Организация Объединенных Наций S/2021/621

Совет Безопасности

Distr.: General
1 July 2021
Russian
Original: English

Письмо Председателя Совета Безопасности от 1 июля 2021 года на имя Генерального секретаря и постоянных представителей членов Совета Безопасности

Имею честь приложить к настоящему письму копию сообщения, представленного Высоким представителем по вопросам разоружения Идзуми Накамицу, а также заявления, сделанные Каей Каллас, Премьер-министром Эстонии; Ухумуду Махамаду, Премьер-министром Нигера; Саймоном Коувени, Министром иностранных дел и обороны Ирландии; Буй Тхань Шоном, Министром иностранных дел Вьетнама; Джо Мучеру, секретарем кабинета министров Кении по информационно-коммуникационным технологиям, инновациям и делам молодежи; Линдой Томас-Гринфилд, Постоянным представителем Соединенных Штатов, членом кабинета Президента Байдена; Харшем Вардханом Шринглой, государственным секретарем по иностранным делам Индии; Кейсал М. Питерс, государственным министром, ответственным за иностранные дела и международную торговлю Сент-Винсента и Гренадин; Эдуном Хальворсеном, первым заместителем министра иностранных дел Норвегии; лордом Уимблдонским Тариком Ахмадом, государственным министром по делам Содружества, Организации Объединенных Наций и Южной Азии Соединенного Королевства Великобритании и Северной Ирландии; Франком Ристером, министром-делегатом по вопросам внешней торговли и экономической привлекательности при министре по делам Европы и иностранных дел Франции, а также представителями Китая, Мексики, Российской Федерации и Туниса в связи с видеоконференцией «Поддержание международного мира и безопасности: кибербезопасность», состоявшейся во вторник, 29 июня 2021 года.

В соответствии с договоренностью, достигнутой между членами Совета относительно проведения этой видеоконференции, заявления в письменном виде, копии которых также прилагаются, представили следующие делегации и структуры: Австралия, Австрия, Аргентина, Бахрейн, Бельгия, Бразилия, Гватемала, Германия, Греция, Грузия, Дания, Европейский союз, Египет, Индонезия, Исламская Республика Иран, Италия, Казахстан, Катар, Канада, Латвия, Лихтенштейн, Мальта, Марокко, Международная организация уголовной полиции, Международный комитет Красного Креста, Нидерланды, Новая Зеландия, Объединенные Арабские Эмираты, Пакистан, Перу, Польша, Республика Корея, Румыния, Сальвадор, Сенегал, Сингапур, Словакия, Словения, Таиланд, Турция, Украина, Чешская Республика, Чили, Швейцария, Эквадор, Южная Африка и Япония.

21-09125X (R) 310821 290921

В соответствии с процедурой, изложенной в письме Председателя Совета Безопасности от 7 мая 2020 года на имя постоянных представителей членов Совета Безопасности (S/2020/372), которая была согласована в свете чрезвычайных обстоятельств, вызванных пандемией коронавирусного заболевания (COVID-19), эти сообщения и заявления будут опубликованы в качестве документа Совета Безопасности.

(*Подпись*) Никола **де Ривьер**
Председатель Совета Безопасности

Приложение I

Заявление Высокого представителя по вопросам разоружения Идзуми Накамицу

Я хотела бы выразить признательность Эстонии за организацию этого заседания и приглашение выступить с сообщением на этих открытых дебатах по теме поддержания международного мира и безопасности в киберпространстве.

По состоянию на январь этого года, в мире насчитывается более 4,6 миллиарда активных пользователей Интернета. Согласно оценкам, к 2022 году к Интернету будет подключено 28,5 млрд сетевых устройств, что значительно больше показателя в 18 млрд устройств, отмеченного в 2017 году.

Поскольку достижения в области цифровых технологий продолжают радикально менять жизнь людей, мы должны сохранять бдительность и должны понимать возможности злонамеренного использования таких технологий, которое может поставить под угрозу безопасность будущих поколений.

Цифровые технологии все больше ставят под угрозу существующий порядок, затрагивающий правовые, гуманитарные и этические нормы, нераспространение, международную стабильность, мир и безопасность.

Они также снижают барьеры, ограждающие нас от новых потенциальных конфликтов, и создают новые возможности для того, чтобы как государственные, так и негосударственные субъекты совершали нападения, в том числе через международные границы.

Если говорить конкретно об информационно-коммуникационных технологиях (ИКТ), то в последние годы мы наблюдаем резкое увеличение частотности злонамеренных инцидентов. Эти инциденты проявляются в разных формах — от распространения дезинформации до нарушения работы компьютерных сетей.

Такие действия ведут к подрыву доверия в отношениях между государствами.

Они также создают конкретные риски для важнейших объектов инфраструктуры, зависящих от ИКТ, таких как учреждения финансового сектора, сети электроснабжения и ядерные объекты. Генеральный секретарь привлекал внимание к тому факту, что во время пандемии совершались кибератаки на медицинские учреждения, и призывал международное сообщество активизировать усилия в целях предотвращения и пресечения этих новых форм агрессии, которые могут принести еще больше вреда гражданскому населению[1].

Такие угрозы в сфере ИКТ имеют также гендерный аспект и должны рассматриваться через эту призму. Насильственный экстремизм и торговля людьми с использованием Интернета оказывают подчас никем не учитываемое различное влияние на женщин, мужчин и детей, как и другие угрозы, связанные с ИКТ, в том числе киберпреследование, насилие со стороны интимного партнера и распространение информации и изображений интимного характера без разрешения. Вот почему мы должны приложить все усилия для обеспечения равноправного, активного и эффективного участия как женщин, так и мужчин в принятии решений, касающихся цифрового пространства.

Угрозы в сфере ИКТ множатся, но в то же время предпринимаются и усилия по их устранению. За последние полтора десятилетия в Организации

[1] См. URL: www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered.

Объединенных Наций пять групп правительственных экспертов изучали существующие и возникающие угрозы в связи с ИКТ для международной безопасности и рекомендовали меры по их устранению. Два других механизма, созданные в рамках Организации Объединенных Наций в 2018 году, — Рабочая группа открытого состава и шестая по счету Группа правительственных экспертов — недавно успешно завершили свою работу, достигнув значительных успехов в этой теме, которые выразились в конкретных практических рекомендациях.

Обе эти группы одобрили набор добровольных, необязательных норм ответственного поведения государств, признав, что со временем могут быть разработаны дополнительные нормы. Они также подтвердили, что международное право, в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира, безопасности и стабильности в сфере ИКТ. Эти группы рекомендовали меры по укреплению доверия, наращиванию потенциала и развитию сотрудничества на основе итогов работы в рамках предыдущих процессов. Кроме того, Рабочая группа открытого состава, действуя в соответствии со своим мандатом, сделала выводы и дала рекомендации по налаживанию регулярного институционального диалога по вопросам ИКТ.

Как отметила в своем докладе последняя Группа правительственных экспертов, меры, рекомендованные предыдущими группами правительственных экспертов и Рабочей группой открытого состава, в совокупности закладывают исходную базу для обеспечения ответственного использования ИКТ государствами[2].

Новая Рабочая группа открытого состава — вторая по счету — только что провела свою организационную сессию и приступит к своей основной работе в конце этого года.

На региональном уровне в настоящее время главные усилия по вопросам ИКТ предпринимают региональные организации. Региональные подходы принимают различные формы в зависимости от приоритетов и потребностей. Некоторые регионы уделяют больше внимания внедрению добровольных, необязательных норм ответственного поведения государств путем наращивания потенциала, а другие стали инициаторами собственных региональных мер по укреплению доверия в целях снижения рисков возникновения конфликтов в результате деятельности в сфере ИКТ или взяли на вооружение другие региональные инструменты для борьбы с угрозами в этой сфере. Существуют также различные региональные документы, посвященные конкретным аспектам ИКТ.

Хотя государства несут главную ответственность за поддержание международной безопасности, информационно-коммуникационные технологии являются неотъемлемой частью нашего общества, и поэтому другие основные заинтересованные стороны призваны играть ключевую роль, а также имеют свои интересы и обязанности в деле обеспечения безопасности киберпространства.

В частном секторе было разработано много отличных киберинициатив, таких как Техническое соглашение по кибербезопасности — под руководством компании «Майкрософт», Хартия доверия — под руководством компании «Сименс» и Мюнхенской конференции по безопасности, а также Глобальная инициатива по обеспечению прозрачности, разработанная Лабораторией Касперского.

Парижский призыв к доверию и безопасности в киберпространстве 2018 года объединил усилия промышленности, государств, гражданского

[2] См. пункт 21 доклада Группы правительственных экспертов. Предварительная копия — URL: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

общества и научных кругов, направленные на обеспечение приверженности девяти принципам кибербезопасности. Эти принципы охватывают целый ряд аспектов — от разработки способов предотвращения распространения вредоносных средств и методов в сфере ИКТ до содействия широкому признанию и введению в действие международных норм ответственного поведения, а также мер по укреплению доверия в киберпространстве.

Мнения, выраженные представителями частного сектора, гражданского общества и научных кругов, вносят уникальный и важный вклад в выработку такого коллективного решения проблемы кибербезопасности, к которому стремится международное сообщество.

Организация Объединенных Наций в свою очередь готова поддержать усилия государств и других заинтересованных сторон по обеспечению мира в сфере ИКТ. Генеральный секретарь созвал группу высокого уровня по цифровому сотрудничеству, которая опубликовала свой доклад в 2019 году. В ходе последующей серии обсуждений за круглым столом с участием государств и других ключевых заинтересованных сторон была разработана «дорожная карта», в которой рекомендованы дальнейшие действия по развитию сотрудничества в ключевых областях цифрового пространства.

В связи с вопросами мира и безопасности Генеральный секретарь также инициировал повестку дня в области разоружения, в которой особое внимание уделяется познанию и рассмотрению технологий нового поколения, способных бросить вызов существующим правовым, гуманитарным и этическим нормам, нераспространению, миру и безопасности.

В рамках своей повестки дня Генеральный секретарь обязуется сотрудничать и работать с учеными, инженерами и промышленным сектором для поощрения ответственного инновационного развития науки и техники и обеспечения их применения в мирных целях.

Он также обязуется сотрудничать с государствами-членами в целях содействия формированию культуры подотчетности и соблюдения новых норм, правил и принципов ответственного поведения в киберпространстве.

Цифровое пространство уже пронизало все стороны нашей повседневной жизни, но степень и сфера нашей незащищенности от угроз, создаваемых информационно-коммуникационными технологиями, стали такими, что это превратилось в серьезную проблему. Политические и технические трудности установления ответственности за кибератаки могут привести к серьезным последствиям, в том числе к непреднамеренному применению вооруженных сил и к эскалации.

Такая динамика может подтолкнуть государства к наступательной политике враждебного использования этих технологий. Это также может позволить негосударственным вооруженным и преступным группам и частным лицам разработать или получить в свое распоряжение потенциально дестабилизирующие средства, оставаясь при этом практически безнаказанными. Учитывая эти последствия для поддержания международного мира и безопасности, вызванные угрозами в сфере ИКТ, участие Совета Безопасности в решении этого вопроса имеет огромное значение.

Поэтому я рада предоставленной мне возможности проинформировать Совет, и я с интересом ожидаю последующей дискуссии.

Приложение II

Заявление Премьер-министра Эстонии Каи Каллас

Организация Объединенных Наций была создана с прицелом на будущее. Даже сегодня, когда мы сталкиваемся с целым рядом новых вызовов, моральные ценности и принципы, согласованные в Уставе Организации Объединенных Наций 76 лет назад, остаются столь же актуальными. Их защита в нашем все более «оцифрованном» будущем стала одной из самых актуальных глобальных задач. Сегодня я хотела бы поговорить о возможностях, угрозах и механизмах, которые мы используем для их решения.

Во-первых, возможности: последние полтора года удаленной работы, учебы и жизни наглядно показали, что наша зависимость от цифровых и коммуникационных технологий со временем будет только расти. Мы несем ответственность за построение такого будущего, в котором все участники будут соблюдать определенные правила поведения в киберпространстве.

Вот почему мы говорим сегодня не о технологиях, а о том, как можно использовать киберпространство. Стив Джобс прекрасно выразил эту идею: «Технологии — ничто. Важно то, что вы верите в людей, что они по своей сути добрые и умные, и, если вы дадите им инструменты, они сделают с их помощью замечательные вещи».

Будучи процветающим цифровым обществом, Эстония испытала это на собственном опыте. Свободное, открытое, стабильное и безопасное киберпространство — часть нашей жизни. Благодаря переводу большинства государственных услуг в Интернет мы ежегодно дополнительно экономим 2-3 процента валового внутреннего продукта. Наше каждодневное государственное управление вот уже более 15 лет осуществляется без бумажных носителей. Эстония создала также наибольшее количество технологических «компаний-единорогов» на душу населения.

Во-вторых, угрозы: мы должны признать, что быстрая цифровизация имеет свои темные стороны. Злоумышленники могут использовать киберпространство как еще одну сферу своей разрушительной деятельности. Например, представьте себе, что произойдет, если в разгар засухи в стране перестанет работать система водоснабжения или в холодные зимние месяцы произойдет сбой в системе энергоснабжения.

За последний год мы убедились в том, что вредоносная кибердеятельность, направленная против системы здравоохранения, может создавать реальную и ощутимую угрозу. Гуманитарные последствия вмешательства в работу важнейших объектов инфраструктуры могут быть губительными.

Мы можем возвести высокую ограду и поставить охрану вокруг наших электростанций и других важнейших объектов инфраструктуры, но таким образом мы никогда не решим наши задачи в киберпространстве. Вместо этого мы должны коллективно взять на себя роль защитников.

И наконец, как устранить эти угрозы: к счастью, как отметила наш уважаемый докладчик г-жа Накамицу, у нас есть прочная основа для нашей работы. За последнее десятилетие государства-члены согласовали эффективную нормативную базу для обеспечения стабильности и предотвращения конфликтов в киберпространстве. Она включает действующее международное право, одиннадцать добровольных необязательных норм ответственного поведения государств, меры по укреплению доверия и наращивание потенциала.

Эстония убеждена в том, что действующее международное право, включая весь Устав Организации Объединенных Наций, международное гуманитарное право и международное право прав человека, применимо в киберпространстве.

Позвольте мне подчеркнуть, что государства несут ответственность за любые действия, противоречащие их обязательствам по международному праву.

В частности, для обеспечения защиты гражданских лиц и гражданских объектов в ходе вооруженных конфликтов, — а Совет Безопасности регулярно обсуждает такие темы — жизненно важно, чтобы любое использование киберпотенциала в таких условиях соответствовало обязательствам по международному гуманитарному праву.

Одиннадцать норм ответственного поведения государств, которые мы согласовали, отражают ожидания международного сообщества и устанавливают важные дополнительные ориентиры для деятельности государств в киберпространстве.

Этой весной международное сообщество очень эффективно подтвердило эту нормативную базу. Мы воодушевлены и руководствуемся единогласно принятыми документами, которые стали результатом успешной работы последней Группы правительственных экспертов и Рабочей группы открытого состава. Реализация положений этих базовых документов является важной задачей международного сообщества.

Глобальные усилия должны сопровождаться также мероприятиями и усилиями по наращиванию потенциала на региональном уровне. В связи с этим мы отмечаем важную работу, проделанную региональными организациями для укрепления доверия и развития сотрудничества. Эстония также уделяет приоритетное внимание усилиям по устранению отставания в цифровой сфере, которые должны идти рука об руку с усилиями по укреплению киберустойчивости и защите прав человека в Интернете.

Мы также должны признать, что мы боремся с киберугрозами вместе с частным сектором, гражданским обществом и научными кругами. В частности, фирмы должны сыграть важную роль, инвестируя в кибербезопасность и помогая устранить причины уязвимости.

Я убеждена в том, что сегодняшняя дискуссия оставит свой след в истории Совета Безопасности, ибо мы рассматриваем вопросы, которые станут еще более актуальными для поддержания международного мира и стабильности в предстоящие годы.

Наше цифровое будущее будет обеспечено только в том случае, если мы будем следовать общим правилам поведения.

Приложение III

Заявление Премьер-министра Республики Нигер Ухумуду Махамаду

[Подлинный текст на французском языке]

Позвольте мне прежде всего поблагодарить Эстонию за включение вопроса о рисках, связанных с киберпространством, в повестку дня Совета. Я хотел бы также поблагодарить г-жу Идзуми Накамицу за ее выступление и за ее твердое намерение заниматься рассмотрением этого вопроса.

В течение двух последних десятилетий Интернет и информационно-коммуникационные технологии (ИКТ) стремительно развивались. В наши дни киберпространство стало одной из главных сфер действия геополитики, где страны могут усиливать свое экономическое, политическое и культурное влияние.

Эта цифровая революция, которая произошла у нас, преодолев все наши границы, в то же время создала новые проблемы сохранения суверенитета вследствие экстерриториальности законов, регулирующих эту сферу. Это пространство может способствовать укреплению наших демократий, предоставляя всем людям, даже инакомыслящим, возможности и средства для выражения своих взглядов, но оно может также стать убежищем для преступников и криминальных групп, единственной целью которых является дестабилизация наших стран.

Пандемия коронавирусного заболевания (COVID-19) показала нам обе стороны этого пространства: с одной стороны, наша зависимость от цифровых технологий, которая становится все сильнее, и данное виртуальное заседание является примером, а с другой стороны, она показывает хрупкость наших систем перед лицом киберпреступности и кибершпионажа, о чем свидетельствуют преступные атаки с применением вируса-вымогателя на системы здравоохранения и кампании дезинформации, цель которых — подорвать моральный дух граждан наших стран и тем самым сорвать работу по вакцинации.

Кроме того, широкое использование социальных сетей и других дискуссионных площадок привело к распространению определенных видов дискуссий, подстрекающих к актам мятежа, терроризма, покушения на наши моральные ценности и основы нашей демократии.

В связи со всем вышесказанным позвольте мне предложить несколько рекомендаций, способных, на мой взгляд, содействовать уважению международного права, а также соблюдению норм ответственного поведения государств в киберпространстве.

Прежде всего речь идет о необходимости преодоления цифрового отставания некоторых стран, особенно стран Африканского континента, в сфере цифровых технологий, поскольку три четверти жителей этого континента не имеют достаточного доступа или вообще не имеют никакого доступа к Интернету.

Как отмечают эксперты, эта ситуация является фактором, усугубляющим обнищание населения, а ее последствия проявляются по всему миру и в каждой сфере — от здравоохранения до экономики и образования; она делает такие группы населения более подверженными дезинформации и другим угрозам, создаваемым цифровизацией. Мы не можем обеспечить здоровую и защищенную киберсреду, не гарантируя при этом достаточной степени равенства в цифровой сфере.

Поэтому моя вторая рекомендация заключается в создании всемирной архитектуры на основе комплексного и согласованного подхода, который позволил бы ясно определить нормы международного права, применимые в киберпространстве, в таких широких областях, как здравоохранение, международное гуманитарное право, выборы и экономика, не говоря уже о других.

Однако, несмотря на это, мы должны понимать, что эта архитектура должна быть справедливой в плане как применения, так и использования ее преимуществ, с тем чтобы можно было избежать создания новых механизмов с двойными стандартами, которые лишь усилят неравенство между странами и заставят их столкнуться с другими негативными последствиями.

В соответствии с этой логикой было бы целесообразным, чтобы любая новая система регулирования на мировом уровне была основана на тех системах, которые уже существуют на региональном уровне, и чтобы она привела к согласованию национальных систем регулирования в государствах. В этой связи мы хотели бы упомянуть о Директиве Экономического сообщества государств Западной Африки (ЭКОВАС) о борьбе с киберпреступностью, которая налагает на государства-члены обязательства в этой области, включая наказание за определенные действия, и создает основу для регионального сотрудничества в области кибербезопасности.

Моя последняя рекомендация заключается в том, чтобы Совет Безопасности взял на вооружение более широкое и менее дискриминационное толкование Устава Организации Объединенных Наций, а также собственных полномочий, благодаря чему наши дискуссии отражали бы реалии современного мира и могли бы затронуть такие темы, как кибербезопасность, изменение климата и пандемии, поскольку эти угрозы реальны и, как пандемия COVID-19, не знают границ.

Приложение IV

Заявление Министра иностранных дел и обороны Ирландии Саймона Коувени

Я поздравляю Эстонию с успешным председательством в Совете.

Я также благодарю Высокого представителя за ее ценные замечания.

Я приветствую это своевременное обсуждение, первое в своем роде в Совете Безопасности.

Выступая в прошлом году, Генеральный секретарь призвал государства навести порядок в том, что он назвал «Диким Западом киберпространства».

Хотя в последние месяцы в Организации Объединенных Наций был достигнут отрадный прогресс на этом направлении, проблемы кибербезопасности, с которыми сталкиваются государства, продолжают множиться, ставя под угрозу международный мир и безопасность.

Сегодня я хотел бы сосредоточиться в своем выступлении на трех аспектах:

- вызовы и возможности;
- необходимость практического принятия государствами мер, согласованных в Организации Объединенных Наций;
- важность подхода к этому вопросу на основе моральных ценностей.

Цифровые и коммуникационные технологии продолжают стимулировать экономический рост и преобразуют то, как мы живем, общаемся и работаем.

Инновации являются ключом к решению некоторых из важнейших глобальных проблем современности, включая изменение климата. Они также способствуют большим достижениям в области медицинских исследований, улучшают доступ к образованию и расширяют возможности наших миротворцев, помогая им обеспечивать собственную безопасность.

За последний год пандемия выявила нашу растущую зависимость от информационно-коммуникационных технологий, объединяя людей в те моменты, когда они вынуждены были держаться на расстоянии, и в то же время обнажая наши уязвимые места.

Я говорю об этом с учетом последних событий. В прошлом месяце государственные системы здравоохранения Ирландии подверглись очень опасной атаке с использованием вируса-вымогателя, и эта атака отразилась на работе самых важных медицинских служб.

Подобная атака во время глобальной пандемии ужасает. К сожалению, то, что произошло в Ирландии, это не единственный случай в мире.

В последние годы наблюдается усиление вредоносной киберактивности, включая парализующие атаки с применением вирусов-вымогателей, киберпреступность, кражу интеллектуальной собственности и распространение дезинформации и ненависти.

Важнейшие объекты инфраструктуры все чаще становятся объектами нападения.

Ирландия серьезно озабочена тем, что эта деятельность создает угрозу международному миру и безопасности.

Существующие проблемы безопасности усугубляются киберугрозами, такими как уязвимость систем управления и контроля за ядерным оружием в условиях проведения кибератак. Это делает продвижение по пути ядерного разоружения еще более необходимым.

Мы не можем допустить, чтобы деятельность в киберпространстве не подчинялась никаким правилам или законам, и чтобы злоумышленники действовали по своему усмотрению.

Международные споры в киберпространстве должны разрешаться мирными средствами.

Совет должен направить четкий сигнал о поддержке мирного и безопасного глобального киберпространства, построенного на консенсусе и взаимном доверии.

Переходя к моему второму вопросу, я хотел бы подчеркнуть, что Ирландия приветствует достигнутые в последнее время успехи Организации Объединенных Наций в деле согласования основ ответственного поведения государств в киберпространстве.

Теперь государства подтвердили, что существующее международное право, особенно Устав Организации Объединенных Наций, обеспечивает прочную, формируемую правилами основу для всех подходов к кибербезопасности.

Ирландия поддерживает усилия, направленные на содействие более глубокому пониманию государствами вопросов применения международного права к киберпространству.

Мы опубликуем в ближайшее время меморандум о нашей национальной позиции и призываем других сделать то же самое.

Ответственное поведение государств, разумеется, также имеет огромное значение.

Все государства-члены согласились руководствоваться одиннадцатью добровольными нормами поведения государств в киберпространстве.

Теперь нам надо добиваться понимания и внедрения этих норм на основе международного права, чтобы укрепить глобальную кибербезопасность. Это приведет к уменьшению вероятности конфликтов и улучшению международных отношений.

Меры укрепления доверия, включая диалог, способствуют доверию и уменьшают напряженность в отношениях между государствами. Я знаю, что это очевидная истина, но о ней надо сказать.

Мы приветствуем ведущую роль, которую играют в этом процессе региональные организации, включая Организацию по безопасности и сотрудничеству в Европе. Ирландия и наши партнеры по Европейскому союзу готовы поддерживать инициативы по укреплению потенциала.

В тесно взаимосвязанном киберпространстве ни у одной страны не будет безопасности, пока не будут в безопасности все страны. Само собой разумеется, что пандемия коронавирусного заболевания (COVID-19) заставила нас сделать этот вывод.

Мы также сохраняем приверженность устранению цифрового разрыва между странами. Доступ к Интернету для всех станет ключевым элементом достижения целей в области устойчивого развития в следующем десятилетии.

Мой третий тезис заключается в том, что поддержание международного мира и безопасности в киберпространстве должно быть ориентировано на человека и должно быть основано на моральных ценностях.

Ирландия выступает за безопасное и доступное киберпространство, в котором царят права человека и основные свободы, — как в сети, так и вне ее.

Мы решительно подтверждаем применимость международного права прав человека к действиям государств в киберпространстве.

Защита гражданского населения остается важнейшим приоритетом на всех направлениях нашей работы. В связи с этим Ирландия стремится обеспечить соблюдение международного гуманитарного права в киберпространстве.

Печально то, что гендерное насилие, которому подвергаются слишком многие женщины и девочки, сегодня нередко сопровождается и умножается насилием в Интернете и киберугрозами.

Поэтому становится еще более важным, чтобы мы как лидеры, все лидеры, сознательно способствовали участию женщин в процессах принятия решений и проведения политики Организации Объединенных Наций в области киберпространства.

Нам надо прилагать больше усилий для преодоления гендерного цифрового разрыва.

Ирландия последовательно выступает за включение более широкого круга специалистов в дискуссии Организации Объединенных Наций по кибербезопасности и наращиванию потенциала.

Правительства наряду с теми, кто стимулирует и возглавляет технологические инновации, несут ответственность за поддержание безопасного и свободного киберпространства.

Вклад гражданского общества, технических экспертов, ученых и частного сектора обогатил предыдущие обсуждения вопросов, связанных с киберпространством, в Организации Объединенных Наций. Пока же их участие в обсуждении вопросов кибербезопасности, на наш взгляд, слишком ограниченное.

Мы также поддерживаем инициативы, включая Парижский призыв к доверию и стабильности в киберпространстве, которые объединяют государственные и негосударственные заинтересованные стороны с общей целью укрепления мира и безопасности.

Мы должны работать сообща, для того чтобы достичь более правильных коллективных решений.

В заключение я хотел бы сказать, что Ирландия будет продолжать поддерживать конструктивные, многосторонние и основанные на консенсусе подходы с участием многих заинтересованных сторон для укрепления киберустойчивости во всем мире.

Мы призываем все государства ответственно вести себя согласно международному праву и выполнять базовые нормы.

Мы высоко ценим роль Совета Безопасности в предотвращении конфликтов и укреплении мира и безопасности, в том числе в киберпространстве.

И мы настоятельно призываем все государства идти дальше на основе успехов, достигнутых в Организации Объединенных Наций в последние месяцы.

Только так мы сможем обеспечить более безопасное и мирное глобальное киберпространство для всех.

Приложение V

Заявление Министра иностранных дел Вьетнама Буй Тхань Шона

Я благодарю Председателя и Эстонию за созыв этого заседания по исключительно актуальной теме. Я признателен заместителю Генерального секретаря Накамицу за ее вдумчивые замечания.

Бурное развитие информационно-коммуникационных технологий (ИКТ) существенно повлияло на то, как люди живут, работают и общаются друг с другом. Оно способствовало глобальной коммуникации, обмену знаниями и культурному обмену, помогло народам и странам сблизиться, а также обновить производство путем внедрения более эффективных, устойчивых и всеобъемлющих моделей.

С другой стороны, эти передовые технологии, если они попадают не в те руки и используются со злым умыслом, могут создавать серьезную угрозу суверенитету, безопасности и процветанию государств. В руках террористов или транснациональных преступников они могут подрывать экономические системы, социальную стабильность, культурные и человеческие ценности.

Возьмем, к примеру, экономические потери, вызванные кибератаками. Глобальные ежегодные расходы на кибербезопасность достигли 1 трлн долл. США в 2020 году, что на 50 процентов больше, чем в 2018 году, и в три раза больше, чем в 2013 году. Наибольшая часть этих расходов идет на устранение ущерба и восстановление.

Более тревожными являются сообщения о транснациональных кибератаках, которые подрывают глобальную и национальную безопасность и даже могут привести к кибервойне.

Поэтому кибербезопасность чрезвычайно актуальна и исключительно важна для мира, безопасности, развития и процветания как на национальном, так и на глобальном уровнях. С учетом этого я хотел бы поделиться следующими мыслями.

Во-первых, каждое государство имеет свой собственный суверенитет и преследует свои интересы в киберпространстве, которые должны полностью соблюдаться. Каждое государство-член несет главную ответственность за создание правовой базы для регулирования поведения в киберпространстве на своей территории и применительно к своим гражданам. Кроме того, регулирование поведения в соответствии с законом, предотвращение незаконных вредоносных действий и содействие позитивной деятельности являются руководящими принципами для создания безопасного, стабильного киберпространства в интересах мира, развития и человечества.

Вьетнам — страна с высоким уровнем охвата Интернетом, поскольку почти 70 процентов нашего населения активно пользуются Интернетом и социальными сетями. Наши успехи достигнуты благодаря всеобъемлющей правовой базе, которая способствует развитию ИКТ и предотвращает злоупотребление ими. Вьетнам также уделяет особое внимание повышению уровня самозащиты, самообеспеченности и устойчивости в сочетании с эффективным международным сотрудничеством.

Во-вторых, природа кибератак носит транснациональный характер, когда глобальные Интернет-сети становятся объектом постоянной эксплуатации со стороны злоумышленников. Это, соответственно, требует глобальных и транснациональных решений в области кибербезопасности. Вьетнам поддерживает

международные рамки, устанавливающие правила и нормы ответственного поведения в киберпространстве на основе консенсуса и при самом широком участии стран, включая нынешние процессы в Организации Объединенных Наций. Мы озабочены злонамеренным, вредоносным использованием ИКТ, особенно кибератаками на медицинские учреждения и системы электроснабжения, водоснабжения и снабжения продовольствием, столь необходимые людям, и ведем борьбу с такими действиями. Деятельность в киберпространстве должна соответствовать принципам Устава Организации Объединенных Наций и международного права, в том числе таким, как уважение суверенитета, невмешательство во внутренние дела государств, неприменение силы и мирное урегулирование споров.

В-третьих, для укрепления кибербезопасности необходимы развитие международного сотрудничества, укрепление доверия и подотчетности. Все страны, независимо от их размера и уровня развития, получают выгоды от глобального защищенного и безопасного киберпространства. Поэтому им надо активно участвовать в усилиях по обеспечению безопасности в глобальном киберпространстве во имя мира, стабильности и устойчивого развития всех стран и вносить в эту деятельность более практический и ответственный вклад.

Развитие ИКТ — это важная основа для реализации наших общих устремлений к процветанию. Вьетнам активно проводит в жизнь национальную стратегию цифровой трансформации. Мы стремимся к тому, чтобы к 2030 году доля цифровой экономики в валовом внутреннем продукте составила 30 процентов. В Юго-Восточной Азии Вьетнам активно участвует в работе региональных механизмов обеспечения кибербезопасности, включая стратегию сотрудничества в области кибербезопасности Ассоциации государств Юго-Восточной Азии. Мы также развиваем эффективное двустороннее сотрудничество со многими странами и международными партнерами в этой области. Вьетнам готов и впредь вносить свой вклад в укрепление международного сотрудничества в целях создания мирного, стабильного, защищенного и безопасного киберпространства для нашего общего процветания и устойчивого развития.

Приложение VI

Заявление Секретаря кабинета министров Кении по информационно-коммуникационным технологиям, инновациям и делам молодежи Джо Мучеру

Я поздравляю Председателя в связи с проведением впервые в Совете Безопасности независимой дискуссии по теме кибербезопасности. Я благодарю Высокого представителя Организации Объединенных Наций по вопросам разоружения г-жу Накамицу за ее содержательное сообщение.

Наша растущая зависимость от информационно-коммуникационных технологий (ИКТ) несет в себе как преимущества, так и уязвимости.

Усилия тех, кто разрабатывает и использует ИКТ и новые технологии в мирных целях, предпринимаются параллельно с противоположными усилиями тех, кто направляет их в целях контроля, незаконного наблюдения, мошенничества, радикализации и дестабилизации.

Кения привержена делу поддержания и защиты свободного и открытого Интернета. Мы рассматриваем его как ключевую движущую силу национального развития и стремимся к тому, чтобы наша молодежь могла конкурировать в деле его использования.

Мы принадлежим к числу мировых лидеров в области цифровых валют, поскольку стали первопроходцами в применении M-PESA — первой широко используемой платформы мобильных денег. Наше правительство также внедрило цифровую платформу предоставления государственных услуг через наши центры обслуживания по принципу «одного окна», известные как центры «Худума», которые работают по всей стране.

Молодые кенийцы внедряют инновации и создают компании, которые ведут к глубоким преобразованиям. Это признано инвесторами во всем мире: наша «Кремниевая саванна» привлекает больше всего инвестиций в нашем регионе. Мы считаем, что многие достойные рабочие места появятся именно в этих компаниях.

Учитывая столь широкое распространение цифровых технологий, Кения считает обеспечение безопасности ИКТ одной из важнейших задач наших органов национальной безопасности.

Для этого у нас есть строгий режим регулирования. Кроме того, у нас растут возможности реагирования на эти угрозы. Наша Группа реагирования на инциденты в области компьютерной безопасности сотрудничает с другими национальными группами такого рода и на международном уровне в рамках глобального Форума групп реагирования на инциденты и обеспечения безопасности.

Наша задача сегодня — представить предложения о том, как Совет Безопасности может лучше обеспечить международный мир и безопасность перед лицом угроз, исходящих из киберпространства или задействующих его.

Я остановлюсь на трех областях, которые, по нашему мнению, выиграют от развития международного сотрудничества.

Первая область касается ИКТ и стран с развивающейся экономикой. Киберпреступность все больше концентрируется в странах с развивающейся экономикой. Надо расширять сотрудничество в укреплении существующих региональных и международных механизмов урегулирования экономических конфликтов, включая скоординированные усилия по выявлению и снижению

рисков, связанных с деятельностью в сфере ИКТ, таких как мошенничество в цифровом формате, влияние криптовалют на национальные системы центральных банков и кибератаки на важнейшие объекты инфраструктуры.

