуры и критически важной информационной инфраструктуры, работать над фиксированием инцидентов в области кибербезопасности, реагированием на них и последующим восстановлением, а также заниматься выработкой комплексного подхода к наращиванию потенциала в области кибербезопасности.

Кроме того, можно было бы рассмотреть возможность включения в тематическую повестку дня Совета пункта, посвященного угрозам миру и безопасности, возникающим в цифровой сфере, включая ИКТ и другие новые технологии, такие как искусственный интеллект, чтобы дополнить усилия, прилагаемые в рамках Генеральной Ассамблеи и других вспомогательных органов.

Важно также отметить необходимость дальнейшего рассмотрения вопроса о влиянии цифровых технологий на защиту мирного населения и гражданских объектов в ходе вооруженных конфликтов, включая применение и полное соблюдение принципов международного гуманитарного права в цифровой сфере. Считаем, что вопросы расширения и влияния дезинформационных кампаний, а также распространения ложной информации и ненавистнических высказываний через цифровые платформы также заслуживают внимания Совета Безопасности.

В интересах экономии времени полный текст заявления можно будет получить через Секретариат.

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

**Г-жа Стоева** (Болгария) (*говорит по-английски*): Болгария присоединяется к заявлению, сделанному от имени Европейского союза. Я хотела бы обратить внимание на несколько моментов в своем национальном качестве.

Мы признательны Республике Корея за организацию сегодняшних прений высокого уровня и привлечение внимания Совета Безопасности к этой важной теме. Хотели бы также поблагодарить докладчиков за их крайне информативные и содержательные выступления.

Проблема меняющихся угроз в киберпространстве приобретает все большее значение в контексте безопасности и стабильности наших обществ. Сегодня киберпространство все чаще используется в политических и идеологических целях, при этом усиливающаяся поляризация на международном уровне препятствует эффективной реализации принципа многосторонности.

Как было продемонстрировано докладчиками, в числе самых серьезных рисков, с которыми мы сталкиваемся в результате злонамеренного использования киберпространства, — все более активные кампании по распространению дезинформации, в рамках которых предпринимаются попытки использовать факторы уязвимости общества посредством подрыва демократических процессов и институтов, обеспечения зарождения недоверия и в конечном итоге ослабления общества. Кроме того, серьезную общемировую угрозу представляют собой злонамеренные атаки на критически важную инфраструктуру и основные службы. Вся такая деятельность сказывается на международной безопасности и стабильности, а также преимуществах использования киберпространства для достижения экономического, социального и политического развития.

Хотя национальная безопасность, в том числе кибербезопасность, остается прерогативой национальных правительств, потенциальные трансграничные последствия киберинцидентов свидетельствуют о необходимости совместных усилий. По этой причине важно расширять международное сотрудничество по вопросам обеспечения кибербезопасности. И хотя из-за геополитической напряженности эффективность многосторонних прений по вопросам международной безопасности в киберпространстве в целом снижается, Совету Безопасности явно необходимо занять более активную позицию по этой теме.

По мнению Болгарии, международная безопасность и стабильность зависят от наличия глобального, открытого, стабильного и безопасного киберпространства, в котором соблюдаются нормы международного права, в частности Устав Органи-

зации Объединенных Наций, а также добровольные и не имеющие обязательной силы нормы, правила и принципы ответственного поведения государств. В этой связи крайне важно международное сотрудничество. Именно поэтому расширение роли Совета Безопасности в области борьбы с киберугрозами имеет решающее значение. Активное участие Совета в процессе обеспечения кибербезопасности вкупе с его главной ответственностью за поддержание международного мира и безопасности позволяет этому органу занять уникальную позицию для принятия мер реагирования на злонамеренную активность с использованием киберсредств.

Ввиду взаимосвязанного характера киберпространства необходимо, чтобы все заинтересованные стороны обменивались информацией и в контексте киберпространства принимали на себя свои конкретные обязанности для поддержания глобального, открытого, стабильного и безопасного киберпространства. Соответственно, для надлежащего противодействия меняющимся угрозам в киберпространстве жизненно важно применять подход с участием многих заинтересованных сторон. Государства и международные учреждения, в том числе Совет Безопасности, должны стремиться к укреплению регулярных и структурированных обменов мнениями со всеми заинтересованными сторонами, включая частный сектор, научные круги и гражданское общество. Именно таким образом можно также продвигать и развивать меры предотвращения, обеспечения готовности и устойчивости, а также оперативного реагирования в киберпространстве.

Наконец, стоит отметить, что уровень потенциала противодействия киберугрозам и способность выявлять злонамеренную активность с использованием киберсредств и реагировать на нее существенно различаются в разных странах с точки зрения как самих возможностей, так и эффективности. По этой причине необходимо повышать общий уровень кибербезопасности путем укрепления потенциала и установить общие стандарты в области кибербезопасности, особенно для защиты критически важной инфраструктуры, а также для разработки и применения новых технологий.

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

**Г-жа Андриани** (*говорит по-английски*): Для меня честь выступить сегодня в Совете Безопасности по этому важнейшему вопросу, а именно: злонамеренное использование современных технологий и растущие угрозы в области киберпространства.

Киберпреступность многократно увеличивает существующие угрозы, создавая возможность для осуществления иных форм преступности, усугубляя глобальные потрясения и подрывая устойчивое развитие, мир и безопасность.

Интерпол поддерживает эти открытые прения и выскажет три соображения по поводу укрепления глобальной архитектуры безопасности в целях противодействия киберугрозам, исходящим от преступных негосударственных субъектов.

Во-первых, мы должны лучше понять современную ситуацию с киберугрозами, которая до сих пор сильно различается по регионам и секторам. В этой связи в дополнение к обмену информацией между странами — членами Интерпола разработал модель шлюза для упрощения доступа к отраслевым данным. Наша платформа «система связи I-24/7» позволяет объединить усилия 196 стран-членов, обеспечивая безопасный обмен полицейской информацией в рамках всего мира. Кроме того, мы предлагаем специализированные платформы для ведения борьбы с киберпреступностью посредством обмена передовой практикой и аналитическими целями. Далее, список контактных лиц в рамках системы связи I-24/7 и региональные рабочие группы способствуют обеспечению оперативного реагирования в экстренных случаях и укреплению доверия между структурами. Работая сообща и используя существующие и отлаженные механизмы обмена информацией, мы можем добиться значительных успехов в защите киберпространства и обеспечении глобальной безопасности.

Во-вторых, мы должны устранять пробелы в потенциале. В области потенциала противодействия киберугрозам по-прежнему сохраняется значительное неравенство. Интерпол оказывает странам-членам поддержку в преодолении цифрового разрыва посредством предоставления технической помощи и наращивания потенциала. Мы стремимся вооружить правоохранительные органы знаниями и навыками, необходимыми для противодействия проблемам, возникающим сегодня в киберпространстве.

В-третьих, мы должны обеспечивать максимальное взаимодействие структур с помощью регулярного ведения институционального диалога и задействования многосторонних механизмов. Давайте помнить о том, что главное — это сотрудничество, а не дублирование усилий. Именно поэтому Интерпол принимает активное участие в различных процессах в киберпространстве как в рамках Организации Объединенных Наций, так и за ее пределами, в том числе в рамках Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Киберугрозы не знают границ — не должна их знать и осуществляемая нами защита. Интерпол по-прежнему настроен способствовать обеспечению более безопасного киберпространства для всех благодаря сотрудничеству, инновациям и бесконечной самоотверженности.

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

**Г-н Рагуттахалли** (Индия) (*говорит по-английски*): Поздравляю Республику Корея со вступлением на пост Председателя Совета Безопасности в июне. Я приветствую данную инициативу по проведению открытых прений на тему «Противодействие меняющимся угрозам в киберпространстве». Благодарю также Генерального секретаря и представителей гражданского общества за их вклад.

Современный мир — это цифровая эпоха. Цифровые преобразования не ограничиваются рамками каких-либо привычных географических, политических и экономических границ. Ввиду стремительного прогресса и внедрения новых и новейших технологий, таких как искусственный интеллект, наша жизнь начинает все больше переплетаться с цифровой сферой. В этом взаимосвязанном мире зависимость от киберпространства велика, будь то личное общение или функционирование критически важной инфраструктуры.

Цифровые преобразования также заставляют нас сталкиваться с бесчисленным множеством киберугроз. Кибератаки на критически важные объекты инфраструктуры, информационные и финансовые системы, а также сети органов власти становятся все более частыми и изощренными. Совершение криптовалютных хищений, перехват данных, «дипфейки», дезинформация и подстрекательство уже стали обычным делом. Кроме того, следует отметить потенциал искусственного интеллекта, который может придать кибератакам еще больший размах и масштаб.

Подрываются неприкосновенность и безопасность продуктов информационно-коммуникационных технологий (ИКТ), которые составляют основу киберпространства. Такие акты совершаются как государственными, так и негосударственными субъектами, а также транснациональными преступными сетями. Подобные вредоносные действия подрывают доверие к глобальным цепочкам поставок в сфере ИКТ, ставят под угрозу безопасность и создают потенциальные очаги напряженности в отношениях между государствами. По оценкам Всемирного банка, в период с 2019 по 2023 год кибератаки, вероятно, нанесли миру ущерб в размере около 5,2 трлн долл. США.

Благодаря киберпространству террористы также находят новые пути для совершения насилия, радикализации молодежи, осуществления вербовки, организации соответствующей подготовки и привлечения финансовых ресурсов. Новые методы оплаты в виде использования виртуальных активов и криптовалюты становятся нормой в рамках финансовых сделок, осуществляемых террористами. Терроризм использует новые каналы и новые методы финансирования, доступные в киберпространстве, в результате чего возникает крайне важная проблема для безопасности и процветания всех стран. Индия вот уже несколько десятилетий является жертвой терроризма, и мы осознаем всю серьезность такой проблемы, как кибертерроризм.

В этой связи позвольте мне обратить внимание на четыре момента.

Существующие в киберпространстве угрозы способны не только поставить под удар национальную безопасность, но и разрушить сам каркас глобальной стабильности и сотрудничества. Ни одна страна или организация не может вести борьбу с киберугрозами в одиночку — для этого необходимо выступить единым фронтом.

Растет потребность в международных инструментах для борьбы с угрозами, исходящими из киберпространства. Нынешнее международное право не очень хорошо приспособлено к реагированию на кибератаки. Кибератаки на критически важные объекты инфраструктуры, информационные и финансовые системы, а также сети органов власти необходимо рассматривать как террористические акты. Необходимо рассмотреть применимость существующих антитеррористических договоров к киберпространству. Международное сообщество должно обеспечить единообразие законов о борьбе с террористическими актами. Глобальное сотрудничество в этой области поможет согласовать целевые показатели в области кибербезопасности, передовые практики и нормативные акты.

Индия участвует в санкционированных Организацией Объединенных Наций киберпроцессах и консультациях, которые поддерживают глобальное, инклюзивное и транспарентное межправительственное участие с целью создания безопасного и надежного киберпространства. Мы считаем, что для получения информации и понимания возникающих угроз в киберпространстве необходимо сотрудничество между многими заинтересованными сторонами.

В заключение следует отметить, что Индия входит в число мировых лидеров по развитию цифровых технологий, предоставлению доступа к Интернету и обеспечению устойчивости. Индия преисполнена решимости содействовать созданию открытой, безопасной, свободной, доступной и стабильной ИКТ-среды. Индия будет продолжать сотрудничать с мировым сообществом в борьбе с киберугрозами и обеспечивать, чтобы цифровая революция продолжала приносить пользу человечеству, не ставя под угрозу его коллективное благополучие и стабильность.

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

**Г-н Мао** (Камбоджа) (*говорит по-английски*): Прежде всего я хотел бы выразить Вам, г-н Председатель, свою признательность за созыв сегодняшних открытых прений высокого уровня, которые позволяют государствам-членам обменяться мнениями по вопросу о киберпространстве, поскольку киберугрозы становятся все более серьезной проблемой для всех стран. Я также благодарю Его Превосходительство Антониу Гутерриша и наших докладчиков и выступающих за их глубокие замечания.

Невозможно отрицать, что наш мир сейчас сильно зависит от цифровых технологий. Стремительное развитие информационно-коммуникационных технологий (ИКТ) открывает огромные возможности, но в то же время подвергает нас все новым и новым рискам, которые угрожают международному миру и безопасности. Участившиеся в последнее время кибератаки показывают, что ИКТ-системы уязвимы как никогда.