По мере ускорения автоматизации производства потерянные рабочие места должны быть заменены другими достойными рабочими местами, иначе пострадают мир и безопасность. Надо активнее заниматься инвестированием в развитие цифровых навыков, что позволит странам со слаборазвитой промышленностью привлечь инвестиции, обеспечивающие миллионы новых рабочих мест.

Вторая область связана с ИКТ и насильственным экстремизмом. Новые технологии появляются повсюду, их можно запрограммировать, а в их основе лежат массивы данных, и все они приносят пользу, но в то же время открывают двери для злоупотреблений со стороны вооруженных групп и террористов. Эти группы используют непрозрачные механизмы управления, алгоритмы, 3D-печать, криптографию и упрощенный пользовательский интерфейс для вербовки, планирования и совершения террористических актов. Это подпитывает радикализацию и милитаризацию.

Кения призывает к расширению сотрудничества между Советом Безопасности и Контртеррористическим управлением для создания такого органа по обеспечению безопасности киберпространства, который быстро и эффективно реагировал бы на потребности государств-членов в укреплении потенциала.

В мандатах миротворческих операций Организации Объединенных Наций также надо будет учитывать использование киберпространства враждебными милитаризованными силами.

Третья область моего внимания — это ИКТ и социальные сети. Невозможно переоценить растущее влияние фальшивых новостей, тщательно продуманных подлогов, ложной информации и дезинформации на мир и безопасность. В последнее время мы были свидетелями того, как фальшивые новости подрывали усилия по борьбе с пандемией коронавирусного заболевания (ковид-19), распространяя сомнения в целесообразности вакцинации.

Компании, владеющие социальными сетями, должны привлекаться к ответственности и обязаны обеспечить, чтобы на их платформах не распространялись фальшивые новости, особенно те, которые подготовлены изощренными организациями, некоторые из которых поддерживаются государствами. Такие усилия по регулированию должны базироваться на многосторонней платформе для обеспечения единообразного эффекта.

В заключение я подтверждаю готовность Кении внести свой вклад в активизацию глобальных усилий и в разработку институциональных основ и норм, которые увеличат потенциал свободной, мирной и стабильной киберсферы и в то же время ослабят исходящие от нее угрозы.

Приложение VII

Заявление Постоянного представителя Соединенных Штатов Америки при Организации Объединенных Наций Линды Томас-Гринфилд

Благодарю Вас, Председатель, и выражаю признательность Эстонии за организацию сегодня этой важной дискуссии. Мы очень признательны Эстонии за привлечение внимания Совета к этому вопросу. Я благодарю также Высокого представителя Накамицу за ее обстоятельное сообщение.

Эти дебаты проходят в нужный момент. Мы никогда не полагались на технологии так сильно, как сегодня, особенно в связи с пандемией коронавирусного заболевания (COVID-19). Однако как государственные, так и негосударственные субъекты пользуются сейчас этим возросшим доверием. В Соединенных Штатах отдельные громкие инциденты с использованием вирусов-вымогателей нарушили работу «Джей-Би-Си», крупной компании по производству продуктов питания, и трубопровода «Колониал», компании, обеспечивающей топливом значительную часть нашего Восточного побережья. Эти инциденты свидетельствуют о серьезном и неприемлемом риске, который киберпреступность создает для важнейших объектов инфраструктуры. Последствия этой вредоносной деятельности зачастую выходят за пределы страны. Вредоносная киберактивность была направлена, например, на компанию «Солнечный ветер», занимающуюся разработкой программного обеспечения, и на программное обеспечение сервера “Exchange” компании «Майкрософт».

Риск очевиден. Наша инфраструктура — онлайн и офлайн — находится под угрозой. Самые необходимые и самые важные для нас услуги — от продуктов питания, которые мы едим, и воды, которую мы пьем, вплоть до медицинских услуг, на которые мы все полагались во время пандемии, — становятся объектами для нападений. Поэтому в современном мире, когда мы говорим о глобальной безопасности, мы должны говорить о кибербезопасности. К счастью, несмотря на наши идеологические разногласия, за последнее десятилетие государства-члены неоднократно объединялись, чтобы попытаться предотвратить конфликты, вызванные кибернетическими возможностями. Совместными усилиями мы создали нормативно-правовую базу ответственного поведения государств в киберпространстве в результате работы Группы правительственных экспертов. Эта нормативно-правовая база ясно гласит, что международное право применимо к киберпространству. Там также изложены добровольные нормы и практические меры сотрудничества, которые следует принять государствам.

В последние месяцы Рабочая группа открытого состава, состоящая из представителей всех государств-членов, достигла консенсуса по новому докладу, в котором прямо одобрена эта нормативно-правовая база ответственного поведения государств в киберпространстве. А буквально в прошлом месяце шестая Группа правительственных экспертов Организации Объединенных Наций также успешно завершила свою работу, представив впечатляющий набор рекомендаций и новых указаний, касающихся этой нормативно-правовой базы. Это и есть прогресс. Эти доклады содержат реальные рекомендации, начиная от использования кибервозможностей государствами и заканчивая подходом к сложному вопросу о присвоении ответственности за киберинциденты. В этих рамках также рассматривается вопрос о том, как государства должны сотрудничать для смягчения последствий значительной вредоносной кибердеятельности, исходящей с территории конкретного государства, включая деятельность, осуществляемую преступниками.

Мы все разделяем эту ответственность. Как недавно отметил Президент Байден, цитирую: «Страны должны принимать меры против преступников, которые занимаются деятельностью с использованием вирусов-вымогателей на территории данного государства». Итак, позвольте мне внести ясность: когда государство получает уведомление о вредоносной деятельности, исходящей с его территории, оно должно предпринять разумные шаги для ее пресечения. В силу транснационального характера киберпространства такое сотрудничество абсолютно необходимо.

Нормативно-правовая база, созданием которой так усердно занимались государства-члены, определяет теперь правила поведения. Мы все обязались соблюдать эти положения. Теперь настало время применить их на практике. Нам предстоит выполнить большую работу для того, чтобы все государства, которые желают действовать ответственно в киберпространстве, обладали для этого как политическими знаниями, так и техническими возможностями. Выполняя эту работу, мы также должны и впредь защищать свободу Интернета. Те же права, которые люди имеют вне Интернета, — включая право на свободу слова, ассоциации и мирных собраний, — должны быть защищены и в Интернете.

Государства-члены продемонстрировали замечательную готовность преодолеть разногласия и достичь единогласия по этим вопросам. Давайте и впредь демонстрировать эту добрую волю и единым фронтом обеспечивать кибербезопасность во всем мире. Сообща мы построим открытое, безопасное и стабильное киберпространство, которое принесет блага всем.

Приложение VIII

Заявление государственного секретаря по иностранным делам Индии Харша Вардхана Шринглы

Я благодарю Председателя и приветствую инициативу Эстонии по организации этих открытых дебатов с целью привлечь внимание к одной из важных новых областей кибербезопасности. Я благодарю также заместителя Генерального секретаря Накамицу за ее сообщение.

Если значение слова «мир» остается неизменным с момента создания Совета Безопасности, то природа конфликта и базовые механизмы конфликтов за десятилетия претерпели огромные изменения. Сегодня мы являемся свидетелями растущих угроз для безопасности государств-членов, исходящих из киберпространства, которые больше нельзя игнорировать. Поэтому данные открытые дебаты своевременны.

Все более широкое использование кибертехнологий и информационно-коммуникационных технологий (ИКТ) ускорило экономическое развитие, улучшило обслуживание граждан, повысило уровень социальной осведомленности и дало информацию и знания каждому человеку. Большинство видов деятельности в эту киберэпоху — политическая, социальная, экономическая, гуманитарная и в области развития (включая нынешнее заседание высокого уровня Совета Безопасности) — сегодня осуществляется в киберпространстве или связано с ним. Пандемия коронавирусного заболевания (COVID-19) только ускорила и расширила цифровизацию этой деятельности.

Динамичность и постоянное развитие киберпространства также привели к тому, что кибербезопасность затронула обсуждение вопросов мира и безопасности. Отсутствие границ у киберпространства и, что еще важнее, анонимность действующих в нем лиц поставили под сомнение традиционные концепции суверенитета, юрисдикции и неприкосновенности частной жизни. Эти уникальные черты киберпространства создают для государств-членов свой набор многочисленных вызовов. В своем выступлении я сосредоточусь на трех ключевых проблемах.

Во-первых, некоторые государства используют свои знания киберпространства для достижения своих политических целей и целей, связанных с безопасностью, и потворствуют современным формам трансграничного терроризма. Мир уже является свидетелем использования киберсредств для подрыва государственной безопасности, в частности с помощью атак на важнейшие объекты национальной инфраструктуры, включая медицинские учреждения и системы энергоснабжения, и даже для нарушения социальной гармонии путем радикализации. Открытые общества особенно уязвимы в случае проведения кибератак и кампаний по дезинформации.

Во-вторых, мы являемся свидетелями изощренного использования киберпространства террористами по всему миру для усиления их влияния, распространения злобной пропаганды, разжигания ненависти и насилия, вербовки молодежи и сбора средств. Террористы также используют социальные сети для планирования и совершения своих террористических атак и провоцирования хаоса. Будучи жертвой терроризма, Индия всегда подчеркивала необходимость того, чтобы государства-члены занимались последствиями использования террористами киберпространства, подходя к этой проблеме с более стратегических позиций.

В-третьих, нарушается целостность и безопасность продуктов ИКТ, которые являются составными частями киберпространства. Широко распростра-

нены опасения в отношении того, что государственные и негосударственные субъекты внедряют в сети и продукты ИКТ факторы уязвимости и вредные скрытые функции, в том числе через пути обхода систем защиты. Такие злонамеренные действия подрывают доверие к глобальной системе ИКТ, ставят под угрозу безопасность и могут вызвать напряженность в отношениях между государствами. В интересах международного сообщества сделать так, чтобы все действующие лица соблюдали свои международные обязательства и не потворствовали практике, которая может подорвать глобальные системы обеспечения и торговлю продукцией ИКТ.

Взаимосвязи, существующие в киберпространстве, требуют, чтобы сложные проблемы и угрозы, исходящие из киберпространства, не устранялись по отдельности. Как государства-члены мы должны принять основанный на правилах сотрудничества подход к киберпространству и должны добиваться его открытости, стабильности и безопасности. Необходимо использовать импульс, порожденный положительными результатами работы Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и Рабочей группы открытого состава по достижениям в сфере ИКТ, для поиска дальнейших точек соприкосновения и совершенствования уже согласованных кибернорм и правил. Эти правила должны быть направлены на обеспечение коллективной кибербезопасности на основе международного сотрудничества. Участие многих заинтересованных сторон будет иметь ключевое значение для достижения этой цели.

Содействие равноправному доступу к киберпространству и его благам также должно стать важным компонентом этого международного сотрудничества. Растущие «цифровые разрывы» и «пропасти в цифровых знаниях» между странами создают неустойчивую среду в киберпространстве. Растущая цифровая зависимость в эпоху после COVID-19 усугубила риски цифрового неравенства и обнажила эти расколы. Такие проблемы должны быть решены путем наращивания потенциалов. Всепроникающая и не имеющая границ природа киберпространства подразумевает, что мы сильны лишь настолько, насколько сильно самое слабое звено в глобальной сети. Только совместными усилиями мы сможем достичь цели создания глобального безопасного и устойчивого киберпространства, и мы должны обеспечить, чтобы ни одна страна не осталась в стороне от этой коллективной работы.

Индия стремится к созданию открытой, безопасной, свободной, доступной и стабильной среды киберпространства, которая станет двигателем инноваций, экономического роста, устойчивого развития, обеспечит свободный поток информации и уважение культурного и языкового разнообразия. Благодаря нашим технологическим инициативам революционного характера последних лет, таким как «ИндияСтэк», «Аадхар» и «Ю-Пи-Ай», мы успешно использовали огромный потенциал кибертехнологий для реализации повестки дня в области устойчивого развития на период до 2030 года и для улучшения управления. В рамках своей кампании по вакцинации от COVID-19, одной из крупнейших в мире, Индия разработала Co-WIN — масштабируемую, всеобъемлющую и открытую технологическую платформу. Платформа Co-WIN может быть адаптирована к нуждам клиентов и расширена для проведения медицинских мероприятий по всему миру. Мы стремимся поделиться этой платформой со странами-партнерами.

Наша главная цель — использовать киберпространство для умножения и расширения возможностей людей, причем не только граждан нашей страны, но и всего человечества. Индия готова предложить свои знания и поделиться своим опытом в этом деле.

Приложение IX

Заявление государственного министра, ответственного за иностранные дела и международную торговлю Сент-Винсента и Гренадин, Кейсал М. Питерс

Мы хотели бы выразить признательность председательствующей в Совете Безопасности Эстонии за инициативу проведения сегодняшних открытых дебатов на высоком уровне по важнейшей теме — подведению итогов работы Совета Безопасности по выполнению его задачи поддержания международного мира и безопасности. Позвольте мне также выразить признательность всем выступающим сегодня за их содержательные речи.

В современном мире киберпространство затрагивает практически все сферы нашей повседневной жизни. Роль информационно-коммуникационных технологий (ИКТ) в обеспечении социально-экономических благ очевидна. Однако, несмотря на эти блага, мир должен осознавать наличие серьезных проблем в сфере ИКТ. Глобальная среда ИКТ сталкивается с резким ростом злонамеренного использования ИКТ государственными и негосударственными субъектами. Безусловно, неправомерное использование ИКТ создает угрозы для всех государств и способно негативно повлиять на международный мир и безопасность. Поэтому крайне важно, чтобы мы опирались на ранее взятые обязательства по выработке мер укрепления доверия, которые способствуют укреплению международного мира и безопасности и развитию сотрудничества, повышению уровня прозрачности, предсказуемости и стабильности в отношениях между государствами-членами в этой области.

Открытая, безопасная, стабильная, доступная и мирная среда ИКТ необходима всем и требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Кроме того, ключевую роль в обеспечении кибербезопасности играют другие субъекты с различными возможностями из разных секторов на всех уровнях глобальной цепочки ИКТ. Мы должны изучить возможности дальнейшего наращивания потенциала и выделения ресурсов на оказание технической помощи. Организации Объединенных Наций надо увеличить помощь государствам-членам и в дальнейшем содействовать обеспечению согласованности усилий целого ряда структур Организации Объединенных Наций, работающих в киберпространстве. Эти усилия должны быть увязаны с более широкими целями Организации.

Несмотря на многочисленные проблемы, с которыми мы сталкиваемся как малое островное развивающееся государство, Сент-Винсент и Гренадины предприняли конкретные шаги для повышения своей способности бороться с таким злом, как киберпреступность. Два закона — Закон об электронных доказательствах (2004 год) и Закон об электронных сделках (2007 год) — заложили фундамент законодательства по вопросам кибербезопасности в нашей стране. В августе 2016 года законодатели приняли законопроект о киберпреступности 2016 года и тем самым дали нашей стране материальное и процессуальное право для более эффективной борьбы с киберпреступностью. Мы также привержены нашим региональным соглашениям по кибербезопасности в рамках ОАГ и КАРИКОМ.

В связи с пандемией коронавирусного заболевания (COVID-19) и новым ущербом, нанесенным недавним извержением вулкана, школы в нашей стране перешли на дистанционное обучение, как и во всем мире. Поскольку тысячи детей получили от правительства планшеты для облегчения этого перехода, увеличились масштабы использования Интернета и экранного времени. Учитывая

это, Министерство образования и национального примирения дало старт кампании #GoCyberSmart по обеспечению кибербезопасности. Эта кампания представляет собой инициативу по повышению осведомленности, чтобы учащиеся могли принимать правильные решения, касающиеся Интернета. Три основных направления — это информационная безопасность, безопасность аппаратуры и безопасная навигация в Интернете.

Обмен информацией между государствами-членами и региональными и международными организациями имеет большое значение для обеспечения стабильности и предотвращения эскалации инцидентов в области кибербезопасности. Более того, мы призываем государства-члены сохранять приверженность международному праву и базовым положениям об ответственном поведении государств в киберпространстве.

В ходе наших усилий по поощрению ответственного поведения государств в киберпространстве в контексте международного мира и безопасности мы должны руководствоваться оценками и рекомендациями, содержащимися в одобренных консенсусом докладах Группы правительственных экспертов в 2010, 2013, 2015 и 2021 годах, а также выводами и рекомендациями заключительного доклада Рабочей группы открытого состава Организации Объединенных Наций.

В заключение следует отметить, что, если мы не договоримся о правилах участия, нормах политики и механизмах международного сотрудничества для создания мирной среды ИКТ, это приведет лишь к появлению новых источников нестабильности и конфликтов. Мы призываем всех членов международного сообщества соблюдать в киберпространстве свои международно-правовые обязательства, в том числе уважать суверенитет и политическую независимость, как сказано в Уставе Организации Объединенных Наций, и принципы мирного разрешения споров, как это происходит в реальном мире. Мы не должны никогда прекращать столь необходимые усилия по поддержанию международного мира и безопасности в киберпространстве.

Приложение X

Заявление первого заместителя министра иностранных дел Норвегии Эудуна Хальворсена

Доступное, свободное, открытое и безопасное глобальное киберпространство необходимо для поддержания международного мира и безопасности. Мы приветствуем то, что Эстония привлекла к этой теме внимание Совета Безопасности — главного органа Организации Объединенных Наций, ответственного за поддержание международного мира и безопасности в соответствии с Уставом Организации Объединенных Наций.

Информационно-коммуникационные технологии (ИКТ) являются фундаментальной частью глобальной инфраструктуры. Они лежат в основе развития, стабильности и безопасности всех государств. Однако киберпространство также все чаще становится ареной для конкуренции и потенциальных конфликтов между государствами.

За последнее десятилетие мы стали свидетелями того, как злонамеренные кибер-операции, проводимые как государствами, так и негосударственными субъектами, становятся все более масштабными, опасными и изощренными. Мы находимся в самом разгаре глобальной пандемии, когда даже самые важные медицинские учреждения стали объектами такой злонамеренной деятельности, угрожающей безопасности граждан и ставящей под удар наши глобальные усилия по преодолению кризиса, вызванного COVID-19.

Тем не менее есть основания и для оптимизма. Прошедший год продемонстрировал готовность международного сообщества справиться с этой ситуацией и работать сообща в целях обеспечения ответственного поведения государств в киберпространстве. Одобренные консенсусом доклады Рабочей группы открытого состава и Группы правительственных экспертов демонстрируют приверженность всех государств-членов поддержанию основанного на правилах международного порядка в киберпространстве. Это победа многостороннего подхода.

Подтверждение применимости международного права к киберпространству является краеугольным камнем одобренных консенсусом докладов — как Группы правительственных экспертов, так и Рабочей группы открытого состава. Международное право является основой для выполнения государствами совместных обязательств по предотвращению конфликтов и поддержанию международного мира и безопасности. Оно играет ключевую роль в укреплении доверия в межгосударственных отношениях. Оба доклада подтверждают, что международное право, особенно Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира и стабильности и содействия открытой, безопасной, стабильной, доступной и мирной среде ИКТ.

Мы считаем большим шагом вперед содержащееся в докладе Группы правительственных экспертов признание того, что международное гуманитарное право применяется во всех вооруженных конфликтах, а также в киберпространстве.

Международное гуманитарное право направлено на минимизацию человеческих страданий, порожденных вооруженным конфликтом. Оно регулирует и ограничивает кибероперации во время вооруженных конфликтов, точно так же, как регулирует и ограничивает любые другие средства и методы ведения войны. Следовательно, нападения на гражданских лиц или на гражданские объекты запрещены, а медицинская служба должна пользоваться защитой и уважением. Поэтому запрещены нападения на важнейшие объекты инфраструктуры, такие

как системы энергоснабжения, производства продуктов питания, снабжения питьевой водой или другие объекты, необходимые для выживания населения.

Признание применимости международного гуманитарного права к киберпространству не узаконивает кибервойну. Любое применение силы государствами по-прежнему регулируется Уставом Организации Объединенных Наций и соответствующими нормами обычного международного права. Международные споры должны разрешаться мирными средствами — как в киберпространстве, так и во всех других сферах.

Все государства-члены Организации Объединенных Наций поддержали нормативно-правовую базу ответственного поведения государств в киберпространстве. В ее основе — применимость международного права, соблюдение согласованных добровольных норм, практические меры укрепления доверия и усилия по наращиванию потенциала для повышения всеобщей устойчивости и безопасности. Это крупное достижение, но его ценность можно использовать на практике только при условии выполнения и соблюдения этих базовых положений всеми государствами.

Созыв сегодняшнего заседания — это признание того, что злонамеренная деятельность в киберпространстве может серьезно влиять на международный мир и безопасность. Сегодняшнее заседание также ясно показывает всем государствам, что от нас ожидают соблюдения согласованных нами базовых положений об ответственном поведении государств в киберпространстве. Мы должны выполнять наши обязательства по международному праву и придерживаться согласованных нами норм.

Приложение XI

Заявление государственного министра по делам Южной Азии и Содружества Соединенного королевства Великобритании и Северной Ирландии лорда Ахмада Уимблдонского

Сегодня почти все имеет цифровое измерение.

Международное сообщество должно осознать те огромные возможности, которые предоставляет Интернет для обучения, бизнеса, общения и даже для развлечений.

Однако нам также надо относиться к угрозам в этой сфере со всей серьезностью, которой они заслуживают. Угрозы, исходящие от вредоносной и опасной деятельности в киберпространстве, сегодня понятны как никогда.

Действительно, только в прошлом месяце преступная группировка напала на трубопровод «Колониал» (“Colonial Pipeline”), вымогая деньги у владельцев этого самого крупного в Америке топливного трубопровода и создав угрозу серьезных экономических потрясений.

Целями некоторых из таких действий являются кража или вымогательство. Зачастую это просто саботаж и подрывная деятельность.

Однако мы, международное сообщество, несем коллективную ответственность за создание такого киберпространства, от которого получат блага все страны и вообще все люди. Сообща мы должны сформулировать правила, которые послужат общему благу.

И здесь мы, разумеется, не начинаем с нуля.

Десять лет назад Соединенное Королевство собрало представителей более 60 стран в Лондоне, с тем чтобы разработать базовые принципы, такие как всеобщий доступ к Интернету и защита прав человека в сети.

За эти прошедшие десять лет мы прошли долгий путь.

Только в этом году Генеральная Ассамблея единогласно подтвердила применимость международного права к киберпространству и согласовала пакет добровольных принципов, включая важность защиты медицинских учреждений.

Группа правительственных экспертов добилась более глубокого понимания норм, правил и принципов киберпространства и сформулировала четкие толкования того, как международное право должно применяться в этой сфере.

Однако мы хотим двигаться дальше. Не секрет, что в настоящее время государства разрабатывают кибероперации для поддержки своих вооруженных сил и органов национальной безопасности. И Соединенное Королевство является одним из таких государств.

Позвольте мне со всей ясностью заявить: мы будем использовать такие силы и средства для защиты от тех, кто стремится причинить нам вред. Мы обязуемся использовать эти силы и средства там, где это необходимо, соразмерно и в соответствии с международным правом.

Наша общая задача состоит в том, чтобы прояснить, каким образом применять нормы международного права к деятельности государств в киберпространстве, защитить государства от злоумышленников, нарушающих правила, и обеспечить ответственность за последствия злонамеренной кибердеятельности.

Соединенное Королевство стремится сотрудничать со всеми странами и с многочисленными заинтересованными сторонами и сделать все необходимое для того, чтобы киберпространство регулировалось правилами и нормами, которые укрепляют нашу коллективную безопасность: это правила и нормы, способствующие продвижению демократических ценностей, поддерживающие глобальный экономический рост и противодействующие распространению цифрового авторитаризма.

Мы должны поддерживать верховенство права в киберпространстве: демонстрировать ответственное поведение государства, стимулировать соблюдение положений права, предотвращать атаки и, более того, привлекать других к ответу за безответственное поведение государств.

Мы также должны уделять максимальное внимание защите прав человека в Интернете, как и вне его, с тем чтобы обеспечить создание свободного, открытого, мирного и безопасного киберпространства, доступного для всех.

Нормативно-правовая база Организации Объединенных Наций по вопросам ответственного поведения государств в киберпространстве является нашей отправной точкой. Мы должны поддержать усилия всех государств по выполнению этих базовых положений.

В прошлом месяце Соединенное Королевство было радо объявить о том, что мы инвестируем более 30 млн долл. США, чтобы поддержать укрепление кибернетического потенциала в уязвимых странах, особенно в Африке и Индо-Тихоокеанском регионе.

Наша работа с Интерполом поможет странам, включая Эфиопию, Гану, Нигерию, Руанду и Кению, поддерживать совместные операции против киберпреступников.

В других местах финансирование из Соединенного Королевства поможет создать национальные команды реагирования на чрезвычайные ситуации для защиты стран от этих угроз.

Разумеется, мы не смогли бы сделать ничего из перечисленного без наших партнеров в частном секторе и, конечно, без партнеров в научных кругах и гражданском обществе.

Однако сегодня надо сказать, когда мы собрались здесь все вместе, что Совет Безопасности тоже призван сыграть ключевую и важную роль.

Там, где злонамеренная деятельность создает риски для международного мира и безопасности, — обостряя конфликт или причиняя гуманитарные страдания, — Совет Безопасности должен быть готов к ответным действиям.

Совету следует реагировать точно так же, как он реагировал бы на угрозы, сопряженные с использованием обычных средств.

У нас есть шанс воспользоваться возможностями киберпространства и обеспечить, чтобы оно оставалось движущей силой процветания и прогресса для всех.

Для этого нам жизненно необходимо работать сообща, чтобы противостоять тем, кто ставит под угрозу нашу коллективную безопасность.

И позвольте мне заверить вас в следующем: Соединенное Королевство полностью привержено защите свободного, открытого, мирного и безопасного киберпространства и его сохранения для будущих поколений.

Приложение XII

Заявление министра-делегата при министре по делам Европы и иностранных дел Франции Франка Ристера

[Подлинный текст на французском языке]

Я хотел бы поблагодарить Премьер-министра Эстонии за организацию этого мероприятия. Совет Безопасности Организации Объединенных Наций несет ответственность за поддержанием мира и международной безопасности и имеет право действовать в киберпространстве.

Киберпространство — это сфера возможностей, но также и новых угроз. Оно стало местом стратегического соперничества держав. Все шире распространяется вредоносное использование информационно-коммуникационных технологий (ИКТ) как государственными, так и негосударственными субъектами.

Мы убедились в этом в течение последних месяцев, в частности в контексте пандемии коронавирусного заболевания (COVID-19), которая усилила нашу зависимость от этих технологий. Я имею в виду прежде всего одиозные кибератаки, совершаемые с помощью вирусов-вымогателей, против медицинских учреждений и других важнейших объектов инфраструктуры. Я хотел бы выразить полную солидарность Франции с жертвами этих нападений. Я имею в виду также кампании манипулирования информацией с помощью «инфодемий» и масштабы фрагментации Интернета, которые противоречат демократическим ценностям. Действия в киберпространстве имеют совершенно реальные последствия, которые могут очень сильно сказаться на нашей жизни и нашем обществе.

Задача на ближайший век заключается в том, чтобы создать систему управления и коллективного регулирования киберпространства. Мы не желаем ни «дикого Запада» в цифровом пространстве, ни фрагментированности киберпространства. Мы подтвердили это в Парижском призыве к доверию и безопасности в киберпространстве, а также в рамках Большой семерки (Г-7) в принятой на встрече в Динаре Декларации об инициативе по разработке норм в киберпространстве. Франция намерена вместе со своими партнерами строить открытое, надежное, стабильное, нефрагментированное, доступное и мирное киберпространство.

Международное право, в том числе Устав Организации Объединенных Наций, применимо к киберпространству в полном объеме. Это подразумевает также соблюдение международного гуманитарного права при проведении кибероперациий во время вооруженных конфликтов.

Перед лицом растущего числа угроз в киберпространстве и кибератак правительства должны ответить на них укреплением сотрудничества и применением права. На протяжении более чем десятилетия Франция играла роль первопроходца в рамках различных многосторонних мероприятий. Эти усилия позволили разработать нормативно-правовую базу ответственного отношения государств к использованию ИКТ. Эти базовые положения основаны на международном праве, на совокупности соответствующих норм поведения, не противоречащих друг другу, и на мерах по обеспечению прозрачности и доверия. Они позволяют укреплять сотрудничество и взаимопонимание между государствами в киберпространстве. Я приветствую успехи, достигнутые Рабочей группой открытого состава и шестой Группой правительственных экспертов, которые приняли два сбалансированных, полезных и одобренных консенсусом доклада. Франция готова продолжать конструктивное участие в многосторонних дискуссиях в рамках Организации Объединенных Наций, в том числе в рамках новой

Рабочей группы открытого состава, созданной в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

На будущее следует подчеркнуть, что необходимо прежде всего в сжатые сроки реализовать на практике все согласованные нормы и принципы. Франция вместе с 52 партнерами предлагает разработать программу действий по кибербезопасности в рамках Организации Объединенных Наций. Этот новый механизм, дополняющий новую Рабочую группу открытого состава, позволяет создать единую структуру. Она должна будет содействовать укреплению потенциала и созданию пространства для диалога с гражданским обществом, научными кругами и частными лицами. Франция готова к диалогу со всеми государствами и заинтересованными сторонами, чтобы сформулировать и уточнить это предложение, ориентированное на действия.

Такое коллективное взаимодействие с участием многих сторон абсолютно необходимо. В киберпространстве государства несут определенную ответственность, которую никто не может взять на себя в одиночку. Мы должны полностью включиться в эту работу в этом новом дипломатическом формате.

Приложение XIII

Заявление Постоянного представителя Китая при Организации Объединенных Наций Чжан Цзюня

[Подлинный текст на китайском языке]

В современном мире только разворачивается новый виток технологической и промышленной революции и быстро развиваются цифровые и Интернет-технологии, которые значительно изменили способ производства и образ жизни человечества, способствуя социально-экономическому развитию стран. В то же время кибернаблюдение, кибератаки, киберпреступления и кибертерроризм превратились в глобальные угрозы для общества, а киберпространство становится все более милитаризованным, политизированным, небезопасным и идеологизированным. В киберпространстве страны не только пользуются общими возможностями и имеют общие интересы, но и сталкиваются с общими проблемами и несут общую ответственность. Они все больше становятся сообществом с общим будущим — и в горе, и в радости.

Председатель Китая Си Цзиньпин заявил, что, хотя страны отличаются по национальным условиям и этапам развития Интернета и имеют разные проблемы, они в одинаковой мере стремятся к развитию цифровой экономики, в одинаковой мере заинтересованы в решении проблем кибербезопасности и в одинаковой мере нуждаются в укреплении системы управления киберпространством. Китай всегда призывал международное сообщество к совместной работе, чтобы общими усилиями защищать кибербезопасность и поддерживать международный мир.

- Мы должны содействовать безопасности путем поддержания мира и не должны допустить превращения киберпространства в новое поле боя. Международное сообщество должно придерживаться целей и принципов Устава Организации Объединенных Наций, в частности принципов суверенного равенства, запрета на применение силы, невмешательства во внутренние дела и мирного разрешения споров. Важно уважать право всех стран на самостоятельный выбор пути развития своего Интернета и модели управления им, а также на равноправное участие в управлении киберпространством. Страны должны воздерживаться от такой кибердеятельности, которая ставит под угрозу безопасность других стран. Следует осторожно подходить к применению права вооруженных конфликтов к киберпространству, а гонку вооружений в киберпространстве надо предотвратить.

- Мы должны содействовать безопасности посредством обменов и сотрудничества и создавать благоприятные условия для использования киберпространства. Обеспечение безопасности в Интернете — это глобальная тема, и ни одна страна не может оставаться в стороне или справляться в одиночку. Гегемонизм, односторонность и протекционизм в киберпространстве только усилят конфронтацию и отравят атмосферу сотрудничества, что должно быть отвергнуто и против чего международное сообщество должно выступить сообща. Страны должны совместно работать над углублением обменов и сотрудничества в области технологических исследований и разработок, нормотворчества и обмена информацией, а также совместно пресекать злоупотребление информационными технологиями. Мы должны совместно противостоять киберслежке и кибератакам, бороться с кибертерроризмом и киберпреступлениями, а также повышать возможности обеспечения кибербезопасности. Важно дать компаниям открытую, справедливую и недискриминационную бизнес-среду, гарантировать

открытость, стабильность и безопасность глобальной цепочки ИТ-индустрии и цепочки поставок, способствовать здоровому развитию мировой экономики и избегать вмешательства человека в нормальную деятельность компаний под любым предлогом.

- Мы должны содействовать безопасности путем совершенствования управления и должны пропагандировать понятия честности и справедливости в киберпространстве. Все страны должны поддерживать эффективную многосторонность, начать открытый, всеобъемлющий и устойчивый процесс управления кибербезопасностью в рамках Организации Объединенных Наций с равным участием всех, сформулировать международные правила для киберпространства, признаваемые всеми странами, и противостоять кликам и групповой политике. Китай высоко оценивает успешную подготовку доклада Рабочей группы открытого состава Организации Объединенных Наций и Группы правительственных экспертов и ожидает, что новая Рабочая группа открытого состава внесет свой вклад в поддержание кибербезопасности. Мы готовы сотрудничать со всеми сторонами, чтобы в рамках Организации Объединенных Наций была разработана международная конвенция о борьбе с киберпреступностью. На основе широких консультаций, совместного вклада и общей пользы мы должны в полной мере использовать роль многих заинтересованных сторон, таких как правительства, Интернет-компании, технологические сообщества, гражданское общество и частные лица.

- Мы должны содействовать обеспечению безопасности с помощью всеобъемлющего развития и должны добиваться всеобщего процветания в киберпространстве. В настоящее время мировое экономическое развитие идет вяло. Цифровые и Интернет-технологии могут стать важными инструментами восстановления стран и возобновления социально-экономического развития после пандемии. Страны должны проводить более активную, всеобъемлющую и скоординированную политику для содействия сбалансированному развитию информационно-коммуникационных технологий во всем мире, энергично развивать новые модели и новые форматы, такие как цифровая экономика, и противостоять технологической гегемонии. Мы должны развивать цифровую инфраструктуру и взаимосвязанность, разрушать информационные барьеры, преодолевать цифровые пропасти и помогать развивающимся странам, которые стремятся к цифровизации, подключению к Интернету и развитию интеллекта с целью реализации Повестки дня в области устойчивого развития на период до 2030 года. Мы должны активизировать сотрудничество в области кибербезопасности с развивающимися странами и оказывать им помощь, а также должны улучшить их возможности раннего предупреждения и предотвращения инцидентов в сфере кибербезопасности и экстренного реагирования на них.

Китай придает большое значение кибербезопасности и информатизации и стремится построить цифровую экономику, цифровое общество и цифровое правительство, используя цифровую революцию для изменения моделей производства, образа жизни и моделей управления. Китай продолжит совершенствовать национальные законы, нормативные акты и институциональные стандарты в области кибербезопасности на основе Закона о кибербезопасности и Закона о безопасности данных.

В прошлом году Китай выдвинул Глобальную инициативу по безопасности данных, сосредоточив внимание на таких вопросах, как защита важнейших объектов инфраструктуры и персональной информации, хранение и поиск данных для зарубежных компаний, а также безопасность цепочки поставок, что

обеспечило бы конструктивное решение проблем, касающихся поддержания глобальной безопасности данных и кибербезопасности. Недавно Китай совместно с Лигой арабских государств (ЛАГ) выступил с инициативой о сотрудничестве между Китаем и ЛАГ в целях обеспечения безопасности данных, в которой воплощен совместный призыв обеих сторон к поддержанию кибербезопасности и безопасности данных. Мы приветствуем активный отклик и участие всех сторон в этой инициативе, чтобы совместными усилиями сформулировать глобальные правила цифрового управления. Китай также активно занимается строительством Цифрового шелкового пути и вместе с другими странами работает над созданием новой системы умной взаимосвязи, ориентированной в будущее.

Киберпространство воплощает мечты человечества и несет людям благосостояние, мир и безопасность. Китай готов работать со всеми странами, чтобы использовать возможности информационной революции, дать новый импульс инновациям и развитию, создать новый ландшафт цифрового сотрудничества, сформировать новую модель обеспечения кибербезопасности, построить общество, у которого киберпространство будет общим, и вместе строить более светлое будущее человечества.

Приложение XIV

Заявление Постоянного представительства Мексики при Организации Объединенных Наций

[Подлинный текст на испанском языке]

Мексика приветствует созыв этих открытых дебатов и презентацию заместителя Генерального секретаря, Высокого представителя по вопросам разоружения Идзуми Накамицу.

Как мы убедились — в качестве участника этого заседания, как, впрочем, и других форумов, — невозможно оспорить растущую важность киберпространства. Мир становится все более зависимым от информационно-телекоммуникационных технологий, особенно в условиях пандемии. Международные отношения также быстро перешли в виртуальный формат, поэтому Совет Безопасности не может и не должен оставаться в стороне от последствий этого для международного мира и безопасности.

Хотя почти половина населения планеты не имеет доступа к Интернету, это вовсе не освобождает никого от угрозы стать жертвой тысяч кибератак, которые день за днем совершаются против государственных сетей, банковских и финансовых учреждений, научно-исследовательских институтов и медицинских учреждений.

Эти потенциальные риски привели к тому, что различные органы системы Организации Объединенных Наций начали действовать и пытаются достичь межгосударственных договоренностей с целью обеспечить, чтобы киберпространство не использовалось в преступных, враждебных и даже террористических целях, не упуская при этом из виду баланса между мирным использованием и огромными возможностями, которые киберпространство создает для устойчивого развития.

Мексика считает исключительно важным предотвращение любого роста угроз в киберпространстве. Использование киберпространства, как и любого физического пространства, должно подлежать регулированию с помощью ясных рекомендаций и параметров, и в то же время надо способствовать созданию открытого, свободного, безопасного, стабильного, доступного и устойчивого киберпространства.

В связи с этим Мексика с удовлетворением отмечает, что по итогам работы Группы правительственных экспертов и Рабочей группы открытого состава стало возможным принятие консенсусом содержательных докладов, которые создали важный прецедент для многосторонних усилий. С точки зрения нашей страны, это и есть подтверждение веры в многосторонность и в конструктивную роль, которую может сыграть Организация Объединенных Наций в достижении комплексных, легитимных и долговременных решений проблем киберпространства и информационно-коммуникационных технологий.

Однако этого еще недостаточно. Надо двигаться вперед к применению в полном объеме международного права в киберпространстве, в том числе не только Устава Организации Объединенных Наций, но и международного права прав человека, международного гуманитарного права и решений судебных органов в этой сфере.

Мы твердо убеждены в необходимости повышения уровня транспарентности деятельности в киберпространстве, отчетности и призыва к разработке норм ответственного поведения государств, одобренных самой Генеральной

Ассамблеей и дополненных мерами по содействию международному сотрудничеству для создания и укрепления киберпотенциала государств.

Мексика надеется, что в будущем в рамках обсуждений и деятельности Совета Безопасности будут услышаны все более громкие голоса представителей гражданского общества, научных кругов и частного сектора. Они с полным на то основанием преследуют общую цель: обеспечить мирное использование киберпространства для развития и применения цифровых технологий.

Приложение XV

Выступление Постоянного представителя Российской Федерации при Организации Объединенных Наций В.А. Небензи

[Подлинный текст на русском языке]

Год с момента начала пандемии коронавируса стал для всего мира серьезным испытанием и запомнился, прежде всего, сложностями и потерями. Пострадали в том числе и многие дипломатические усилия, на целом ряде направлений застопорилась переговорная работа.

Однако на этом фоне есть, как минимум, одно позитивное исключение. Речь о многосторонней дискуссии по вопросам международной информационной безопасности в Организации Объединенных Наций. Она сумела не только сохранить набранный динамичный темп, но и выйти на, не побоюсь этого слова, исторические результаты. Обе профильные экспертные площадки под эгидой Генеральной Ассамблеи Организации Объединенных Наций — Группа правительственных экспертов и Рабочая группа открытого состава — смогли консенсусом согласовать итоговые доклады.

Переговоры в этих группах не были простыми. Но тем ценнее этот выстраданный итог. Он наглядно показал, что международное сообщество способно договориться по ключевым вопросам, когда диалог ведется в прагматичном, деполитизированном и конструктивном ключе. Благодаря этим усилиям сегодня мы находимся на пороге нового большого этапа, старт которому дан в июне 2021 года в ходе организационной сессии новой Рабочей группы открытого состава 2021–2025 годов.

Считаем такой результат общим достижением международного сообщества. Со своей стороны, мы уже не одно десятилетие стараемся вносить в процесс становления глобальной системы международной информационной безопасности свой вклад. Именно Россия еще в 1998 году впервые подняла в Организации Объединенных Наций вопрос о необходимости бороться с угрозами в сфере международной информационной безопасности, предложив соответствующую резолюцию Генеральной Ассамблеи Организации Объединенных Наций. В начале 2000-х годов мы предложили создать экспертную площадку для обсуждения темы международной информационной безопасности — Группу правительственных экспертов. Когда стало понятно, что эта тема «переросла» узкие рамки экспертной группы, мы, реагируя на запрос международного сообщества, совместно с единомышленниками инициировали запуск в 2019 году открытого и демократичного переговорного процесса по международной информационной безопасности с участием всех государств-членов Рабочей группы открытого состава.

Тем самым была пройдена очень серьезная веха. Впервые доступ к обсуждению вопросов безопасности в цифровой сфере получило «ооновское большинство». Наша логика здесь очень простая — мы выступаем за равноправный и взаимоуважительный диалог. Если перед лицом угроз международной информационной безопасности все равны, то и обсуждаться они должны не узким кругом технологически развитых государств, а всеми членами Организации Объединенных Наций. Не должно быть никакого навязывания со стороны тех, кто считает себя более «продвинутым».

Наши предложения, что в свое время с Группой правительственных экспертов, что позднее с Рабочей группой открытого состава, не всем с ходу

нравились. Ряд государств, в том числе участвующих в сегодняшней встрече, голосовали против их создания. Однако постепенно и они подключились к дискуссии, а затем и стали активно и конструктивно в ней участвовать.

Эффективная многосторонняя дипломатия по международной информационной безопасности в Организации Объединенных Наций, дополняющая двустороннее взаимодействие государств по этой теме, — прекрасный пример того, как надо решать эти вопросы в целях снижения взаимного недоверия и снятия озабоченностей, на контрасте с печально известной «мегафонной дипломатией», к которой иной раз, к сожалению, прибегают некоторые наши партнеры.

К сожалению, параллельно мы наблюдаем опасную тенденцию, когда Совету Безопасности Организации Объединенных Наций пытаются навязать односторонние трактовки договоренностей в рамках Группы правительственных экспертов и Рабочей группы открытого состава, фактически предлагая их поддержать или, что еще хуже, пересмотреть итоги дискуссии на профильных площадках Генеральной Ассамблей Организации Объединенных Наций. Считаем такие попытки деструктивными. Они подталкивают международное сообщество к реализации непредсказуемых и нежелательных конфронтационных сценариев.

В частности, речь идет о стремлении некоторых стран путем передергивания достигнутых договоренностей, в том числе по международно-правовым аспектам использования информационно-коммуникационных технологий (ИКТ), оправдать одностороннее давление и санкции в отношении других государств-членов, а также возможное применение силы против них. Особое беспокойство вызывает установка ряда технологически продвинутых государств на военизацию информационного пространства через продвижение концепции «превентивных военных кибердаров», в том числе по критически важной инфраструктуре. Эти конфронтационные доктрины противоречат декларируемой ими, в том числе сегодня, приверженности предотвращению конфликтов в сфере использования ИКТ. Видим в этом попытку с позиции силы навязать свои «правила игры» в информационной сфере.

Хочу подчеркнуть — хотя цифровая сфера не является нерегулируемой, дискуссия по вопросам того, как именно международное право может в ней применяться, далека от завершения. Эти вопросы предстоит еще как минимум пять лет обсуждать на профильной площадке под эгидой Генеральной Ассамблеи Организации Объединенных Наций — в новой Рабочей группе открытого состава.

Положения докладов итоговых Группы правительственных экспертов и Рабочей группы открытого состава на этот счет представляют собой четко выверенный, сбалансированный комплекс договоренностей, в том числе по поводу необходимости выработки новых норм ответственного поведения государств в информационном пространстве, отражающих его специфику. Первоначальный перечень таких правил закреплен в принятой по инициативе России резолюции Генеральной Ассамблеи Организации Объединенных Наций по международной информационной безопасности в 2018 году. Сегодня же мы, к сожалению, наблюдаем попытки вычленить из этого комплекса отдельные, наиболее выгодные для наших западных коллег положения, причем в некорректной трактовке об «автоматической» применимости международного права в цифровой сфере, что допускает и возможность применения силы в нем, и преподнести свои национальные воззрения как результат глобального консенсуса. Поэтому мы будем противостоять любым попыткам ревизовать через Совет Безопасности Организации Объединенных Наций сбалансированные договоренности, достигнутые на профильных площадках Генеральной Ассамблеи.

Российские же доктринальные подходы к формированию глобального режима обеспечения международной информационной безопасности, как указал Президент Российской Федерации В. В. Путин в ходе заседания Совета безопасности Российской Федерации 26 марта 2021 года, остаются открытыми, прозрачными и неизменными. Они закреплены и утверждены им в апреле 2021 года в Основах госполитики в области международной информационной безопасности. Это открытый документ, призываю всех с ним ознакомиться.

Наша доктрина основана на тезисах об использовании ИКТ только в мирных целях, необходимости предотвращения конфликтов в информационном пространстве и важности укрепления для этого многостороннего и двустороннего сотрудничества. Мы считаем важным, чтобы были заключены универсальные международно-правовые договоренности, которые позволили бы эффективно эти задачи реализовывать. На пути к этой цели необходимо общими усилиями разработать и согласовать универсальные, справедливые, всеобъемлющие и учитывающие сегодняшние реалии правила поведения государств в информационном пространстве, четко разграничить допустимые и недопустимые действия в нем и придать этим правилам юридически обязывающий характер, чтобы они неукоснительно соблюдались всеми государствами.

При этом мы выступаем за незыблемость суверенитета государств в цифровой сфере. Каждая страна должна самостоятельно определять параметры регулирования собственного информационного пространства и соответствующей инфраструктуры.

Не менее важная задача — построение мирной, равноправной и справедливой системы международной информационной безопасности, где будут учтены интересы всех стран вне зависимости от уровня развития их «цифрового потенциала». Необходимо всемерно поддерживать усилия по его наращиванию, предпринимаемые под эгидой Организации Объединенных Наций и нацеленные на преодоление «цифрового разрыва». Рассчитываем, что новая Рабочая группа открытого состава в соответствии со своим мандатом сможет продолжить детальное изучение этого вопроса и выработку соответствующих рекомендаций.

Кроме того, необходимо сообща противодействовать использованию ИКТ в преступных целях. Призываем государства-члены внести конструктивный вклад в работу профильного специального комитета, задачей которого является выработка к 2023 году проекта соответствующей конвенции.

Ключевой площадкой для обсуждения вопросов международной информационной безопасности остается Генеральная Ассамблея Организации Объединенных Наций. Именно там на протяжении пяти лет будет идти экспертная дискуссия по всем аспектам этой тематики. Давайте сосредоточимся на поддержке этого уникального процесса. Нужно сохранить конструктивную атмосферу многостороннего взаимодействия по теме международной информационной безопасности под эгидой Организации Объединенных Наций в формате Рабочей группы открытого состава, на практике доказавшем свою эффективность и востребованность. Тогда у новой Рабочей группы открытого состава будет реальный шанс выйти на осязаемые, практические результаты. Наш общий долг как членов Совета Безопасности Организации Объединенных Наций — этому всемерно содействовать.

Приложение XVI

Заявление Постоянного представителя Туниса при Организации Объединенных Наций Тарека Ладеба

Прежде всего я хотел бы выразить нашу признательность Эстонии, действующей в качестве Председателя, за организацию этого заседания по кибербезопасности и поддержанию международного мира и безопасности в киберпространстве.

Я благодарю г-жу Накамицу, заместителя Генерального секретаря, Высокого представителя по вопросам разоружения, за ее содержательное выступление.

Тунис глубоко озабочен значительным увеличением в последние годы масштабов вредоносной деятельности в киберпространстве, которая может создавать серьезную угрозу международному миру и безопасности, особенно когда совершаются атаки на важнейшие объекты инфраструктуры.

Многие государства также открыто развивают киберпотенциал для военных целей, и эта тенденция может привести к гонке кибервооружений и дальнейшему увеличению числа кибератак и контратак, а также рисков просчетов, которые могут привести к вооруженному конфликту.

Тунис также встревожен тем, что кибервозможности, которые ранее были доступны только государствам, стали доступны негосударственным субъектам, включая террористические организации, и те злонамеренно пользуются ими. Согласно сообщениям, эти киберсредства зачастую приобретались путем организации утечки сведений или краж из государственных структур, в связи с чем еще более актуальным становится вопрос об ответственности государств.

Возможность проведения террористическими группами опаснейших кибератак на важнейшие объекты инфраструктуры, такие как атомные электростанции, уже нельзя исключать, и к этому вопросу следует подходить со всей серьезностью.

Тунис подтверждает применимость международного права при рассмотрении вопроса об использовании государствами информационно-коммуникационных технологий и подчеркивает в связи с этим важность соблюдения принципов, закрепленных в Уставе Организации Объединенных Наций, включая разрешение международных споров мирными средствами, отказ от угрозы силой или ее применения и уважение прав человека и основных свобод.

Мы также хотели бы еще раз подчеркнуть применимость международного гуманитарного права к кибероперациям, проводимым во время вооруженных конфликтов.

Наша делегация приветствует принятие консенсусом в начале этого года докладов Рабочей группы открытого состава по достижениям в сфере информатики и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, которые способствовали углублению понимания государствами-членами вопросов применения международного права и содержали дополнительные рекомендации о том, как добровольные, необязательные нормы тоже могут играть важную роль в предотвращении конфликтов и в создании открытого, безопасного, стабильного, доступного и мирного киберпространства.

Мы надеемся на продолжение открытого и всеобъемлющего диалога по теме кибербезопасности на заседаниях новой Рабочей группы открытого состава (по безопасности и использованию информационно-коммуникационных технологий в 2021-2025 годах) для укрепления потенциала всех государств и для предотвращения или смягчения последствий злонамеренной кибердеятельности, киберугроз и кибератак.

Со своей стороны, под контролем Совета национальной безопасности и при участии частного сектора и гражданского общества Тунис принял в октябре 2019 года национальную стратегию кибербезопасности, которая направлена на повышение устойчивости Туниса к киберугрозам путем развития национального потенциала и правовой системы при полном соблюдении основных прав и свобод, а также путем укрепления международного сотрудничества.

Наконец, учитывая взаимосвязанность киберпространства, мы считаем, что обмен информацией об известных уязвимостях и наращивание потенциала тех, кто просит об этом, имеют решающее значение для снижения рисков для международного мира и безопасности, создаваемых киберугрозами.

Приложение XVII

Заявление Постоянного представительства Аргентины при Организации Объединенных Наций

[Подлинный текст на испанском языке]

Аргентина выражает признательность Эстонии за инициативу по проведению открытых дебатов с целью содействия более глубокому пониманию растущих рисков, возникающих в результате злонамеренных действий в киберпространстве, и их влияния на международный мир и безопасность. Совет Безопасности — в силу своего мандата и самой его сути — способен рассмотреть эту тему и придать ей надлежащую актуальность и значимость.

Регулярное и постоянно растущее число серьезных инцидентов, связанными с киберрисками, в различных частях земного шара указывает на необходимость дальнейших усилий по достижению более глубокого понимания того, как вести борьбу с такими инцидентами, некоторые из которых чреваты угрозой международному миру и безопасности, создать основы для сотрудничества и способствовать укреплению потенциала стран для борьбы с этими вызовами, затрагивающими все международное сообщество. Поэтому требуется немало усилий на национальном, региональном и международном уровне.

На международном уровне для решения одного из наиболее существенных аспектов данного вопроса Аргентина считает крайне важным сохранение широких и инклюзивных пространств, в которых страны всех регионов и различных взглядов могли бы активно участвовать в усилиях с целью формирования консенсуса по поводу правил, норм и принципов ответственного поведения государства и форм применения международного права в отношении кибербезопасности, а также других аспектов. Аргентина сознает, что существует немало норм, правил и принципов, принятых консенсусом всеми членами Генеральной Ассамблеи Организации Объединенных Наций для руководства использованием информационно-коммуникационных технологий на уровне государств и соблюдения ответственности государств в киберпространстве, что является необходимым условием для сохранения его мирного использования и стабильности. Это и есть точка отсчета и та основа, которую необходимо сохранять и развивать.

Мы придаем особое значение консенсусу, достигнутому в рамках первой Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в основу которого положены эти характеристики открытости. Кроме того, мы выражаем особую признательность за доклад, представленный последним составом Группы правительственных экспертов по поощрению ответственного поведения государства в киберпространстве в контексте международной безопасности. Следует отметить, что в этом году обе группы опубликовали одобренные консенсусом доклады, содержащие важные рекомендации и предложения для продолжения работы на основе уже достигнутого консенсуса.

Продолжение дискуссии в рамках открытого и инклюзивного форума с еще более широкими горизонтами настоятельно необходимо для дальнейшего укрепления уже имеющихся договоренностей и достижения новых. Поэтому мы приветствуем создание новой Рабочей группы открытого состава по безопасности и использованию информационно-коммуникационных технологий, мандат которой будет действовать до 2025 года и в деятельности которой наша страна продолжит активно и конструктивно участвовать.

В связи с этим и с целью применения более эффективного подхода Аргентина совместно с многими странами из всех регионов участвует в реализации международной инициативы, а именно программы действий по развитию информационно-коммуникационных технологий в контексте международной безопасности. Эта программа действий, находящаяся на стадии полномасштабного концептуального развития, обеспечивает открытый, всеобъемлющий, гибкий и постоянный форум для обсуждений под эгидой Организации Объединенных Наций, при ведущей роли государств и надлежащем участии многих сторон, задействованных в киберпространстве. Мы приглашаем все страны участвовать в реализации этой инициативы.

Аргентина считает, что основой и принципом наших подходов должны быть защита и гарантирование прав человека и основных свобод, закрепленных в Уставе Организации Объединенных Наций и международных договорах. Вопрос гендерной принадлежности и особой защиты уязвимых групп населения также должен быть сквозным элементом всех предпринимаемых нами действий.

В контексте непрерывного процесса инноваций в этой области нам надо активно работать на тем, чтобы благами этих технологий могли пользоваться все государства мира на основе равноправия. В связи с этим мы считаем, что сокращение цифрового разрыва между государствами и внутри самих государств должно стать постоянной темой в ходе этих дебатов.

Эта озабоченность касается и развития национальных потенциалов. У нас огромное поле для работы на этом направлении, и в этом заключается один из главных принципов достижения согласованности действий с другими субъектами, участвующими в борьбе с киберпреступностью, такими как частный сектор, гражданское общество, научные круги и технические специалисты. Региональные и субрегиональные организации зарекомендовали себя как важные и активные участники, выступающие в качестве катализаторов развития национальных потенциалов, формирования общих представлений и содействия международному сотрудничеству.

Нет сомнения в том, государства должны предпринять большие усилия на национальном уровне, создать мощный потенциал, разработать эффективные нормы и подготовить столь же эффективные структуры, чтобы придать этой теме такое значение и такую степень приоритетности, которых она заслуживает.

Мы уверены в том, что это мероприятие позволит нам выйти на новый уровень понимания проблем, способствующего созданию свободного, открытого, безопасного, совместимого и стабильного киберпространства.

Приложение XVIII

Заявление Постоянного представителя Австралии при Организации Объединенных Наций Митча Файфилда

Австралия благодарит Эстонию за предоставленную возможность выступить с заявлением в Совете Безопасности по вопросам международного мира и безопасности в киберпространстве. По мере роста стратегической значимости киберпространства все больше групп будут пытаться оказывать через него свое влияние. Киберпроблемы стали стратегическими вопросами внешней политики, уже сейчас вызывающими озабоченность всех стран, и жизненно важно, чтобы международное сообщество относилось к ним именно так.

В то время как частотность, масштабы, сложность и серьезность злонамеренных киберинцидентов растут, Организация Объединенных Наций накапливает богатый опыт содействия международному сотрудничеству в целях понимания этих угроз и создания открытого, свободного, безопасного, совместимого и мирного киберпространства.

Все государства-члены Организация Объединенных Наций согласились с тем, что существующее международное право — в том числе Устав Организации Объединенных Наций во всей его полноте — применимо к киберпространству и необходимо для поддержания мира и стабильности, а также для содействия открытой, безопасной, стабильной, доступной и мирной среде информационно-коммуникационных технологий (ИКТ)[3].

Австралия сформулировала свои взгляды на то, как конкретные принципы международного права применяются к поведению государств в киберпространстве (2017 год; 2019 год; 2021 год) и опубликовала гипотетические юридические прецеденты (2020 год). [4]

Международное гуманитарное право (включая принципы гуманности, необходимости, соразмерности и различия) применяется к кибердеятельности в ходе вооруженного конфликта. Международное гуманитарное право предусматривает правила, которые применяются к кибердеятельности в условиях вооруженного конфликта; такая кибердеятельность не является «нападением» или не поднимается до его уровня и включает общие системы, предоставляемые гражданскому населению и частным гражданским лицам для защиты, от угроз, возникающих в результате военных операций.

Международное право прав человека также применяется к поведению государств в киберпространстве. Согласно международному праву прав человека, государства обязаны защищать соответствующие права человека лиц, находящихся под их юрисдикцией, включая право на неприкосновенность частной жизни, когда эти права осуществляются или реализуются через киберпространство или в его рамках.

Признавая уникальные характеристики киберпространства, в 2015 году все государства-члены договорились руководствоваться при использовании ИКТ одиннадцатью добровольными и необязательными нормами ответственного поведения государств в киберпространстве.[5] Эти нормы дополняют — но не заменяют — существующие правовые обязательства государств. Во всей своей совокупности международное право и эти нормы устанавливают ясные параметры

[3] См. резолюции 68/243 и 70/237, а также решение 75/564 Генеральной Ассамблеи.
[4] См. URL: www.internationalcybertech.gov.au/international-security-at-the-un.
[5] См. резолюцию 70/237 Генеральной Ассамблеи.

ответственного поведения государств и тем самым способствуют предсказуемости, стабильности и безопасности.

Все государства также признали необходимость принятия мер укрепления доверия и скоординированного наращивания потенциала. [6] Меры укрепления доверия, призванные предотвратить недопонимание, ведущее к конфликтам, сегодня важны как никогда, и необходимо целенаправленное наращивание потенциала для того, чтобы все страны могли реагировать на вызовы и использовать возможности, появившиеся в результате крепнущих взаимосвязей.

Взятые вместе, эти меры (международное право, нормы, меры укрепления доверия и наращивание потенциала) создают основу безопасного, стабильного и процветающего киберпространства, и их часто называют нормативно-правовой базой Организации Объединенных Наций по вопросам ответственного поведения государств в киберпространстве. Каждый элемент этой нормативно-правовой базы усиливает другие элементы, и ни один элемент нельзя рассматривать изолированно.

Всеобщее одобрение этой нормативно-правовой базы всеми государствами-членами говорит о больших успехах в деле укрепления международного мира и стабильности в киберпространстве[7]. Если положения, заложенные в этой нормативно-правовой базе, будут выполняться, это обеспечит прочную основу для противодействия угрозам, связанным со злонамеренной кибердеятельностью, генерируемой и спонсируемой государствами.

Австралия подтверждает свое обязательство действовать в соответствии с нормативно-правовой базой ответственного поведения государств в киберпространстве, разработанной в сводных докладах групп правительственных экспертов в 2010, 2013, 2015 и 2021 годах[8] и в докладе Рабочей группы открытого состава за 2021 год [9], и призывает все страны сделать то же самое.

Однако небольшое число государственных и спонсируемых государством субъектов все чаще нарушает международное право и нормы, несмотря на вполне понятные ожидания международного сообщества. Тем самым они угрожают международному миру и стабильности.

Нам не нужно больше правил и не нужны новые правила, а нужны соблюдение правил, которые мы уже согласовали, и более высокая степень ответственности за их нарушение. Для предотвращения злонамеренной деятельности надо предусмотреть реальные последствия для тех, кто действует вопреки существующему международному праву и согласованным нормам ответственного поведения государств.

Австралия твердо намерена пресекать, предотвращать и дестимулировать злонамеренную кибердеятельность, особенно со стороны государств и их ставленников. Австралия будет работать с партнерами, чтобы усилить скоординированные меры реагирования на неприемлемое поведение в киберпространстве. Сдерживание вредоносной деятельности укрепляет международную стабильность. Целью австралийской политики киберсдерживания является предотвращение значительных киберинцидентов, которые наносят ущерб интересам Австралии и наших международных партнеров.

Эффективное сотрудничество между государствами и сообществом заинтересованных сторон (включая гражданское общество, частный сектор, научные

[6] Там же.
[7] Решение 75/564 Генеральной Ассамблеи; A/75/816.
[8] A/65/201; A/68/98; A/70/174.
[9] A/75/816.

круги и технических специалистов) оказывает практическое влияние на безопасность, повышает потенциал и создает цикл подкрепляющих друг друга элементов развития, открытости и стабильности в киберпространстве. Зачастую будучи первыми жертвами киберинцидентов, защитниками самой важной инфраструктуры, благодетелями и бенефициарами технического опыта, эволюционирующие интересы негосударственных участников деятельности в киберпространстве создают единую базу для поддержания мирной Интернет-среды.

Гендерное неравенство подрывает глобальный мир, стабильность и безопасность в киберпространстве. Оно провоцирует и часто усугубляет целый ряд проблем, включая бедность, плохое управление, конфликты и насильственный экстремизм. Ценность гендерного равенства и участия женщин в принятии решений, руководстве и миростроительстве, которые связаны с международным миром и безопасностью в киберпространстве, неоспорима. Австралия продолжит принимать значительные меры для поддержки активного и эффективного участия женщин во всех форумах, обсуждающих вопросы международного мира и безопасности в киберпространстве.

Потенциальный ущерб или сбой в работе вследствие злонамеренных кибердействий значителен, и положение дел в этой сфере ухудшается. Нельзя попусту растрачивать растущее внимание и растущую информированность международного сообщества по этим вопросам. Этой возможностью надо воспользоваться, то есть надо углубить понимание того, как международное право применяется в киберпространстве, содействовать практическому выполнению норм ответственного поведения государств и принятию мер по укреплению доверия, координировать наращивание потенциала, с тем чтобы все страны понимали и могли применять базовые положения, и добиться, чтобы были услышаны разные голоса.

Приложение XIX

Заявление Постоянного представительства Австрии при Организации Объединенных Наций

Австрия хотела бы поблагодарить Эстонию, председательствующую в Совете Безопасности в июне 2021 года, за созыв этих открытых дебатов по вопросам международного мира и безопасности в киберпространстве. Австрия присоединяется к заявлению Европейского союза. От нашей страны мы хотели бы добавить следующие ниже замечания.

Сегодня Совет Безопасности впервые рассматривает кибербезопасность как отдельный вопрос, и это отрадное событие. Для поддержания своей значимости и для выполнения своего мандата Совет Безопасности должен продолжать реагировать на современные угрозы международному миру и безопасности.

Растущее число злонамеренных кибердействий умножило угрозы в киберпространстве за последние годы. В современном взаимосвязанном мире, где инфраструктура все больше зависит от цифровых систем управления, последствия кибератак могут иметь такие же, а порой и более серьезные последствия, чем обычные атаки. Эти тенденции в сочетании с трудностями, связанными с присвоением ответственности за кибератаки, делают ситуацию все менее безопасной, увеличивают риск просчетов и возможность человеческой ошибки при принятии решения о том, как реагировать на действия атакующих.

Хотя киберпространство функционирует не так, как физический мир, нельзя заблуждаться относительно одного простого факта: международное право полностью применимо к киберпространству. Это было подтверждено недавно результатами обсуждений в Рабочей группе открытого состава по информационно-коммуникационным технологиям (ИКТ), а также в Группе правительственных экспертов по кибербезопасности, которые консенсусом приняли субстантивные итоговые документы, позволяющие нам лучше понимать проблемы, возникающие перед нами в киберпространстве. Поскольку все больше государств развивают не только оборонительный, но и наступательный киберпотенциал, важно, чтобы все государства при использовании ИКТ придерживались действующего международного права, а также норм ответственного поведения в киберпространстве. Мы надеемся, что эти документы напомнят государствам об их обязательствах и, следовательно, будут способствовать укреплению стабильности в киберпространстве.

Само собой разумеется, что основополагающие положения Устава Организации Объединенных Наций должны служить руководством для поведения всех государств в киберпространстве. В частности, государства обязаны соблюдать запрет на применение силы, который является основой режима международной безопасности. Кроме того, предшествующие группы правительственных экспертов согласовали нормы ответственного поведения государств в киберпространстве, которые были одобрены всеми государствами-членами. Таким образом, ясно, что не отсутствие правил и норм, а их недостаточная реализация усугубляет нестабильность и отсутствие безопасности. Поэтому мы призываем все государства полностью соблюдать международное право и следовать всем нормам ответственного поведения государств.

Если вооруженный конфликт или его элементы присутствуют в киберпространстве, необходимо, чтобы международное гуманитарное право пользовалось уважением и соблюдалось: принципы гуманности, необходимости, соразмерности и различия полностью применимы в киберпространстве.

В контексте пандемии коронавирусного заболевания (COVID-19) мы с тревогой отмечаем участившиеся в последнее время кибератаки на медицинские и оздоровительные учреждения, что является вопиющим нарушением норм, согласно которым самые важные элементы инфраструктуры, в том числе медицинской инфраструктуры, должны всегда быть вне сферы злонамеренной кибердеятельности.

Во избежание конфликтных сценариев необходимо укреплять доверие как имеющее ключевое значение: государства должны конструктивно участвовать в обмене информацией о своем понимании киберпространства и способах военного взаимодействия, чтобы не допускать просчетов. В этом отношении нельзя недооценивать роль региональных организаций, многие из которых проводили мероприятия по укреплению доверия. Мы особенно приветствуем участие Организации по безопасности и сотрудничеству в Европе в решении этих вопросов и убеждены в том, что, опираясь на опыт работы координационных центров по вопросам кибербезопасности, мы также сможем развернуть глобальную сеть на уровне Организации Объединенных Наций.

Хотя государства, международные и региональные организации находятся на переднем крае развития международного права и норм ответственного поведения государств, они не могут сами решить стоящие перед нами задачи. Коммерческие структуры играют важную роль и несут свою долю ответственности в киберпространстве, а гражданское общество и научные круги помогают нам высвечивать различные точки зрения в ходе наших обсуждений. Именно поэтому будущие дискуссии по киберпространству должны проводиться на основе комплексного подхода с участием многих заинтересованных сторон, с тем чтобы все, кто играет роль в поддержании свободного, безопасного, открытого и стабильного киберпространства, были услышаны и внесли свой вклад в достижение наших общих целей.

Несмотря на все успехи, достигнутые в области кибербезопасности, многие открытые вопросы остаются нерешенными, и международному сообществу предстоит найти общие ответы на них. Сотрудничество останется ключевым фактором, и Австрия готова внести конструктивный вклад в соответствующие процессы. Поэтому мы надеемся, что в дальнейшем открытые дебаты в Совете вернутся к прежней практике, позволяющей нечленам Совета выступать с устными заявлениями, чтобы все заинтересованные государства были услышаны.

Приложение XX

Заявление Постоянного представителя Бахрейна при Организации Объединенных Наций Джамаля Фареса ар-Ровайея

[Подлинный текст на арабском языке]

Преобразования в технологической и цифровой областях и появление современных технологий содействуют достижению прогресса, процветанию и развитию всего человечества. Их огромное значение усиливается благодаря опоре на удаленные формы работы, образования и предоставления услуг во всех сферах во время пандемии коронавирусного заболевания (COVID-19) и зависимости от них. Несмотря на множество благ, получаемых благодаря развитию технологий, это сопряжено с многочисленными рисками. Особенно это проявляется в случае отсутствия четко сформулированной системы защиты информационной безопасности и киберпространства, поскольку мы являемся свидетелями различного рода кибератак, нацеленных на базовые инфраструктуры государств и создающих угрозу жизненно важным секторам, институтам и людям.

Организация Объединенных Наций уделяет огромное внимание этому вопросу. Совет Безопасности рассматривал его косвенным образом на нескольких заседаниях, посвященных поддержанию международного мира и безопасности, а также на заседаниях по формуле Аррии. Генеральная Ассамблея также учредила ряд механизмов, в том числе Рабочую группу открытого состава по вопросам безопасности и использованию информационно-коммуникационных технологий (ИКТ) (2021-2025 годы). Эта Группа была учреждена в 2020 году с целью изучения угроз, создаваемых использованием ИКТ в контексте международной безопасности, разработки кодекса поведения государств в киберпространстве, применения международного права к использованию ИКТ, мер укрепления доверия и наращивания потенциала.