В этой связи Камбоджа стремится создать безопасную цифровую среду для всех. Мы используем нашу платформу Ассоциации государств Юго-Восточной Азии (АСЕАН) для содействия программам наращивания потенциала и обмена передовым опытом. Мы твердо верим в силу международного сотрудничества и призываем мировое сообщество оказывать техническую помощь и обмениваться знаниями для укрепления кибербезопасности, особенно в развивающихся странах.

На национальном уровне Камбоджа приняла решительные меры, создав в начале этого года Комитет по цифровой безопасности. Этот комитет, состоящий из представителей соответствующих министерств, возглавляет наши усилия в области кибербезопасности, предотвращения киберпреступлений, киберзащиты и кибердипломатии. Такой скоординированный подход позволяет нам оценить наши потребности, устранить пробелы в навыках и реализовать эффективные стратегии по защите нашей цифровой инфраструктуры.

Камбоджа высоко ценит важность создания потенциала в области кибербезопасности. В прошлом месяце министр почт и телекоммуникаций нашей страны принял активное участие в глобальном круглом столе по созданию потенциала безопасности в сфере ИКТ. Мы воздаем должное Рабочей группе открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, возглавляемой Сингапуром, за ее неустанные усилия по развитию международного диалога и сотрудничества по этому важнейшему вопросу.

Кроме того, Камбоджа выступает в поддержку надежной правовой базы и международных норм, которые способствуют ответственному поведению в киберпространстве, поддерживают националь-

ный суверенитет и предотвращают злонамеренные действия. Сотрудничество между правительствами, деловыми кругами и гражданским обществом жизненно важно для обмена информацией и разработки инновационных решений. Мы также уделяем приоритетное внимание образовательным и просветительским инициативам, чтобы предоставить нашим гражданам знания и навыки, необходимые для безопасной навигации в цифровом мире.

В заключение хочу отметить, что Камбоджа намерена сотрудничать со всеми странами для построения безопасного и устойчивого цифрового будущего. Мы подтверждаем нашу приверженность сотрудничеству и взаимодействию в стремлении к более сильному, безопасному и киберустойчивому будущему для всех. Наша делегация верит, что вместе мы сможем создать киберпространство, способствующее инновациям, экономическому росту и благополучию всех наших граждан.

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

**Г-н Франса Данези** (Бразилия) (*говорит по-английски*): Я благодарю делегацию Республики Корея за организацию этого заседания.

Как мы заявили на организованном Республикой Корея заседании по формуле Аррии в апреле, Бразилия разделяет со многими другими делегациями озабоченность по поводу эволюции угроз в области кибербезопасности. Мы также согласны с необходимостью многосторонних решений, способных повысить киберустойчивость для всех.

Однако мы по-прежнему убеждены в том, что наилучший способ достичь этой цели — это сделать наши обсуждения инклюзивными, не дублируя существующую работу. Хотя мы высоко ценим искренние усилия Республики Корея по поиску более широких форматов для обсуждения в Совете Безопасности, как через формат заседаний по формуле Аррии, так посредством этих открытых прений, мы считаем, что правильным форумом для этих обсуждений по-прежнему является Генеральная Ассамблея.

В этом году мы убедились в ограниченности возможностей Совета устанавливать правила в новых сферах, когда он дважды не смог принять проект резолюции по оружию в космическом пространстве (см. S/PV.9616 и S/PV.9630). В обоих случаях делегации выражали обеспокоенность по поводу вынесения на рассмотрение Совета комплексных вопросов, которые лучше всего рассматривать полным членским составом Организации Объединенных Наций. Эти опасения вполне обоснованны и применимы и здесь.

Действующая Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ уполномочена обсуждать именно эту тему, и ее деятельность продуктивна в плане выявления киберугроз. Она отметила угрозы, связанные с применением вирусов-вымогателей и криптовалютами, а также другие потенциальные объекты нападений, включая критически важную инфраструктуру. В ее рамках обсуждались побочные эффекты кибератак и способы защиты и обособления систем, имеющих особое гуманитарное значение. Она прояснила вопрос о применимости международного права и международного гуманитарного права к киберпространству. В настоящее время она обсуждает конкретные меры по внедрению рамок ответственного поведения государств в киберпространстве. Это важные достижения, которые свидетельствуют о возможности и важности проведения подобных прений на соответствующем форуме.

Это не значит, что Совет не играет никакой роли. В соответствии со своими полномочиями и функциями, предусмотренными Уставом Организации Объединенных Наций, этот орган может реагировать на конкретные и специфические киберинциденты, представляющие угрозу международному миру и безопасности.

В эпоху, когда движение вперед в области разоружения практически остановилось, исключением остается область кибербезопасности, в которой на Генеральной Ассамблее был достигнут значительный прогресс. Необходимо поддерживать эту динамику.

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

**Г-жа Родригес Мансия** (Гватемала) (*говорит по-испански*): Гватемала хотела бы поблагодарить Республику Корея в ее качестве Председателя Совета Безопасности за созыв этих важных открытых прений.

Наша делегация признает, что киберпространство стало центральной и незаменимой областью глобальной деятельности и, в силу своего гражданского характера и двойного назначения, оно не раз использовалось преступными и террористическими группировками. Это привело к увеличению числа случаев эксплуатации объектов критически важной инфраструктуры и кибератак на них, в результате чего страдают электросети, транспортные системы, больницы, школы и т. д., что оказывает разрушительное воздействие на жизнь людей и экономику. Глобально взаимосвязанные сети и перевод в цифровой формат мировой экономики создали ситуацию, в которой нарушения кибербезопасности могут представлять значительную угрозу для экономики и международной безопасности.

Вредоносная деятельность в киберпространстве может усиливать конфликты несколькими способами. Она может усиливать напряженность в отношениях между государствами, позволяя совершать тайные нападения с правдоподобным отрицанием вины, усложняя установление ответственности и способствуя росту недоверия. Кроме того, государственные и негосударственные субъекты могут использовать киберпространство для пропаганды, распространения дезинформации и шпионажа, обостряя внутренние разногласия и разжигая внутренние и транснациональные конфликты.

Кроме того, искусственный интеллект (ИИ), безусловно, предоставляет очень важную возможность внести вклад в прогресс человечества, начиная от предотвращения и урегулирования кризисов и заканчивая предоставлением услуг в области здравоохранения и образования, и позволяет расширить работу правительств, гражданского общества и Организации Объединенных Наций во всех областях. Однако злонамеренное использование ИИ может подорвать доверие к институтам, ослабить социальную сплоченность и поставить под угрозу демократию. С учетом вышесказанного наша делегация считает необходимым активизировать текущие усилия, во-первых, по предотвращению и, во-вторых, по противодействию существующим и потенциальным угрозам.

Уже предприняты определенные шаги по включению вопросов кибербезопасности в программы работы нашей Организации. Однако необходимо подкрепить энергичными действиями усилия по эффективному включению этих вопросов в повестку дня Совета Безопасности. В качестве примеров таких действий можно привести создание санкционного механизма для регулирования поведения в киберпространстве; оказание более активной помощи государствам в укреплении их потенциала в области кибербезопасности и продолжение работы с частным сектором и гражданским обществом по разработке надежных стратегий контроля над информационно-коммуникационными технологиями.

Совет Безопасности должен играть более активную руководящую роль в борьбе с киберугрозами, которые подрывают международный мир и безопасность.

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

**Г-н Криделька** (Бельгия) (*говорит по-английски*): Прежде всего позвольте мне искренне поблагодарить Республику Корея за организацию этого заседания.

Я имею честь выступить с этим заявлением от имени стран Бенилюкса: Люксембурга, Королевства Нидерландов и моей страны, Бельгии. Страны Бенилюкса присоединяются к заявлению, сделанному от имени Европейского союза. И мы хотели бы подчеркнуть четыре дополнительных момента.

Во-первых, что касается угроз, то, как уже отмечалось в Совете, страны Бенилюкса по-прежнему глубоко обеспокоены растущей и эволюционирующей угрозой, создаваемой злонамеренной деятельностью с использованием киберсредств. Масштабы этой угрозы продолжают расти, и она может еще больше усугубляться появлением новых технологий, включая искусственный интеллект и достижения в области квантовых вычислений. Одна из тревожных тенденций, которую мы наблюдаем, — это увеличение числа атак с использованием вирусов-вымогателей, применение модели «программа-вымогатель как услуга» и совершение вредоносных кибератак против объектов критически важной инфраструктуры, включая учреждения здравоохранения и образования, а также кибератак на избирательные процессы. Последствия таких инцидентов и риск побочных эффектов представляют собой угрозу международному миру и безопасности.

Это подводит меня ко второму тезису. В рамках Первого комитета Генеральной Ассамблеи мы все приняли на основе консенсуса разработанные Организацией Объединенных Наций рамки ответственного поведения государств в киберпространстве. В этих рамках подтверждается, что нормы международного права, в частности положения Устава Организации Объединенных Наций, применимы в киберпространстве. Применение этих рамок по-прежнему имеет важнейшее значение для устранения существующих и потенциальных угроз международной безопасности, связанных с информационно-коммуникационными технологиями. В этой связи страны Бенилюкса поддерживают разработку программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Другие соответствующие процессы Организации Объединенных Наций включают разработку конвенции Организации Объединенных Наций по борьбе с киберпреступностью.

Кроме того — и это мой третий тезис, — в соответствии с главой VI Устава Организации Объединенных Наций Совет Безопасности призван играть четкую роль в мирном урегулировании споров, в том числе в киберпространстве, призывая стороны к урегулированию любого спора, который может поставить под угрозу поддержание международного мира и безопасности. Страны Бенилюкса считают, что Совету отведена важная роль в содействии созданию открытого, свободного и безопасного киберпространства. Поэтому мы приветствуем растущее внимание Совета к теме кибербезопасности, о чем свидетельствует увеличение числа заседаний по вопросу о киберпространстве с 2016 года. Продолжающиеся конфликты демонстрируют, что киберугрозы являются неотъемлемой частью более широкого спектра угроз международному миру и безопасности. Поэтому страны Бенилюкса также поддерживают Ваши предложения, г-н Председатель, об учете киберпроблематики в текущей работе Совета.

В заключение — и это мой четвертый тезис — страны Бенилюкса призывают уделять больше внимания жертвам кибероперации. Хотя злонамеренную деятельность в киберпространстве часто рассматривают сквозь призму геополитической конкуренции, она приводит к разрушительным последствиям для людей, серьезно ущемляя их права человека. Поэтому, чтобы благополучию и достоинству людей уделялось первоочередное внимание в ходе наших обсуждений, мы призываем применять подход, ориентированный на интересы и потребности пострадавших.

И давайте не будем забывать о значительных рисках в плане защиты, которые цифровые преобразования, в том числе в киберпространстве, создают для людей, пострадавших от гуманитарных кризисов. Мы видим, что Международный комитет Красного Креста, в том числе через свой Глобальный киберцентр, расположенный в Люксембурге, находится в авангарде решения некоторых из этих проблем, в частности разрабатывая и тестируя новые инструменты для предоставления цифровых услуг пострадавшему населению на нейтральной, беспристрастной и независимой основе.

Страны Бенилюкса еще раз благодарят Вас, г-н Председатель, за организацию этих прений и приветствуют Ваши усилия по повышению осведомленности о важности киберугроз и рассмотрению данного вопроса.

**Председатель** (*говорит по-английски*): Я предоставляю слово представителю Норвегии.

**Г-н Лёвольд** (Норвегия) (*говорит по-английски*): Я имею честь выступать от имени Северных стран: Дании, Финляндии, Исландии, Швеции и моей страны, Норвегии.

Прежде всего позвольте мне поблагодарить Республику Корея за инициативу по организации этого своевременного заседания. Это всего лишь второе официальное заседание, на котором Совет обсуждает важную тему кибербезопасности.

Изменения в сфере киберугроз, произошедшие с тех пор, как Совет впервые обсудил этот вопрос под председательством Эстонии в 2021 году (см. S/2021/621), вызывают тревогу.

Позвольте мне кратко остановиться на трех видах угроз.

Во-первых, сохраняется угроза кибероперации, организуемых государствами, особенно в контексте незаконной агрессивной войны России против Украины. Россия использует киберсредства на Украине для того, чтобы подорвать доверие к властям и разрушить критически важную инфраструк-

туру. Мы продолжаем придавать большое значение киберзащите Украины, а также защите наших собственных обществ от злоумышленников. В этом контексте мы хотели бы еще раз подчеркнуть, что нормы международного права должны применяться и в киберпространстве.