В соответствии со своей убежденностью в важности защиты киберпространства от атак и обеспечения интересов государств и народов Бахрейн выступает в поддержку учреждения таких механизмов. Он принимал участие в деятельности Рабочей группы открытого состава по достижениям в сфере ИКТ в контексте международной безопасности, которая завершила свою работу в 2021 году. Бахрейн надеется на активное участие в деятельности недавно созданной рабочей группы.

В контексте большого внимания, которое Бахрейн уделяет вопросу кибербезопасности в свете цифровых преобразований и стремительного развития в сфере ИКТ, он работает над созданием ясной и всеобъемлющей системы регулирования для защиты киберпространства по линии Национального центра кибербезопасности Министерства внутренних дел, который занимается вопросами кибербезопасности в различных областях в Королевстве, а также по линии Управления по вопросам информации и деятельности электронного правительства, которое занимается вопросами защиты информации в сети данных правительства Королевства Бахрейн. Управление регламентации телекоммуникаций занимается вопросами укрепления сотрудничества между государственным и частным секторами с целью обеспечения готовности противостоять угрозам для кибербезопасности.

Бахрейн также занимается разработкой законодательства и правовой базы для обеспечения информационной безопасности с целью защиты людей и институтов. Такое законодательство включает Закон № 30 (2018) о защите

информации и государственных документов и Закон № 60 (2014) о преступлениях в сфере информационных технологий.

На региональном уровне Бахрейн активно участвует в работе Постоянного комитета по вопросам кибербезопасности Совета сотрудничества арабских государств Залива (ССАГЗ). Он предложил создать электронную платформу для обмена информацией и данным по вопросам кибербезопасности между государствами-членами. Каждое государство-член назначило сотрудника по связи для обмена информацией по вопросам кибербезопасности, в том числе об угрозах и передовой практике в этой области.

Королевство Бахрейн ратифицировало Конвенцию Лиги арабских государств о борьбе с преступлениями в области информационных технологий в 2017 году.

В заключение Королевство Бахрейн подтверждает свою поддержку международного сотрудничества в сфере кибербезопасности во имя осуществления чаяний народов мира и обеспечения прогресса, процветания и развития на пути к достижению целей в области устойчивого развития на период до 2030 года.

Приложение XXI

Заявление Постоянного представителя Бельгии при Организации Объединенных Наций Филиппа Криделки

Позвольте мне прежде всего выразить признательность Эстонии, выполняющей функции Председателя, за организацию этих первых открытых дебатов Совета Безопасности по теме мира и безопасности в киберпространстве. Эти своевременные дебаты показывают неотложность решения этой проблемы и актуальность участия в этом Совета Безопасности. Риски, возникающие в результате злонамеренной деятельности в киберпространстве, действительно растут, а их влияние на международный мир и безопасность сейчас как никогда пагубно. Поэтому крайне важно подтвердить приверженность государств-членов международному праву и базовым положениям об ответственном поведении государств как ключевым элементам предотвращения конфликтов и поддержания мира и безопасности в киберпространстве.

Достижение этой цели требует как общего международного понимания управления киберпространством, так и практических действий по реализации этой концепции.

Международные дебаты о регулировании киберпространства находятся на решающем этапе. Бельгия твердо поддерживает нынешние дебаты в Организации Объединенных Наций, в том числе в Первом комитете, в различных рабочих группах открытого состава и группах правительственных экспертов.

Ниже указаны ключевые элементы.

Во-первых, Бельгия выступает за общее понимание глобального, свободного, открытого, стабильного, мирного и безопасного киберпространства, где применяются нормы, касающиеся прав человека, основных свобод и верховенства права. Это общее понимание основано на всеобъемлющем подходе, при котором все заинтересованные стороны, включая гражданское общество, частный сектор и научные круги, услышаны.

Во-вторых, международное сообщество должно продолжать стремиться к разработке действительно универсальной нормативно-правовой базы кибербезопасности для обеспечения ответственного поведения государств. Главные положения этой нормативно-правовой базы должны быть основаны на полном применении действующего международного права — включая Устав Организации Объединенных Наций во всей его полноте, — международного гуманитарного права и международного права прав человека. В прошлом году Бельгия в качестве непостоянного члена Совета Безопасности приняла участие в заседании Совета Безопасности по формуле Аррии, посвященном кибератакам на самые важные объекты инфраструктуры. Кибератаки, направленные на важнейшие элементы инфраструктуры, подвергают риску человеческие жизни и должны быть осуждены международным сообществом. Кибератаки на медицинские учреждения, такие как больницы, недопустимы.

Что касается нормативно-правовой базы Организации Объединенных Наций по вопросам ответственного поведения государств в киберпространстве, то необходимо подчеркнуть, что государства-члены Организации Объединенных Наций одобрили — посредством принятия резолюции 70/237 Организации Объединенных Наций — выводы докладов Группы правительственных экспертов 2010, 2013 и 2015 годов, которые представляют собой прочную и одобренную консенсусом основу для дальнейшей работы. Организация Объединенных Наций и ее государства-члены предприняли значительные усилия как для формирования общего международного понимания управления киберпростран-

ством, так и для разработки практических действий по реализации этой общей концепции. В эффективной многосторонней системе настоятельно необходимо, чтобы любое дальнейшее обсуждение начиналось с этой консенсусной основы во избежание пересмотра компромиссов, достигнутых ранее с таким трудом, и во избежание блокировки будущих усилий.

В-третьих, мы считаем, что нам следует лучше согласовывать международное уголовное правосудие с вызовами XXI века. Вот почему Бельгия поддержала инициативу Лихтенштейна по учреждению Совета консультантов по распространению действия Римского статута на войну в киберпространстве, с тем чтобы изучить роль, которую Международный уголовный суд мог бы играть в контексте этой новой нормативной базы. Мы с интересом ожидаем заключительного доклада Совета консультантов, представление которого запланировано на этот год.

Чтобы изменить сложившуюся ситуацию, за разработкой руководящих принципов должны последовать действия. В связи с этим Бельгия убеждена в том, что предложение Египта и Франции о разработке программы действий является правильным шагом на пути к реализации нашей концепции. Бельгия с гордостью поддерживает эту инициативу вместе с более чем 50 другими странами, и мы надеемся, что к ней присоединятся многие другие государства.

На национальном уровне Бельгия совсем недавно, в мае 2021 года, приняла новую Национальную стратегию кибербезопасности 2.0 на 2021–2025 годы, в которой изложен комплексный подход нашей страны к повышению киберустойчивости и борьбе с киберугрозами. Основная цель этой национальной стратегии — «вывести Бельгию в число наименее уязвимых стран Европы».

Политика кибербезопасности Бельгии также предусматривает новый механизм присвоения ответственности, который задуман как инструмент сдерживания. Если мы хотим эффективно предотвращать и сдерживать злонамеренную кибердеятельность в условиях, когда кибератаки становятся все более многочисленными и сложными, то официальное присвоение ответственности за злонамеренную кибердеятельность, направленную на одну из жизненно важных организаций в Бельгии, является важным инструментом. Национальную процедуру присвоения ответственности тоже можно использовать с целью поддержки дружественной нам страны, пострадавшей от аналогичных атак.

Кроме того, национальная стратегия устанавливает ясные международные обязательства. И это потому, что Бельгия переходит от слов к делу, будучи убежденной в необходимости расширения международного сотрудничества для обеспечения безопасности и стабильности в киберпространстве.

Расширение международного сотрудничества также означает наращивание потенциала и более активную поддержку мер укрепления доверия, в том числе благодаря усилиям региональных организаций, таких как Организация по безопасности и сотрудничеству в Европе (ОБСЕ). Бельгия принимает активное участие в работе ОБСЕ, цель которой — придать этим мерам укрепления доверия конкретный и практический характер. Что касается наращивания потенциала, то в глобальном масштабе потребности являются важными и неотложными. Существующие программы сотрудничества или наращивания потенциала, такие как программы, предлагаемые Европейским союзом или Глобальным форумом по обмену опытом в области компьютерных технологий, надо укреплять и расширять. Мы все заинтересованы в повышении глобальной устойчивости перед лицом киберугроз.

Приложение XXII

Заявление Постоянного представительства Бразилии при Организации Объединенных Наций

Прежде всего я хотел бы поздравить Эстонию с прекрасной инициативой — впервые провести официальные открытые дебаты Совета Безопасности по теме кибербезопасности в более широком контексте поддержания международного мира и безопасности. Быстрое развитие информационно-коммуникационных технологий (ИКТ), которые проникли во все сферы жизни человека, заставляет нас обновить концепцию угроз, адаптировать существующую нормативную базу к этой новой реальности и разработать новые модели ответственного поведения государств, с тем чтобы решить современные проблемы и пресечь возникновение конфликтов.

Хотя тема кибербезопасности только недавно была поднята в этом органе, несущем главную ответственность за поддержание международного мира и безопасности, государства-члены обсуждают ее уже более двух десятилетий — как минимум, с 1998 года, когда эта тема была впервые включена в повестку дня Генеральной Ассамблеи. В этот период мы стали свидетелями консенсусного принятия четырех докладов групп правительственных экспертов — в двух из них председателями были бразильские эксперты — и одного доклада Рабочей группы открытого состава, который тоже был принят консенсусом. В совокупности эти документы образуют *acquis*, то есть общий свод толкований и необязательных, добровольных норм, правил и принципов, которые помогают регулировать использование ИКТ государствами.

Одним из важнейших вкладов этого свода документов в поддержание международного мира и безопасности является утверждение о том, что международное право, включая международное гуманитарное право, применимо к киберпространству. В нашем добровольном национальном вкладе в официальное собрание документов последней Группы правительственных экспертов мы подтвердили твердую убежденность Бразилии в том, что при использовании информационно-коммуникационных технологий государства должны соблюдать положения международного права, в том числе Устава Организации Объединенных Наций, международного права прав человека и международного гуманитарного права. Организация Объединенных Наций и региональные организации признали, что международное право, и, в частности, Устав Организации Объединенных Наций, применимо к киберпространству и имеет большое значение для поддержания мира и стабильности и для создания открытой, безопасной, мирной и доступной среды информационно-коммуникационных технологий. Таким образом, в ходе нынешних дискуссий вопрос заключается уже не в том, применимо ли международное право к использованию ИКТ государствами, а в том, как оно применяется.

Хотя аналогии с физическим миром могут по большей части работать для определения такого применения, уникальные характеристики киберпространства создают новые ситуации, для регулирования которых международное право изначально не предназначалось. Взаимосвязанность информационных систем, нематериальный характер среды ИКТ и сложность проблемы присвоения ответственности за злонамеренные и наступательные действия в киберпространстве, среди прочих факторов, ставят новые задачи перед международным правом, развитие которого основывалось на физическом и территориальном международном порядке.

Различия в интерпретации государствами того, как международное право применяется к использованию ИКТ, повышают риск непредсказуемого поведе-

ния, недопонимания и эскалации напряженности. Поэтому важно постепенно выявлять области сближения позиций государств в этом вопросе, а в случае выявления расхождений совместно работать над повышением согласованности в толковании существующих правил. При необходимости следует также рассмотреть возможность разработки дополнительных норм в качестве средства заполнения потенциальных правовых пробелов и устранения остающихся неопределенностей.

Поддержание международного мира и безопасности в значительной степени зависит от уровня доверия между государствами. Поэтому, помимо признания применимости международного права и установления и реализации норм, правил и принципов ответственного поведения государств, первостепенное значение имеет осуществление правительствами мер укрепления доверия. Создание сети координационных центров на техническом и политическом уровнях, а также обмен национальными данными об угрозах и методах реагирования на инциденты в сфере ИКТ являются важными мерами сотрудничества и обеспечения транспарентности. Эти инициативы не только помогают предотвратить недопонимание и неправильное восприятие, но и полезны, когда надо реагировать на серьезные инциденты в сфере ИКТ и уменьшать напряженность в кризисных ситуациях.

Наращивание потенциала — это еще один важный инструмент создания мирной среды ИКТ. Как и в других сферах, неравенство между странами может порождать отсутствие безопасности и в киберпространстве, оказывая прямое воздействие на кинетический мир. Международное сотрудничество в деле развития национальных институтов, людских ресурсов и государственной политики способствует снижению уязвимости государств и имеет огромное значение для универсализации имплементации международного права и норм, правил и принципов ответственного поведения государств в киберпространстве. Если пандемия и научила нас чему-то, так это тому, что никто не будет в безопасности, пока все не будут в безопасности, причем ту же самую логику можно применить и к тесно взаимосвязанному и взаимозависимому киберпространству.

Поскольку в киберпространстве действуют многие заинтересованные стороны, Бразилия считает, что эффективное обсуждение вопросов кибербезопасности не может быть успешным без участия гражданского общества, научных кругов и частного сектора. Участие многих заинтересованных сторон необходимо для выявления угроз и борьбы с ними, для предотвращения конфликтов, достижения общего понимания, повышения киберустойчивости и развития сотрудничества. Более широкое взаимодействие между государственными и частными субъектами из разных стран и обмен опытом и передовой практикой имеют большое значение для создания более открытой, безопасной, мирной и доступной среды ИКТ.

Бразилия активно участвует в дискуссиях по кибербезопасности в Организации Объединенных Наций. Мы всегда занимали активную позицию как в Группе правительственных экспертов, так и в последней Рабочей группе открытого состава. Бразилия будет и в дальнейшем конструктивно подходить к дебатам в новой Рабочей группе открытого состава, которая проведет свою первую основную сессию в декабре, а также в других механизмах регулярного институционального диалога, которые могут быть созданы, таких как программа действий по кибербезопасности. В то же время, недавно став избранным непостоянным членом Совета Безопасности, мы намерены внести свой вклад в проходящие в этом органе дискуссии о влиянии использования ИКТ в контексте международной безопасности. По мнению Бразилии, Совет должен руководствоваться прежде всего установкой на содействие выполнению предыдущих и будущих рекомендаций Генеральной Ассамблеи, касающихся кибербезопасности.

Приложение XXIII

Заявление Постоянного представительства Канады при Организации Объединенных Наций

[Подлинный текст на французском языке]

Мы благодарим Эстонию за организацию этого заседания Совета Безопасности по столь своевременной и актуальной теме. Канада рада возможности внести свой вклад в эту дискуссию.

Мир все больше зависит от цифровых технологий и Интернета. Угрозы международному миру и безопасности, исходящие из киберпространства, многочисленны. Вмешательство в демократические процессы — одна из областей, вызывающих особую озабоченность. Другая область — недавнее увеличение числа инцидентов, связанных с вымогательством. Поэтому мы должны продолжать предпринимать шаги по поддержанию свободного, открытого и безопасного киберпространства.

Согласованная нормативно-правовая база ответственного поведения государств в киберпространстве является для него основой мира и стабильности. Эти базовые положения включают признание применимости международного права к киберпространству, соблюдение согласованных на международном уровне норм, наращивание потенциала и использование мер укрепления доверия. В совокупности эти элементы снижают риски эскалации и конфликта.

Эта нормативно-правовая база была подтверждена в одобренных консенсусом докладах, недавно принятых Рабочей группой открытого состава и Группой правительственных экспертов Организации Объединенных Наций. Все государства-члены Организации Объединенных Наций обязались руководствоваться этими базовыми положениями.

Международное право жизненно важно для обеспечения того, чтобы основанный на правилах международный порядок распространялся на киберпространство. В последних докладах Рабочей группы открытого состава и Группы правительственных экспертов была подтверждена применимость международного права к киберпространству и отмечены достигнутые большие успехи в этом направлении. В докладе Рабочей группы открытого состава рекомендуется расширить сотрудничество в области укрепления международного права, чтобы больше государств могли разработать свои национальные подходы, а также общую концепцию. В докладе Группы правительственных экспертов была подтверждена применимость международного права, а международное гуманитарное право было особо упомянуто.

В докладе Группы правительственных экспертов, опубликованном в мае 2021года, содержится руководство по реализации одиннадцати добровольных норм ответственного поведения государств. Эти нормы были приняты Группой правительственных экспертов Организации Объединенных Наций в 2015 году и одобрены всеми государствами-членами в резолюции 70/237 Генеральной Ассамблеи Организации Объединенных Наций. Канада считает, что этих согласованных норм и международного права в основном достаточно для того, чтобы направлять поведение государств в киберпространстве. Однако еще предстоит выполнить работу по их распространению и внедрению. Например, недавние громкие инциденты с попытками вымогательства, совершенными преступными группами. Они привели к большим сбоям в работе ключевых отраслей, таких как энергетика и снабжение продовольствием. Они также негативно повлияли на финансовые рынки.

Хотя ответственность за эти действия несут преступные группы, эти примеры подчеркивают важность международного права и одиннадцати норм Группы правительственных экспертов. Многие из этих норм прямо или косвенно касаются угроз, которые ИТК создают для важнейших объектов инфраструктуры. Одна из норм предусматривает, что «государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, важнейшая инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ». Другая норма гласит: «Государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с применением ИКТ».

Группы, которые совершают преступные действия, включая нападения, связанные с рассылкой вирусов-вымогателей, живут и работают в государствах. Они пользуются цифровой инфраструктурой этих государств, чтобы совершать такие действия, и подпадают под их юрисдикцию. Получив информацию о вредоносной деятельности, исходящей с их территории, государства обязаны реагировать, обеспечивая соблюдение своих законов и сотрудничая с другими государствами. Согласившись руководствоваться нормами Группы правительственных экспертов, мы все обязались это делать. Именно поэтому все больше государств принимают строгие законы по борьбе с киберпреступностью. Во многих случаях государства основывают свои законы на Будапештской конвенции о киберпреступности, участниками которой сегодня являются представители всех регионов мира.

Судя по недавним ситуациям, не все государства, к сожалению, и не всегда соблюдают положения нормативно-правовой базы об ответственном поведении государств. Некоторые из них позволяют киберпреступникам совершенно безнаказанно действовать со своей территории. Другие используют своих ставленников или умышленно занимаются злонамеренной кибердеятельностью, которая противоречит вышеупомянутым базовым положениям. Несколько раз Канада вместе со своими международными партнерами осуждала эти действия и реагировала на угрозы для мира и международной безопасности.

Канада была одной из 27 стран, подписавших в сентябре 2019 года Совместное заявление о поощрении ответственного поведения государств в киберпространстве. Подтвердив базовые положения об ответственном поведении государств, мы обязались «работать вместе на добровольной основе для привлечения государств к ответственности, когда они действуют вразрез с этими базовыми положениями, в том числе путем принятия транспарентных мер, которые соответствуют международному праву».

Именно так мы и поступаем и будем продолжать это делать. Важно показывать случаи неправомерного поведения, чтобы обеспечить выполнение утвержденных базовых положений об ответственном поведении государств в киберпространстве. Мы призываем всех это делать.

Что касается перспектив Организации Объединенных Наций, то Канада надеется на конструктивное участие в деятельности Рабочей группы открытого состава 2021-2025 годов. Мы также внесем свой вклад в разработку программы действий Организации Объединенных Наций по кибербезопасности. Канада является одним из спонсоров этой программы действий, поскольку, на наш взгляд, эта программа может служить полезным, ориентированным на практическую работу форумом для содействия выполнению базовых положений об ответственном поведении государств.

Успех этих двух процессов будет зависеть от их способности учитывать различные мнения и ракурсы, чтобы претворять их в свои методы и результаты

работы. В рамках Рабочей группы открытого состава Канада выступала за активное участие неправительственных заинтересованных сторон. Дело в том, что гражданское общество, научные круги, технические специалисты и частный сектор могут внести большой вклад в эти обсуждения, поскольку они играют важную роль в выполнении рекомендаций Группы правительственных экспертов и Рабочей группы открытого состава. Мы будем выступать также за активное участие заинтересованных сторон в осуществлении программы действий и — по ходу дела — в ее разработке.

Кроме того, важно следить за тем, чтобы голоса женщин были услышаны, будь то в рамках Рабочей группы открытого состава или программы действий. Гендерные вопросы должны учитываться в ходе этих двух процессов с самого начала, чтобы обе эти группы занимались гендерными аспектами кибербезопасности. Есть убедительные документальные доказательства того, что процессы посредничества в конфликтах, проходящие с активным участием женщин, приводят к гораздо более весомым результатам и снижают вероятность возобновления войны.

Киберпроцессы Организации Объединенных Наций можно аналогичным образом усилить, обеспечив активное участие женщин в них. Всеобщий охват имеет большое значение для успеха обоих процессов.

Одним словом, Канада остается твердым приверженцем базовых положений об ответственном поведении государств в киберпространстве. Мы будем продолжать содействовать выполнению рекомендаций предыдущих групп правительственных экспертов и недавно созданной Рабочей группы открытого состава. Мы также будем сурово осуждать злонамеренные кибердействия, которые противоречат установленным базовым положениям, и будем реагировать на такие действия. Мы надеемся на дальнейшее сотрудничество с международным сообществом в целях укрепления международного мира и безопасности путем повышения стабильности и безопасности в киберпространстве.

Приложение XXIV

Заявление Постоянного представительства Чили при Организации Объединенных Наций

Чили подтверждает свою позицию, согласно которой международное право, и в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира и стабильности и содействия открытой, безопасной, стабильной, доступной и мирной среде информационно-коммуникационных технологий (ИКТ). Этот принцип, наряду с конкретными принципами Устава Организации Объединенных Наций, в частности мирным разрешением споров, запретом прибегать к угрозе силой или ее применению против территориальной целостности или политической независимости любого государства, невмешательством во внутренние дела других государств и уважением прав человека и основных свобод, неделим как в физической, так и в цифровой сферах, и поэтому Чили будет продолжать содействовать его применению.

Вредоносная деятельность в сфере ИКТ со стороны источников постоянных угроз, включая государства и других субъектов, может серьезно угрожать международной безопасности и стабильности, социально-экономическому развитию, а также безопасности и благополучию людей. Злонамеренная деятельность против важнейших объектов инфраструктуры, предоставляющих услуги на национальном, региональном или глобальном уровне, становится все более опасной и включает вредоносную деятельность ИКТ, затрагивающую такие важнейшие элементы инфраструктуры, как информационная инфраструктура, базовые системы обслуживания населения, технические системы, необходимые для обеспечения общей доступности или работоспособности Интернета, и медицинские учреждения. В ходе будущих конфликтов эта вредоносная деятельность может стать еще более пагубной и может серьезно повлиять на благополучие и жизнь людей. Поэтому страны могут серьезно пострадать от кибератак, совершаемых в условиях вооруженных конфликтов.

Во время вооруженных конфликтов государства должны планировать, проводить и направлять свои операции в киберпространстве, строго соблюдая нормы международного права, уделяя особое внимание международному праву прав человека и международному гуманитарному праву.

Чили полностью поддерживает работу Группы правительственных экспертов и ее доклады и рекомендации, принятые в 2010, 2013, 2015 и 2021 годах, поскольку они олицетворяют собой огромные достижения в сфере международного права, норм и мер укрепления доверия в области ИКТ. Чили также поддерживает Рабочую группу открытого состава и ее рекомендации. Для сокращения масштабов злонамеренного использования кибервозможностей и создания более стабильного киберпространства важно следовать этим рекомендациям и выполнять их на всех уровнях.

Программа действий по поощрению ответственного поведения государств в киберпространстве — это позитивная, конструктивная и реалистичная инициатива, которая может помочь нам идти вперед и достичь конкретных результатов в сфере ИКТ. Эта программа действий может стать постоянным, всеобъемлющим, консенсусным и практическим международным инструментом для обеспечения ответственного поведения при использовании ИКТ в контексте международной безопасности. Будучи одним из спонсоров этой инициативы, Чили считает, что эта программа действий станет платформой для принятия практических рекомендаций, содействия международному сотрудничеству и развития программ помощи с учетом потребностей государств-бенефициаров, в том числе в наращивании потенциала.

Что касается соблюдения действующего международного права и реализации норм ответственного поведения государств в киберпространстве, то важно, чтобы государства могли развивать и доводить до сведения других государств свои взгляды на то, как международное право применяется в киберпространстве. Наращивание потенциала в этой области также имеет огромное значение. Разработка руководящих принципов по применению норм является важным шагом, который должен помочь государствам продвинуться в этом вопросе. Региональные организации могут играть ключевую роль в оказании помощи государствам в осуществлении ими норм и соблюдении международного права, разработке региональных стратегий в этой области, а также в обучении и наращивании потенциала.

Чили считает необходимым усиливать меры по укреплению доверия в киберпространстве и наращивать потенциал, и здесь региональные организации должны играть видную роль. В связи с этим мы отмечаем усилия Организации американских государств, предпринимаемые в рамках ее Рабочей группы по сотрудничеству и мерам укрепления доверия в киберпространстве, а также работу и успехи Организации по безопасности и сотрудничеству в Европе и Ассоциации государств Юго-Восточной Азии.

Важно развивать диалог между регионами по этому вопросу, а также по вопросам наращивания потенциала и соблюдения установленных норм. В рамках этого диалога следует рассмотреть возможность обмена опытом, информацией, инструкциями, передовой практикой и извлеченными уроками, а также возможность приглашения членов организаций к участию в этих региональных процессах. Государства должны укреплять свои национальные координационные центры, а также повышать роль своих министерств иностранных дел в разработке политики в области киберпространства и ИКТ. Кибердипломатия — важный инструмент, который может помочь государствам развивать сотрудничество между ними на основе укрепления доверия. Государствам следует также рассмотреть возможность создания двусторонних механизмов для диалога и сотрудничества по вопросам кибербезопасности и киберпространства.

Чили полагает, что многосторонние процессы должны быть в максимально возможной степени всеобъемлющими и транспарентными. В обсуждении вопросов ИКТ должны участвовать частный сектор, научные круги, гражданское общество, представители промышленности и технические специалисты. Невозможно создать стабильное и безопасное киберпространство, если мы не гарантируем участие и работу всех заинтересованных сторон. Чем больше будет участников обсуждения, тем больше вероятность достижения результатов, полезных для всех. Поэтому мы считаем необходимым, чтобы мы могли выслушать все заинтересованные стороны, и чтобы они также могли изложить свои мнения и внести свой вклад в работу на официальных заседаниях. Это означает, что государствам надо привлекать все заинтересованные стороны к разработке политики, стратегий и других инициатив, направленных на предотвращение конфликтов, формирование общего понимания и повышение киберустойчивости.

Приложение XXV

Заявление Постоянного представительства Чешской Республики при Организации Объединенных Наций

Чешская Республика выражает признательность Эстонской Республике за проведение поистине исторических первых открытых дебатов Совета Безопасности по теме кибербезопасности в контексте международного мира и безопасности. Соблюдение государствами международного права и ответственное поведение государств в киберпространстве являются ключевыми элементами предотвращения конфликтов и поддержания международного мира и безопасности.

Чешская Республика присоединяется к заявлению Европейского союза и хотела бы особо выделить еще два момента.

Существующие и возникающие киберугрозы международному миру и безопасности

Киберпространство предлагает огромные блага для развития человеческого потенциала и экономики, однако оно также становится областью растущей зависимости и проблем в сфере безопасности. Наша возросшая зависимость от информационно-коммуникационных технологий (ИКТ) во время пандемии коронавирусного заболевания (COVID-19), которая постоянно используется злоумышленниками в их интересах, является наглядным напоминанием о все более острых проблемах в киберпространстве. В частности, мы наблюдаем тревожный рост вредоносных действий в сфере ИКТ, направленных против важнейших объектов инфраструктуры, оказывающих основные услуги населению, в том числе против медицинских учреждений, объектов водоснабжения, энергоснабжения и канализации, против избирательной системы и вообще против систем обеспечения всеобщей доступности Интернета. Так, растущее число кибератак, нарушающих работу медицинских учреждений, приводит к гибели людей, подрывает нашу коллективную способность реагировать на COVID-19 и в конечном счете угрожает международному миру и стабильности.

Такие безрассудные действия в сфере ИКТ, направленные на преднамеренное повреждение важнейшей инфраструктуры, также чреваты возможными страшными гуманитарными последствиями, а если они приписываются какому-либо государству, то они равносильны нарушениям обязательств государств по международному праву. Поэтому Чешская Республика приветствует тот факт, что все государства-члены недавно подтвердили в заключительных докладах Группы правительственных экспертов и Рабочей группы открытого состава, что деятельность в сфере ИКТ, направленная против важнейшей инфраструктуры, неприемлема. Хотя политическая приверженность является первым необходимым условием, защита самой важной инфраструктуры от угроз ИКТ также потребует постоянных практических усилий со стороны международного сообщества, в том числе посредством активизации технического сотрудничества и конкретных программ по наращиванию киберпотенциала. Совет Безопасности также может сыграть очень важную роль, обеспечив, чтобы спонсируемая государством деятельность в сфере ИКТ, направленная против важнейших объектов инфраструктуры, имела последствия.

Новые и только возникающие киберугрозы влияют на национальную безопасность государств, а также все больше угрожают благополучию и безопасности конкретных людей. Чешская Республика особенно озабочена растущим политическим расколом между государствами, пропагандирующими защиту личных свобод в киберпространстве, и государствами, призывающими к усилению

слежки с помощью технических средств. По нашему мнению, расширение массовой слежки с помощью ИКТ, частичное или полное отключение Интернета и широко распространенная цензура контента вызывают серьезные опасения в отношении прав человека. Необходимы решительные действия по защите граждан от произвольного и незаконного осуществления государственной власти в киберпространстве. Эти тенденции в сочетании с потенциальными рисками, связанными с внедрением искусственного интеллекта в различные аспекты нашей жизни, порождают новые проблемы безопасности, способны подорвать доверие и уверенность в сфере киберпространства и в конечном счете могут негативно сказаться на нашей способности поддерживать международный мир и безопасность.

Более эффективное обеспечение соблюдения международного права и норм ответственного поведения государств

Чешская Республика хотела бы еще раз подчеркнуть, что соблюдение государствами своих обязательств по международному праву является необходимым условием поддержания свободного, мирного, стабильного, безопасного, взаимосвязанного и доступного киберпространства. Применимость существующего международного права к использованию государством ИКТ была подтверждена всеми государствами, в частности, путем всеобщего одобрения докладов Группы правительственных экспертов 2013 и 2015 годов в резолюциях 68/243 и 70/237 Генеральной Ассамблеи.

В связи с этим Чешская Республика также напоминает, что права государств на осуществление исключительной юрисдикции в отношении ИКТ, находящихся на их территории, предполагают наличие не только прав, но и конкретных обязательств по международному праву. В частности, Чешская Республика хотела бы подтвердить, что существующие правовые базы, включая международное гуманитарное право и международное право прав человека, применяются к поведению государств в киберпространстве без каких-либо исключений.

К сожалению, незначительное меньшинство государств продолжает сомневаться в применимости существующего международного права к киберпространству, включая применимость международного гуманитарного права к использованию ИКТ в контексте вооруженного конфликта. Чешская Республика хотела бы подчеркнуть, что, по ее мнению, применимость международного гуманитарного права к операциям ИКТ не способствует милитаризации киберпространства, равно как и милитаризации любой другой области. Напротив, международное гуманитарное право накладывает ограничения на применение силы, требуя, чтобы все применяемые средства и методы ведения войны в контексте вооруженного конфликта соответствовали его правилам, включая принципы гуманности, различия и принцип соразмерности.

Кроме того, Чешская Республика напоминает, что в соответствии с правовыми положениями об ответственности за международно-противоправные деяния все государства обязаны проявлять должную осмотрительность и принимать конкретные меры в рамках своих возможностей для обеспечения того, чтобы их территория не использовалась для проведения злонамеренной кибердеятельности против других государств.

Чешская Республика также признает, что способность государства реализовать существующие базовые положения об ответственном поведении государства в киберпространстве, включая его способность адекватно проявлять должную осмотрительность, неразрывно связана с возможностями этого государства. В связи с этим Чешская Республика подчеркивает необходимость активизации международных усилий по наращиванию киберпотенциала и повышению

киберустойчивости на глобальном уровне, в том числе путем скорейшей разработки программы действий Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве, которая позволит государствам-членам продвигать выполнение существующих обязательств посредством практических действий, ориентированных на результат.

В заключение следует отметить, что Чешская Республика безоговорочно привержена подходу к кибербезопасности, ориентированному на человека, который подчеркивает необходимость защиты безопасности людей в среде ИКТ, будь то защита самой важной инфраструктуры от угроз ИКТ или обеспечение того, чтобы меры кибербезопасности не использовались в качестве предлога для ограничения полного осуществления прав человека и основных свобод в киберпространстве.

Приложение XXVI

Совместное заявление постоянных представительств Дании, Исландии, Норвегии, Финляндии и Швеции при Организации Объединенных Наций

Я имею удовольствие выступать от имени стран Северной Европы: Исландии, Норвегии, Финляндии, Швеции и моей страны — Дании. Мы благодарны Эстонии, выполняющей функции Председателя, за включение этой очень актуальной темы в повестку дня Совета. Это прекрасная возможность для всех государств-членов укрепить нашу приверженность применению международного права в киберпространстве и базовых положений об ответственном поведении государств в киберпространстве с целью содействия миру и стабильности.

Развитие информационных и телекоммуникационных технологий приносит миру бесчисленные блага. Оно принесло с собой огромный экономический прогресс и социальное развитие. В условиях нынешней пандемии киберпространство позволило многим из нас оставаться на связи с семьей, друзьями и коллегами и поддерживать важные функции общества, включая работу важнейших объектов инфраструктуры, жизненно необходимых для преодоления кризиса в области здравоохранения. Но в то же время киберпространство использовалось для распространения дезинформации о коронавирусном заболевании (COVID-19), обнажая нашу коллективную подверженность нарушениям и злоупотреблениям в информационном пространстве. Более того, пандемия выявила глубокие цифровые пропасти, и не в последнюю очередь цифровую пропасть между мужчинами и женщинами. Мы, представители Северной Европы, твердо убеждены в том, что доступное, свободное, открытое и безопасное глобальное киберпространство исключительно важно не только для функционирования современного мира, но и для исполнения наших общих надежд на построение более светлого, более экологически чистого и более безопасного будущего.

К сожалению, злонамеренная кибердеятельность по-прежнему бросает вызов безопасности и стабильности киберпространства. Последние полтора года показали, что государственные и негосударственные субъекты пользуются любой возможностью, даже глобальной пандемией, для осуществления вредоносной деятельности в киберпространстве. Подобные действия недопустимы. Они угрожают целостности, безопасности и процветанию наших обществ и подрывают международный мир и стабильность.

Позвольте мне обозначить три взаимосвязанные тенденции, которые бросают вызов международному миру и безопасности.

Во-первых, участившиеся в последнее время кибератаки на цепочки поставок компаний, организаций и правительств привели к тому, что десятки, если не сотни тысяч, компьютерных систем оказались незащищенными. Такие атаки демонстрируют вопиющее пренебрежение к пострадавшим. Нередко целью является кража конфиденциальной информации и интеллектуальной собственности для получения преимуществ в геополитической конкуренции. Такие атаки могут иметь и другие непредвиденные последствия, поскольку пути обхода системы защиты остаются открытыми для всех желающих.

Во-вторых, спонсируемые государством губительные кибератаки, такие как “WannaCry” и “NotPetya”, обрушились на мир при полном безразличии к их негативным системным последствиям на глобальном уровне. Такие атаки привели не только к огромным финансовым потерям, но и к нарушению работы систем ИКТ, в том числе в больницах и промышленных системах управления,

влияющих на исключительно важные поставки электроэнергии. Эта деятельность ставит под угрозу здоровье и безопасность наших граждан.

В-третьих, государства должны принять меры по противодействию исходящей с их территории киберпреступности со все более серьезными и дестабилизирующими последствиями, Недавние атаки с применением вирусов-вымогателей на поставки топлива в США, больницы в Ирландии и предприятия по производству продуктов питания в Бразилии, США и Австралии свидетельствуют о том, что последствия киберпреступлений стали проблемой для национальной безопасности и могут повлиять на международный мир и безопасность. Растущее слияние государственных и негосударственных групп еще больше усложняет эту угрозу.

С каждым днем порог допустимого поведения в киберпространстве продолжает снижаться до неприемлемого уровня. Мы должны обратить эту тенденцию вспять, выполнив общее обязательство, которое мы, государства-члены, взяли на себя, когда одобрили доклады Группы правительственных экспертов и принятый консенсусом доклад Рабочей группы открытого состава. В связи с этим мы еще раз подтверждаем, что международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека, применимо к поведению государств в киберпространстве. Мы также призываем к более строгому соблюдению 11 добровольных необязательных норм ответственного поведения государств в киберпространстве, сформулированных в докладе Группы правительственных экспертов 2015 года, принимая во внимание рекомендации и дополнительные толкования этих норм, содержащиеся в докладе Группы правительственных экспертов 2021 года. Это в значительной степени способствовало бы решению вышеупомянутых проблем.

Мы должны строже наказывать за злонамеренную кибердеятельность, коллективно привлекая виновных к ответственности. Все государства должны проявлять должную осмотрительность и принимать соответствующие меры для борьбы с вредоносной кибернетической деятельностью, исходящей с их территории. Хакерским группам нельзя позволять действовать безнаказанно.

Мы поддерживаем продолжение обмена информацией и передовым опытом в Организации Объединенных Наций, в частности по вопросам реализации норм ответственного поведения государств, мер укрепления доверия и применения действующего международного права в киберпространстве. Нам следует идти по пути практических действий, опираясь на согласованные базовые положения, одобренные Генеральной Ассамблеей, когда она утвердила доклад Рабочей группы открытого состава и доклады Группы правительственных экспертов. Это является основой для любого дальнейшего обсуждения. Предложение о разработке программы действий открывает перед нами хорошие перспективы продвижения к полному выполнению уже согласованных норм.

Мы должны признать, что, хотя киберугроза — это глобальная проблема, в разных странах и регионах она проявляется по-разному. Упрочение киберустойчивости во всех наших обществах имеет огромное значение не только для нашей общей безопасности, но и для осуществления прав человека. Нам надо сотрудничать для наращивания потенциала в глобальном масштабе.

Государства не могут делать это в одиночку. Противодействие угрозам в киберпространстве требует участия многих заинтересованных сторон для предотвращения конфликтов, формирования общего понимания, укрепления доверия и наращивания потенциала. Организация Объединенных Наций нужна нам как организатор и платформа для налаживания эффективного сотрудни-

чества между правительствами, гражданским обществом, научными кругами и частным сектором. Мы поддерживаем «дорожную карту» Генерального секретаря по цифровому сотрудничеству, в частности, когда речь идет о привлечении частного сектора, что жизненно необходимо для управления важнейшей инфраструктурой, для сбора информации и защиты систем и персональных данных.

Все государства должны выполнять свои обязательства, соблюдать международное право и уважать нормы в киберпространстве. Если этого не делать, то масштабы угрозы со стороны злонамеренной кибердеятельности для международного мира и безопасности будут продолжать расти. Кибератаки будут продолжать повышать риски возникновения конфликтов, подвергать опасности человеческие жизни, нарушать права человека, подавлять экономическую деятельность, углублять разделительные линии и провоцировать споры. Все государства должны сыграть свою роль в создании и поддержании основанного на правилах, предсказуемого, открытого, равноправного, свободного, доступного, стабильного и безопасного киберпространства на благо всех.

Приложение XXVII

Заявление Постоянного представителя Эквадора при Организации Объединенных Наций посла Кристиана Эспиносы

[Подлинный текст на испанском языке]

Прежде всего позвольте мне поблагодарить Эстонию за включение этой темы в официальную повестку дня Совета Безопасности после того, как в течение одного года было проведено заседание по формуле Аррии, посвященное этой теме. Кроме того, мы отмечаем руководящую роль Премьер-министра Каи Каллас в этой сфере и приветствуем презентацию заместителя Генерального секретаря, Высокого представителя по вопросам разоружения Идзуми Накамицу.

Прогресс, достигнутый в период 2020-2021 годов, стал знаковым явлением в области кибердипломатии не только благодаря мандату и результатам, достигнутым 12 марта 2021 года первой Рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, и консенсусу, достигнутому 28 мая этого года Группой правительственных экспертов по поощрению ответственного поведения государств в области кибербезопасности, но и в свете того факта, что все это происходило в условиях кризиса, вызванного пандемией коронавирусного заболевания (COVID-19), которая ускорила цифровую трансформацию.

Пандемия оказала влияние различными способами на все аспекты мира и безопасности. Кибербезопасность не стала исключением. Безопасность объектов по оказанию базовых услуг стала одним из самых серьезных вопросов, как и необходимость защиты критически важных инфраструктур от возможных кибератак, способных вызвать разрушения в физическом мире.

Угрозы, с которыми мы сегодня сталкиваемся, носят в основном транснациональный характер, и единственная форма борьбы с ними, как в физическом, так и в виртуальном пространстве, — это сотрудничество и международный диалог. Таким образом, если одно государство-член не находится в безопасности, то никто не находится в безопасности.

Поэтому Эквадор подтверждает свою приверженность действующим нормам в соответствии с международным правом, которые нашли отражение в докладах Группы правительственных экспертов и результатах Рабочей группы открытого состава. Моя делегация хотела бы подчеркнуть, что ни одна область не может оставаться вне сферы действия международного права, включая международное право прав человека и международное гуманитарное право, но это отнюдь не означает, что милитаризация киберпространства приемлема.

Напротив, Эквадор выступает за использование киберпространства в исключительно мирных целях. Устав Организации Объединенных Наций запрещает применение силы, поэтому все международные споры, касающиеся киберпространства, должны разрешаться мирными средствами.

Поэтому мы способствуем укреплению доверия и наращиванию потенциала, и для этого, на наш взгляд, необходима оперативная платформа, содействующая осуществлению положений существующей нормативно-правой базы государствами. Такая платформа может быть создана в виде программы действий.

Мы защищаем и поддерживаем любой механизм, способствующий более широкому международному сотрудничеству для уменьшения дисбаланса

возможностей по выполнению, правил, обеспечивающих ответственное поведение государств.

Кроме того, мы признаем вклад, который региональные организации могут внести в развитие потенциала и внедрение упомянутых норм. Например, мы отмечаем достойную похвал работу Организации американских государств в этой области, в частности ее усилия по борьбе с киберпреступностью и кибертерроризмом.

В заключение следует отметить необходимость сохранения и поощрения ответственного использования информационно-коммуникационных технологий в качестве ключевого фактора, гарантирующего стабильность и безопасность в киберпространстве. Мы также считаем, что существующие нормы следует укреплять с учетом быстрого технического прогресса. Со своей стороны, Совет Безопасности должен рассмотреть механизмы для активизации использования технологий в качестве средств укрепления мира в дополнение к традиционным усилиям.

Приложение XXVIII

Заявление Постоянного представительства Египта при Организации Объединенных Наций

Египет придает большое значение аспектам международной безопасности информационных и коммуникационных технологий (ИКТ) и настоятельно призывает Организацию Объединенных Наций играть центральную и ведущую роль в продвижении и разработке правил и принципов использования ИКТ государствами посредством всеобъемлющего и справедливого процесса с участием всех государств.

Некоторые государства развивают возможности ИКТ для потенциального использования в злонамеренных целях и в наступательных военных целях. Возможность использования ИКТ в будущих конфликтах между государствами становится все более реальной, а риск вредоносных атак ИКТ на важнейшие объекты инфраструктуры реален и серьезен. Эта новая гонка вооружений имеет далеко идущие последствия для международного мира, безопасности и стабильности, особенно в условиях, когда границы между обычными и неконвенциональными вооружениями продолжают стираться.

Кроме того, соответствующие технологии, разработанные государствами, передаются, копируются или воспроизводятся террористами и преступниками. Злонамеренное использование ИКТ террористическими и преступными организациями представляет собой серьезную угрозу международному миру и безопасности, особенно в свете проблем, связанных с присвоением ответственности.

Согласно международному праву и Уставу Организации Объединенных Наций, все государства-члены должны воздерживаться от любых действий, которые сознательно или намеренно наносят ущерб или иным образом затрудняют использование и функционирование самой важной инфраструктуры других государств, а также от вмешательства в их внутренние дела.

Нет сомнений в том, что аспекты международной безопасности ИКТ стали слишком важными и стратегическими, чтобы оставить их без четких обязательных правил на международном уровне. Всеобъемлющий процесс в рамках системы Организации Объединенных Наций является наилучшим и самым эффективным способом создания справедливых, всеобъемлющих и эффективных механизмов в этой области.

Организация Объединенных Наций уже сделала некоторые шаги по созданию нормативно-правовой базы, дополняющей принципы международного права. Благодаря тому, что недавно был принят консенсусом заключительный доклад созданной в соответствии с резолюцией 73/27 Генеральной Ассамблеи Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Организация Объединенных Наций уже создала начальные элементы системы предотвращения конфликтов и обеспечения стабильности в киберпространстве.

Генеральная Ассамблея призвала государства-члены руководствоваться при использовании ИКТ нормами ответственного поведения государств, содержащимися в ряде докладов групп правительственных экспертов, созданных в рамках Первого комитета. Однако реализация этих ограниченных норм остается в лучшем случае минимальной именно из-за их добровольного характера и отсутствия какого-либо механизма последующих действий.

Успех Рабочей группы открытого состава, которая впервые обеспечила всеобъемлющий процесс по этой важной теме, и создание новой Рабочей группы

открытого состава в соответствии с резолюцией 75/240 Генеральной Ассамблеи ознаменовали собой многообещающее продвижение к возможному достижению важного взаимопонимания между государствами-членами по ряду ключевых аспектов.

Всеобъемлющие процессы в Организации Объединенных Наций, в первую очередь под эгидой Генеральной Ассамблеи, являются наиболее эффективным способом создания справедливых, комплексных и эффективных механизмов в этой области. Со своей стороны, Совету Безопасности рекомендуется учитывать возможности, предоставляемые новыми технологиями, при рассмотрении таких тем, как поддержание мира и борьба с терроризмом. Однако Совет не следует использовать в качестве директивного органа, который пытается устанавливать нормы и правила от имени государств-членов по вопросам, которые обязательно требуют, чтобы процессы были всеобъемлющими и транспарентными.

Рекомендации, одобренные Генеральной Ассамблеей консенсусом, могут стать основой для политически или юридически обязывающих правил, особенно если они вытекают из принципов международного права и Устава Организации Объединенных Наций.

Египет также призвал рассмотреть вопрос о создании всеобъемлющей институциональной платформы, предназначенной для международного сотрудничества в области защиты мирного использования ИКТ и снижения связанных с ними рисков.

Хотя мы считаем, что международное право и принципы Устава действительно применимы ко всем областям, включая киберпространство, мы также считаем, что существует острая необходимость в определении конкретных обязательств, которые делают поведение государств в киберпространстве соответствующим международному праву и целям Устава Организации Объединенных Наций.

В мире, который становится все более взаимосвязанным, любой международный режим кибербезопасности будет настолько сильным, насколько надежно его самое слабое звено. К счастью, существует консенсус относительно необходимости активизации и наращивания усилий по укреплению потенциала для предотвращения потенциальных атак на важнейшие объекты инфраструктуры и для развития возможностей и технических навыков, необходимых в развивающихся странах. Организация Объединенных Наций должна возглавить скоординированные усилия по оказанию необходимой помощи развивающимся странам.

Наконец, ИКТ предлагают огромные возможности, но и создают вызовы. А мы подчеркиваем, что назрела острая необходимость в определении и разработке правил ответственного поведения государств для укрепления стабильности и безопасности в глобальной среде ИКТ и для недопущения того, чтобы киберпространство превратилось в еще одну арену конфликтов и гонки вооружений.

Приложение XXIX

Заявление Постоянного представительства Сальвадора при Организации Объединенных Наций

[Подлинный текст на испанском языке]

Сальвадор выражает признательность делегации Эстонии за то, что она в своем качестве Председателя Совета Безопасности в июне 2021 года созвала эти открытые дебаты, а это означает, что Совет Безопасности впервые рассматривает вопрос о кибербезопасности в официальном формате. Эта инициатива исключительно важна для выполнения этим органом международной ответственности по рассмотрению на многостороннем уровне существующих и потенциальных угроз безопасности в сфере информационно-коммуникационных технологий.

Развитие новых технологий открывает большие возможности для содействия социально-экономическому развитию государств. Однако эти информационные системы уязвимы для атак со стороны лиц, которые намерены манипулировать коммуникационными сетями в идеологических целях или для собственной выгоды. Поскольку преступники и террористы используют новые информационно-коммуникационные технологии для достижения своих целей, необходимо направить усилия и ресурсы на подготовку специальных рекомендаций для разработки и применения норм, которые помогут предотвратить эти виды преступлений, а также содействовать привлечению к ответственности тех, кто нарушает их.

Поэтому мы хотели бы особо подчеркнуть важность деятельности международных и региональных механизмов, связанных с борьбой против киберпреступности, а также достижений в этой области, таких как учреждение Рабочей группы открытого состава для разработки всеобъемлющей международной конвенции о борьбе против использования информационно-коммуникационный технологий в преступных целях.

Мы с удовлетворением отмечаем усилия, предпринимаемые государствами-членами Организации Объединенных Наций в борьбе с терроризмом в рамках повестки дня по поддержанию международного мира и безопасности. В то же время мы отмечаем, что среди международных документов обязывающего характера, имеющих отношение к этой теме, невозможно найти прямую ссылку на киберпространство. Это и есть те пробелы, которые мы все должны заполнить как можно скорее. Мы ценим усилия Совета Безопасности по обсуждению этой серьезной угрозы в поисках надежных и эффективных путей и средств ее устранения. Мы настоятельно призываем этот орган продолжать эти усилия, отложив в сторону любые политические и/или личные интересы и поддержать цель предотвращения новых конфликтов и создания сценариев для ее достижения.

Сальвадор напоминает о резолюции 58/199 Генеральной Ассамблеи, принятой в 2004 году, включающей перечень всех важнейших объектов инфраструктуры государств, которые из-за растущей взаимозависимости технологий подвергаются все большему числу все более разнообразных угроз. В этой резолюции признается, что уязвимость этих важнейших объектов инфраструктуры создает серьезные проблемы в области безопасности.

Кроме того, чтобы создать необходимые условия для продвижения к нашей общей цели поддержания международного мира и безопасности, осуществления в полном объеме прав человека и социально-экономического развития, на наш

взгляд, надо расширить рамки, предусмотренные в резолюции 58/199 Генеральной Ассамблеи, с тем чтобы защитить критически важные инфраструктуры от кибератак и обеспечить их функционирование, прилагая реальные усилия во избежание того, чтобы киберпространство стало платформой для пропаганды радикализма, вербовки и сбора средств на преступную деятельность.

Мир продолжает противостоять одному из самых серьезных вызовов со времен создания Организации Объединенных Наций, а именно: вызову в виде вспышки коронавирусного заболевания (COVID-19), которая вскрыла уязвимости важнейших систем государств. Мы стали свидетелями того, как во время пандемии COVID-19 увеличилось число кибератак на национальные системы здравоохранения, что поставило под угрозу жизнь миллионов людей и оказало прямое влияние на самые уязвимые слои населения и сектора. Мы хотели бы, чтобы этот форум осудил кибератаки против Всемирной организации здравоохранения и попытки уничтожения идентичности, которые имели место в течение последних месяцев. Нет сомнений в том, что вследствие обострения межконфессиональных трений такие нападения могут происходить чаще в ближайшие годы.

В последние месяцы злонамеренное использование информационно-коммуникационных технологий стало включать и кибератаки против энергетического, финансового и продовольственного секторов; среди других секторов они являются исключительно уязвимыми перед кибератаками. Кроме того, с целью повлиять на восприятие правительствами и институтами усилилась, как мы видим, кибердеятельность с использованием дезинформации, а ее возможности снижения эффективности труда, повышения нестабильности и провоцирования социальных конфликтов довольно большие.

Все вышеизложенное указывает на необходимость дальнейшей работы по предотвращению злонамеренных действий в киберпространстве и кодификации международного права, ориентированной на предотвращение его неправомерного использования, которая отражала бы взаимосвязь с международным гуманитарным правом, применимым, в том числе, в контексте кибероперaций во время вооруженных конфликтов.

Мы подчеркиваем важность работы на основе консенсуса, без намерения навязать решения, несовместимые с реальной ситуацией в государствах, равно как и обеспечения того, что будут учитываться достижения Генеральной Ассамблеи благодаря различным консенсусным договоренностям Группы правительственных экспертов и Рабочей группы открытого состава по достижениям в области информатизации и коммуникаций в контексте международной безопасности. В частности, мы отмечаем принятие одобренного консенсусом соглашения Группой по открытого состава в 2021 году с участием 193 государств-членов Организации Объединенных Наций, включая 15 членов Совета Безопасности и другие заинтересованные стороны, имеющие отношение к этому процессу.

Сальвадор надеется на конструктивную работу в Рабочей группе открытого состава по достижениям в сфере информатизации и коммуникаций в контексте международной безопасности, которая будет развивать свои наработки в период 2021-2025 годов, и с удовлетворением отмечаем работу Бурхана Гафура, Постоянного представителя Сингапура при Организации Объединенных Наций, в качестве Председателя этого процесса.

Следует упомянуть огромную роль региональных организаций, частного сектора, гражданского общества, научных кругов и других соответствующих секторов в предотвращении этих угроз и борьбе ними. Настоятельно необходимо продолжать работу над укреплением механизмов регионального и

международного сотрудничества с целью предотвращения этих вызовов и их устранения посредством динамичного обмена информацией и передовой практикой, укрепления потенциала, стандартизации правовых основ и использования новых технологий для продвижения по пути развития и борьбы с организованной преступностью.

Приложение XXX

Заявление главы делегации Европейского союза при Организации Объединенных Наций Улофа Скога

Для меня большая честь участвовать в открытых дебатах по вопросу о кибербезопасности от имени Европейского союза и его государств-членов.

К этому заявлению присоединяются также страны-кандидаты: Турция, Республика Северная Македония*, Черногория* и Албания*, страна — участница процесса стабилизации и ассоциации и потенциальный кандидат Босния и Герцеговина, а также Украина и Республика Молдова.

Во-первых, мы хотели бы поблагодарить Эстонию за проведение открытых дебатов по этой важнейшей теме именно сейчас, когда злонамеренная кибердеятельность продолжает активизироваться, а все более частые вызовы представляют опасность для международной безопасности и стабильности в киберпространстве, особенно в нынешних особых условиях пандемии.

Влияние, которое оказывает цифровизация на нашу безопасность, экономику и общество в целом, усиливается, создавая как возможности, так и проблемы. Транспорт, энергетика, здравоохранение, телекоммуникации, финансы, безопасность, демократические процессы, космос и оборона в значительной степени зависят от сетевых и информационных систем, которые становятся все более взаимосвязанными.

Поэтому нас особенно тревожат участившиеся в последнее время случаи злонамеренной кибердеятельности, направленной против крупных операторов по всему миру, в том числе в сфере здравоохранения, и влияющей на доступность, безопасность и целостность продуктов и услуг информационно-коммуникационных технологий (ИКТ) и, следовательно, на непрерывность операций, что может иметь побочные и системные последствия и повысить риски возникновения конфликтов.

По этой причине мы приветствуем возможность обсудить этот важный вопрос в Совете Безопасности, который несет главную ответственность за поддержание международного мира и безопасности. Это возможность особо выделить ряд стоящих перед нами проблем, подтвердить достижения Организации Объединенных Наций на сегодняшний день и определить перспективы решения этих вопросов в ее рамках.

В связи с этим Европейский союз и его государства-члены приветствуют содержательные и одобренные недавно консенсусом доклады Рабочей группы открытого состава по достижениям в сфере информатики и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве.

Эти доклады представляют собой значительный вклад в повышение осведомленности в вопросах предотвращения киберугроз и злонамеренной кибердеятельности, реагирования на них и последующего восстановления и позволяют расширить необходимые для этого возможности. Это крайне важно, так как нехватка осведомленности и потенциала сама по себе представляет угрозу, поскольку все страны все больше зависят от ИКТ.

* Республика Северная Македония, Черногория, Сербия и Албания остаются участниками Процесса стабилизации и ассоциации.

Поэтому повышение глобальной киберустойчивости имеет огромное значение, поскольку оно снижает возможности потенциальных злоумышленников использовать ИКТ в неблаговидных целях. Оно также позволяет государствам проявлять должную осмотрительность и принимать соответствующие меры против субъектов, которые занимаются такой деятельностью с территории данных государств, в соответствии с международным правом и одобренными консенсусом докладами групп правительственных экспертов Организации Объединенных Наций (ГПЭ ООН) в 2010, 2013, 2015 и 2021 годах в области информации и телекоммуникаций в контексте международной безопасности.

В докладах сменяющих друг друга групп правительственных экспертов Организации Объединенных Наций и Рабочей группы открытого состава предлагается основа для предотвращения конфликтов, развития сотрудничества и обеспечения стабильности в киберпространстве, то есть подтверждается применение международного права, рассматриваются нормы ответственного поведения государств, меры укрепления доверия в киберпространстве и наращивание киберпотенциала.

Европейский союз и его государства-члены подтверждают, что основой предотвращения конфликтов, развития сотрудничества и укрепления стабильности в киберпространстве может быть только существующее международное право, которое включает в себя Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека, которые были одобрены Генеральной Ассамблеей с 2013 года.

Более глубокое понимание того, как международное право применяется в киберпространстве, должно способствовать дальнейшему уменьшению неверных толкований и повышению ответственности в киберпространстве, а члены Организации Объединенных Наций должны продолжать пропагандировать и применять эти базовые положения в интересах международной безопасности и стабильности в киберпространстве.

Например, Европейский союз и его государства-члены считают, что международное гуманитарное право полностью применимо в киберпространстве в контексте вооруженного конфликта. Мы вновь заявляем, что его применение в киберпространстве не должно быть неправильно истолковано как узаконивание любого применения силы, несовместимого с Уставом Организации Объединенных Наций. Международное гуманитарное право устанавливает основные меры защиты для тех, кто не участвует или уже не участвует в военных действиях, в частности, для защиты гражданских лиц от последствий военных действий, а комбатантов — от ненужных страданий. Оно также накладывает ограничения на допустимые средства и методы ведения войны, в том числе и новые.

Во-вторых, крайне важно соблюдение норм ответственного поведения государства. Набор согласованных норм отражает общие ожидания международного сообщества, которые предопределяют стандарты ответственного поведения государств. Он позволяет международному сообществу оценивать деятельность и намерения государств с целью предотвращения конфликтов и укрепления стабильности и безопасности в киберпространстве.

В-третьих, меры укрепления доверия в киберпространстве — это практические средства предотвращения конфликтов. Благодаря сотрудничеству и обмену информацией региональные меры укрепления доверия доказали, что они снижают риск неправильного толкования, эскалации и конфликта, которые могут возникнуть в результате инцидентов в сфере ИКТ.

И наконец, эти базовые положения охватывают важный вопрос об укреплении потенциала. Мы активно поддерживаем призыв к улучшению координа-

ции для повышения согласованности усилий по наращиванию потенциала в области использования ИКТ с целью устранения цифровой пропасти, в том числе благодаря нашим многочисленным усилиям с партнерами по всему миру.

Европейский союз поддерживает работу по наращиванию киберпотенциала с помощью своих инструментов внешнего финансирования, которые охватывают целый ряд глобальных программ, включая мероприятия, проводимые в Африке, Азии и Латинской Америке, а также в странах-соседях Европейского союза и на Западных Балканах. Если говорить конкретно, то в настоящее время Европейский союз инвестирует в деятельность по всему миру, чтобы поддержать реализацию — в сотрудничестве со своими партнерами-исполнителями — таких проектов, как «Киберустойчивость Европейского союза для развития», «Глейси+», «ЕС КиберДирект» и Инициатива по укреплению безопасности в Азии и с Азией.

Чтобы особо выделить базу для предотвращения конфликтов, сотрудничества и стабильности в киберпространстве, Европейский союз продолжит усилия по поощрению ответственного поведения в киберпространстве. Поэтому Европейский союз и его государства-члены подтверждают свою приверженность разрешению международных споров мирными средствами также и в тех случаях, когда такие споры возникают в киберпространстве.

Поэтому база совместного дипломатического ответа Европейского союза является частью подхода Европейского союза к кибердипломатии, что способствует предотвращению конфликтов, смягчению угроз кибербезопасности и повышению стабильности международных отношений. В целях создания и защиты открытого, свободного, стабильного и безопасного киберпространства Европейский союз продолжит использовать свой инструментарий кибердипломатии и сотрудничать с международными партнерами в этой области.

Учитывая сложный характер киберпространства, государствам, а также многостороннему сообществу заинтересованных сторон крайне важно с самого начала решать проблемы, которыми потенциально чревато киберпространство, развивать сотрудничество и укреплять свой потенциал. Мы также несем главную ответственность за то, чтобы все заинтересованные стороны могли взять на себя обязательства по созданию открытого, свободного, безопасного и стабильного киберпространства, базирующегося на уважении прав человека, основных свобод, демократии и верховенства права, и мы поддерживаем их усилия. Подход Европейского союза к кибердипломатии также учитывает важность гендерных аспектов для сокращения «гендерного цифрового разрыва» и содействия эффективному и значимому участию женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

В контексте укрепления сотрудничества мы видим центральную роль Организации Объединенных Наций в содействии имплементации уже принятых решений. Совершенно ясно, что для содействия эффективному обсуждению с участием многих заинтересованных сторон в целях укрепления мира и безопасности в киберпространстве надо развивать нормативно-правовую базу Организации Объединенных Наций по вопросам ответственного поведения государств в киберпространстве. Вместе с 53 государствами-членами Европейский союз предлагает разработать программу действий по поощрению ответственного поведения государств в киберпространстве.

Эта программа действий, которая будет исходить из действующих положений, одобренных Генеральной Ассамблеей, станет постоянной платформой для сотрудничества и обмена передовым опытом в Организации Объединенных Наций. Эта программа действий дает возможность содействовать выполнению

проектов по наращиванию потенциала, разработанных с учетом потребностей, определенных государствами-бенефициарами. Она также обеспечивает институциональный механизм в системе Организации Объединенных Наций для развития сотрудничества с другими заинтересованными сторонами, такими как частный сектор, научные круги и гражданское общество, в отношении их соответствующих обязанностей по поддержанию открытой, свободной, безопасной, стабильной, доступной и мирной среды ИКТ

Учитывая постоянный и ориентированный на действия характер этой платформы, мы считаем, что данное предложение о программе действий своевременно и заслуживает дальнейшего изучения международным сообществом. Она станет прочной практической основой для дальнейшей работы над базовыми положениями, касающимися предотвращения конфликтов, сотрудничества и стабильности в киберпространстве, и для обеспечения того, чтобы государства могли пользоваться благами глобального, открытого, стабильного и безопасного киберпространства.

Приложение XXXI

Заявление Постоянного представительства Грузии при Организации Объединенных Наций

Мы хотели бы выразить признательность Эстонии, выполняющей функции Председателя, за созыв сегодняшних дебатов высокого уровня по этому важному вопросу и поблагодарить уважаемых ораторов.

Грузия давно привержена развитию ответственного и этичного киберпространства, в том числе обеспечению кибербезопасности и киберустойчивости, с тем чтобы разработать всеобъемлющие базовые положения в целях создания безопасной, надежной и пользующейся доверием цифровой среды на благо всей нации. За последнее десятилетие мы заложили необходимую правовую базу информационной безопасности и кибербезопасности и выявили важнейшие элементы информационных систем, приняли и претворили в жизнь две стратегии кибербезопасности вместе с соответствующими планами действий, а в настоящее время идет работа в целях принятия третьей национальной стратегии кибербезопасности.

Однако, как мы все знаем, киберпространство не только открывает большие социально-экономические возможности и обеспечивает инновации и развитие, но и несет в себе новые виды угроз для безопасности. В последние годы мы стали свидетелями того, как киберпространство используется не только в целях терроризма, мошенничества и совершения преступлений, но и как мощный инструмент гибридной войны и вмешательства во внутренние дела государств.

К сожалению, гибридная война также стала мощным инструментом в руках некоторых государств, используемым для продвижения своих национальных интересов, и, как хорошо известно данному органу, Грузия имеет большой и болезненный опыт борьбы с гибридными угрозами, исходящими от одного из его постоянных членов. Российская Федерация ведет гибридную войну против Грузии с начала 1990-х годов и никогда не оставляла попыток подорвать суверенитет, территориальную целостность, а также европейские и евроатлантические устремления нашей страны.

Список инцидентов обширен. В августе 2008 года во время полномасштабной военной агрессии России против Грузии мы стали свидетелями первого прецедента массированной кибератаки, совершенной одновременно с продолжающейся агрессией. В 2019 году была проведена масштабная кибератака на вебсайты, серверы и другие операционные системы Администрации Президента Грузии, судов, муниципальных собраний, государственных учреждений, организаций частного сектора и средств массовой информации. Расследование, проведенное грузинскими властями в сотрудничестве с нашими партнерами, позволило сделать вывод, что эта кибератака была спланирована и совершена Главным управлением Генерального штаба Вооруженных сил Российской Федерации.

К сожалению, даже сейчас, когда международное сообщество ведет борьбу с пандемией коронавирусного заболевания (COVID-19), Российская Федерация все еще пытается получить политические дивиденды, усиливая пропагандистскую войну против одного из самых успешных учреждений Грузии, которое ведет борьбу с распространением коронавируса, — против Центра медицинских исследований имени Ричарда Лугара. Обвинения России представляют собой типичный образец дезинформации и пропагандистской кампании против этой уникальной лаборатории, которая была создана для выявления и пресечения вспышек заболеваний наподобие данной пандемии.

Сегодня мы все являемся свидетелями агрессивного применения Россией гибридного инструментария не только в нашем регионе, но и по всему миру. Главными элементами этого российского гибридного инструментария являются военное присутствие, информационные операции, кибератаки, поддержка политических групп, выступающих в качестве пособников, вмешательство во внутренние дела и экономическое влияние.

В заключение мы должны подчеркнуть, что кибератаки и гибридная война против суверенных государств представляют собой грубые нарушения международного права, его норм и принципов и подрывают международный мир и безопасность. Подтверждая нашу приверженность дальнейшему укреплению кибербезопасности на национальном и международном уровне, мы также призываем международное сообщество уделять больше внимания злонамеренной деятельности в сфере информационно-коммуникационных технологий, которую Российская Федерация проводит в Грузии и других странах.

Приложение XXXII

Заявление Постоянного представительства Германии при Организации Объединенных Наций

Полтора года назад на мир обрушилась пандемия коронавирусного заболевания (COVID-19), которая заставила нас внезапно осознать, в какой степени цифровые технологии определяют как нашу повседневную жизнь, так и нашу экономическую устойчивость. В то же время она безжалостно обнажила наши уязвимые места. Кибератаки, включая те, которые совершаются против важнейших объектов инфраструктуры, могут представлять собой угрозу международному миру и безопасности, и Германия по-прежнему убеждена в том, что это одна из важных тем для Совета Безопасности.

Международный мир и безопасность находятся под давлением с разных сторон: прежде всего деятельность киберпреступников подрывает надежность технологий и доверие к ним, хотя сегодня эти технологии имеют огромное значение для функционирования нашей экономики, правительств и современного общества в целом. Приведу всего лишь несколько примеров: после вспышки пандемии ковид-19 резко возросло число атак, нарушающих процессы обслуживания, случаев фишинга и распространения вредоносных программ. Растет число атак на важнейшие объекты инфраструктуры в Европе и Северной Америке, а также кибератак, используемых для вымогательства.

Во-вторых, спонсируемая государствами злонамеренная кибердеятельность с целью шпионажа, саботажа, дезинформации и дестабилизации или получения финансовой выгоды подрывает как международное доверие, так и совместные механизмы смягчения конфликтов и тем самым угрожает безопасности во всем мире.

В-третьих, гражданское общество в целом, включая правозащитников, подвергается все большему давлению в киберпространстве. Простор для свободы слова, транспарентности и подлинного общения, который по идее должен обеспечиваться Интернетом, продолжает сужаться.

Для того чтобы справиться с этими растущими угрозами, надо использовать многокомпонентный подход: один из компонентов — укрепление нашей устойчивости на национальном и международном уровнях. Этот компонент включает в себя улучшение технической инфраструктуры, наращивание политического и правового потенциала, а также развитие международного сотрудничества.

Второй компонент — дальнейшее продвижение и определение нашего общего понимания ответственного поведения государств в киберпространстве и установление «красных линий», которые нельзя пересекать. Поэтому мы должны отстаивать результаты, достигнутые Рабочей группой открытого состава и Группой правительственных экспертов, и продолжать разработку норм ответственного поведения государств.

Позиция Германии заключается в том, что международное право, включая Устав Организации Объединенных Наций и международное гуманитарное право, применимо в Интернете и вне его. Государства должны всячески воздерживаться от поддержки деятельности в сфере информационно-коммуникационных технологий (ИКТ), противоречащей их обязательствам по международному праву, причем — не в последнюю очередь — в свете возможности появления и эскалации напряженности в отношениях между государствами. Деятельность в сфере ИКТ не должна преднамеренно наносить ущерб важнейшим объектам инфраструктуры или иным образом нарушать их использование и работу. В

частности, никто не должен ставить под угрозу общую доступность или целостность общественного ядра Интернета, что жизненно важно для стабильности киберпространства. Мы призываем все государства строго выполнять свои обязательства по проявлению должной осмотрительности и быстро принимать меры — в соответствии с международным правом — против тех, кто ведет злонамеренную кибердеятельность со своей территории.