Во-вторых, различия между атаками, организуемыми государствами, и атаками, совершаемыми негосударственными и преступными субъектами, становятся все менее четкими. Основную озабоченность вызывает растущее число атак с использованием вирусов-вымогателей и доступность передовых киберсредств и методов более широкому кругу как государственных, так и негосударственных субъектов.

Наконец, в связи со всеми этими угрозами особую озабоченность вызывает растущее число нападений злоумышленников на критически важные сектора и инфраструктуру.

Страны Северной Европы хотели бы особо подчеркнуть важность взаимодействия различных заинтересованных сторон в сфере кибербезопасности в целях реагирования на эти угрозы. Мы должны стремиться к усилению координации действий между правительствами и всеми заинтересованными сторонами, включая гражданское общество, академические круги и частный сектор. Благодаря своему доступу к информации частный сектор играет важную роль в киберпространстве, поскольку технологические компании и компании, занимающиеся кибербезопасностью, играют ключевую роль в прогнозировании угроз и реагировании на них. Важно более эффективно использовать знания и возможности соответствующих заинтересованных сторон для создания свободного, открытого, мирного и безопасного киберпространства.

В свете меняющегося характера угроз Северные страны видят все большую пользу в том, чтобы Совет Безопасности обсуждал вопросы кибербезопасности на более регулярной основе. Обсуждение в Совете Безопасности существующих и новых киберугроз в ходе тематических и страновых дискуссий может способствовать повышению осведомленности об угрозах, обмену накопленным опытом и выработке соответствующих мер реагирования.

Работа Совета также дополняет обсуждения в других форумах. С учетом вышесказанного и в заключение я хотел бы вновь заявить, что Северные страны поддерживают разработку программы действий в области кибербезопасности в качестве постоянного, инклюзивного и ориентированного на практические действия механизма поощрения ответственного поведения государств в этой сфере.

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

**Г-н Шимонович** (Хорватия) (*говорит по-английски*): Я благодарю Вас, г-н Председатель, за организацию этих своевременных открытых прений, а также благодарю докладчиков за выступления.

Хорватия присоединяется к заявлению, сделанному представителем Европейского союза, и я хотел бы высказать несколько замечаний в своем национальном качестве.

В настоящее время мы сталкиваемся с растущим числом все более сложных киберугроз. К ним относятся, в числе прочих, атаки, совершаемые с использованием вирусов-вымогателей против объектов критически важной инфраструктуры, постоянные кампании и иностранное вмешательство в демократические процессы. Каждый из этих видов деятельности может дестабилизировать правительства в частности и привести к подрыву мира и безопасности в целом.

В зонах конфликтов кибероперации могут усиливать последствия обычных боевых действий, особенно в тех случаях, когда они направлены против критически важной инфраструктуры, что приводит к эскалации боевых действий и причинению большего вреда гражданскому населению. В этой связи мы воздаем должное Международному комитету Красного Креста за его работу по разъяснению того, что киберпространство не является сферой, не регулируемой правовыми нормами, и подтверждаем, что международное гуманитарное право в равной степени применимо как в физическом, так и в киберпространстве.

Именно поэтому Совет Безопасности должен рассмотреть возможные способы дальнейшего углубления своего понимания этого чрезвычайно сложного вопроса и с этой целью проводить регулярный обмен мнениями с различными заинтересованными сторонами не только в сфере кибербезопасности, но и в области миростроительства, а также в области предотвращения конфликтов и по-

среднических усилий. Этому могут способствовать регулярные брифинги и представление периодических докладов о киберугрозах, с тем чтобы Совет и государства-члены были информированы о последних событиях и тенденциях.

Кроме того, роль Совета Безопасности в противодействии киберугрозам может меняться на взаимоукрепляющей основе, с тем чтобы дополнять текущую работу других органов Организации Объединенных Наций и многосторонние инициативы. К таким инициативам относится деятельность Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий и других существующих профильных и будущих структур, которая позволяет обеспечивать скоординированный и всеобъемлющий общесистемный подход. Совет мог бы также рассмотреть возможность внести вклад в деэскалацию напряженности путем содействия диалогу и мерам укрепления доверия между государствами, тем самым снижая риск перерастания конфликтов в киберпространстве в вооруженное противостояние.

Предпринимая упреждающие шаги с целью понимания и уменьшения киберугроз, содействия международному сотрудничеству и включения аспектов кибербезопасности в свой более широкий мандат, Совет мог бы взять на себя важную роль в существующей экосистеме кибербезопасности Организации Объединенных Наций и обеспечить более эффективное поддержание международного мира и безопасности в цифровую эпоху.

**Председатель** (*говорит по-английски*): Слово предоставляется представителю Чили.

**Г-жа Нарваэс Охеда** (Чили) (*говорит по-испански*): Мы признательны за предоставленную нам возможность принять участие в этих открытых прениях. Принимаем к сведению прозвучавшие сообщения и мнения докладчиков. Хотели бы воспользоваться этой возможностью, чтобы поздравить Республику Корея с вступлением на пост Председателя Совета Безопасности в этом месяце.

Как мы уже заявляли ранее, Чили считает, что кибератаки и злонамеренная деятельность в киберпространстве представляют собой угрозу международному миру и безопасности и могут затрагивать государства в различной степени, в частности в зависимости от уровня их цифровизации, потенциала, ситуации в плане безопасности, инфраструктуры и степени развития. В частности, мы подчеркиваем, что эти угрозы также могут по-разному влиять на различные группы и субъекты, особенно на женщин, девочек, мальчиков и подростков.

Что касается новых и меняющихся тенденций злонамеренной деятельности в киберпространстве, мы отмечаем, в частности, использование искусственного интеллекта и машинного обучения, сочетание различных векторов атаки, совершение атак через цепочку поставок, которые могут повлиять на безопасность продуктов и услуг, а также атаки на устройства, подключенные к интернету вещей.

Мы также отмечаем опасность, которую представляют вредоносные программы, такие как вирусы-вымогатели, вайперы (стиратели) и троянские программы, и такие методы, как фишинг и распределенные атаки типа «отказ в обслуживании». Эти угрозы, исходящие от злоумышленников, могут нанести серьезный ущерб функционированию стран и повлиять как на их экономику, так и на благосостояние их населения.

Поэтому мы считаем необходимым укреплять взаимодействие и сотрудничество между государствами. Это включает обмен опытом и извлеченными уроками, применение существующих норм ответственного поведения государств в киберпространстве, применение норм международного права и международного гуманитарного права, меры укрепления доверия и наращивание потенциала — все это будет способствовать снижению недоверия между государствами и обеспечению стабильности в киберпространстве. Мы согласны с вышесказанным и отмечаем, что во всех соответствующих прениях и обсуждениях должны участвовать все заинтересованные стороны, в частности представители гражданского общества, научных кругов, частного сектора, технического сообщества и другие соответствующие субъекты.

Подчеркиваем важность укрепления роли Совета Безопасности в противодействии киберугрозам и считаем, что он может внести существенный вклад в создание безопасного, открытого и мирного киберпространства на благо всех государств. Чили придает большое значение этому вопросу, поскольку злоумышленники пользуются уязвимостью

стран, не имеющих необходимых инструментов и подготовки для борьбы с такими угрозами.

В этом смысле Совет мог бы стать ценной площадкой для диалога и сотрудничества по вопросам наращивания потенциала и оказания технической помощи, которая могла бы быть полезна странам, нуждающимся в ней больше всего. Мы призываем этот орган рассматривать вопрос о меняющемся характере угроз в киберпространстве наряду с международным сотрудничеством, которое, по нашему мнению, должно быть основано на консенсусе.

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

**Г-н Тхапа** (Непал) (*говорит по-английски*): Прежде всего я хотел бы поблагодарить председательствующую в Совете делегацию Республики Корея за созыв этих открытых прений. Я хотел бы также поблагодарить докладчиков за их содержательные и полезные выступления.

Стремительный прогресс в области информационно-коммуникационных технологий и искусственного интеллекта произвел революцию в нашей жизни, предоставив беспрецедентные возможности для ускорения социально-экономического развития. Наша зависимость от технологий постоянно растет. Однако их злонамеренное использование породило новые и серьезные угрозы. Мы обеспокоены резким ростом числа атак с использованием вирусов-вымогателей, всплеском киберпреступности, распространением дезинформации и разжиганием ненависти по всему миру.

Ни одна инфраструктура или система не застрахована от кибератак — будь то гражданская инфраструктура, такая как финансовые учреждения, больницы, транспорт, системы водоснабжения или энергоснабжения, или военная система командования и управления ядерными силами или автономные системы вооружений. Это создает угрозы международному миру, безопасности, стабильности и развитию.

Непал также сталкивается с серьезными проблемами, связанными с этой угрозой, поскольку банковские учреждения, правительственные веб-сайты и серверы в Непале периодически подвергаются кибератакам и атакам с использованием программ-вымогателей.

В связи с этим позвольте мне остановиться на нескольких моментах.

Во-первых, нам необходимо принять эффективную нормативную базу, основанную на общепризнанных нормах международного права, включая Устав Организации Объединенных Наций, обеспечивая при этом открытость, стабильность и безопасность киберпространства. Мы должны выработать общее понимание применения правил и содействовать мерам укрепления доверия в киберпространстве, а также поощрять ответственное поведение государств в киберпространстве.

Во-вторых, следует проводить регулярные брифинги и оценки с учетом мнений технологических компаний, частного сектора, гражданского общества и научных кругов, а также обмен своими знаниями и передовым опытом о том, как мы можем обеспечить нашу готовность к меняющемуся характеру и спектру киберугроз.

В-третьих, такие страны, как Непал, более уязвимы для таких возникающих новых угроз. Отсутствие надлежащей нормативно-правовой базы и ограниченность человеческого потенциала и финансовых ресурсов — это некоторые из проблем, с которыми мы сталкиваемся в процессе подготовки к предотвращению этих угроз и реагированию на них. Поэтому важнейшее значение для укрепления потенциала таких стран, как Непал, с тем чтобы они могли предотвращать кибератаки и реагировать на них, имеет оказание на постоянной основе международной поддержки и помощи. В интересах преодоления институционального, квалификационного, технологического и ресурсного дефицита нам необходимо развивать партнерские отношения с участием многих заинтересованных сторон.

В-четвертых, нам следует содействовать кибербезопасности с помощью обеспечения инклюзивного развития и процветания для всех посредством сокращения цифрового разрыва между государствами.

В заключение следует отметить, что киберугрозы, с которыми мы сталкиваемся, весьма значительны. Принимая упреждающие, комплексные и скоординированные меры, мы сможем обеспечить безопасное, открытое и мирное киберпространство для всех. В порядке продолжения осуществления нашей повестки дня касательно построения устойчивого и цифрового будущего для всех мы должны

сообща создать устойчивое глобальное сообщество, способное противостоять угрозам, сопряженным с цифровой эпохой, и справляться с ними.

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

**Г-н Мухитх** (Бангладеш) (*говорит по-английски*): Я благодарю нынешнего Председателя Совета Безопасности Республику Корея за организацию этих важных открытых прений. Также благодарю докладчиков за их содержательные выступления.

В условиях меняющегося цифрового ландшафта киберугрозы становятся повсеместными и зачастую неотвратимыми, разрушая глобальные финансовые, демократические, социально-культурные и силовые структуры. В Докладе о глобальных рисках 2024 года подчеркивается, что киберугрозы являются одними из самых серьезных проблем нашей современности, а потенциальные затраты на борьбу с киберпреступностью, согласно оценкам, к 2027 году составят 24 трлн долл. США. Такая поражающая воображение цифра требует от нас немедленного принятия срочных мер. Однако, помимо экономических издержек, нельзя недооценивать и ужасающее воздействие киберпреступности на отдельных людей и общество.

В связи с ориентировочными вопросами, поставленными Председателем, я хотел бы остановиться на нескольких моментах.

Во-первых, рост числа киберугроз, в том числе атак с использованием программ-вымогателей, актов кибершпионажа, а также кампаний по распространению недостоверной и заведомо ложной информации с помощью «дипфейков» и других средств, представляет собой значительные риски для мира и стабильности на планете. Цели этих угроз — объекты критически важной инфраструктуры и подрыв демократических процессов и спокойствия в обществе посредством распространения ксенофобии, нетерпимости и стереотипов. Кроме того, ввиду достижений в области искусственного интеллекта и квантовых вычислений растут как масштабы, так и сложность киберугроз. Поскольку миллиарды людей ежедневно используют цифровые платформы в своей обычной жизни, насущная необходимость борьбы с этими угрозами достигла беспрецедентного уровня.