В целях стимулирования нынешних дискуссий о международном праве в киберпространстве Германия опубликовала меморандум о применимости международного права в киберпространстве, и мы призываем других сделать то же самое.

Но одного лишь согласия на существование общих базовых положений недостаточно. Не менее важно, чтобы на неприемлемое поведение был дан суровый ответ. Можно рассматривать с этой целью различные инструменты — начиная от диалога и обмена мнениями до политических деклараций государств или групп государств, разоблачающих и осуждающих безответственное поведение или вводящих санкции против соответствующих лиц и организаций. Вместе с нашими партнерами в Европейском союзе мы ввели режим санкций за кибератаки, который позволяет нам реагировать на кибератаки решительно, эффективно и целенаправленно и в полном соответствии с международным правом. Мы ранее использовали этот инструмент и без колебаний будем делать это и впредь, если наша безопасность окажется под угрозой. Кроме того, система присвоения ответственности может укрепить нормативную базу и способствовать подотчетности в киберпространстве.

Для повышения нашей устойчивости в киберпространстве и совершенствования системы управления Интернетом очень важно наладить постоянный обмен мнениями с гражданским обществом, частным сектором и научными кругами. С целью поддержания международного мира и безопасности в киберпространстве надо использовать и интегрировать в эти усилия богатый опыт, накопленный вне государственного сектора.

Приложение XXXIII

Заявление Постоянного представительства Греции при Организации Объединенных Наций

Цифровые технологии вносят весомый вклад в происходящую трансформацию экономики и общества, предлагая значительные возможности для экономического роста, а также устойчивого и всеобъемлющего развития. Киберпространство, в частности, стало одним из столпов нашего общества. В то же время активизация вредоносного поведения в киберпространстве, включая злоупотребление информационно-коммуникационными технологиями (ИКТ) в неблаговидных целях — как государственными, так и негосударственными субъектами, — стал источником новых рисков и вызовов. Такое поведение угрожает экономическому росту и может привести к цепной реакции с дестабилизирующими последствиями и к эскалации рисков возникновения конфликтов.

Поэтому мы полностью поддерживаем стратегические основы предотвращения конфликтов, сотрудничества и стабильности в киберпространстве, одобренные Генеральной Ассамблеей, и подчеркиваем необходимость сосредоточения наших коллективных усилий на развитии навыков и потенциала для адекватного противодействия киберугрозам. Необходимость обеспечения глобальной киберустойчивости подтверждается нынешним глобальным кризисом в области здравоохранения, в ходе которого мы наблюдаем киберугрозы и злонамеренные кибердействия, направленные на здравоохранение.

Глобальная киберустойчивость снижает способность потенциальных злоумышленников неправомерно использовать ИКТ и укрепляет способность государств эффективно реагировать на киберинциденты и восстанавливаться после них. В рамках наших нынешних усилий по укреплению глобальной устойчивости и разработке практических мер сотрудничества мы сейчас занимаемся организацией регионального семинара по кибербезопасности, в котором будут участвовать представители Западных Балкан.

Активно участвуя в деятельности международных организаций, таких как Организация Объединенных Наций, НАТО и Организация по безопасности и сотрудничеству в Европе, мы стремимся развивать сотрудничество, обмениваться опытом и передовой практикой, а также вносить максимально возможный вклад в разработку соответствующих средств противодействия киберугрозам. Кроме того, будучи членом Европейского союза, мы выполняем базовые положения всеобъемлющего и многогранного стратегического характера о предотвращении конфликтов и обеспечении стабильности в киберпространстве. В рамках Европейского союза кибербезопасность подразумевает скоординированные и коллективные усилия государств-членов, которые создают уникальный и ценный прецедент в области многостороннего сотрудничества.

Мы глубоко привержены идее глобального, мирного, безопасного, открытого и независимого киберпространства, регулируемого международным правом, где в полной мере уважаются права человека, основные свободы и верховенство права. Мы активно делимся нашим опытом применения норм, осуществления мер укрепления доверия и действий по наращиванию потенциала — как на двусторонней, так и на многосторонней основе — на всех региональных и международных форумах, в которых мы участвуем. Мы твердо намерены и впредь активно участвовать в последующих дискуссиях в Организации Объединенных Наций по вопросам кибербезопасности и подтверждаем нашу готовность к позитивному взаимодействию в целях достижения конструктивного прогресса.

Приложение XXXIV

Заявление Постоянного представительства Гватемалы при Организации Объединенных Наций

Гватемала хотела бы выразить свою признательность делегации Эстонии, председательствующей в Совете Безопасности, за созыв этих открытых прений по вопросу, который, несомненно, является чрезвычайно важным для государств. Киберпространство стало центральной и незаменимой областью глобальной деятельности, а его защита путем обеспечения ответственного поведения государств имеет огромное значение для поддержания международного мира и безопасности. Мы уверены в том, что заседания такого рода дают нашим странам прекрасные возможности обменяться мнениями и передовым опытом осуществления этой все более актуальной работы на том или ином уровне.

В настоящее время мир сталкивается с целым рядом проблем в области безопасности, которые усугубляются появлением новых угроз, таких как вызовы кибербезопасности. Если вспомнить предыдущие кибератаки, а также увеличение их частотности и масштабов во время пандемии коронавирусного заболевания (COVID-19), то необходимость обращения к этой теме станет очевидной, особенно если учесть, что она может затронуть самые уязвимые слои нашего общества.

Киберугрозы и кибератаки возникают и эволюционируют в результате различных видов деятельности, которые развиваются благодаря взаимосвязи цифровых средств массовой информации, что представляет собой комплекс условий, требующих участия и сотрудничества всех секторов в наших странах для разработки технических и правовых базовых положений, укрепляющих кибербезопасность как внутри страны, так и на глобальном уровне.

Активное использование информационных и коммуникационных технологий (ИКТ) получило широкое распространение во всех странах и во всех слоях нашего общества. Этот новый сценарий способствует беспрецедентному развитию обмена информацией и систем связи, но в то же время он влечет за собой новые риски и угрозы, которые могут повлиять на безопасность нашего населения.

Поэтому наша делегация хотела бы выразить свою обеспокоенность по поводу этих новых технологий, особенно учитывая гражданский и двойной характер киберпространства и цифровых сетей, которые могут быть использованы преступными и террористическими группировками. Крайне тревожно то, что несколько государств развивают возможности ИКТ в военных целях и что использование этих технологий в будущих конфликтах между государствами становится все более вероятным.

Гватемала признает, что взаимосвязанный и сложный характер киберпространства требует совместных усилий правительств, частного сектора, гражданского общества и научных кругов для комплексного и сбалансированного решения проблем кибербезопасности. Ответственность за поддержание открытого, свободного, безопасного и стабильного киберпространства лежит на всех этих секторах.

По этой причине наша страна поощряет меры укрепления доверия и транспарентности и поддерживает мероприятия по наращиванию потенциала, обмену информацией и распространению передового опыта на субрегиональном, региональном и международном уровнях.

Наша делегация подчеркивает сохраняющуюся исключительную важность применимости международного права к поведению государств в киберпространстве, добровольных необязательных норм поведения государств в мирное время и осуществления мер укрепления доверия. Кроме того, учитывая существующий разрыв между странами в области кибербезопасности и обороны, наша страна уделяет особое внимание усилиям по наращиванию потенциала, с тем чтобы создать более справедливые условия, которые помогут поддерживать международный мир и безопасность.

Гватемала считает, что региональные организации играют незаменимую роль в установлении мира на местах. Существует значительный потенциал для усиления их присутствия в киберпространстве — как на региональном, так и на глобальном уровне — для инновационного продвижения повестки дня по поддержанию мира. Региональные и субрегиональные организации сосредоточили свои усилия на укреплении безопасности государств, что позволило добиться больших успехов в реализации практических мер по укреплению доверия в различных регионах для повышения киберстабильности. Нет сомнения в том, что без вклада этих организаций усилия по предотвращению конфликтов и обеспечению стабильности были бы менее эффективными.

В настоящее время в Гватемале действует Национальная стратегия кибербезопасности, главными целями которой являются укрепление потенциала страны и создание среды и условий, необходимых для обеспечения участия, развития и реализации прав людей в киберпространстве. Кроме того, функционирует Центр реагирования на инциденты в области компьютерной безопасности, который предоставляет услуги по аудиту кибербезопасности, сканированию уязвимостей и классификации предупреждений. Оба эти инструмента были созданы при поддержке со стороны Организации американских государств.

Кроме того, Гватемала находится в процессе разработки закона о киберпреступности, четко определяющего направления деятельности и виды преступлений с использованием ИКТ и в сфере ИКТ с целью содействия наращиванию потенциала посредством международного сотрудничества, благоприятствующего надлежащей правовой процедуре благодаря наличию четко определенных протоколов для цепочки хранения и обработки цифровых доказательств. Необходимо также отметить, что наша страна имеет честь быть страной-наблюдателем Будапештской конвенции, которая направлена на борьбу с компьютерными преступлениями и преступлениями в Интернете путем согласования законов между странами, совершенствования методов расследования и расширения сотрудничества между странами.

Наша делегация считает необходимым продолжать изменение и корректировку законов, которые регулируют положение в каждой стране согласованным образом, и разрабатывать системы, позволяющие выявлять, расследовать и преследовать вероятные преступления в рамках, которые защищают права отдельных лиц и в то же время снижают риск использования компьютерных сетей против конфиденциальности, целостности и доступности информации. Мы надеемся, что наше сегодняшнее обсуждение внесет позитивный вклад в процесс кибернормотворчества в Генеральной Ассамблее, осуществляемый, в частности, благодаря конструктивной работе Группы правительственных экспертов и Рабочей группы открытого состава в 2021-2025 годах, и дополнит его.

В заключение мы напоминаем всем государствам, что ИКТ должны использоваться в мирных целях и на благо всего человечества, способствуя устойчивому развитию всех стран, независимо от уровня их научно-технического развития.

Приложение XXXV

Заявление Временного поверенного в делах Постоянного представительства Индонезии при Организации Объединенных Наций Мохаммада Курниади Кобы

Позвольте мне поблагодарить Эстонию за созыв этого заседания. Я также хотел бы поблагодарить докладчика за ее ценный брифинг.

По мере роста зависимости людей от цифровой связи информационно-коммуникационные технологии (ИКТ) стали неотъемлемой частью нашей повседневной жизни.

Более того, во время пандемии коронавирусного заболевания (COVID-19) ИКТ стали своего рода спасательным кругом для государственного и частного секторов в деле предоставления жизненно важных услуг населению.

В связи с этим необходимо подчеркнуть, что злонамеренная кибердеятельность государственных и негосударственных субъектов, особенно направленная на важнейшие объекты инфраструктуры, может поставить под угрозу национальную стабильность, а также международный мир и безопасность.

В связи с этим Индонезия хотела бы подчеркнуть следующие ниже моменты.

Во-первых, примат верховенства права, которым мы должны руководствоваться в своем поведении в отношении использования ИКТ, а также его влияние на международный мир и безопасность.

Принципы международного права и Устав Организации Объединенных Наций являются основополагающими правовыми нормами, которыми руководствуются государства при использовании ИКТ, в том числе при реагировании на любые злонамеренные атаки.

Все государства должны руководствоваться одним и тем же сводом правил и законов. Никто не должен быть исключением.

Кроме того, Индонезия поддерживает нормы ответственного поведения государства, изложенные в резолюции 70/237 Генеральной Ассамблеи.

В то время, когда мы продолжаем заниматься проблемой растущей потребности в определении и разработке международной правовой базы по этому вопросу, наши усилия должны быть также направлены на устранение разрыва между странами и регионами.

Надо не только устранить разрыв технического порядка, но и укрепить национальную политическую базу, а также активизировать применение существующего международного права и добровольных необязательных норм в киберпространстве.

Во-вторых, роль двусторонних, региональных и многосторонних подходов в области укрепления доверия в киберпространстве.

Совместные меры на двустороннем, региональном и многостороннем уровнях взаимно усиливают понимание и укрепляют стабильность в киберпространстве, особенно в области наращивания потенциала и укрепления доверия.

Меры доверия АСЕАН, осуществляемые посредством создания координационных центров, регулярного обмена информацией, диалога и обмена передовым опытом, способствуют киберстабильности в Юго-Восточной Азии и за ее пределами, особенно в рамках Регионального форума АСЕАН.

Кроме того, Индонезия подчеркивает, что надо обеспечить конструктивное партнерство с другими многосторонними организациями, чтобы помочь государствам применять базовые положения об ответственном поведении при использовании ИКТ.

В связи с этим мы подчеркиваем, что развитые страны должны делиться технологиями ИКТ с развивающимися странами. Как и в процессе решения всех других глобальных проблем, обеспечение того, чтобы другие имели необходимые инструменты и возможности для борьбы с этой угрозой, будет способствовать общей стабильности в сфере ИКТ.

В-третьих, роль Организации Объединенных Наций в руководстве скоординированными усилиями по урегулированию конфликтов, которые могут возникнуть в результате инцидентов, связанных с ИКТ.

Сегодняшнее обсуждение — это первая официальная дискуссия в Совете, посвященная вопросу о влиянии информационно-коммуникационных технологий на поддержание международного мира и безопасности.

Оно знаменует собой крупный шаг вперед в решении данного вопроса в Организации Объединенных Наций.

В дальнейшем Совету надо будет предвидеть рост угроз в киберпространстве, а также возможные значительные инциденты в сфере ИКТ, которые могут привести к крупной войне.

Мы подчеркиваем важность обеспечения того, чтобы действия Организации Объединенных Наций оставались скоординированными и согласованными. Совет должен продолжать реагировать на угрозы международному миру и безопасности, а также на гуманитарные последствия развития событий в сфере ИКТ.

В то же время Совет должен руководствоваться нормами и правилами, которые обсуждаются и разрабатываются Генеральной Ассамблеей.

В заключение позвольте мне подтвердить приверженность Индонезии продвижению наших общих усилий по надлежащему реагированию на постоянно растущие вызовы для поддержания мира и безопасности, связанные с использованием ИКТ.

Приложение XXXVI

Заявление Международного комитета Красного Креста

Международный комитет Красного Креста (МККК) признателен за возможность внести свой вклад в открытые дебаты Совета Безопасности по теме «Поддержание международного мира и безопасности в киберпространстве».

За последние два десятилетия враждебные кибероперации стали более серьезной проблемой для поддержания международного мира и безопасности. По мере цифровизации общества растет и военный потенциал государств и других субъектов. Сегодня международное сообщество признает, что ряд государств развивает потенциал ИКТ в военных целях и что «использование ИКТ в будущих конфликтах между государствами становится все более вероятным». [10]

В свете этой реальности МККК хотел бы напомнить о потенциальном вреде для людей, который может нанести использование кибертехнологий, а затем изложить свое мнение о том, как государства могут смягчить эти негативные гуманитарные последствия посредством действий на международном и национальном уровнях.

Сегодня хорошо известно, что кибероперации против важнейших объектов гражданской инфраструктуры нанесли значительный экономический ущерб, нарушили жизнь общества и вызвали напряженность в отношениях между государствами. В заключительном докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности все государства признали, что кибероперации против важнейших объектов инфраструктуры могут иметь «катастрофические гуманитарные последствия». [11] Хотя МККК не может подтвердить ни одной кибероперации с человеческими жертвами, мы обеспокоены их пагубными последствиями, такими как нарушение работы объектов электроснабжения, систем водоснабжения или медицинских служб[12]. Такие операции всегда создают серьезные угрозы для людей. Вместе с тем наш опыт показывает, что нарушение работы важнейших объектов гражданской инфраструктуры имеет особенно тяжелые последствия в обществе, которое и без того ослаблено вооруженным конфликтом.

Пагубные гуманитарные последствия не являются неизбежными. Государства должны предпринять решительные шаги для обеспечения того, чтобы проведение кибероперацийво время вооруженного конфликта соответствовало существующим нормам международного права. По мнению МККК, для этого необходимы действия на международном и национальном уровнях.

На международном уровне государства подтвердили, что в сфере ИКТ применяется международное право. Это включает в себя прежде всего обязательства государств по Уставу Организации Объединенных Наций, в частности запрет на применение силы и обязательство разрешать международные споры мирными средствами. Совсем недавно Группа правительственных экспертов также отметила, что «нормы международного гуманитарного права применимы только в ситуациях вооруженных конфликтов». Группа напомнила об «установленных международно-правовых принципах, включая, где это применимо, принципы гуманности, необходимости, соразмерности и избирательности, которые были отмечены в докладе 2015 года», и признала «необходимость дальнейшего изучения вопроса о том, как и когда эти принципы применяются к

[10] Рабочая группа открытого состава, Заключительный доклад, 2021 год, пункт 16; Группа правительственных экспертов, Заключительный доклад, 2021 год, пункт 7.
[11] Рабочая группа открытого состава, Заключительный доклад, 2021 год, пункт 18.
[12] URL: www.icrc.org/en/document/potential-human-cost-cyber-operations.

использованию ИКТ государствами», и подчеркнула, что «напоминание об этих принципах ни в коем случае не узаконивает и не поощряет конфликты»[13]. МККК полностью поддерживает эту точку зрения: кибероперации во время вооруженного конфликта не происходят в «правовом вакууме» или «серой зоне» — на них распространяются установленные принципы и нормы международного гуманитарного права.

Для обеспечения понимания и эффективного применения международного гуманитарного права МККК приветствует дальнейшее изучение того, как и когда применяется эта область права. Чтобы избежать негативных гуманитарных последствий и дезорганизации общества, мы просим государства толковать и применять нормы и принципы международного гуманитарного права таким образом, чтобы были учтены специфические особенности сферы ИКТ. Важнейшие вопросы защиты жизни мирных граждан требуют дальнейшего изучения и четкого позиционирования со стороны государств. Например, в мире, где данные все чаще играют ключевую роль, приоритетом для государств должно стать достижение договоренности о том, чтобы данные о гражданском населении пользовались защитой от нападений, как и гражданские бумажные архивы. Кроме того, государства должны подтвердить, что кибероперации, наносящие ущерб гражданским объектам в результате нарушения их работы, подпадают под действие всех норм международного гуманитарного права, касающихся ведения боевых действий[14].

Несмотря на важность дальнейшего изучения и согласования ограничений, налагаемых международным правом на кибероперации во время вооруженного конфликта, эти правила станут эффективными только в результате их соблюдения на национальном уровне. По итогам обсуждений с военными практиками и экспертами МККК определил ряд ключевых шагов, с помощью которых государства могут и должны избегать ущерба гражданскому населению в результате военных операций во время вооруженных конфликтов[15]. Сегодня мы хотели бы особенно выделить четыре из них.

– Во-первых, каждое государство несет ответственность за все свои органы, участвующие в кибероперациях, и за тех, кто действует по указанию этого государства или под его руководством или контролем. Государства должны обеспечить, чтобы все они соблюдали международное гуманитарное право.

– Во-вторых, государства должны разработать ясные внутренние процессы для обеспечения того, чтобы в случае использования киберсредств или методов ведения войны они соответствовали применимой правовой базе.

– В-третьих, государства обязаны принимать все возможные меры предосторожности, чтобы избежать или по крайней мере свести к минимуму случайный ущерб гражданскому населению при совершении нападений, в том числе с использованием киберсредств и методов ведения кибервойны. В сфере ИКТ это может включать применение технических мер, таких как «системное ограждение», «геоограждение» или «аварийные кнопки»[16].

[13] Группа правительственных экспертов, Заключительный доклад, 2021 год, пункт 71(f).

[14] См. также МККК, Международное гуманитарное право и кибероперации во время вооруженных конфликтов: документ с изложением позиции МККК, 2019 год.

[15] ICRC, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

[16] «Системное ограждение» означает предотвращение запуска вредоносного программного обеспечения без точного совпадения с целевой системой, «геоограждение» означает ограничение работы вредоносного программного обеспечения только в определенном диапазоне IP-адресов, а «аварийные кнопки» означают способ отключения вредоносного программного обеспечения через определенное время или при удаленной активации.

– В-четвертых, государства также обязаны принимать меры по защите гражданского населения от угроз, возникающих в результате военных кибероперациий. Некоторые из этих мер, возможно, придется принимать и в мирное время.

В заключение МККК выражает признательность государствам-членам за стремление к международному диалогу и достижению согласия о возможной цене кибероперациий для людей и мерах по предотвращению и смягчению наносимого им ущерба. По нашему мнению, международное гуманитарное право должно быть одним из предметов таких дебатов, и МККК всегда готов поделиться своим опытом в ходе таких дебатов.

Приложение XXXVII

Заявление Исполнительного директора Международной организации уголовной полиции (Интерпол) по полицейским службам

Введение

В цифровую эпоху киберпреступность является глобальной проблемой. Ее воздействие выходит далеко за рамки того, что сообщается или обнаруживается; через Интернет она влияет на повседневную жизнь более чем 4,5 миллиарда человек. Возросшая в последнее время зависимость от цифровой среды создала больше возможностей для совершения преступлений в киберпространстве. Поскольку мишенями киберпреступников сегодня являются правительства, предприятия, ключевые объекты инфраструктуры и даже больницы, киберпреступность стала серьезной угрозой для безопасности во всем мире. Принимая во внимание рост масштабов киберпреступности и степени тяжести киберпреступлений, Международная организация уголовной полиции (Интерпол) уделяет приоритетное внимание борьбе с такими преступлениями.

Будучи глобальной и нейтральной межправительственной организацией, Интерпол знает международное право, нормы, меры укрепления доверия и потенциала в целях поддержания мира и безопасности в киберпространстве. Учитывая цель этих открытых дебатов, направленных на углубление нашего понимания растущих рисков, обусловленных злонамеренной деятельностью в киберпространстве, Интерпол представляет Совету Безопасности данное письменное заявление, чтобы поддержать приверженность членов Совета обеспечению мира и безопасности в киберпространстве. В заявлении освещаются последние тенденции киберпреступности и ее последствия, а также глобальные механизмы и решения Интерпола, которые доступны его 194 странам-членам для урегулирования этих насущных проблем.

Существующие и возникающие киберугрозы

За последний год Интерпол проанализировал широкий спектр киберугроз. В его недавно подготовленном аналитическом документе подчеркивается, что пандемия коронавирусного заболевания (COVID-19) открыла киберпреступникам новые возможности для совершения различных Интернет-преступлений независимо от региона. Среди основных угроз — вымогательство с помощью специальных вирусов, компрометация деловой электронной почты, незаконные операции по сбору данных, дезинформация и повторное появление более старых типов вредоносных программ, перепрофилированных с учетом глобальной пандемии.

В числе выявленных тенденций — работа против крупных корпораций, правительств и важнейших объектов инфраструктуры[17]. Киберпреступники и мошенники эксплуатируют базовые социальные потребности и социальную встревоженность. С марта 2020 года Интерпол получил ряд просьб от его стран-членов об отражении атак, совершаемых с использованием вирусов-вымогателей на больницы и другие учреждения, находящиеся на переднем крае борьбы с коронавирусом[18]. Атакуя эти важнейшие объекты инфраструктуры, которые

[17] INTERPOL, Assessment Report of the Impact of COVID-19 on Cybercrime, URL: https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

[18] URL: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

играют видную роль в реагировании на эту пандемию, преступники смогли максимизировать наносимый ущерб и свою финансовую выгоду.

Атаки с использованием вирусов-вымогателей не являются чем-то новым, но сегодня это самая быстрорастущая разновидность киберпреступности. Использование вирусов-вымогателей представляет собой весьма привлекательную и прибыльную «бизнес-модель» для киберпреступников благодаря использованию как вымогательства, так и системы предоставления своего рода услуг. Мы также заметили, что такие атаки не ограничивались географическими рамками, а это говорит о том, что преступники расширяют сферу своей деятельности, чтобы можно было атаковать любые учреждения по всему миру. Например, тот же вирус-вымогатель, который остановил работу одной из больниц в Европе, был использован и в Азии.

Кроме того, мы видели, как люди становились жертвами сложных мошеннических схем в Европе, а поступившие деньги в считанные часы переправлялись аж в Западную Африку и Юго-Восточную Азию. Кроме того, продолжают происходить массовые утечки данных, что наносит значительный финансовый ущерб бизнесу по всему миру. В то же время киберпреступники скрываются в «сером Интернете», который гарантирует анонимный и неотслеживаемый доступ. Это повышает важность и актуальность использования уведомлений Интерпола, особенно уведомления с фиолетовым углом, которые являются инструментом, позволяющим странам-членам обмениваться информацией об этих мошеннических схемах[19]. Цель состоит в том, чтобы распространить эту важную информацию еще до того, как произойдет следующая атака.

Кроме того, сочетание киберпреступлений и финансовых преступлений представляет собой сложную проблему. Этот вид преступности состоит из многих этапов: — от кибератаки до эксплуатации данных, после чего наступают фазы отмывания денег — это наслоение и в конечном счете обналичивание. Использование криптовалют в этом процессе тоже препятствует эффективному и своевременному реагированию. Учитывая сложность этих схем, надо применять модель совместной деятельности, которая объединяет силы и средства различных специализированных подразделений правоохранительных органов для более эффективной борьбы с кибермошенничеством и отмыванием денег. Чтобы предложить полный спектр оперативной и аналитической поддержки в этой области, Интерпол в конце 2020 года создал Глобальную целевую группу по борьбе с финансовыми преступлениями.

Глобальный механизм для смягчения киберугроз

Международное сотрудничество полицейских структур безусловно является жизненно важным для обеспечения безопасности столь взаимосвязанного мира. Как признается во Всестороннем исследовании киберпреступности, проведенном силами УНП ООН, Интерпол играет уникальную роль в усилиях по содействию сотрудничеству между органами полиции[20]. Чтобы поддержать деятельность 194 стран-членов, Интерпол должен содействовать трансграничному сотрудничеству правоохранительных органов и, когда это необходимо, оказывать помощь правительственным и межправительственным организациям, органам и службам, чья миссия заключается в предупреждении или пресечении преступности — в рамках законов, существующих в разных странах, и в духе Всеобщей декларации прав человека.

[19] URL: https://www.interpol.int/en/How-we-work/Notices/About-Notices.

[20] Всестороннее исследование УНП ООН по киберпреступности, стр.195.

Благодаря своему нейтралитету и глобальному присутствию Интерпол имеет уникальные возможности для координации глобальных правоохранительных мер по борьбе с киберпреступностью и для руководства ими. Он также дает возможность правоохранительным органам всего мира обмениваться информацией о киберпреступности и источниках угроз и предлагает широкий спектр экспертных знаний, технических рекомендаций и видов оперативной помощи. На основании этой уникальной роли Интерпол отстаивал и подчеркивал важность международного сотрудничества между органами полиции в рамках различных политических процессов Организации Объединенных Наций, таких как Группа экспертов Организации Объединенных Наций для проведения всестороннего исследования киберпреступности[21] и Рабочая группа открытого состава Организации Объединенных Наций по безопасности ИКТ.

23 ноября 2020 года был единогласно принят второй двухлетний обзор резолюции Генеральной Ассамблеи о сотрудничестве между Организацией Объединенных Наций и Интерполом, что ознаменовало собой выход партнерства на новый уровень[22]. Это стало крупным достижением, поскольку были разработаны новые формулировки по ключевым областям сотрудничества, включая киберпреступность, что сделало еще более легитимным дальнейшее сотрудничество между этими двумя организациями в данной области.

В нашу эпоху цифровизации национальных и даже региональных решений уже недостаточно. Для содействия достижению международного мира и безопасности в киберпространстве Интерпол может стать глобальным механизмом эффективной борьбы с киберпреступностью и предоставлять странам-членам различные услуги и инструменты, такие как:

- защищенная глобальная полицейская система связи “I-24/7” для безопасного и срочного обмена полицейской информацией в режиме реального времени;
- 19 баз данных[23] и типов уведомлений[24], которые играют важную роль в оповещении международного сообщества и поддержке транснациональных расследований;
- Глобальная программа Интерпола по борьбе с киберпреступностью, которая предоставляет правоохранительные силы и средства в области предотвращения, выявления, расследования и пресечения киберпреступлений с целью снижения глобального воздействия киберпреступности и защиты групп населения во имя построения более безопасного мира;
- Глобальная экспертная группа Интерпола по киберпреступности и региональные рабочие группы с руководителями подразделений по борьбе с киберпреступностью для обсуждения актуальных вопросов, касающихся киберпреступности, и разработки оперативных и стратегических планов;
- коммуникационные платформы, такие как Платформа для обмена знаниями о киберпреступности, для безопасного обмена информацией в рамках более широкого правоохранительного сообщества и Платформа сотрудни-

[21] URL: https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf и https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf.

[22] Резолюция 75/10 Генеральной Ассамблеи по вопросу о сотрудничестве между Организацией Объединенных Наций и Международной организацией уголовной полиции (Интерпол).

[23] URL: https://www.interpol.int/en/How-we-work/Databases/Our-19-databases.

[24] URL: https://www.interpol.int/en/How-we-work/Notices/About-Notices.

чества в области киберпреступности — оперативная деятельность для закрытых оперативных обсуждений;

- Платформа киберинтеграции для сбора данных о киберпреступлениях и проведения углубленного анализа;
- круглосуточный Координационный центр Интерпола по киберпреступности для установления связи в режиме реального времени между подразделениями по борьбе с киберпреступностью из разных стран в целях обеспечения сотрудничества правоохранительных органов;
- Глобальная группа Интерпола по реагированию на инциденты в киберпространстве для координации действий правоохранительных органов по реагированию на крупные кибер-инциденты;
- Глобальная целевая группа Интерпола по борьбе с финансовыми преступлениями для сокращения общемирового числа и воздействия финансовых преступлений путем расширения международного сотрудничества и инноваций, с акцентом на кибермошенничество и схемы отмывания денег.

Многосторонний подход

Расследование киберпреступлений сопряжено с рядом проблем, которые не встречаются в физической сфере. Для правоохранительных органов непросто узнать из первых рук, что нападение произошло, и даже в этом случае количество поступающих сигналов невелико. Для расследования киберпреступлений нужны также специальные навыки и технологии, которые доступны не всем. Киберпреступность, будучи по своей сути глобальной, зачастую препятствует эффективному реагированию, поскольку улики и подозреваемые находятся одновременно в нескольких юрисдикциях.

Чтобы преодолеть эти трудности, Интерпол сделал партнерство главным элементом своих усилий по борьбе с киберпреступностью. На 88-й сессии Генеральной ассамблеи Интерпола, которая состоялась в 2019 году, страны-члены одобрили правовую основу под названием «Гейтуэй», которая позволяет Интерполу обмениваться информацией с компаниями частного сектора[25]. Это решение было основано на том, что правоохранительным органам необходимо тесно сотрудничать с частным сектором, где сосредоточено большинство данных и знаний, касающихся киберпреступности.

В настоящее время в рамках Глобальной программы Интерпола по борьбе с киберпреступностью действуют 12 частных партнеров, которые обмениваются актуальной информацией и знаниями в области киберпреступности, а также оказывают техническую помощь правоохранительным органам. Доступ к данным — как из государственного, так и частного секторов — позволяет Интерполу оказывать специализированную оперативную поддержку и давать технические рекомендации странам-членам.

Кроме того, сотрудничество с различными членами глобальной экосистемы кибербезопасности имеет огромное значение, поскольку разные базы данных могут содействовать разработке эффективной политики и оперативных мер по борьбе с киберпреступностью. Это также помогает нам накапливать опыт, с тем чтобы быть устойчивыми и гибкими, особенно во времена неопределенности. В конце прошлого года Интерпол совместно со своим частным партнером помог полиции Нигерии арестовать членов организованной преступной группы, ответственной за проведение фишинговых и мошеннических операций с

[25] URL: https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-roadmap-for-global-policing.

использованием деловой электронной почты, затрагивающих правительства и компании частного сектора в более чем 150 странах[26].

Интерпол также уделяет особое внимание профилактике. Для предотвращения киберпреступлений Интерпол тесно сотрудничает со своими государственными и частными партнерами в целях пропаганды надлежащей кибергигиены, проводя серию глобальных информационных кампаний. Эти усилия также помогают правоохранительным организациям преодолевать многочисленные трудности в борьбе с киберпреступностью путем повышения осведомленности общественности о самих преступлениях, способах защиты и действиях в случае совершения таких преступлений.

Выводы

Поскольку все связи между преступниками, объектами инфраструктуры и жертвами простираются за пределы национальных границ и юрисдикций, местные правоохранительные органы не всегда обладают возможностями или потенциалом для того, чтобы заняться этими транснациональными элементами в ходе борьбы с киберпреступностью. Государства-члены должны помнить о том, что недостаточные кибервозможности или силы и средства правоохранительных органов в разных регионах — это по-прежнему главный фактор, позволяющий преступным организациям распространять свои сети и деятельность там, где меньше риска.

В целях смягчения этих постоянно меняющихся угроз и рисков, связанных с киберпространством, страны-члены должны использовать и максимально расширять сотрудничество между полицейскими структурами для своевременного и эффективного реагирования. Благодаря своему присутствию в каждой стране Интерпол способен свести все воедино, выявить и пресечь деятельность преступников в киберпространстве вместе с нашими странами-членами и партнерами.

Очевидно, что эффективная борьба с киберпреступностью возможна только при условии глобально скоординированного — и, что важно, быстрого — реагирования. Мы должны защитить системы, подготовить наше руководство, поделиться решениями и стимулировать правильное реагирование. В частности, правоохранительные органы должны быть надежным и эффективным партнером, поскольку обмен данными имеет ключевое значение — в том числе между национальными полицейскими силами, частным сектором и глобальными экспертами, такими как Интерпол. Укрепление доверия в мировом правоохранительном сообществе — с позиции «смело делись» — имеет решающее значение для достижения общей цели борьбы с киберпреступностью.

В то время как международное сообщество находится под исключительным давлением, для выполнения задачи обеспечения нашей общей безопасности мы должны двигаться в сторону более тесного сотрудничества и интеграции. Именно за это и выступает Интерпол: за содействие международному сотрудничеству правоохранительных органов в интересах строительства более безопасного мира. Поскольку все мы убеждены в том, что безопасность и правосудие являются ключом к обеспечению мира и устойчивости в киберпространстве, Интерпол вместе с Организацией Объединенных Наций содействует международному сотрудничеству в правоохранительной сфере. Для того чтобы эта работа увенчалась успехом, Интерпол будет продолжать оказывать поддержку своим странам-членам в борьбе с киберпреступностью.

[26] URL: https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group.

Приложение XXXVII

Заявление Постоянного представителя Исламской Республики Иран при Организации Объединенных Наций Маджида Тахта Равранчи

Киберпространство предоставляет человечеству поистине золотые возможности для постоянного развития и достижения прогресса во всех областях его жизни. Поэтому такой выдающийся инструмент необходимо не только продвигать по всему миру, особенно в развивающихся странах, но и защищать от любых угроз.

Киберпространство также может использоваться для совершения актов агрессии, нарушения мира, «угрозы силой или ее применения», «для вмешательства в дела, которые по существу относятся к внутренней юрисдикции любого государства», для нарушения суверенитета государств или для принуждения других государств. Их также необходимо эффективно предотвращать.

В качестве руководящего принципа существующие «применимые» принципы и нормы международного права, разумеется, без неправильного или произвольного толкования, должны регулировать права, обязанности и поведение государств в отношении киберпространства.

Однако, когда нет консенсуса относительно применимости международного права или даже отсутствуют международные нормы, касающиеся киберпространства, международному сообществу надо работать над определением необходимых норм.

С этой целью и с учетом того, что Генеральная Ассамблея уполномочена Уставом на «прогрессивное развитие международного права и его кодификацию», Ассамблея должна продолжать свои нынешние усилия по разработке и кодификации международных принципов и норм, необходимых для киберпространства, в том числе в форме международного юридически обязывающего документа.

Параллельно с такими усилиями государства должны предпринимать все шаги для содействия максимально широкому использованию киберпространства в целях своего развития и при этом должны действовать ответственно и согласно применимым нормам международного права, прежде всего, в соответствии с целями и принципами Организации Объединенных Наций.

Главная ответственность за поддержание безопасного, надежного и заслуживающего доверия киберпространства лежит на самих государствах. Поэтому, учитывая нынешнюю сложную ситуацию с управлением киберпространством, необходимо поощрять и обеспечивать заметную роль и серьезное участие государств в управлении киберпространством на глобальном уровне, особенно в области разработки политики и принятия решений.

В то же время намечаемое управление киберпространством должно быть разработано таким образом, чтобы оно не оказывало негативного влияния на права государств в выборе путей развития, управления и законодательства в отношении киберпространства.

Право государств иметь «свободный доступ к информации и в полной мере развивать без вмешательства свою систему информации и средств массовой информации и использовать свои средства информации для продвижения своих политических, социальных, экономических и культурных интересов и чаяний», а также «право и обязанность государств бороться, в рамках своих конститу-

ционных прерогатив, с распространением ложных или искаженных новостей», что также было подтверждено Генеральной Ассамблеей в Декларации о недопустимости вмешательства и интервенции во внутренние дела государств 1981 года, должно полностью соблюдаться.

При выполнении своих обязанностей по поддержанию безопасного, надежного и пользующегося доверием киберпространства государства должны придерживаться подхода, основанного на сотрудничестве, а не на конфронтации.

Как подтвердила Генеральная Ассамблея в Декларации о недопустимости вмешательства во внутренние дела государств и защите их независимости и суверенитета 1965 года, «ни одно государство не имеет права прямо или косвенно вмешиваться по какой бы то ни было причине во внутренние или внешние дела любого другого государства». Поэтому все государства должны предотвращать такие действия и воздерживаться от действий, направленных, в частности, против политических, экономических и культурных элементов или важнейших объектов инфраструктуры государств, связанных с киберпространством, в том числе с помощью кибернетических путей и средств.

Кроме того, в принятой в 1981 году Декларации о недопустимости интервенции и вмешательства во внутренние дела государств Ассамблея подтвердила обязанность государства «обеспечить, чтобы его территория не использовалась каким-либо образом, который нарушал бы суверенитет, политическую независимость, территориальную целостность и национальное единство или подрывал политическую, экономическую и социальную стабильность другого государства»; «воздерживаться от любых действий или попыток в любой форме и под любым предлогом дестабилизировать или подорвать стабильность другого государства или любого из его институтов», а также «воздерживаться от любых клеветнических кампаний, оскорбительной или враждебной пропаганды с целью осуществления интервенции или вмешательства во внутренние дела других государств». Эти правила должны соблюдаться государствами и в отношении киберпространства.

Согласно одному из принципов, подтвержденных Генеральной Ассамблеей в Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, 1970 года, государства не должны использовать «какие-либо другие меры принудительного характера, направленные на ущемление его суверенных прав или на извлечение из этого какой-либо выгоды». Поэтому государства не должны использовать достижения, связанные с киберпространством, в качестве инструментов для экономических, политических или любых других видов принудительных мер, в том числе путем ограничения или блокирования мер против других государств.

Точно так же государства должны воздерживаться от угрозы силой или ее применения в киберпространстве или через него. Они также должны воздерживаться от злоупотребления и не допускать злоупотребления связанными с киберпространством цепочками поставок, разработанными под их контролем и юрисдикцией, для создания или стимулирования уязвимости в продуктах, услугах и обслуживании, ставящей под угрозу суверенитет и защиту данных других государств.

Государства также должны осуществлять должный контроль за компаниями и платформами, связанными с киберпространством, находящимися под их юрисдикцией, и принимать соответствующие меры для привлечения их к ответственности за их поведение в сфере ИТК, в том числе за нарушение национального суверенитета, безопасности и общественного порядка других государств.

В любом случае государства несут ответственность за свои международно-противоправные действия в киберпространстве или через него.

Кроме того, все международные споры, связанные с киберпространством, должны урегулироваться исключительно мирными средствами и на основе «суверенного равенства государств и в соответствии с принципом свободного выбора средств», как указано в Манильской декларации 1970 года о мирном разрешении международных споров.

В этой связи стоит напомнить, что в последние годы мы наблюдаем тревожную тенденцию систематических обвинений одних государств в адрес других государств в совершении кибератак или аналогичной деятельности в киберпространстве. Учитывая существующие проблемы, связанные с присвоением ответственности за действия в киберпространстве, а также отсутствие набора разработанных и согласованных на международном уровне стандартов в отношении подлинных, надежных и адекватных доказательств для обоснования присвоения ответственности, такие обвинения следует считать просто политически мотивированными.

В целом киберпространство и связанные с ним средства, методы и технологии должны использоваться исключительно в мирных целях, и для этого государства должны действовать сообща, ответственно и в полном соответствии с применимым международным правом.

Наконец, мы разделяем мнение о том, что рассмотрение вопросов, связанных с киберпространством, должно быть продолжено в Генеральной Ассамблее. Со своей стороны, Исламская Республика Иран, как одна из жертв кибератак с помощью вредоносного компьютерного червя «Стракснет», который, как считается, был создан совместно Соединенными Штатами и израильским режимом для нанесения ущерба иранским мирным ядерным установкам, готова внести свой вклад в усилия Ассамблеи по разработке принципов и норм, необходимых для киберпространства.

Приложение XXXIX

Заявление Постоянного представительства Италии при Организации Объединенных Наций

Италия выражает признательность Эстонии за привлечение внимания Совета Безопасности к вопросу о кибербезопасности и рада принять участие в сегодняшних открытых дебатах.

Мы также высоко ценим поддержку и преданность Высокого представителя по вопросам разоружения г-жи Накамицу и ее готовность провести брифинг в Совете Безопасности в то время, когда государства-члены озабочены ростом числа инцидентов в сфере кибербезопасности.

Италия присоединяется к заявлению Европейского союза, и наша делегация хотела бы добавить несколько замечаний от своей страны.

Время проведения этих дебатов как никогда подходящее. Генеральная Ассамблея отметила работу последних двух лет, проведенную Первым комитетом по достижениям в области информационно-коммуникационных технологий по вопросам международной безопасности и поощрению ответственного поведения государств в киберпространстве. Два доклада, принятые Рабочей группой открытого состава и Группой правительственных экспертов в этом полугодии, представляют собой важные достижения, призванные способствовать укреплению доверия между государствами-членами. Они также высветили область, которая в течение нескольких лет считалась исключительно технической.

Темпы цифровизации ускоряются во всем мире, но у этого процесса есть не только преимущества, связанные с таким развитием, но и сложности, которые касаются сохранения киберпространства как глобальной, открытой и стабильной области. Участившиеся в последние месяцы инциденты, порой направленные против важнейших объектов инфраструктуры и наносящие большой ущерб мировой экономике, вызывают сожаление. Некоторые из этих атак показали возможность человеческих жертв, к которым могут привести такие действия, особенно во время пандемии. Губительные последствия злоупотребления новыми технологиями становятся все более очевидными, как и необходимость держать эти технологии под контролем. Италия считает, что Организация Объединенных Наций лучше всего подходит для выполнения этой задачи и для содействия миру и стабильности в киберпространстве.

Италия хотела бы присоединиться к заявлению Европейского союза в отношении применимости международного права в киберпространстве, включая международное гуманитарное право и право прав человека, важность соблюдения норм ответственного поведения государств, а также пользу мер по укреплению доверия как практического средства предотвращения конфликтов. Мы также хотим подчеркнуть важную роль, которую региональные организации могут сыграть в области кибербезопасности. Будучи убежденными сторонниками многостороннего подхода, мы поощряем диалог между Организацией Объединенных Наций и региональными организациями и в связи с этим приветствуем недавно состоявшиеся дискуссии между Генеральным секретарем Организации Объединенных Наций и Европейским советом как хорошую возможность обменяться мнениями о вызовах, с которыми мы сталкиваемся. Мы также высоко ценим усилия, которые предпринимала Швеция, когда она председательствовала в Организации по безопасности и сотрудничеству в Европе и выдвигала на первый план взаимосвязь между правами человека, гендерными вопросами и кибербезопасностью.

В условиях постоянно растущей взаимосвязанности мира диалог становится еще более важным средством продвижения общего понимания и расширения возможностей для сотрудничества. Поэтому мы поддерживаем диалог Европейского союза с Организацией Объединенных Наций и региональными организациями, включая Африканский союз, Региональный форум Ассоциации государств Юго-Восточной Азии и Канцелярию Специального советника.

Через региональные организации государства-члены могут максимально расширить свои двусторонние контакты, обмениваясь передовым опытом и извлеченными уроками, обеспечивая тем самым, чтобы региональные подходы не расходились. Дальнейшие усилия должны быть направлены на механизмы мирного урегулирования споров, а также на инициативы по развитию кибердипломатии и киберпосредничества.

Мы считаем, что киберпространство должно оставаться открытым, свободным, безопасным и стабильным в качестве средства, дающего государствам возможность проводить политику, которая позволит обществу процветать и гарантировать устойчивое развитие для всех, способствуя достижению ЦУР. Важность наращивания потенциала нельзя недооценивать, поскольку оно гарантирует одинаковую устойчивость государств, повышает осведомленность и стимулирует развитие возможностей. Многое еще предстоит сделать в этой области, и мы считаем, что программа действий по поощрению ответственного поведения государств в киберпространстве, продвигаемая совместно с другими 52 государствами-членами, может стать приоритетной платформой для координации и поощрения этих усилий. Мы уже заявили о своей готовности к дальнейшему обмену мнениями по этой инициативе в контексте обсуждений в Первом комитете и хотим подтвердить свою решимость сегодня. Эта программа действий может также стать форумом, где вырабатывается подход с участием многих заинтересованных сторон и развиваются государственно-частные партнерства.

В 2020 и 2021 годах вследствие пандемии произошел драматический откат назад. Наши совместные усилия надо направить на возобновление устойчивого развития, и киберсфера является для этого очень важным компонентом. Италия работает над достижением этой цели как член Группа семи и продвигает эту концепцию в контексте своего нынешнего председательства в Группе двадцати. Сегодняшние дебаты — это жизненно важный шаг к повышению осведомленности и обеспечению того, чтобы события, связанные с цифровизацией, происходили в безопасной и стабильной киберсфере без попыток подорвать какие-либо усилия.

Эти дебаты проходят в то время, когда министры иностранных дел стран Группы двадцати встречаются в Матере для обсуждения вопросов восстановления и устойчивого развития, чтобы никто не был забыт. Мы надеемся, что эти усилия будут подкреплять друг друга и что Совет Безопасности будет и впредь уделять внимание киберпроблемам, следить за прогрессом и быть готовым призвать к ответственности государства, не выполняющие свои обязательства. Надеемся, что таких случаев будет очень мало, поскольку государства-члены сходятся во мнении о необходимости посвятить время и усилия позитивной повестке дня в области кибербезопасности — той, которая содействует укреплению доверия, транспарентности и всеобъемлющего подхода.

Приложение XL

Заявление посла по делам Организации Объединенных Наций и киберполитике Министерства иностранных дел Японии Акахори Такеси

Япония хотела бы выразить искреннюю признательность Кае Каллас, Премьер-министру Эстонской Республики, за организацию этих открытых дебатов по теме кибербезопасности. Япония благодарит Эстонию за то, что в ее концептуальной записке были отмечены открытые дебаты по сложным современным вызовам международному миру и безопасности, организованные в 2017 году под председательством Японии.

Япония приветствует принятие доклада Рабочей группы открытого состава в марте и принятие доклада шестой Группой правительственных экспертов в мае, отмечая, что оба эти доклада были приняты консенсусом.

Наибольшая ценность доклада Рабочей группы открытого состава заключается в том, что он был принят консенсусом в результате процесса, в котором могли принять полноценное участие все государства-члены; они напрямую подтвердили положения свода международно-правовых документов, в том числе те, в которых утверждается, что международное право, в частности Устав Организации Объединенных Наций во всей его полноте, применимо в киберпространстве.

Доклад Группы правительственных экспертов имеет дополнительную ценность. По каждой из 11 норм, включенных в доклад Группы правительственных экспертов 2015 года, в новом докладе представлены рекомендации и примеры реализации. Япония надеется, что это содержание будет способствовать дальнейшему развитию сотрудничества между государствами в поощрении ответственного поведения государств. Кроме того, теперь стало более ясно, что международно-противоправные деяния, приписываемые государству, влекут за собой ответственность этого государства. Применимость международного гуманитарного права выражена четко. Группа вновь отметила неотъемлемое право государств принимать меры, признанные в Уставе.

Мы надеемся на углубление конкретных дискуссий по применению международного права в киберпространстве на различных форумах в будущем. Япония надеется, что меморандум, который она представила для сборника национальных позиций, выраженных в Группе правительственных экспертов, станет вкладом в такие обсуждения. Здесь я хотел бы поделиться наиболее важными аспектами в позиции Японии.

Япония считает, что государство не должно нарушать суверенитет другого государства посредством кибероперaций. Более того, государство не должно вмешиваться в вопросы, входящие во внутреннюю компетенцию другого государства, посредством кибероперaций. Международно-противоправные деяния, совершенные государством в киберпространстве, влекут за собой ответственность государства.

В соответствии с международным правом государства обязаны проявлять должную осмотрительность в отношении кибероперaций. Нормы 13(c) и (f) и второе предложение пункта 71(g) доклада Группы правительственных экспертов 2021 года связаны с этим обязательством. Касаясь недавнего инцидента с трубопроводом «Колониал», Президент США упомянул об усилиях по созданию «своего рода международного стандарта, согласно которому правительства, зная, что на их территории происходит преступная деятельность, принимают

меры против этих преступных организаций». Мы признаем сложность присвоения ответственности за кибероперации тому или иному государству. Обязательство проявлять должную осмотрительность может служить основанием для привлечения к ответственности государства, с территории которого произошла кибероперация, не приписываемая ни одному государству.

Любой международный спор, связанный с кибероперациями, должен решаться мирными средствами в соответствии со статьей 2(3) Устава Организации Объединенных Наций. В целях мирного урегулирования споров, возникающих в связи с кибероперациями, следует использовать полномочия Совета Безопасности, основанные на главах VI и VII Устава Организации Объединенных Наций, а функции других органов Организации Объединенных Наций следует использовать для урегулирования споров, связанных с кибероперациями. У Японии есть оговорки, касающиеся идеи создания нового международного механизма присвоения ответственности.

По мнению Японии, когда кибероперация представляет собой вооруженное нападение по смыслу статьи 51 Устава Организации Объединенных Наций, государства могут воспользоваться неотъемлемым правом на индивидуальную или коллективную самооборону, признанным в той же статье. Международное гуманитарное право применимо к кибероперациям. Это утверждение способствует регулированию методов и средств ведения войны. Аргумент о том, что данное утверждение приведет к милитаризации киберпространства, безоснователен.

Международное право прав человека также применимо к кибероперациям. Люди пользуются теми же правами человека в отношении киберопераций, что и в других ситуациях.

Что касается взаимосвязи между международным правом и добровольными нормами, то для стабилизации киберпространства необходимо, чтобы международное право и нормы работали в тандеме для предотвращения международно-противоправных деяний с использованием ИКТ и для поощрения ответственного поведения государств в киберпространстве. Как ясно сказано в докладе Рабочей группы открытого состава, нормы не заменяют и не изменяют обязательства государств по международному праву.

Япония надеется, что многие государства-члены добровольно опубликуют свои национальные позиции относительно способов применения международного права.

По мнению Японии, настало время сделать приоритетным выполнение согласованных добровольных норм и обязательств по международному праву, а также принятие мер по укреплению доверия и наращиванию потенциала.

Говоря об имплементации, Япония хотела бы предложить правительствам активно объявлять о своей правовой оценке в случае проведения злонамеренной кибероперации, в том числе о том, представляет ли она собой нарушение международного права. Такая практика будет способствовать общему пониманию того, как международное право применяется к кибероперациям. Применение международного права международными и национальными судами и трибуналами к киберинцидентам будет иметь аналогичный эффект. Япония надеется, что все более частое применение такой практики позволит сдержать злонамеренную деятельность в киберпространстве.

Япония твердо поддерживает разработку программы действий. Мы считаем, что такая программа действий станет эффективным механизмом обеспечения и мониторинга выполнения согласованных норм, обязательств по международному праву, мер по укреплению доверия и наращивания потенциала. Мы с

нетерпением ждем более глубокого обсуждения такой программы действий. Мы также продолжим активное участие в деятельности новой Рабочей группы открытого состава.

Япония привержена сохранению свободного, справедливого и безопасного киберпространства и будет продолжать активно участвовать в обсуждениях и усилиях по обеспечению верховенства права в киберпространстве, в том числе и в Организации Объединенных Наций.

Приложение XLI

Заявление Постоянного представителя Казахстана при Организации Объединенных Наций Магжана Ильясова

Мы выражаем благодарность Эстонии, выполняющей функции Председателя, за организацию и проведение дебатов по теме «Поддержание международного мира и безопасности: кибербезопасность».

В условиях глобальных угроз обеспечение безопасности требует координации действий международного сообщества и урегулирования многих аспектов политического и экономического характера. В этом контексте следует отметить, что в мире появилась новая и одновременно сложная составляющая — кибербезопасность.

Должно быть ясно, что информационно-коммуникационные технологии обладают огромным потенциалом для развития государств. В то же время они создают новые возможности для преступников и могут способствовать повышению уровня и сложности преступлений, потенциальному риску неправомерного использования новых технологий, включая искусственный интеллект. В связи с этим предупреждение и пресечение использования информационно-коммуникационных технологий в преступных целях должно стать приоритетом в работе государств на нынешнем этапе.

В связи с этим мы приветствуем создание специального межправительственного комитета экспертов открытого состава, представляющего все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях с полным учетом существующих международных документов и усилий на национальном, региональном и международном уровнях по борьбе с использованием информационно-коммуникационных технологий в преступных целях, предусмотренных резолюцией 74/247, принятой Генеральной Ассамблеей 27 декабря 2019 года.

Мы считаем, что на работу Организации Объединенных Наций в этой области окажут дальнейшее влияние принятый в марте 2021 года заключительный субстантивный доклад Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности и консенсус по резолюции 75/240 о создании Рабочей группы открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025, а также одобренный консенсусом доклад, принятый Группой правительственных экспертов по поощрению ответственного поведения в киберпространстве в контексте международной безопасности в мае 2021 года.

Государства должны продолжать усиливать меры по защите всех важнейших объектов инфраструктуры от угроз ИКТ и расширять обмен передовым опытом в этой сфере.

В связи с этим мы приветствуем переговорный процесс по кибербезопасности в Организации Объединенных Наций и понимание его участниками и странами-членами того, что все решения по этой конкретной повестке дня должны приниматься консенсусом.

Приложение XLII

Заявление Постоянного представительства Латвии при Организации Объединенных Наций

Развитие информационно-коммуникационных технологий (ИКТ) дало государствам и обществу множество преимуществ в сфере экономики, услуг, образования и коммуникации. Отмечая огромный положительный эффект от применения ИКТ, Латвия выражает растущую обеспокоенность последствиями злонамеренного и губительного использования ИКТ, которые могут сказаться как на международном мире, безопасности и стабильности, так и на правах человека.

Чаще всего от таких правонарушений страдают государства, в том числе от тех, которые затрагивают демократические институты и важнейшие объекты инфраструктуры. Еще больше тревоги вызывает тот факт, что злонамеренная кибердеятельность использует пандемию коронавирусного заболевания, нацеливаясь на системы медицинского обслуживания, необходимые для поддержания здоровья людей, исследования вакцин, а также на информационное пространство.

Широкое участие и само обсуждение темы на заседании по формуле Аррии Совета Безопасности Организации Объединенных Наций в прошлом году подтвердили растущую актуальность кибербезопасности для вопросов международного мира и стабильности. Поэтому включение вопроса о кибербезопасности в официальную повестку дня Совета Безопасности своевременно и уместно. Латвия полностью поддерживает усилия Эстонии по надлежащему осмыслению смягчения последствий безответственного поведения в киберпространстве для международного мира и безопасности.

Организация Объединенных Наций должна оставаться важным глобальным игроком для продвижения мира, безопасности и стабильности, в том числе в киберпространстве. Активная работа Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности за последние годы заложила хорошую основу для сегодняшней дискуссии.

Два принятых консенсусом заключительных доклада Группы правительственных экспертов и Рабочей группы открытого состава — это отрадные вехи на пути к дальнейшей работе с целью достижения общего понимания по широкому кругу вопросов.

В этом отношении программа действий по поощрению ответственного использования ИКТ государствами в контексте международной безопасности является ценным результатом подготовки докладов Группы правительственных экспертов и Рабочей группы открытого состава. Программа действий в сфере киберпространства должна служить прочной и, главное, ориентированной на действия основой для дальнейшей работы по достижению существенного прогресса в деле реализации норм ответственного поведения.

В связи с этим Латвия хотела бы подчеркнуть многосторонний характер киберпространства, который требует вовлечения в дискуссии целого ряда негосударственных субъектов из частного сектора, гражданского общества и научных кругов. Учитывая их весомую долю в экосистеме ИКТ, следует ожидать, что эти заинтересованные стороны могут внести значительный вклад различными способами, делясь своими взглядами, знаниями и опытом.

Государствам следует продолжать активную работу и быть готовыми к углубленным дискуссиям в рамках будущих процессов Организации Объединенных Наций для обеспечения ответственного поведения государств в киберпространстве в контексте международной безопасности. Хотя все мы должны неустанно работать над укреплением защиты и безопасности наших собственных ИКТ, государства не должны позволять другому государству или негосударственному субъекту использовать ИКТ на своей территории для совершения международно-противоправных деяний. Мы призываем все государства воздержаться от проведения подобной деятельности, ее поощрения или терпимого к ней отношения, что не соответствует международному праву, в том числе Уставу Организации Объединенных Наций, чтобы не препятствовать обеспечению безопасности, связанной с использованием ИКТ. Ответственность, укрепление доверия и предсказуемость должны стать ключевыми элементами международного сотрудничества в области кибербезопасности.

Для того чтобы предотвратить недопонимание и ошибочные представления, с одной стороны, и ввести практику общения по инцидентам ИКТ, с другой стороны, мы должны установить открытые каналы связи между членами Организации Объединенных Наций. Создание сети контактных пунктов на политическом и техническом уровнях в Организации Объединенных Наций может внести крупный вклад в повышение эффективности глобального общения. Сеть контактных пунктов уже доказала свою эффективность на региональном уровне в Организации по безопасности и сотрудничеству в Европе.

В заключение Латвия хотела бы поблагодарить все государства-члены за демонстрацию приверженности сотрудничеству и совместной работе для достижения консенсуса по докладам в процессах Группы правительственных экспертов и Рабочей группы открытого состава. Это правильный путь и прекрасная возможность для дальнейшего укрепления международного сотрудничества на пути к глобальному, открытому, стабильному, мирному и безопасному киберпространству, где в полной мере осуществляются права человека и основные свободы и царит верховенство права.

Приложение XLIII

Заявление Временного Поверенного в делах, заместителя Постоянного представителя Лихтенштейна при Организации Объединенных Наций Георга Шпарбера

Кибероперации служат уравнителем в современной войне, предоставляя новые возможности как для наступательных, так и для оборонительных операций всем субъектам, включая тех, у кого меньше ресурсов. В результате в последние годы частотность и опасность кибероперациий возросли, а это создает угрозу международному миру и безопасности. Вызывает тревогу тот факт, что такие нападения способны причинить большие страдания гражданскому населению, включая гибель людей и нарушение работы базовых служб. В связи с этим мы напоминаем, что государства все чаще соглашаются с тем, что международное право, — в частности Устав Организации Объединенных Наций во всей его полноте и нормы обычного международного права, вытекающие из принципов Устава, а также Римский статут Международного уголовного суда и международное гуманитарное право, — применимо к киберпространству.

Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности придала официальный характер обсуждениям вопросов, касающихся международного мира и безопасности в киберпространстве, в Организации Объединенных Наций. Кроме того, заключительный доклад, опубликованный Группой правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, подтверждает применимость и необходимость международного права в киберпространстве. Лихтенштейн отмечает совместный вклад Рабочей группы открытого состава и Группы правительственных экспертов в развитие дискуссии о том, как международное право, в частности Устав Организации Объединенных Наций, применяется к киберпространству.

Одним из знаковых достижений Устава Организации Объединенных Наций является запрет на применение силы. Применение силы запрещено, за исключением случаев, когда оно санкционировано Советом Безопасности в соответствии с главой VII или осуществляется в порядке самообороны в соответствии со статьей 51 Устава. Однако на статью 51 все чаще ссылаются как на правовую основу применения силы без необходимых юридических обоснований. Существует значительный риск распространения этой тенденции на киберпространство по мере развития новых технологий и возможностей государств. Мы должны обеспечить, чтобы киберпространство не способствовало неоправданным операциям по самообороне. И, напомним, что ссылка на статью 51 прежде всего требует доказательств неотвратимости вооруженного нападения и всегда требует доказательств необходимости и соразмерности мер, принятых в ответ.

Устав Организации Объединенных Наций предусматривает правоприменительную роль Совета Безопасности в отношении наиболее серьезных нарушений соответствующих норм международного права, которые равносильны актам агрессии. В дополнение к инструментам, содержащимся в Уставе, Совет теперь также имеет возможность устанавливать индивидуальную уголовную ответственность для лиц, совершивших преступление агрессии, путем передачи соответствующих ситуаций в МУС. В этой связи Лихтенштейн считает, что ясное понимание того, как Римский статут применяется к кибероперациям, будет содействовать работе Совета.

Стремясь прояснить применение Римского статута к кибероперациям, Лихтенштейн вместе с десятью другими государствами-участниками МУС создал Совет консультантов для изучения роли МУС в регулировании кибервойн. Совет консультантов, состоящий из 16 выдающихся юристов-международников, собирался трижды в 2019 и 2020 годах для того, чтобы обсудить, в какой степени основные положения Римского статута применимы к кибероперациям. Заключительный доклад планируется представить в этом году. Мы надеемся, что это будет способствовать общему пониманию ответственности в контексте кибероперациий, но прежде всего предотвращению таких преступлений.

Лихтенштейн подчеркивает необходимость создания надежной правовой базы для регулирования киберпространства в интересах международного мира и безопасности. Мы рады внести свой вклад в глобальные усилия по борьбе со злонамеренными кибероперациями с помощью нашего предстоящего доклада, посвященного Римскому статуту, и мы будем и впредь стремиться к международному миру и безопасности, проявляя непоколебимую приверженность международному праву.

Приложение XLIV

Заявление Постоянного представительства Мальты при Организации Объединенных Наций

Мальта благодарит Эстонию за организацию этих своевременных дебатов по вопросу, который, по нашему мнению, должен быть в повестке дня Совета Безопасности. Хотя вопросы кибербезопасности затрагивались в ходе некоторых дебатов в Совете Безопасности, мы считаем, что этим вопросам следует уделять больше внимания, учитывая, что они входят в число самых важных и постоянно эволюционирующих вопросов, касающихся международного мира и безопасности.

Мальта присоединяется к заявлению Европейского союза и хотела бы со своей стороны особо выделить ряд моментов. Эволюция киберпространства принесла с собой некоторые возможности для государств-членов и граждан по всему миру и привела к росту благосостояния, подключению к Интернету и экономическому росту. Однако киберсфера также открыла двери для злонамеренной деятельности, направленной на подрыв и использование уязвимостей общества и проведение атак, которые могут иметь значительные последствия для государств-членов и их граждан, например, в отношении конфиденциальных данных и важнейших объектов инфраструктуры. И действительно, чем больше мы переходим в виртуальный и взаимосвязанный мир, тем больше мы подвержены такого рода вредоносной деятельности.

Мальта считает, что Организация Объединенных Наций должна играть центральную роль в регулировании поведения государств в киберпространстве, в частности, благодаря большому своду международно-правовых документов, который уже существует. Нас также очень воодушевляют результаты, достигнутые Группой правительственных экспертов и Рабочей группой открытого состава Организации Объединенных Наций, которые приняли консенсусом доклады, в частности, по улучшению поведения государств в киберпространстве. Нам необходимо, чтобы эти процессы продолжались в системе Организации Объединенных Наций и развивались в направлении применения международного права в киберпространстве, признания важности мер укрепления доверия и разработки дополнительных рекомендаций и норм. Мы ценим участие стран-членов в этих процессах и их вклад и призываем продолжать эти дискуссии и идти в ногу с быстрым развитием событий в этой области.

Мы уже были свидетелями катастрофических последствий кибератак для конфиденциальных данных и объектов инфраструктуры. Жизненно важно, чтобы нормы и правила поведения государства в киберсфере были четко прописаны. Это приведет к повышению предсказуемости и позволит избежать просчетов при оценке киберугроз. Злонамеренное использование киберпространства имеет настолько долгосрочные последствия, что сотрудничество на международном уровне также необходимо для того, чтобы избежать любых потенциальных конфликтов, которые могут возникнуть.

Меры укрепления доверия между государствами посредством применения передового опыта и установленных норм являются жизненно важным компонентом процесса продвижения вперед. Это уменьшит возможные недоразумения и позволит лучше оценивать злонамеренное поведение.

Международное сообщество также должно обратиться ко многим другим заинтересованным сторонам, включая гражданское общество и частный сектор, с тем чтобы обеспечить равные условия и справедливый набор правил. Все потенциальные пользователи киберпространства должны осознать ту роль,

которую они играют в повышении киберустойчивости и предотвращении злонамеренного использования имеющихся в нашем распоряжении инструментов.

Мальта полагает, что Совет Безопасности призван играть важную роль, когда речь идет о новых технологиях, способных повлиять на международный мир и безопасность. Совет Безопасности должен обеспечить, чтобы все соответствующие субъекты в киберпространстве соблюдали международное право и установленные правила, равно как и руководящие принципы во избежание потенциальных конфликтов, возникающих в результате кибератак. Мы призываем Совет продолжать заниматься этим вопросом и добиваться, чтобы мы совместными усилиями укрепляли взаимопонимание и взаимное доверие.

Приложение XLV

Заявление Постоянного представительства Марокко при Организации Объединенных Наций

[Подлинный текст на французском языке]

Королевство Марокко сначала хотело бы выразить благодарность Эстонии за организацию этих первых открытых дебатов Совета Безопасности, посвященных актуальному и своевременному вопросу о поддержании международного мира и безопасности в киберпространстве. Марокко приветствует исчерпывающее выступление Премьер-министра Эстонской Республики г-жи Каи Каллас, а также превосходный подход Эстонии к руководству рассмотрением вопросов кибернетики и безопасности киберпространства. Марокко благодарит также Высокого представителя по вопросам разоружения Накамицу за ее содержательный брифинг о существующих вызовах, связанных с поддержанием международного мира и безопасности в киберпространстве.

Будучи страной, находящейся в процессе развития на высоком уровне подключения к Интернету, Королевство Марокко уже давно уделяет особое внимание развитию информационно-коммуникационных технологий (ИКТ) и их преимуществам в качестве движущей силы долгосрочного развития. Хотя мы проявляем единодушие в вопросах преимуществ и благ, которые человечество получает благодаря развитию этих технологий, во всем мире приходит осознание угроз, которые могут возникать в то же время, – от простого распространения фальшивых новостей и до реальных посягательств на мир и безопасность как на национальном, так и на международном уровне.

В наше время, когда мы говорим о терминах «Интернет вещей» (ИВ), «цифровая революция» или «кибервойна», наша способность бороться с киберугрозами по-прежнему сильно зависит от таких инструментов, применения которых невозможно избежать. Прежде всего, важно признать, что современная ситуация, характеризующаяся пандемией коронавирусного заболевания (COVID-19), не только сильнее привязывает нас к киберсреде, но и ставит нас в экспоненциальную и необратимую зависимость перед лицом кибератак и угроз, включая те, которые могут поразить критически важные объекты инфраструктуры.

Подобные злонамеренные операции — помимо того, что создают угрозы для суверенитета государств, — к сожалению, способны увеличить риск конфликтов в киберпространстве, а также нанести значительный людской и материальный ущерб. Все это может подорвать международный мир и безопасность и превратить кибератаки в новую серьезную угрозу.

«Мы живем в опасную эпоху», — так сказал г-н Антониу Гутерриш, Генеральный секретарь Организации Объединенных Наций, во время обнародования Повестки дня в области разоружения в 2018 году.

Действительно, потенциальные и реальные риски в киберпространстве сейчас больше, чем когда-либо ранее, затрагивают международное сообщество и государства-члены Организации Объединенных Наций. Только прилагая коллективные и индивидуальные усилия по предотвращению вредоносного использования ИКТ, мы можем гарантировать, что киберпространство будет и впредь движущей силой мира, безопасности, стабильности и развития.