Во-вторых, мы твердо убеждены в том, что перед лицом столь серьезных угроз мы сильны лишь настолько, насколько прочно наше самое слабое звено. Поэтому сегодня крайне важно укреплять международное сотрудничество и координацию действий. Для повышения устойчивости к киберугрозам настоятельно необходимо заниматься усилением мер обеспечения кибербезопасности, развитием механизмов обмена информацией и инвестированием в инициативы по наращиванию потенциала. В этой связи мы подчеркиваем важность обеспечения соблюдения в цифровой сфере принципов суверенного равенства и международного права. Мы должны найти способы уравновесить свободу выражения мнений с необходимостью вести борьбу с пагубным распространением ложной информации.

В-третьих, в условиях быстро меняющегося киберпространства мы выражаем признательность Рабочей группе открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий за содействие международной дискуссии и международному сотрудничеству, имеющим жизненно важное значение. Генеральная Ассамблея, которая отражает глобальную волю и чаяния международного сообщества, остается ключевой платформой для ведения таких критически важных дискуссий, которая позволяет всем государствам принимать активное участие в формировании нашего коллективного будущего в киберпространстве. Мы также надеемся, что разрабатываемый в настоящее время глобальный цифровой договор сыграет важнейшую роль в решении этой проблемы, и выступаем за применение Генеральной Ассамблеей и Советом Безопасности совместного подхода в интересах эффективного осуществления этого договора.

Наконец, что касается вопроса о том, относится ли тема противодействия меняющимся угрозам в киберпространстве к компетенции Совета, поскольку она не является частью традиционного понятия безопасности, то мы считаем, что в силу новых угроз для мира и безопасности, которые возникают в этой связи, кибербезопасность заслуживает самого пристального внимания Организации Объединенных Наций. Правильная платформа для рассмотрения этого важнейшего вопроса должна быть определена в ходе открытых и транспарент-

ных диалогов, а не становиться еще одной причиной расхождения мнений и поляризации.

В то же время мы считаем, что Совет мог бы сыграть жизненно важную роль в содействии мерам укрепления доверия, в том числе путем эффективного обмена информацией и мнениями. Мы должны работать сообща, будь то под эгидой Совета или на любом другом соответствующем форуме Организации Объединенных Наций, включая Рабочую группу открытого состава, в целях разработки норм, стандартов и правил, способствующих созданию безопасной, надежной, недискриминационной и стабильной цифровой среды для всех. Бангладеш еще раз подтверждает свою готовность сотрудничать с мировым сообществом в интересах борьбы с меняющимся ландшафтом глобальных угроз кибербезопасности.

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

**Г-н Данг** (Вьетнам) (*говорит по-английски*): Масштабы и сложность угроз в киберпространстве постоянно меняются, что создает значительные проблемы для международного мира и безопасности. Эти угрозы включают в себя злонамеренную активность с использованием киберсредств, в том числе шпионаж, атаки на объекты критически важной инфраструктуры и утечку данных; распространение недостоверной и заведомо ложной информации и ведение психологической войны в киберпространстве. Такая деятельность может представлять значительный риск для национальной безопасности, наносить существенный экономический ущерб и подрывать доверие общества к институтам.

Ни одна страна не застрахована от этих угроз. В частности, развивающиеся страны, которые зачастую не располагают надежным потенциалом в области кибербезопасности, без сомнения, находятся в наиболее уязвимом положении и порой используются в качестве полигонов для испытания национальными государствами средств ведения войны киберпространстве, а также для совершения негосударственными субъектами киберпреступлений.

В глобальном масштабе, принимая во внимание не имеющий границ характер киберпространства и проблемы установления ответственности, кибератаки могут провоцировать конфликты и усугублять геополитическую напряженность. Поэтому решение этой сложной проблемы требует применения многоаспектного подхода, в рамках которого Организация Объединенных Наций играет важную роль.

Во-первых, крайне важно, чтобы государства соблюдали и выполняли существующие нормы и правила применимого международного права, которые представляют собой всеобъемлющее руководство для поведения государств в киберпространстве.

В то же время для дальнейшего укрепления мира, безопасности и сотрудничества между странами в цифровой сфере нам необходимо продолжать укреплять международные рамки, регулирующие активность в киберпространстве, в частности посредством выражения приверженности текущим процессам в этой области, включая разработку глобального цифрового договора и конвенции по борьбе с киберпреступностью.

Во-вторых, наращивание потенциала имеет ключевое значение для поддержания открытого, безопасного, стабильного, устойчивого и мирного киберпространства, особенно для тех, кто имеет ограниченные возможности в киберпространстве, с тем чтобы эффективно предотвращать злонамеренную активность с использованием киберсредств, готовиться к ней и реагировать на ее последствия. Крайне важно, чтобы все государства разделяли общую цель, а именно укрепление потенциала и сокращение разрыва в развитии информационно-коммуникационных технологий между странами и регионами.

В-третьих, в соответствии со своим мандатом Совет должен уделять больше внимания этому вопросу и рассматривать взаимосвязь между киберугрозами и другими ключевыми вопросами своей повестки дня, такими как предотвращение конфликтов, борьба с терроризмом и защита критически важной инфраструктуры. Кроме того, в целях создания единой и комплексной системы мер реагирования на киберугрозы Совету настоятельно необходимо налаживать сотрудничество с другими органами Организации Объединенных Наций, региональными организациями и частным сектором.

Посредством принятия в 2018 году закона о кибербезопасности правительство Вьетнама взяло на вооружение всеобъемлющий подход к борьбе с киберугрозами, предусматривающий участие всех слоев общества. Вьетнам вновь заявляет о том, что

поддерживает согласованные глобальные усилия по созданию надежных рамок и механизмов, направленных на обеспечение соблюдения принципов суверенитета, невмешательства и ответственного поведения в киберпространстве. Благодаря конструктивному диалогу и сотрудничеству мы сможем эффективно решать проблемы, возникающие в связи с развитием технологий, обеспечивая при этом целостность глобального киберпространства и информационной экосистемы.

**Г-жа Оппонг-Нтири** (Гана) (*говорит по-английски*): Прежде всего, г-н Председатель, я хотела бы поблагодарить Вас за организацию сегодняшних открытых прений по столь важной теме. Мы также благодарны докладчикам за то, что они поделились своими содержательными взглядами.

Ощущая на себя все возрастающее влияние революции в области информационно-коммуникационных технологий (ИКТ), Гана в то же время прекрасно осознает, какие риски эта революция несет для международного мира и безопасности. У нас дома, на Африканском континенте, мы стали свидетелями преобразующего воздействия ИКТ и последствий их стремительного роста для целого ряда проблем и угроз национальной безопасности. Будь то фишинг и кража личных данных, вербовка террористами своих сторонников или торговля стрелковым оружием и боеприпасами в «темной паутине» - риски для безопасности, исходящие из цифровой сферы, не ослабевают. Частные предприятия и важнейшие объекты государственной инфраструктуры также не защищены от них, что в некоторых случаях создает серьезные риски для мира и стабильности. Даже в области демократического управления положительное влияние ИКТ на расширение возможностей африканских граждан продвигать выбранные ими политические цели в рамках свободы ассоциаций и собраний сильно пострадало от злоупотребления этими технологиями в целях распространения фальшивых новостей, дезинформации и ложной информации, что представляет собой большой риск для национального единства и сплоченности.

Хотя для борьбы с этими все более распространенными тенденциями, снижающими уверенность и доверие общества, необходимо создавать надежные средства киберзащиты, мы предупреждаем, что необходимо принимать взвешенные меры, чтобы избежать таких действий правительства, которые бы превышали его полномочия и ущемляли права и свободы граждан, что само по себе может стать источником большого недовольства и нестабильности. Действительно, осознавая стоящую перед Африкой проблему, лидеры нашего континента принимают ряд мер по укреплению киберзащиты. В ходе тридцать седьмой очередной сессии Ассамблеи глав государств и правительств Африканского союза, состоявшейся в этом году, вопросу о кибербезопасности было отведено центральное место, и были приняты ключевые решения, направленные на содействие реализации Стратегии цифровых преобразований для Африки. Помимо того, что африканские лидеры решили ускорить создание континентальной стратегии кибербезопасности, они согласовали общую позицию по применению международного права в киберпространстве. Мы согласны с тем, что еще многое предстоит сделать для создания надежного киберпространства, способного противостоять постоянно эволюционирующим угрозам. Мы должны приложить все усилия для преодоления цифрового разрыва путем наращивания потенциала и оказания технической помощи.

Отвечая на вопрос о роли, которую Совет Безопасности может играть в устранении угроз международному миру и безопасности в киберпространстве, Гана хотела бы высказать следующие три дополнительных соображения.

Во-первых, чтобы в полной мере использовать огромный потенциал киберпространства для роста и процветания, необходимо предпринять согласованные глобальные действия по устранению возникающих рисков и созданию надежного, безопасного и устойчивого киберпространства для всех. Это подчеркивает важное значение консенсусных докладов Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ и Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, которые не оставляют сомнений в том, что международное право и Устав Организации Объединенных Наций применимы и необходимы для поддержания мира, безопасности и стабильности в сфере ИКТ.

Во-вторых, сегодняшние открытые прения, одни из немногих состоявшихся за последнее время, являются еще одним важным шагом в признании растущей опасности для глобального мира и ста-

бильности, которую представляют злонамеренные субъекты в киберпространстве. Действия Совета должны быть направлены на дополнение роли Генеральной Ассамблеи в разработке и продвижении норм ответственного поведения в киберпространстве. Он также мог бы рассмотреть вопрос о создании юридически обязательных рамок для цифровой сферы, регулирующих любые действия правительственных или неправительственных организаций, которые угрожают международному миру и безопасности. Подобные рамки могли бы использовать опыт ключевых заинтересованных сторон в сфере ИКТ для координации международных усилий по реагированию на киберпреступления, а также установлению и распределению ответственности за них для обеспечения подотчетности. В качестве отправной точки можно было бы создать вспомогательный орган, занимающийся этим вопросом.

В-третьих, учитывая стремительное развитие ИКТ, в частности искусственного интеллекта, и потенциальную опасность его неправомерного использования, Совет мог бы рассмотреть возможность создания отдельного пункта повестки дня, посвященного кибербезопасности, а затем включать его в рассмотрение пунктов повестки дня, связанных с различными тематическими вопросами и географическими регионами. Такой подход предоставит Совету достаточно времени для обсуждения последствий соответствующей проблемы и ее полного понимания, что позволит ему разработать комплексные стратегии по защите глобального мира и безопасности от киберугроз.

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

**Г-жа Консепсьон Харамильо** (Панама) (*говорит по-испански*): В цифровую эпоху угрозы, вызванные злонамеренной активностью с использованием киберсредств, продолжают расти. Панама признает важность создания глобальной архитектуры кибербезопасности для эффективной борьбы с этими эволюционирующими киберугрозами. Совет Безопасности, наряду с другими субъектами и в рамках своего мандата, может сыграть важнейшую роль в решении этих проблем и укреплении международного сотрудничества для защиты нашей общей цифровой среды. На нем лежит главная ответственность за поддержание международного мира и безопасности, и эта ответственность не менее важна в области киберпространства. Активно участвуя в усилиях по обеспечению кибербезопасности и отслеживая возникающие угрозы, Совет может внести значительный вклад в создание безопасного и мирного киберпространства для всех стран. Необходимо изучить способы повышения способности Совета реагировать на вредоносные кибератаки, которые могут затрагивать важнейшие объекты инфраструктуры, гражданское население и гуманитарные усилия.

Ориентируясь в сложном ландшафте этих киберугроз, важно учитывать текущие обсуждения по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, которая поможет дополнить Конвенцию Совета Европы о киберпреступности. Хотя эта Конвенция и протоколы к ней сыграли важную роль в налаживании международного сотрудничества в борьбе с киберпреступностью, меняющийся характер киберугроз требует адаптации и укрепления нашей правовой базы. Обновляя и совершенствуя эти рамки, мы сможем лучше решать новые задачи в киберпространстве и обеспечивать более устойчивую глобальную архитектуру кибербезопасности.

Учитывая транснациональный характер злонамеренных киберугроз, необходимо, чтобы Совет Безопасности сотрудничал с государствами-членами, международными организациями и другими заинтересованными сторонами в решении этих многогранных проблем. Укрепляя сотрудничество, обмениваясь передовым опытом и поощряя ответственное поведение государств в киберпространстве, мы можем коллективно снизить риски и уязвимость, связанные с этими угрозами. Панама считает, что эти усилия можно поддержать в некоторых комитетах Совета, таких как Комитет, учрежденный резолюцией 1540 (2004). В целом Совет Безопасности может взять на себя конкретные функции и действия в целях решения проблем международного мира и безопасности, возникающих в киберпространстве, включая разработку оценок киберугроз и стратегий по их преодолению и включение вопросов кибербезопасности в обсуждение конкретных проблем. Киберугрозы взаимосвязаны с другими вопросами повестки дня Совета Безопасности, включая защиту гражданских лиц, мир и безопасность в вооруженных конфликтах, борьбу с терроризмом, контртерроризм и повестку дня

по вопросу о женщинах и мире и безопасности. В оценках и стратегиях должны учитываться гендерные аспекты и участие женщин в разработке политики, принимая во внимание их различные уровни уязвимости.

Чтобы эффективно интегрировать проблемы, связанные с киберпространством, в свою работу, Совет может изучить способы укрепления киберустойчивости, развития международного сотрудничества и комплексного противодействия киберугрозам. Укрепляя координацию и сотрудничество и совершенствуя потенциал в сфере кибербезопасности, мы сможем создать более безопасную и устойчивую цифровую среду на благо всех стран. Панама призывает Совет Безопасности принять решительные меры в этом направлении, а всех нас - работать сообща, чтобы обеспечить более безопасное и мирное киберпространство для нынешнего и будущих поколений.

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

**Г-н Джованович** (Италия) (*говорит по-английски*): Г-н Председатель, я хотел бы выразить Вам, свою признательность за своевременный созыв этих открытых прений. Сейчас, когда мы переживаем эпоху стремительного технологического прогресса, необходимость в надежном и едином подходе к кибербезопасности как никогда актуальна.

Италия присоединяется к заявлению, сделанному от имени Европейского союза, и хотела бы добавить ряд соображений в своем национальном качестве.

Италия обеспокоена ростом числа злонамеренных кибератак и развитием потенциала использования информационно-коммуникационных технологий (ИКТ) в военных целях. Мы твердо намерены укреплять сотрудничество между всеми государствами-членами в области новых цифровых технологий. Председательство Италии в Группе семи направлено на укрепление усилий международного сообщества по созданию открытого, интероперабельного, безопасного, надежного, устойчивого киберпространства, в котором обеспечивается уважение прав человека и которое регулируется принципами и нормами международного права. Италия призывает соблюдать Устав Организации Объединенных Наций и существующие международные нормы в целях сохранения мира и стабильности и укрепления нашей общей безопасности.

Поскольку Совет Безопасности несет главную ответственность за поддержание международного мира и безопасности, он обладает уникальными возможностями для реагирования на угрозы кибербезопасности в интересах всех стран. Эта деятельность Совета должна дополнять другие продолжающиеся в Организации Объединенных Наций процессы, такие как рассмотрение предложения о разработке программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Предложения, выдвинутые на предыдущих заседаниях Совета Безопасности, нацелены на оптимизацию коллективных инициатив, направленных на устранение последствий использования ИКТ для глобальной безопасности. Одно из таких предложений — рассматривать соответствующие проблемы в области кибербезопасности либо в привязке к ситуациям в конкретных странах, либо в рамках других, более широких тематических вопросов, таких как вопросы о миссиях по поддержанию мира и миростроительству, нераспространении и борьбе с терроризмом.

Более того, мы должны укреплять потенциал Организации Объединенных Наций по реагированию на злонамеренное использование ИКТ, которое ставит под угрозу международный мир и безопасность. Это особенно актуально, когда речь идет о защите мирного населения, критически важной инфраструктуры и гуманитарных операций. В дальнейшем мы должны изучить основные тенденции в области вредоносной деятельности, иногда усиливаемой новыми технологиями, такими как искусственный интеллект, и ее потенциал в качестве фактора увеличения угроз в ходе продолжающихся в настоящее время конфликтов, а также конкретные действия, которые Совет Безопасности и Организация Объединенных Наций в целом могут предусмотреть для решения стоящих перед нами все более сложных задач.

Мы все знаем о потенциально несоразмерном воздействии злонамеренной кибердеятельности на уязвимые слои населения. Мы все можем пострадать от кибератак, направленных на объекты критической важной инфраструктуры, такие как объекты системы здравоохранения или энергетические

объекты, а также на отдельных граждан и предприятия. Для того чтобы не позволить злоумышленникам, совершающим кибератаки, получать вознаграждение за свои противоправные действия, необходимо наращивать потенциал в этой области. В этой связи 2 июля в Италии пройдет национальная конференция, посвященная укреплению экосистемы государственных и частных организаций, занимающихся укреплением потенциала в киберпространстве во всем мире. Это будет способствовать реализации будущих проектов на основе инклюзивного подхода, предусматривающего участие различных заинтересованных сторон.

Подтверждая решительный настрой Италии на успешное применение такого подхода, позвольте мне вновь заявить о нашей готовности сотрудничать со всеми государствами-членами в деле развития и укрепления навыков, процессов и ресурсов, необходимых для адаптации к быстро меняющемуся киберпространству и в конечном счете — для построения более безопасного будущего для всех стран.

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

**Г-н Калмар** (Израиль) (*говорит по-английски*): Израиль хотел бы присоединиться к другим ораторам и поблагодарить Республику Корея за организацию и проведение этих очень своевременных и важных прений по вопросу об угрозах кибербезопасности, а также добавить от имени нашей страны несколько замечаний о существующих и эволюционирующих угрозах в киберпространстве.

Израиль находится на переднем крае борьбы с беспрецедентной волной киберагрессии. Наши противники не ограничиваются традиционными боевыми действиями и террором, а пытаются использовать цифровую сферу, чтобы подорвать нашу безопасность, посеять раздор среди нашего населения и нарушить наш образ жизни. Кибератаки стали для Израиля повседневной реальностью. Наша критически важная инфраструктура, будь то государственная, финансовая или общественная, подвергается постоянным атакам со стороны как государственных, так и негосударственных субъектов. Эти атаки направлены на то, чтобы поставить под угрозу безопасность и благополучие наших граждан, подорвать нашу экономическую стабильность и бросить вызов нашим демократическим институтам. Угрозы, с которыми мы сталкиваемся в киберпространстве, реальны и широко распространены, и для их устранения необходимо, чтобы мы все проявляли бдительность и предпринимали конкретные действия.

Как и многие другие страны, Израиль осознает всю серьезность последствий киберугроз. Наш опыт подсказывает нам, что эти угрозы не являются теоретическими. В субботу, 7 октября 2023 года, тысячи боевиков ХАМАС проникли на южную границу Израиля и убили, сожгли, изнасиловали и изуродовали 1200 ни в чем не повинных людей — женщин, мужчин, стариков, детей и младенцев. Кроме того, тысячи людей были ранены, а более 240 ни в чем не повинных мирных жителей были похищены и взяты в заложники. С 7 октября 2023 года Израиль также подвергается массированным кибератакам. Эти атаки организовывает Иран при активной поддержке и участии своих марионеток — «Хизбаллы», ХАМАС и других террористических групп, которые совершают массированные кибератаки на объекты нашей критически важной инфраструктуры, в том числе объекты системы водоснабжения, энергетической инфраструктуры и больницы. Иран должен быть осужден за вопиющее нарушение правил ответственного поведения государств в киберпространстве, а также норм гуманности и морали. Помимо кибератак, Иран проводит массированную кампанию по оказанию влияния, направленную на запугивание израильских граждан и нарушение уклада нашего свободного и демократического общества, а также причинение новых страданий жертвам жестокого нападения ХАМАС и их семьям. Злоумышленники используют киберпространство как инструмент и место для осуществления своей террористической деятельности, нацеленной на подрыв основ израильского общества.

Израильская и еврейская общины по всему миру переживают глобальную волну подстрекательства, ненавистнических высказываний и антисемитизма, которая значительно увеличивается вследствие скоординированного анонимного распространения недостоверной информации в социальных сетях. Отмечаем, что некоторые крупные технологические компании и их социальные медиа-платформы прилагают все больше усилий для борьбы с ненавистью и насилием, но еще многое предстоит сделать. Призываем все социальные сети демонстрировать бóльшую ответственность в этом

отношении. Никакие ненавистнические высказывания, призывы к уничтожению и призывы, подразумевающие истребление населения, не должны звучать по всему миру.

ХАМАС использует киберпространство для реализации целого ряда стратегий и достижения целого ряда целей, о чем говорилось на состоявшейся 15 мая в Гааге встрече международной коалиции по борьбе с подстрекательством и финансированием ХАМАС, созданной президентом Франции Макроном после теракта 7 октября 2023 года. Боевики ХАМАС используют различные онлайн-платформы для радикализации, индоктринации, подстрекательства к насилию, распространения ненависти и дезинформации, а также для сбора средств — все для достижения заявленной цели организации, которая заключается в уничтожении государства Израиль путем насилия и джихада. Сообщения ХАМАС в киберпространстве, в которых используются сложные значки и символы в целях обхода системы языкового контроля искусственного интеллекта, позволяют группам и отдельным лицам присоединяться к опирающемуся на насилие мировоззрению ХАМАС и переносить эти идеи из киберпространства в реальный мир. Этот перенос проявляется в значительном увеличении объемов пожертвований и перечислении десятков миллионов долларов США на счета ХАМАС, в исполненных ненависти массовых демонстрациях и в нападениях с применением холодного оружия, мотивированных распространяемой в Интернете антиизраильской и антисемитской риторикой ХАМАС. Кибертеррор как таковой пока еще не рассматривается международным сообществом. Кибертеррористы имеют особую мотивацию, и на них не распространяются международные нормы. Сегодня мир все еще не располагает необходимыми средствами для борьбы с кибертеррором.

Всем миролюбивым государствам следует как можно скорее задуматься об устранении этого пробела. То, что начинается на Ближнем Востоке, редко остается только в нашем регионе. В нашем взаимосвязанном мире ни одна страна не застрахована от этой угрозы. Недавний всплеск киберинцидентов по всему миру — от атак с использованием вирусов-вымогателей, разрушающих критически важную инфраструктуру, до кампаний по распространению дезинформации, подрывающих доверие общества, — указывает на настоятельную необходимость нам всем взять на себя соответствующие обязательства. Эти угрозы не только ставят под угрозу наши технологические достижения и влияют на нашу экономику, но и подрывают сами основы наших демократических институтов и глобальную стабильность. Израиль подчеркивает важность международного сотрудничества. Ни одна страна не может противостоять этим угрозам в одиночку. Мы должны укреплять наши партнерские отношения, расширять механизмы обмена информацией и требовать от каждой страны соблюдения норм и правил ответственного поведения в киберпространстве. Это необходимо для создания безопасной и стабильной цифровой среды, в которой возможно развитие инноваций без угрозы эксплуатации. Международное сообщество должно единодушно осудить киберагрессию и обеспечить последствия для тех, кто пытается подорвать нашу коллективную безопасность с помощью киберсредств.

В заключение, пользуясь этой возможностью, я хотел бы подтвердить нашу приверженность защите целостности и безопасности киберпространства. Вместе, благодаря диалогу, сотрудничеству и решительным действиям, мы сможем смягчить угрозы, с которыми сталкиваемся, и использовать преобразующий потенциал цифровых технологий на благо всего человечества.

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

**Г-н Хилале** (Марокко) (*говорит по-французски*): Прежде всего позвольте мне поблагодарить Вас, г-н Председатель, за проведение в Совете Безопасности этих открытых прений по теме, которая приобретает жизненно важное значение в эти переживаемые сейчас нашим миром трудные времена с учетом меняющегося и сложного характера угроз, присущих киберпространству. Приветствую участие в этом заседании министра иностранных дел Республики Корея г-на Чхо Дэ Юля, Генерального секретаря г-на Антониу Гутерриша и докладчиков, которых я хотел бы поблагодарить за их исчерпывающие сообщения.

Марокко гордится тем, что наряду с 62 другими странами выступило одним из авторов совместного заявления об использовании информационно-коммуникационных технологий (ИКТ) в контексте международного мира и безопасности.

Марокко постоянно выступает за расширение сотрудничества между государствами-членами в области киберпространства и заявляет о том, что поддерживает инициативы, предпринимаемые под эгидой Организации Объединенных Наций и направленные на создание безопасного, надежного и устойчивого киберпространства как общей для всех сферы, которая всегда должна оставаться мирной и процветать, а также позволять в полной мере использовать возможности, открывающиеся благодаря ответственному использованию ИКТ.

В условиях столь сложного и непредсказуемого геополитического контекста международное сообщество призвано подготовить почву для глобального, устойчивого и мирного цифрового перехода, который будет определяться нашими коллективными усилиями по содействию обеспечению взаимного доверия, транспарентности, обмена передовым опытом, наращивания потенциала и оказания технической помощи — по просьбе государств-участников и в соответствии с их потребностями, — а также сокращению увеличивающегося разрыва между развитыми и развивающимися странами в сфере ИКТ и, в частности, уважению национального суверенитета и территориальной целостности государств-членов.

Под руководством Его Величества короля Мухаммеда VI Королевство Марокко всегда было ярым поборником ответственного использования ИКТ, укрепления доверия к цифровым технологиям и цифровизации, о чем свидетельствует наша новая Национальная стратегия в области кибербезопасности на период до 2030 года, которая направлена на закрепление и развитие успехов, достигнутых с 2012 года, когда была принята Национальная стратегия в области кибербезопасности, и обеспечение более эффективной поддержки в области цифровых преобразований как важнейшего инструмента социально-экономического развития.

Применяемый Марокко подход к обеспечению кибербезопасности также основан на международном сотрудничестве, в том числе с братскими и дружественными арабскими и африканскими странами, в интересах оптимального использования преимуществ и возможностей, доступных в этой жизненно важной сфере, в рамках сотрудничества Юг — Юг и трехстороннего сотрудничества.

Организация Объединенных Наций создает множество механизмов и платформ, предназначенных для обзора угроз в киберпространстве и цифровых угроз. По мнению Марокко, Совет Безопасности должен действовать в этой сложной области более динамично и активно, с тем чтобы выполнять свой мандат, в частности по поддержанию международного мира и безопасности в киберпространстве, с учетом того факта, что киберугрозы не знают границ.

Мы считаем, что Совету Безопасности следует рассмотреть возможность проведения более глубоких дискуссий по вопросу об определении и приоритизации киберугроз, представляющих непосредственный и постоянный риск для международного мира и безопасности, в том числе путем сосредоточения усилий на следующих задачах. Во-первых, Совет должен обращать особое внимание на ключевые параметры, которые позволяют определить, является ли угроза достаточно серьезной, чтобы ее рассматривал Совет Безопасности. Во-вторых, он должен заниматься вопросом о мерах, которые необходимо принять для предотвращения эскалации киберугроз. В-третьих, Совету следует ежегодно проводить прения, посвященные новым угрозам в киберпространстве. И, в-четвертых, ему следует сосредоточиться на расширении участия женщин, молодежи, частного сектора, гражданского общества и научных кругов, с тем чтобы Совет Безопасности мог оставаться в курсе новых угроз в сфере ИКТ и их последствий для международного мира и безопасности.

Марокко подчеркивает, что дальнейшее обсуждение киберугроз в Совете Безопасности даст Совету возможность играть ведущую роль в разработке ориентированных на конкретные действия мер реагирования и смягчении последствий коллективных киберугроз, с которыми государства-члены сталкиваются на ежедневной основе.

В заключение следует отметить, что, по нашему мнению, настало время поддержать набранную за последнее десятилетие в рамках Организации Объединенных Наций динамику, с тем чтобы сохранить нашу коллективную и конструктивную приверженность делу создания безопасного, надежного и устойчивого киберпространства. Кибербезопасность и киберпреступность существуют не в вакууме — они имеют широкомасштабные по-

следствия, которые неодинаковым образом сказываются на всем международном сообществе.

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

**Г-н Венавезер** (Лихтенштейн) (*говорит по-английски*): Мы благодарим Республику Корея за продолжение начатого Эстонией процесса вовлечения Совета Безопасности в обсуждение вопросов кибербезопасности (см. S/2021/621). Участие Совета Безопасности в обсуждении этой темы помогает с помощью обеспечения верховенства права обеспечить эффективное противодействие современным технологическим вызовам, в том числе меняющимся угрозам в киберпространстве, которые играют центральную роль в рамках мандата Совета.

Появление новых кибертехнологий в сегодняшнем взаимосвязанном мире не только открывает беспрецедентные возможности для международного сотрудничества, но и создает риск осуществления вредоносных кибероперaций, которые могут иметь катастрофические последствия. Все более изощренные и частые кибератаки, в том числе агрессия, совершаемая Россией против Украины, требуют, чтобы мы четко понимали, каким образом международное право применяется в киберпространстве.

Прежде всего, мы напоминаем о широком консенсусе в отношении того, что в киберпространстве применимы нормы международного права, включая международное гуманитарное право, международное право прав человека, международное уголовное право и, разумеется, Устав Организации Объединенных Наций. Международный комитет Красного Креста подтвердил, что международное гуманитарное право распространяется на кибероперации, совершаемые в ходе вооруженных конфликтов, подчеркнув необходимость соблюдения правовых норм и в цифровой сфере. Кроме того, поскольку многие кибероперации все чаще используются для совершения международных преступлений, включая военные преступления и преступления против человечности, существует насущная необходимость в обеспечении понимания их последствий в рамках системы Римского статута Международного уголовного суда (МУС). В результате соответствующих оценок было подтверждено, что Суд уже может расследовать соответствующие кибератаки и осуществлять преследование за их совершение. Это вполне логично: международное гуманитарное право распространяется на кибероперации, поэтому нарушения международного гуманитарного права, соответствующие установленному МУС порогу тяжести, преследуются в судебном порядке. Совет консультантов, созванный Лихтенштейном в 2020 и 2021 годах, подготовил доклад, в котором разъясняется, что означает в контексте кибероперaций каждое из четырех основных преступлений Римского статута — преступление агрессии, военное преступление, преступление против человечности и геноцид.

В рамках МУС судебное преследование за преступления с использованием кибертехнологий имеет важнейшее значение для эффективного противодействия меняющемуся ландшафту киберугроз. Опираясь на доклад указанного Совета консультантов, Прокурор Международного уголовного суда совместно с компанией «Майкрософт» недавно запустил процесс консультаций с участием многих заинтересованных сторон в целях разработки политики МУС по борьбе с преступлениями, совершаемыми с использованием кибертехнологий. Это поможет специалистам в области международного права добиться более глубокого понимания сложностей, связанных с судебным преследованием за преступления, совершаемые с использованием кибертехнологий. Кроме того, расширение диалога между Судом, Организацией Объединенных Наций, правительствами, частным сектором и гражданским обществом будет способствовать разработке важной политики в области киберпространства и в конечном счете позволит поддержать роль Суда как одного из ключевых компонентов международной архитектуры мира и безопасности.

Наконец, благодаря своим полномочиям по передаче дел в МУС и направлению соответствующих ситуаций в Суд в целях проведения расследований Совет Безопасности призван сыграть решающую роль в обеспечении привлечения к ответственности за совершение кибератак. Взаимодействие Суда и Совета Безопасности является настоятельно необходимым для обеспечения того, чтобы правосудие не оставалось позади из-за меняющегося характера и развития таких средств ведения войны.

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

**Г-н Четин** (Турция) (*говорит по-английски*): Г-н Председатель, благодарим Вас за организацию этих открытых прений по меняющимся угрозам в киберпространстве.

Информационно-коммуникационные технологии (ИКТ) стали неотъемлемой частью общества и экономической системы и сказываются на всех аспектах жизни.

На сегодняшний день возможности государств в области разработки и использования технологий играют важную роль в национальном развитии и росте. Хотя развитие технологий открывает перед нами множество возможностей, киберугрозы меняются и приобретают еще более сложный характер. Наличие уязвимых мест в информационно-коммуникационных системах зачастую создает угрозу для экономики, общественного порядка и национальной безопасности. К числу угроз, которые также представляют опасность для международного мира и безопасности, относятся осуществляемые с помощью ИКТ терроризм, цифровой шпионаж, мошенничество, надругательства над детьми и их эксплуатация в интернете, а также неправомерное использование персональных данных.

Мы особенно встревожены ростом числа кибератак. Согласно проведенным исследованиям, в 2023 году в мире было зафиксировано более 317 миллионов случаев использования программ-вымогателей и свыше 6 миллиардов попыток распространения вредоносного программного обеспечения. Благодаря развитию технологий становится все проще совершать кибератаки, при этом стремительно растут их негативные последствия и цена, которую платят их жертвы. Для борьбы с такими атаками и устранения этих угроз необходимы современные методы и инструменты — как в практическом, так и в законодательном плане.

Учитывая трансграничный характер киберугроз, решающее значение имеют расширение международного сотрудничества и наращивание потенциала в этой области. Руководствуясь этим пониманием, Турция принимает участие в обмене оперативной информацией о киберугрозах и вносит свой вклад в разработку соответствующих политики и стратегий сотрудничества в рамках региональных и международных организаций.

Что касается международного права, то Турция является участником Конвенции Совета Европы о киберпреступности. Мы также активно участвуем в усилиях, прилагаемых в рамках Организации Объединенных Наций, в частности в рамках Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Считаем, что будущей конвенцией должны регулироваться в том числе совершаемые с помощью ИКТ преступления, связанные с терроризмом.

Открытым остается вопрос и о применимости международного права в киберпространстве. Турция является одним из авторов программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности и решительно поддерживает резолюции 77/37 и 78/16 Генеральной Ассамблеи.

Поскольку киберпространство не имеет границ, а вопрос кибербезопасности затрагивает множество заинтересованных сторон, международное сотрудничество в этой области имеет первостепенное значение. Поставщики услуг и компании, занимающиеся вопросами безопасности, должны более эффективно сотрудничать с правительствами и международными организациями, чтобы внести свой вклад в обеспечение глобальной кибербезопасности. С удовлетворением отмечаем, что Совет Безопасности уделяет особое внимание использованию киберпространства для борьбы с растущими угрозами, и мы намерены продолжать наше взаимодействие и диалог в этой связи.

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

**Г-н Альвасиль** (Саудовская Аравия) (*говорит по-арабски*): Прежде всего я хотел бы поздравить Постоянного представителя Республики Корея Его Превосходительство посла Джун Гук Хвана с вступлением на пост Председателя Совета Безопасности. Желаю делегации Республики Корея всяческих успехов на посту Председателя. Я также хотел бы поблагодарить Генерального секретаря Его Превосходительство Антониу Гутерриша, главного административного сотрудника Института «Кибермир» г-на Стефана Дюгена и профессора права и технологий г-жу Нненну Ифеани-Аджуфо за их сообщения. Они прилагают неустанные, выдающиеся

и значительные усилия по борьбе с угрозами кибербезопасности и растущими киберугрозами.

Необходимость в безопасном и защищенном киберпространстве, создающем условия для роста и процветания, сегодня актуальна как никогда. Поэтому, для того чтобы государства были способны обеспечивать защиту своих жизненно важных интересов и национальной безопасности, им необходимо включить укрепление кибербезопасности в число своих приоритетных задач. Королевство Саудовская Аравия считает крайне важным и необходимым расширять международное сотрудничество в этой области и объединять международные усилия по противодействию киберугрозам. Пришло время международному сообществу разработать серьезный практический подход, который позволил бы объединить международные усилия по противодействию киберугрозам в рамках соответствующих комиссий и специализированных органов Организации Объединенных Наций.

В настоящее время в Саудовской Аравии наблюдается активный и стремительный прогресс в области кибербезопасности, основа для которого была заложена благодаря Стратегии развития Саудовской Аравии на период до 2030 года, а также предусмотренным в ней целям и инструментам ее реализации. Королевство Саудовская Аравия начало свой путь преобразований с разработки саудовской модели кибербезопасности, основанной на централизованном управлении и возможности децентрализованного функционирования с опорой на ответственность национальных органов. В этой связи в 2017 году мы создали Национальное управление по кибербезопасности в качестве органа, ответственного за кибербезопасность в Королевстве, и национального справочного центра. Разработанная Королевством модель имеет комплексный характер и охватывает все аспекты кибербезопасности — как законодательные и экономические аспекты, так и аспекты, связанные с безопасностью и развитием. Усилия Королевства в области кибербезопасности получили международное признание, прежде всего в составленном на основе Глобального индекса кибербезопасности Международного союза электросвязи рейтинге, в котором мы заняли второе место в мире и первое — среди стран арабского мира, Ближнего Востока и Азии. Более того, в рейтинге мировой конкурентоспособности Международного института развития менеджмента Королевство Саудовская Аравия два года подряд — в 2022 и 2023 году — занимала второе место в мире по уровню кибербезопасности. В 2024 году роль Королевства как глобального первопроходца в области кибербезопасности была подтверждена первым местом в рейтинге, публикуемом в «Ежегоднике по мировой конкурентоспособности».

Королевство Саудовская Аравия считает необходимым расширять международное сотрудничество в области кибербезопасности. В этой связи в Королевстве был создан Глобальный форум по кибербезопасности — глобальная платформа, предназначенная для проведения совещаний принимающих решения лиц со всего мира в целях обсуждения стратегических вопросов, касающихся кибербезопасности. В прошлогодней сессии Форума приняли участие более 120 государств. Кроме того, Королевство учредило в Эр-Рияде Международный форум по кибербезопасности в целях укрепления кибербезопасности во всем мире, содействия международному сотрудничеству и социально-экономическому развитию в этой области и дальнейшей консолидации международных усилий в области кибербезопасности для достижения процветания людей во всем мире.

Королевство Саудовская Аравия участвует в усилиях по наращиванию потенциала в ряде стран и международных организаций. В организованных Королевством киберучениях приняли участие более 40 государств и организаций. Более того, мы стремимся объединить региональные усилия по укреплению региональной кибербезопасности. Эти усилия позволили по рекомендации Королевства создать специализированный министерский комитет по кибербезопасности под эгидой Совета сотрудничества арабских государств Залива. Кроме того, по предложению Королевства Саудовская Аравия под эгидой Лиги арабских государств был создан Арабский совет министров по кибербезопасности. На своем последнем саммите арабские лидеры решили, что Совет министров, его секретариат и канцелярия будут базироваться в городе Эр-Рияд.

В заключение хочу сказать, что укрепление кибербезопасности — это всеобщая обязанность, и для создания безопасного и защищенного киберпространства, которое обеспечит рост и процветание всех людей во всем мире, нам необходимо налаживать сотрудничество и партнерские отношения.

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

**Г-н Майнеро** (Аргентина) (*говорит по-испански*): Мы хотели бы поблагодарить Республику Корея за проведение этих открытых прений высокого уровня по кибербезопасности — вопросу, имеющему для Аргентины огромное значение.

Аргентина считает, что основные угрозы, которым мы должны противостоять, не связаны с геополитическими событиями в мире. Это особенно верно, учитывая глобальный характер киберпространства и транснациональный характер киберинцидентов. В этой связи мы хотели бы подчеркнуть, что меры по выявлению потенциальных или существующих угроз и меры, которые государства должны принять для их предотвращения и смягчения, а также усилия по сотрудничеству и наращиванию потенциала не должны нарушать международное право, включая международные стандарты в области прав человека и международное гуманитарное право. Они также не должны подрывать принципы, закрепленные в Уставе Организации Объединенных Наций, такие как территориальная целостность и суверенитет государств, невмешательство в их внутренние дела и мирное урегулирование споров.

Считаем, что роль Совета Безопасности и его усилия в области кибербезопасности не должны дублировать другую деятельность, а должны дополнять и учитывать многолетние усилия созданной в 2004 году Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и нынешние усилия Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, которая в июле рассмотрит проект третьего ежегодного доклада о проделанной работе в целях его принятия.

Что касается предложения об организации регулярных информационных совещаний для оценки меняющейся ситуации с киберугрозами применительно к текущему мандату и повестке дня Совета, то мы считаем принципиально важным рассмотреть возможность приглашения на такие совещания представителей Управления по вопросам разоружения в их качестве членов секретариата Рабочей группы открытого состава, а также Председателя Рабочей группы и представителей академического сектора, гражданского общества и частного сектора.

В частности, что касается новых угроз в киберпространстве, мы считаем, что Совету Безопасности были бы особенно полезны доклады или брифинги представителей частного сектора, поскольку в большинстве случаев именно они являются владельцами и операторами критически важных объектов инфраструктуры. Кроме того, у них имеется больше возможностей и ресурсов для изучения работы вредоносного программного обеспечения, что позволяет им постоянно обновлять списки существующих угроз.

Мы также приветствуем тот факт, что в концептуальной записке (S/2024/446, приложение) председательствующая делегация признает, что наращивание потенциала является неотъемлемым элементом необходимых усилий. Считаем, что наращивание потенциала имеет решающее значение для устранения пробелов в кибербезопасности, поскольку от них в равной степени страдают все государства, независимо от уровня их развития. Государства, обладающие меньшими возможностями по обеспечению кибербезопасности, часто становятся уязвимыми звеньями цепи, и злоумышленники могут воспользоваться их уязвимостью. Ввиду того, что киберпространство по своей природе является пространством взаимодействия, уязвимость в любой точке глобального киберпространства может иметь значительные и далеко идущие последствия. Поэтому сотрудничество в области наращивания потенциала крайне необходимо. Только благодаря активному и постоянному сотрудничеству в области наращивания потенциала мы сможем обеспечить по-настоящему устойчивое, открытое, безопасное, стабильное, доступное, мирное, свободное и способствующее взаимодействию киберпространство для всех.

В этой связи мы считаем, что наращивание потенциала неразрывно связано с применением рамок ответственного поведения государств в киберпространстве. Соблюдение норм, правил и принципов ответственного поведения государств в киберпространстве должно дополняться поощрением инноваций, технической помощью в наращивании потенциала и передачей технологий для укрепления потенциала противодействия киберугрозам в

соответствии с действующими нормами международного права и с учетом потребностей развивающихся стран. Это будет способствовать не только благосостоянию и экономическому развитию наших стран, но и внедрению и принятию на равных условиях взаимодополняющих и эволюционирующих рамок ответственного поведения при использовании информационно-коммуникационных технологий (ИКТ) и, следовательно, поддержанию международного мира и безопасности.

Аргентина особенно обеспокоена участившимися случаями использования вредоносных программ, вирусов-вымогателей и фишинга, а также их воздействием на важнейшие объекты инфраструктуры. Эти объекты критически важной инфраструктуры становятся гораздо более уязвимыми, что вызывает общую обеспокоенность государств, частного сектора и гражданского общества. В этой связи мы подчеркиваем важность многостороннего сотрудничества для дальнейшего анализа существующих и потенциальных угроз киберпространству и поощрения действий на глобальном уровне, таких как обмен опытом. В то же время мы с большим интересом отмечаем возможности, которые открывают информационные и другие новые технологии для развития наших обществ. Мы понимаем, что новые технологии нейтральны и что проблема заключается в том, как их контролировать и как их использовать. В этой связи мы признаем, что необходимо найти правильный баланс между нормативной базой, которая разрабатывается в отношении передачи информационно-коммуникационных технологий, и правом всех государств на доступ к новым технологиям для обеспечения их благосостояния и социально-экономического развития, а также для содействия повышению устойчивости киберпространства на благо всех.

В заключение следует отметить, что Совет Безопасности может сыграть решающую роль в обеспечении кибербезопасности, опираясь на результаты работы Рабочей группы по вопросам безопасности в сфере использования ИКТ и самих ИКТ и других соответствующих форумов. Важно обеспечить, чтобы работа Совета соответствовала установленным стандартам и рекомендациям. Многосторонняя координация действий будет способствовать сотрудничеству между государствами и международными организациями, поощряя единый подход к обеспечению кибербезопасности.

**Председатель** (*говорит по-английски*): Слово предоставляется представителю Грузии.

**Г-н Инашвили** (Грузия) (*говорит по-английски*): Грузия присоединяется к заявлению, сделанному от имени Европейского союза, и хотела бы добавить несколько замечаний в своем национальном качестве.

Прежде всего мы благодарим председательствующую в Совете Республику Корея за созыв сегодняшних открытых прений. Мы также хотели бы выразить признательность докладчикам за содержательные презентации, с которыми они выступили ранее сегодня.

Последние достижения в киберпространстве открывают широкие возможности для инноваций, экономического прогресса и развития. Они могут повысить способность государств-членов лучше обеспечивать защиту открытых и мирных обществ. Однако они также могут представлять потенциальную угрозу при их неправомерном использовании. Характер угроз кибербезопасности постоянно меняется по мере развития технологий, и к таким угрозам относятся вредоносные программы, фишинг, утечки данных и другие. В условиях глобально взаимосвязанных кризисов Совет Безопасности по-прежнему играет крайне важную роль в устранении и уменьшении угроз международному миру и безопасности, в том числе угроз, исходящих из киберпространства.

В последние годы международное сообщество стало свидетелем того, как некоторые государственные и негосударственные субъекты могут угрожать международному порядку, основанному на правилах, используя обычные методы ведения военных действий наряду с недавно разработанными нетрадиционными методами. Некоторые из них используют кибертактику для получения стратегических преимуществ, в частности выводят из строя коммуникационные сети, совершают кибератаки на критически важные объекты инфраструктуры и взламывают военные системы.

С учетом этого Грузия по-прежнему привержена поощрению ответственного поведения государств в киберпространстве. Наша позиция по вопросам кибербезопасности соответствует нормативной базе, разработанной Группой правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в

контексте международной безопасности и Рабочей группой открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий.

В последние годы женщины вносят все больший вклад в дело обеспечения мира и безопасности. Более активное участие женщин в сфере кибербезопасности позволяет обеспечить более широкий и инклюзивный учет различных точек зрения. Однако, несмотря на усилия правительства Грузии по обеспечению ответственного поведения в киберпространстве, мы являемся свидетелями агрессивного использования Россией гибридных средств против суверенитета Грузии. В ходе полномасштабной военной агрессии России в 2008 году Грузия стала первой страной, которая наряду с обычными военными действиями подверглась многочисленным атакам в киберпространстве.

Поэтому мы считаем наращивание потенциала неотъемлемым элементом многостороннего сотрудничества. Наряду с укреплением национальных возможностей по обеспечению кибербезопасности эти усилия будут способствовать более эффективному международному сотрудничеству в борьбе со сложными киберугрозами, которые часто выходят за пределы национальных границ и требуют скоординированного реагирования. Учитывая разный уровень развития информационно-коммуникационных технологий в различных странах, мы считаем, что Организация Объединенных Наций может более активно поддерживать национальные усилия по разработке нормативной базы и помогать государствам-членам в наращивании потенциала для сокращения существующего разрыва.

В заключение мы подтверждаем нашу приверженность укреплению кибербезопасности как на национальном, так и на международном уровне и подчеркиваем сквозной характер киберугроз и необходимость эффективного реагирования на них путем принятия коллективных мер.

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

**Г-н Ларсен** (Австралия) (*говорит по-английски*): Я благодарю Республику Корея за организацию этого заседания для обсуждения этой важной темы.

Я рад выступить от имени Канады, Новой Зеландии и Австралии.

Киберугрозы препятствуют использованию возможностей цифровых технологий для осуществления преобразований. Они становятся все более масштабными и изощренными и создают особенно серьезные проблемы, когда используются в контексте вооруженных конфликтов. Мы все ежедневно полагаемся на цифровые услуги как граждане и потребители, а это значит, что инциденты в киберпространстве, затрагивающие критическую инфраструктуру, могут иметь разрушительные и многоуровневые последствия для всего общества. Они усиливают существующие угрозы и могут угрожать, на самом базовом и фундаментальном уровне, эффективному функционированию правительств и подорвать доверие общественности к ним.

В разных уголках мира имели место серьезные киберинциденты, выводящие из строя важнейшие объекты инфраструктуры и нарушающие работу основных служб и государственных органов. В наших странах мы столкнулись с этим самым непосредственным образом. В Австралии в результате инцидента в секторе здравоохранения с использованием вируса-вымогателя была раскрыта личная информация миллионов людей. В Канаде инцидент с использованием вируса-вымогателя парализовал работу систем медицинских учреждений в провинциях, что вызвало серьезные задержки и поставило под угрозу безопасность конфиденциальной информации, касающейся тысяч сотрудников и пациентов. В Новой Зеландии доля киберактивности, мотивированной финансовыми соображениями, впервые превысила долю деятельности в киберпространстве, спонсируемой государством.

В ситуациях продолжающихся вооруженных конфликтов проводятся военные кибероперации с целью внедрения разрушительных вредоносных программ в государственные и частные сети, которые создают угрозу для важнейших объектов гражданской инфраструктуры и работы организаций, участвующих в ликвидации последствий кризисов, включая службы экстренной помощи, энергетические, транспортные и коммуникационные сети. Мы также видим четкую связь между использованием вирусов-вымогателей для совершения финансовых преступлений, включая кражу криптовалюты, в целях прямого финансирования ядерных программ и программ создания оружия массового уничто-

жения и подрывом наших усилий по обеспечению глобальной стабильности и разоружения. Совет Безопасности должен сыграть решающую роль в предотвращении этого. Мы приветствуем подобные возможности для обсуждения киберугроз, что помогает обеспечить учет этих вопросов при обсуждениях в Совете Безопасности, повысить внимание к ним и привлечь экспертов из многостороннего сообщества, в том числе организаций гражданского общества.

Все вместе мы недвусмысленно дали понять, что деятельность всех государств в киберпространстве имеет ограничения и регулируется обязательствами, точно так же, как и деятельность в физической сфере. Все государства-члены Организации Объединенных Наций консенсусом согласились с тем, что действующее международное право, и в частности Устав Организации Объединенных Наций, в полной мере применяется в киберпространстве. Государства должны недвусмысленно заявить о своей приверженности тому, чтобы действовать в соответствии с международным правом и ожиданиями, изложенными в согласованных нормах, которые не имеют обязательной силы.

В заключение мы хотим сказать, что у нас есть два ключевых пожелания.

Во-первых, мы просим Совет Безопасности подтвердить согласованные рамки ответственного поведения государств в киберпространстве, которые служат основой мира и стабильности и способствуют созданию открытого, безопасного, стабильного, доступного и мирного киберпространства. Достижение этих ключевых целей требует выполнения и соблюдения соответствующих обязательств с опорой на скоординированное наращивание потенциала для поддержки всех государств в деле повышения их способности реагировать на возникающие вызовы.

Во-вторых, мы призываем Совет Безопасности подтвердить, что международное гуманитарное право применимо к киберпространству в ситуациях вооруженного конфликта. Такие подтверждения укрепляют наши коллективные обязательства по защите критически важной инфраструктуры и укреплению международного права, в частности Устава Организации Объединенных Наций.

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

**Г-жа Куртуа** (*говорит по-английски*): Международный Комитет Красного Креста (МККК) разделяет озабоченность Республики Корея по поводу потенциальных человеческих жертв кибероперациий во время вооруженных конфликтов.

МККК работает над защитой и оказанием помощи людям, пострадавшим в результате более чем 120 вооруженных конфликтов по всему миру. Во все большем числе этих конфликтов кибероперации создают дополнительные риски для безопасности и благополучия людей. Особую озабоченность вызывают три тенденции.

Во-первых, кибероперации нарушают предоставление гражданскому населению основных услуг, таких как электроснабжение, водоснабжение и медицинское обслуживание. Такие кибероперации подвергают опасности людей, и без того страдающих от разрушений и отсутствия безопасности, вызванных вооруженным конфликтом, и часто проводятся в нарушение норм международного гуманитарного права.

Во-вторых, мы глубоко обеспокоены растущим участием гражданских субъектов - отдельных лиц, хакерских групп и технологических компаний - в кибероперациях, связанных с вооруженными конфликтами. Чем ближе гражданские лица и гражданские объекты к местам боевых действий, тем выше риск того, что им будет нанесен ущерб.

В-третьих, МККК и все Международное движение Красного Креста и Красного Полумесяца как гуманитарные организации также сталкиваются с растущей угрозой кибероперациий, включая утечку данных и вредоносные информационные операции. Если наши операции по оказанию помощи будут нарушены или доверие к нашим операциям и работе будет подорвано, наша способность оказывать помощь и защищать людей ослабнет.

Члены Совета Безопасности несут главную ответственность за поддержание международного мира и безопасности и играют ключевую роль в защите гражданского населения во время вооруженных конфликтов. Совет Безопасности всегда четко заявлял: у войн есть пределы. Совет не оставил никаких сомнений относительно того, что воюющие стороны не должны нападать на гражданских лиц или гражданские объекты и что медицинские учреждения, а также операции по оказанию гуманитарной помощи и персонал должны пользовать-

ся уважением и защитой. Соответственно, МККК призывает Совет Безопасности учитывать в своей работе потенциальные человеческие жертвы кибероперaций и систематически поддерживать давно установленные ограничения, которые международное гуманитарное право налагает на все средства и методы ведения войны - старые и новые, кибернетические и кинетические.

Важным первым шагом в этом направлении стала недавно принятая резолюция 2730 (2024), в которой прямо выражается обеспокоенность по поводу злонамеренных действий в области информационно-коммуникационных технологий, которые направлены против гуманитарных организаций, и осуждается дезинформация и подстрекательство к насилию в отношении гуманитарного персонала. В современном цифровом мире Совет Безопасности не должен игнорировать угрозы, которые деятельность в сфере ИКТ представляет для гражданского населения во время вооруженных конфликтов.

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

**Г-н Тито** (Кирибати) (*говорит по-английски*): Кирибати признательна за возможность поделиться своими соображениями по поводу использования информационно-коммуникационных технологий (ИКТ) в контексте международного мира и безопасности. Мы хотели бы поблагодарить Генерального секретаря и докладчиков из неправительственных организаций и научных кругов за то, что они поделились своими мнениями.

Ранее на этой неделе Кирибати поддержала совместное заявление Республики Корея по этому вопросу. Мы хотели бы выразить признательность Республике Корея за ее лидерство в этом вопросе и отметить присутствие министра иностранных дел Республики Корея г-на Чхо Дэ Юля, который председательствует на этом заседании. Я благодарю Вас, г-н Председатель, за то, что Вы подчеркнули роль Совета Безопасности в обеспечении того, чтобы информационно-коммуникационные технологии ответственно использовались для укрепления мира и безопасности во всем мире, а не в целях, которые ставят под угрозу международный мир и безопасность, особенно сейчас, когда региональные войны и насильственные конфликты становятся все более частыми.

Мы разделяем аналогичную озабоченность по поводу использования злонамеренных кибердействий против гражданской инфраструктуры и их воздействия на жизнь и благополучие людей, особенно в отношении наиболее маргинализированных и уязвимых членов наших обществ. Мы хотели бы выразить нашу глубокую озабоченность по поводу кибероперaций, направленных против критически важной гражданской инфраструктуры, такой как водоснабжение и электроснабжение. Соответствующие объекты находятся под защитой международного гуманитарного права. Кроме того, согласно международному гуманитарному праву, медицинские учреждения должны пользоваться уважением и защитой. Во время вооруженных конфликтов необходимо также уважать и защищать операции по оказанию гуманитарной помощи.

Когда заинтересованные стороны высказывают свое мнение о вредоносных кибероперациях в условиях вооруженного конфликта и призывают к применению международного гуманитарного права и обсуждению этого вопроса, они делают это из искренней заботы о безопасности своего населения. Давайте представим себе мир, в котором эти меры защиты не применяются к кибероперациям, и спросим себя, хотим ли мы жить в таком мире и называть его своим домом. Для нас ответ - нет, особенно в Тихом океане, где мы наслаждаемся покоем и гармонией с природой и с самими собой.

Мы должны отстаивать применение международного гуманитарного права в киберпространстве. Поэтому мы твердо убеждены в том, что международное сообщество, особенно Совет Безопасности, должно прислушаться к заинтересованным сторонам и представителям неправительственных организаций и научных кругов, которые выражают обеспокоенность злонамеренной деятельностью киберпреступников. Мы должны быть готовы отстаивать и применять принципы международного гуманитарного права. Поэтому мы настоятельно призываем Совет Безопасности учитывать гуманитарные проблемы, создаваемые кибероперациями, и поддерживать ограничения, налагаемые на все средства ведения войны, включая кибероперации, в соответствии с международным гуманитарным правом. Мы не можем рисковать эрозией международного гуманитарного права в зарождающемся киберпространстве ИКТ.

В заключение я хотел бы напомнить о заявлении, с которым бывший президент Соединенных Штатов Гарри Трумэн выступил 79 лет назад, приветствуя принятый незадолго до этого Устав Организации Объединенных Наций.

> «Только если мы поймем, что такое Устав и что он может означать для мира во всем мире, этот документ станет живой человеческой реальностью».

Давайте же все будем уважать Устав Организации Объединенных Наций во всей его полноте и призовем все глобальные технологические компании, большинство из которых не контролируются тем или иным правительством, контролирующие все информационные и коммуникационные технологии, обеспечить ответственное использование этих технологий для содействия полному соблюдению Устава и продвижению благородной цели Устава - построить более мирный, процветающий, человечный и полный любви мир для всех.

**Председатель** (*говорит по-английски*): Представитель Исламской Республики Иран попросил слова для дополнительного заявления.

**Г-н Ахмади** (Исламская Республика Иран) (*говорит по-английски*): Я понимаю, что сегодняшнее заседание продолжается уже долго, и я не намерен отнимать много времени у членов Совета. Однако я попросил слова для дополнительного заявления, поскольку представители Албании и израильского режима использовали этот зал для выдвижения необоснованных обвинений против Ирана, ложно обвинив нашу страну в поддержке кибератак.

Мы категорически отвергаем и осуждаем эти голословные заявления. Что касается необоснованного упоминания Ирана в заявлении представителя Албании, то мы ответили на это ложное утверждение и отвергли его в нашем письме Совету Безопасности от 10 сентября 2022 года (S/2022/685). Мы считаем, что правительство Албании было введено в заблуждение дезинформацией, распространенной террористической организацией, а именно организацией «Моджахеддин-э хальк», и ошибочно возложило ответственность за кибератаку на Иран.

Организация «Моджахеддин-э хальк», которая в настоящее время базируется в Албании, уже совершила несколько кибертеррористических атак на важнейшие объекты инфраструктуры Ирана при содействии и поддержке некоторых государств, включая израильский режим. Действия этой террористической организации привели к гибели многих иранских чиновников и гражданских лиц в результате террористических взрывов и убийств и с 1981 года унесли жизни почти 17 000 иранских граждан.

Несмотря на это, правительство Исламской Республики Иран в духе доброй воли предложило правительству Албании сотрудничать и конструктивно взаимодействовать, чтобы прояснить необоснованные обвинения, выдвинутые против Ирана. К сожалению, мы не получили ответа на наше предложение.

Что касается необоснованных обвинений, выдвинутых израильским режимом, то мы категорически отвергаем их. Ирония заключается в том, что представитель режима, печально известного своей злонамеренной, преступной и террористической деятельностью как в киберпространстве, так и в реальной жизни, обвиняет других в тех самых действиях, которые неоднократно совершал израильский режим.

Вот уже более девяти месяцев Израиль, оккупационный режим, ведет геноцидную войну и осуществляет военную агрессию против беззащитного палестинского народа и совершает жестокие и террористические акты в регионе, грубо нарушая все международно-правовые нормы, принципы и правила, включая международное гуманитарное право и международное право прав человека. Режим без зазрения совести использует все возможные средства для уничтожения уязвимого населения, включая использование голода в качестве метода ведения войны, неизбирательные нападения на гражданских лиц, включая женщин и детей, преднамеренные нападения на жизненно важную гражданскую инфраструктуру и препятствование оказанию важнейшей гуманитарной помощи и услуг гражданскому населению, что является прямым нарушением соответствующих резолюций Совета Безопасности.

Кроме того, этот террористический режим имеет длинный и печальный послужной список совершения кибератак против критически важной инфраструктуры суверенных государств. Как было упомянуто в заявлении Ирана, сделанном ранее в этом зале, атаки с использованием виру-

сов «Stuxnet» и «Duqu» на мирные ядерные объекты Ирана представляют собой яркие примеры преступной деятельности Израиля и кибератак на объекты критически важной инфраструктуры. Эти преступные действия были открыто признаны режимом и свидетельствуют о его причастности к вредоносным кибероперациям.

Израильский режим с его послужным списком вопиющих нарушений основных принципов международного права не в том положении, чтобы обвинять других или читать им нотации о соблюдении этих принципов. Этот режим не должен остаться безнаказанным, и Совет Безопасности должен привлечь его к ответственности за все международные преступления, которые он совершил и продолжает совершать.

*Заседание закрывается в 17 ч 55 мин.*