Поэтому Марокко считает, что обеспечение безопасности и защиты киберпространства является коллективной обязанностью государств, как лидеров. Именно по этой причине в соответствии с Высшими королевскими указаниями

Марокко стало незамедлительно принимать следующие важные меры законодательного, организационного и превентивного характера:

- разработка стратегии кибербезопасности, сосредоточенной вокруг четырех стратегических направлений: оценка рисков, связанных с информационными системами в административных органах, государственных учреждениях и жизненно важных инфраструктурах; защита и оборона этих информационных систем; укрепление основ безопасности (правовая база, информирование населения, образование и научные исследования и разработки); развитие национального, регионального и международного сотрудничества;

- принятие 25 июля 2020 года Закона № 05-20 о кибербезопасности, который предусматривает разработку юридического кодекса, включающего определенное минимальное количество правил и мер безопасности для обеспечения надежности и устойчивости наших информационных систем. Его целями также являются укрепление доверия в цифровой сфере, цифровизация экономики и в целом обеспечение непрерывности социально-экономической деятельности в Марокко и в других странах, с тем чтобы способствовать укреплению национальной системы кибербезопасности;

- создание в течение этого десятилетия ряда организаций с целью обеспечения государственного регулирования в киберпространстве, таких как Стратегический комитет по обеспечению безопасности информационных систем в 2011 году, Главное управление по обеспечению безопасности информационных систем, Национальное агентство по регулированию телекоммуникаций, Национальная комиссия по управлению защитой персональных данных и Марокканский центр политехнических исследований и инноваций, который проводит национальные кампании по борьбе с киберпреступностью.

Накануне проведения этих открытых дебатов Марокко одобрило 28 июня 2021 года законопроект, касающийся кибербезопасности, в котором содержатся нормы, применимые к безопасности информационных систем, а также Конвенцию Африканского союза о кибербезопасности и защите персональных данных.

Тем не менее в связи с глобальным характером киберугроз важные меры, согласованные на международном уровне, должны применяться в дополнение к действующим национальным нормативным актам. Именно поэтому Марокко ратифицировало Будапештскую конвенцию о киберпреступности и присоединилось к Парижскому призыву 2018 года о доверии и безопасности в киберпространстве. В системе Организации Объединенных Наций оно входит в состав Группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и новой Группы открытого состава по вопросам безопасности цифровых технологий и их использования (2021-2025 годы) и будет участвовать в реализации программы действий по поощрению ответственного поведения государств в киберпространстве. Марокко является, кроме того, членом Группы друзей правительства по вопросам Интернета и кибербезопасности, в которой Эстония великолепно сопредседательствует вместе с Сингапуром.

В заключение Королевство Марокко подчеркивает, что государства обязаны проявить общую твердую волю к защите киберпространства, и это связано прежде всего с тем, что превентивные меры и обеспечение безопасности

киберпространства являются основными факторами использования информационно-коммуникационных технологий.

Совет Безопасности, в частности, призван играть ключевую роль, в особенности потому, что кибератаки создают прямую угрозу международному миру и безопасности, а также потому, что он является первопроходцем в области принятия превентивных мер.

Марокко еще раз выражает свою огромную признательность Эстонии за организацию этих открытых, столь необходимых и своевременных дебатов, поскольку мы нуждаемся в самом широком информировании населения и в дискуссиях по вопросу о поддержании международного мира и безопасности в киберпространстве, и мы признательны Эстонии за включение этого вопроса в повестку дня Совета Безопасности.

Приложение XLVI

Заявление Постоянного представителя Нидерландов при Организации Объединенных Наций Йоки Брандт

Королевство Нидерландов хотело бы поблагодарить Эстонию и Премьер-министра Каллас за организацию этих открытых дебатов по теме поддержания международного мира и безопасности в киберпространстве.

Это своевременное заседание проводится на фоне резкого увеличения числа кибератак, совершаемых как государственными, так и негосударственными субъектами.

Такие злонамеренные кибердействия могут привести к колоссальным потрясениям в нашем обществе, хотя для этого будут использованы довольно ограниченные ресурсы. В результате произойдет дестабилизация международных отношений.

Поэтому настало время для совместной работы по созданию открытого, свободного и безопасного киберпространства путем обеспечения ответственного поведения государств, осуждения безответственного поведения и введения санкций в соответствующих случаях.

Признавая, что в этом вопросе есть много других важных аспектов, Нидерланды ограничатся тремя конкретными элементами, которые остаются главными для повышения стабильности в киберпространстве, а именно:

- соблюдение положений нормативно-правовой базы;
- присвоение ответственности;
- наращивание потенциала.

Соблюдение положений нормативно-правовой базы

За прошедшие годы кибероперации против важнейших элементов инфраструктуры и против гражданской инфраструктуры показали, что они представляют собой реальную и несомненную угрозу. Тем более что за последний год мы стали свидетелями дальнейшего увеличения масштабов, сферы охвата, серьезности и изощренности кибератак. Мы, представители всех слоев общества, все больше переносим почти все аспекты нашей жизни в цифровой мир и должны понимать, что именно Интернет облегчает эти связи по всему миру.

Поэтому не стоит удивляться тому, что пагубные последствия злонамеренных кибероперациий против важнейших объектов инфраструктуры, правительств и общества будут ощущаться без промедления и повсеместно, ибо они создают значительный риск для международной безопасности и стабильности, социально-экономического развития, а также безопасности и благополучия людей.

Благодаря недавнему консенсусу, достигнутому по докладам как Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, так и Группы правительственных экспертов Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве, государства теперь имеют нормативно-правовую базу ответственного поведения государств в киберпространстве. И это позволяет государствам лучше понять применимость международного права и согласованных одиннадцати добровольных необязательных норм. Нидерланды напоминают о том, что действующее международное право, в том числе Устав Организации Объединенных Наций, применимо к киберпространству и имеет большое значение для поддержания мира и

стабильности и для создания свободного, открытого и безопасного киберпространства, в том числе для уважения прав человека и основных свобод в киберпространстве.

Государства согласились с тем, что злонамеренные кибероперации против объектов инфраструктуры и средств массовой информации, оказывающих основные государственные услуги, запрещены, что подтверждает норма 13(f) Группы правительственных экспертов. Прерогатива каждого государства — определять, какие виды инфраструктуры оно относит к числу самых важных, включая, возможно, такие как медицинские учреждения, финансовые службы, энергетика, водоснабжение, транспорт и канализационные системы. Нидерланды неизменно уделяют основное внимание следующим трем видам инфраструктуры (этот список нельзя считать исчерпывающим):

1. техническая инфраструктура, необходимая для обеспечения общей доступности или неприкосновенности Интернета;

2. техническая инфраструктура, необходимая для проведения выборов;

3. система здравоохранения.

В связи с этим мы призываем государства публично определить и объявить, какие объекты инфраструктуры они считают самыми важными, публикуя национальные заявления с подробным изложением мнений государств-членов относительно соблюдения базовых положений об ответственном поведении государств. Только так мы сможем повысить транспарентность, выработать общее понимание, обеспечить предсказуемость и укрепить доверие. Для снижения риска эскалации, а также для соблюдения всеми государствами нормативно-правовой базы необходимы постоянные усилия по реализации согласованных базовых положений.

Присвоение ответственности

Мы все, похоже, согласны с правилами и нормами деятельности в киберпространстве. Тем не менее мы продолжаем наблюдать рост киберугроз. Нидерланды потрясены злоупотреблением пандемией коронавирусного заболевания (COVID-19) для проведения злонамеренных кибероперации против важнейших объектов инфраструктуры, системы здравоохранения, технической инфраструктуры, необходимой для обеспечения общей доступности или неприкосновенности Интернета, а также против технической инфраструктуры, необходимой для проведения выборов.

Давайте ясно заявим: мы будем работать сообща на добровольной основе, с тем чтобы привлечь государства к ответственности, когда они действуют вразрез с этими базовыми положениями, в том числе путем принятия транспарентных мер, соответствующих международному праву. У плохого поведения в киберпространстве должны быть последствия.

Наращивание потенциала

Цифровая устойчивость является ключевым фактором для управления киберрисками и смягчения их последствий. Однако различная степень кибербезопасности, обеспечиваемая государствами, усиливают уязвимость нашего взаимосвязанного мира. Поэтому в наших общих интересах принять участие в целенаправленных усилиях по наращиванию потенциала для обеспечения того, чтобы все ответственные государства могли применять вышеупомянутые базовые положения и лучше защищать свои сети от значительной подрывной, разрушительной или иным образом дестабилизирующей кибердеятельности. Кроме

того, для эффективного наращивания киберпотенциала государственные и негосударственные субъекты должны сотрудничать друг с другом. В связи с этим Нидерланды создали Глобальный форум специалистов по киберпространству, который превратился в мощную государственно-частную платформу по наращиванию потенциала, использующую и объединяющую более 700 существующих программ по укреплению киберпотенциала и содействующую обеспечению технической устойчивости и разработке законодательства, гарантирующего защиту, безопасность и соблюдение прав человека.

Мы отдаем должное Эстонии за то, что она заложила основу для будущих кибердискуссий в Совете Безопасности, и приветствуем сегодняшние первые официальные дебаты по кибербезопасности.

Приложение XLVII

Заявление Постоянного представительства Новой Зеландии при Организации Объединенных Наций

Новая Зеландия хотела бы выразить признательность Эстонии за включение в повестку дня Совета Безопасности важного вопроса о поддержании международного мира и безопасности в киберпространстве.

Киберугрозы являются актуальной и повсеместной проблемой для всех государств-членов. Киберугрозы создают значительный риск для процветания и безопасности Новой Зеландии, а также для международного мира и безопасности.

Мы должны работать сообща над созданием стабильной и безопасной онлайн-среды, с тем чтобы все мы могли пользоваться преимуществами цифрового подключения, которое является важным фактором экономического, социального и культурного развития.

Мы ценим возможность поделиться взглядами Новой Зеландии на международные усилия по поддержанию мира и безопасности в киберпространстве. В связи с этим мы еще раз подчеркиваем исключительную важность согласованной нормативно-правовой базы ответственного поведения государств в Интернете:

- мы должны соблюдать наши обязательства в соответствии с действующим международным правом, которое, как мы все согласились, применимо в Интернете и за его пределами;
- мы должны соблюдать нормы ответственного поведения государств в Интернете, которые каждый из нас одобрил в резолюции 70/237 Генеральной Ассамблеи;
- мы должны обеспечить широкое принятие и применение мер по укреплению доверия;
- мы должны удвоить наши усилия по наращиванию потенциала, с тем чтобы все мы были киберустойчивыми.

Эта нормативно-правовая база требует, чтобы мы поощряли ответственное поведение в Интернете, но, чтобы быть эффективной, надо воплотить ее в жизнь. Нам надо продолжать реализацию этих базовых положений практическими, конструктивными и конкретными способами. Новая Зеландия намерена продолжать сотрудничество со всеми вами в этом направлении.

Международное право

Будучи небольшим государством, Новая Зеландия является убежденным сторонником международного порядка, основанного на правилах. Это особенно верно в отношении трансграничных угроз. Наша географическая обособленность не защищает нас от киберугроз.

Обеспечение того, чтобы эта система способствовала созданию открытой, безопасной, стабильной, доступной и мирной Интернет-среды и поощряла ответственное поведение государств в киберпространстве, является одним из ключевых приоритетов Новой Зеландии.

Достижение консенсуса относительно того, как именно применяется международное право в Интернете, является важнейшим вкладом в поддержание мира и стабильности. Мы все согласны с тем, что международное право

применяется в Интернете так же, как и за его пределами. Применимое международное право включает Устав Организации Объединенных Наций, правовые положения об ответственности государств, международное гуманитарное право и международное право в области прав человека.

Вместе с тем мы признаем, что по этим вопросам сохраняются некоторые разногласия. Чтобы содействовать пониманию того, каким образом международное право применяется в Интернете, в декабре 2020 года Новая Зеландия опубликовала национальный меморандум. Мы призываем другие государства-члены поделиться своими взглядами, чтобы добиться развития и укрепления нашей общей концепции по этим вопросам.

Нормы ответственного поведения государств

Новая Зеландия привержена предотвращению, выявлению и пресечению злонамеренной кибердеятельности и принятию мер реагирования на нее, а также соблюдению норм ответственного поведения государств, одобренных в докладе Рабочей группы открытого состава Организации Объединенных Наций 2021 года. Нормы, которые мы все обязались соблюдать, являются центральным компонентом стабильности и безопасности в киберпространстве. Мы должны продолжать нести ответственность — и заставлять других нести ответственность — за выполнение взятых на себя обязательств.

В частности, мы должны способствовать сотрудничеству между государствами, защищать важнейшие объекты инфраструктуры, охранять глобальные цепочки поставок, оказывать помощь в случае необходимости, соблюдать права человека и неприкосновенность частной жизни, а также предотвращать злонамеренное использование цифровых технологий на своей территории.

Мы продолжаем размышлять о том, как пандемия коронавирусного заболевания (COVID-19) высветила важность безопасного киберпространства. По всему миру мы узнавали о различных видах вредоносной деятельности в Интернете со стороны как государственных, так и негосударственных субъектов. Эта деятельность была направлена, в частности, против важнейших медицинских учреждений, против тех, кто боролся с пандемией, а также против представителей общественности. Это неприемлемо и говорит о том, что угрозы в киберпространстве подвергают риску человеческие жизни. Новая Зеландия, наряду с рядом других государств, публично осудила злонамеренную кибердеятельность, подрывающую работу по борьбе с пандемией.

Меры укрепления доверия

Мы по-прежнему привержены достижению конструктивных, практических и конкретных результатов для упрочения международной и региональной кибербезопасности. Меры укрепления доверия открывают важный путь к достижению этой цели, и мы приветствуем практические инициативы в поддержку взаимопонимания, транспарентности, предсказуемости и стабильности в киберпространстве.

Для Новой Зеландии Региональный форум Ассоциации государств Юго-Восточной Азии (АСЕАН) является ключевым форумом для обсуждения вопросов кибербезопасности в нашем регионе. Мы высоко ценим сотрудничество с членами этого Форума и надеемся на продолжение работы со всеми вами в ближайшие годы. Новая Зеландия приветствует возможность обмена опытом в регионах и между регионами для повышения уровня транспарентности, понимания и доверия между региональными партнерами в киберпространстве.

Наращивание потенциала

Новая Зеландия хотела бы оказать помощь, чтобы все государства могли снизить уровень рисков, связанных с расширением контактов, и в то же время получить пользу от этого. Это включает в себя поддержку более широкого и глубокого понимания и соблюдения базовых положений об ответственном поведении государств в киберпространстве.

Для достижения этой цели мы все должны иметь силы и средства, необходимые для конструктивного участия в нынешних обсуждениях во всех областях, а также для реализации инициатив в самих странах и на региональном уровне, поддерживающих международную стабильность.

Новая Зеландия по-прежнему привержена делу создания регионального потенциала кибербезопасности, уделяя при этом особое внимание сотрудничеству с нашими соседями по Тихоокеанскому региону и Юго-Восточной Азии. Мы продолжаем реализацию инициатив в рамках программы Новой Зеландии по поддержке кибербезопасности в Тихоокеанском регионе на сумму в 10 млн новозеландских долларов и оказываем поддержку Центру передового опыта АСЕАН–Сингапур в области кибербезопасности.

Выводы

Нам еще многое предстоит сделать, но мы не начинаем работу с нуля. Мы еще раз приветствуем результаты недавних процессов в рамках Группы правительственных экспертов и Рабочей группы открытого состава Организации Объединенных Наций. Эти процессы и подготовленные в итоге доклады являются значительными взаимодополняющими и взаимоукрепляющими достижениями. Мы должны продолжать строить на фундаменте, возведенном этими и другими достигнутыми консенсусом договоренностями, поддержанными Генеральной Ассамблеей.

Важно, чтобы в процессе этих обсуждений мы имели весь спектр мнений, включая мнения малых государств и неправительственных заинтересованных сторон. Степень заинтересованности государств-членов в обеспечении кибербезопасности порадовала нас, поскольку мир и безопасность в киберпространстве действительно затрагивают всех нас, и отрадно видеть столь широкий круг государств, реально вовлеченных в усилия по решению этих проблем. Новая Зеландия готова вместе со всеми вами принять участие в решении этой задачи.

Приложение XLVIII

Заявление Постоянного представителя Пакистана при Организации Объединенных Наций

Я хотел бы выразить свою глубокую признательность и искреннюю благодарность Постоянному представительству Эстонской Республики за созыв этих важных и своевременных открытых дебатов Совета Безопасности по теме: «Поддержание международного мира и безопасности в киберпространстве».

Информационно-коммуникационные технологии (ИКТ) предоставляют огромные возможности, и их значение для международного сообщества продолжает расти. В то же время сложность вопросов, связанных с использованием ИКТ, создает серьезные риски для международного мира и безопасности.

Вредоносное использование кибертехнологий стремительно приближается к тому уровню, на котором оно может представлять собой нарушение мира или угрозу международному миру и безопасности.

Неправомерное и нерегулируемое использование ИКТ может иметь серьезные последствия для международного мира и безопасности в случае кибератаки на важнейшие объекты инфраструктуры. Недавние случаи предполагаемых кибератак являются весьма показательными.

Надо безотлагательно рассмотреть возможность роста угроз для кибербезопасности в рамках более широких усилий Организации Объединенных Наций по предотвращению конфликтов.

В связи с этим принятие в марте этого года одобренного консенсусом доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности имело историческое значение для поддержки глобальных усилий по достижению общей цели создания безопасной, надежной, стабильной и мирной среды ИКТ.

Это также стало убедительным подтверждением способности международного сообщества объединяться для решения ключевых глобальных проблем в самых сложных условиях, таких как пандемия.

Понимая, что в докладе не были учтены озабоченности всех государств-членов, мы считаем важным закрепить достигнутые к сегодняшнему дню успехи и сохранить импульс для продолжения этого всеобъемлющего и транспарентного процесса.

Пакистан продолжает позитивно и конструктивно участвовать в деятельности Рабочей группы открытого состава и приветствует новую Рабочую группу открытого состава по вопросам безопасности в сфере использования ИКТ (2021–2025 годы), которая была учреждена в соответствии с резолюцией 75/240 Генеральной Ассамблеи.

Новая Рабочая группа открытого состава дает возможности проведения чрезвычайно полезных форумов для достижения существенного прогресса, опираясь на предыдущие рекомендации с целью усиления правил ответственного поведения в киберпространстве и укрепления конструктивного международного сотрудничества в целях минимизации угроз для международной безопасности, создаваемых злонамеренным использованием ИКТ.

В докладе Группы правительственных экспертов 2015 года и в недавно подготовленном докладе Рабочей группа открытого состава был согласован ряд важных выводов, которые способствовали формированию широкого консенсуса государств-членов относительно того, что международное право, и в частности

Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира и стабильности в среде ИКТ.

В Уставе Организации Объединенных Наций однозначно и категорично отстаиваются принципы суверенитета, территориальной целостности и невмешательства во внутренние дела других государств. Эти принципы должны служить нам путеводной звездой, когда мы будем решать сложные вопросы, касающиеся управления киберпространством.

В то же время масштабы, объем и характер применимости международного права и его толкования, касающиеся поведения государств и использования ими ИКТ, требуют тщательного рассмотрения.

Простого утверждения о применимости существующего международного права к киберпространству недостаточно для решения многогранных правовых проблем, возникающих в связи с ИКТ. Его необходимо адаптировать с учетом особенностей киберсферы.

Пакистан признает важность разработки юридически обязывающего международного документа, конкретно учитывающего уникальные черты ИКТ, для обеспечения нормативно-правового курса на создание стабильности и безопасности в киберпространстве. Такая нормативно-правовая база должна учитывать озабоченности и интересы всех государств, должна опираться на консенсус, и ее надо создавать в Организации Объединенных Наций при равноправном участии всех государств.

Добровольные, необязательные нормы ответственного использования ИКТ государствами могут способствовать смягчению рисков для международного мира и безопасности. Однако, учитывая беспрецедентные угрозы в среде ИКТ и быстрые темпы развития технологий, надо активизировать международные усилия по разработке обязательных правил, которые могут содействовать поддержанию мира и стабильности и способствовать созданию открытой, безопасной, всегда доступной и мирной среды ИКТ.

Мы должны обеспечить, чтобы киберпространство не использовалось для проведения спонсируемых государствами кампаний по дезинформации, подстрекательства к насилию, насаждения языка ненависти и других связанных с этим форм нетерпимости, включая исламофобию.

Организация Объединенных Наций играет центральную роль в развитии диалога и международного сотрудничества между государствами-членами для выработки общего понимания ключевых аспектов, включая применение международного права и норм, правил и принципов ответственного поведения государств, содействие мерам укрепления доверия и транспарентности, а также поддержку наращивания потенциала и распространения передового опыта.

С населением численностью более 200 миллионов человек и процветающим цифровым ландшафтом, характеризующимся ростом числа Интернет-пользователей, Пакистан придает огромное значение использованию цифровых технологий для обеспечения социально-экономического развития и содействия более эффективному управлению и предоставлению государственных услуг.

Пакистан привержен делу развития международного сотрудничества в области ИКТ и делу обеспечения кибербезопасности как средства преодоления цифрового разрыва. Все страны являются равноправными участниками процесса разработки правил, регулирующих цифровую экономику и безопасность киберпространства и ИКТ.

Приложение XLIX

Заявление Постоянного представительства Перу при Организации Объединенных Наций

[Подлинный текст на испанском языке]

Перу приветствует инициативу председательства Эстонии созвать эти открытые дебаты Совета Безопасности на высоком уровне по вопросу, имеющему растущее и первостепенное значение для поддержания международного мира и безопасности. Мы приветствуем также заявления других ораторов.

Мы сознаем актуальность использования информационно-коммуникационных технологий (ИКТ) в контексте международной безопасности, их быстрое развитие и блага, которые они приносят. Вспышка кризиса в области здравоохранения вследствие пандемии коронавирусного заболевания (COVID-19) выявила нашу сильную взаимозависимость, неотложную необходимость сокращения цифрового разрыва и важность защиты критически важных инфраструктур.

Кроме того, мы сознаем риски, которые могут возникнуть в результате неправомерного использования ИКТ, чреватого угрозами вспышки конфликтов в киберпространстве. Их злонамеренное использование террористическими группами, преступными организациями, вооруженными группировками и другими субъектами создает серьезную угрозу международному миру и безопасности.

Учитывая, что опасность исходит не от самих технологий, а от их использования, необходимо углублять понимание того, как правильно их применять и как предотвратить их преднамеренное вредоносное использование, способствуя созданию открытого, свободного, стабильного и безопасного киберпространства.

С этой целью мы признаем первостепенное значение Устава Организации Объединенных Наций как надежной основы в вопросах безопасности и приветствуем применение международного права и международного гуманитарного права в борьбе с киберугрозами. Кроме того, мы считаем первостепенной задачей регулирование международной нормативной базы по этому вопросу путем разработки норм, имеющих обязывающую юридическую силу.

Мы высоко оцениваем усилия и значительные успехи, достигнутые Организацией Объединенных Наций в формулировании элементов для содействия применению международного права и соблюдению норм ответственного поведения государств в киберпространстве в контексте международной безопасности. В связи с этим мы приветствуем содержательные доклады, принятые Рабочей группой открытого состава и Группой правительственных экспертов, и надеемся, что в результате объединения работы в рамках этих двух процессов мы сможем получить единые согласованные заявления и программу действий по вопросам кибербезопасности.

Помимо международных усилий, мы считаем основополагающими региональные и национальные действия, в частности, по содействию мерам укрепления доверия, наращиванию потенциала, обмену информацией и распространению передовой практики для гарантирования кибербезопасности. Для стран с низким уровнем технического прогресса крайне важно конкретизировать положения и договоренности во избежание конфликта из-за возможных последствий, которые могут появиться из-за нехватки потенциала для их предотвращения.

Принимая во внимание естественную взаимосвязь и комплексный характер киберпространства, непрерывные инновации в сфере информационно-коммуни-

кационных технологий и все более активное внедрение новых технологий, мы ратуем за участие частного сектора, в частности информационной индустрии, гражданского общества и научных кругов в усилиях по противостоянию этим вызовам. Мы убеждены в том, что их вклад будет и впредь обогащать многосторонние обсуждения по этому вопросу.

В заключение мы хотели бы подчеркнуть необходимость скоординированной работы международного сообщества в целом и принятия новых мер по изучению существующих угроз и возможных методов сотрудничества для борьбы с ними. Роль Совета Безопасности в предотвращении конфликтов и содействии поддержанию мира и безопасности является основополагающей, преследующей цель гарантировать, чтобы киберпространство было свободным, мирным, безопасным и благотворным и чтобы оно способствовало устойчивому развитию и благополучию населения.

Приложение L

Заявление Постоянного представительства Польши при Организации Объединенных Наций

Первые в истории открытые дебаты в Совете Безопасности по теме кибербезопасности представляют собой важную веху в нашем восприятии современных вызовов международному миру и безопасности.

Мы благодарны и признательны председательству Эстонии за предоставленную нам возможность рассмотреть вопросы кибербезопасности в этот очень своевременный момент.

В 2019 году Польша — во время своего членства в Совете Безопасности — привлекла его внимание к проблемам киберинцидентов на Ближнем Востоке.

Сейчас настало время повысить уровень осведомленности всего международного сообщества о неуклонном росте вредоносной деятельности в киберпространстве. На протяжении двух десятилетий — наряду с беспрецедентным развитием цифровых технологий — мы наблюдаем во всем мире все более изощренные кибератаки и киберинциденты. В Польше они происходят ежедневно.

Они, разумеется, имеют разную природу. Некоторые из них имеют чисто криминальное происхождение, а другие объясняются экономическими целями, но все чаще политическими. Однако у всех этих действий есть один общий знаменатель: все они незаконны. Вредоносную кибердеятельность никогда нельзя ни оправдывать, ни защищать.

Как Вы, г-жа Председатель, справедливо отметили в своей концептуальной записке: «Международное право, в частности Устав Организации Объединенных Наций, содержит достаточные ориентиры для деятельности государств в киберпространстве». Разработать общеприемлемую парадигму деятельности в киберпространстве — грандиозная задача международного сообщества.

Польша решительно поддерживает достижения групп правительственных экспертов и принимает активное участие в усилиях Рабочей группы открытого состава, которая в своем докладе подтвердила применимость международного права в киберпространстве. Мы надеемся, что вторая Рабочая группы открытого состава будет способствовать более глубокому общему пониманию важности мирного использования киберпространства. Мы также придаем большое значение работе Специального комитета в рамках Третьего комитета Генеральной Ассамблеи.

Помимо общей оценки ситуации, еще более важными являются общие и хорошо спланированные действия. Поэтому Польша ратует за широкое участие многих заинтересованных сторон, НПО, частного сектора и научных кругов в международных дебатах по кибербезопасности.

Мы также твердо убеждены в том, что большую работу следует проводить в регионах. С участием региональных организаций, отдельных государств и представителей гражданского общества мы можем разработать полезные механизмы для наращивания потенциала или меры укрепления доверия.

Для того чтобы стимулировать международные усилия как на глобальном, так и на региональном уровне, нам надо объединить наши ресурсы и усилия на дипломатическом поприще. Именно поэтому мы решительно поддерживаем и продвигаем разработку программы действий как наилучшего формата международного сотрудничества в области киберпространства.

Благодаря этим открытым дебатам мы надеемся, что кибербезопасность займет свое постоянное место в повестке дня Совета Безопасности. Политические и экономические издержки злонамеренной деятельности в киберпространстве слишком велики, чтобы этот важный орган Организации Объединенных Наций мог их игнорировать.

Будьте уверены в том, что Польша приложит все усилия, чтобы внести свой вклад во все глобальные и региональные процессы, которые приведут к укреплению киберпорядка, основанного на уважении международного права и общепринятых норм.

Приложение LI

Заявление Постоянного представительства Катара при Организации Объединенных Наций

[Подлинный текст на арабском языке]

Позвольте мне поблагодарить Идзуми Накамицу, Высокого представителя по вопросам разоружения, за ее брифинг. Работа Управления по вопросам разоружения содействует тому, чтобы вопрос о кибербезопасности занял достойное место в повестке дня Организации Объединенных Наций по разоружению.

Каждый день мы ощущаем на себе огромные последствия того, что наш мир все больше зависит от киберпространства. Однако цифровые технологии и глобальная взаимосвязь также способствуют неправомерному использованию киберпространства, что вызывает особую тревогу, если учесть зависимость жизненно важных государственных служб и инфраструктуры от цифровой сферы. Неправомерное использование киберпространства и информационно-коммуникационных технологий (ИКТ) государственными и негосударственными субъектами создает угрозу для национальной безопасности и влияет на региональный и международный мир и безопасность и международные отношения. Более того, появляющиеся цифровые технологии используются террористическими группами для расширения их возможностей по совершению преступлений.

Очевидно, что ни одна страна не застрахована от угрозы злоупотребления киберпространством, и поэтому назрела необходимость предпринять коллективные действия для решения этой глобальной проблемы. К счастью, само киберпространство может стать отличным инструментом для координации международных усилий по решению этой проблемы. Как мы убедились за прошедший год, цифровые платформы незаменимы для обеспечения непрерывности работы органов Организации Объединенных Наций и других форумов международного сотрудничества.

Мы должны оценить потенциальные угрозы и влияние киберпиратства и неправомерного использования киберпространства на мир и безопасность. Необходимы коллективные усилия по укреплению региональной и международной среды безопасности перед лицом таких угроз и усилия по содействию мирному использованию киберпространства и связанных с ним передовых цифровых технологий.

В связи с этим надо уделять должное внимание применимости международного права к использованию ИКТ государствами и способствовать ответственному поведению государств в киберпространстве в контексте международной безопасности.

В то же время надо сохранять свободный поток информации и обеспечивать уважение прав человека и основных свобод в открытой, безопасной и доступной для всех цифровой среде.

Помимо международных рамок, большое значение имеют национальные стратегии для руководства действиями и координации между соответствующими заинтересованными сторонами, включая частный сектор, чья роль является центральной в сфере цифровых технологий.

Катар придает огромное значение обеспечению информационной безопасности и инфраструктуры и с этой целью принимает комплексные меры и

развивает свои возможности в этой области, а также уделяет большое внимание развитию международного сотрудничества и укреплению потенциала.

Вопрос об информационной безопасности и кибербезопасности стоит в повестке дня Организации Объединенных Наций уже много лет. Однако ускоренное развитие событий в этой области требует соответствующих мер. Поэтому мы приветствуем то внимание, которое уделяет этому вопросу Генеральный секретарь, сделавший продвижение мирной среды ИКТ одним из своих приоритетов. Мы также рады, что Группа правительственных экспертов вновь достигла консенсуса. Мы также с нетерпением ждем следующей сессии Рабочей группы открытого состава, чтобы содействовать достижению более широкого международного консенсуса по этим вопросам.

В заключение мне хотелось бы подтвердить, что Государство Катар будет и впредь усердно работать на всех уровнях, чтобы внести свой вклад в глобальные усилия по укреплению мира, безопасности и стабильности в киберпространстве.

Приложение LII

Заявление Постоянного представителя Республики Корея при Организации Объединенных Наций Чо Хёна

Я хотел бы прежде всего поблагодарить Вас за созыв сегодняшних своевременных открытых дебатов на тему «Поддержание международного мира и безопасности в киберпространстве». Я также благодарю Высокого представителя по вопросам разоружения г-жу Накамицу за ее обстоятельный брифинг.

За последние два десятилетия человечество стало свидетелем небывалого технического прогресса в области цифровых технологий. Концепция киберпространства, которая когда-то существовала лишь в воображении научных фантастов, с тех пор стала для всех нас повседневной реальностью, а виртуальное и физическое пространство, окружающее нас, сливается в единую экосистему. И хотя этот прогресс принес нам беспрецедентные социально-экономические выгоды, мы также стали еще более уязвимыми перед лицом злонамеренных кибердействий. За последний год, в разгар глобальной пандемии, наша жизнь стала еще более подверженной киберугрозам, поскольку все больше людей обратились к Интернету. В то же время все более серьезную тревогу вызывает увеличение числа кибератак на важнейшие объекты инфраструктуры, включая медицинские учреждения по всему миру.

В свете этого я хотел бы выделить следующие четыре аспекта, которые имеют особое значение для нашей делегации.

Во-первых, Республика Корея поддерживает центральную роль Организации Объединенных Наций в нынешних дискуссиях о том, как решать стоящие перед нами задачи и поощрять ответственное поведение государств в киберпространстве. В связи с этим наша делегация приветствует принятие в начале этого года одобренного консенсусом доклада Рабочей группы Организации Объединенных Наций открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также принятие четвертого одобренного консенсусом доклада Группы правительственных экспертов в прошлом месяце. Эти события отражают успехи на пути создания общей постоянно развивающейся нормативно-правовой базы ответственного поведения государств при использовании ими ИКТ, и благодаря этим мерам все международное сообщество стало лучше разбираться в этих исключительно важных вопросах.

Поскольку все государства-члены провозгласили консенсусом в предыдущем докладе Рабочей группы открытого состава, что международное право применимо к использованию ИКТ государствами, они должны руководствоваться нормативно-правовой базой ответственного поведения государств при использовании ИКТ, как сказано в докладах Группы правительственных экспертов. Примат международного права и порядок, основанный на правилах, должны в равной степени применяться к киберпространству в целях обеспечения мира и безопасности.

Во-вторых, наша делегация высоко ценит недавно опубликованный одобренный консенсусом доклад Группы правительственных экспертов, в котором излагаются дополнительные положения о толковании норм ответственного поведения государств, мер укрепления доверия, наращивания потенциала и того, как международное право применяется к использованию ИКТ государствами. В докладе подтверждается применимость международного права, включая Устав Организации Объединенных Наций, а также международного гуманитарного права в ситуациях вооруженного конфликта. Мы также решительно

поддерживаем рекомендацию Группы правительственных экспертов о том, что государства, вовлеченные в какой-либо международный спор, в том числе спор, связанный с использованием ИКТ, должны прежде всего урегулировать его мирными средствами, как сказано в статье 33 Устава Организации Объединенных Наций.

Если говорить более конкретно, то наша делегация рада видеть нашедшее отражение в докладе дальнейшее развитие нормы, согласно которой государства не должны умышленно допускать, чтобы их территория использовалась для международно-противоправных деяний с применением ИКТ. Этот принцип «должной осмотрительности», который был предложен Республикой Корея и впервые нашел отражение в докладе Группы правительственных экспертов 2015 года, предусматривает, что каждое государство должно предпринять соответствующие разумные шаги для урегулирования этой ситуации, если ему известно, что речь идет о международно-противоправном деянии или если его уведомили о нем.

В-третьих, мы должны активизировать усилия по укреплению доверия и содействию взаимопониманию. Республика Корея, как ответственное государство-член, являющееся одним из лидеров в сфере цифровых и других технологий, активно участвует в работе различных региональных и многосторонних форумов и вносит свой вклад в эту работу. Только на прошлой неделе, 22 июня, Республика Корея в тесном сотрудничестве с Организацией по безопасности и сотрудничеству в Европе успешно провела на своей территории третью Межрегиональную конференцию по кибербезопасности и безопасности ИКТ для обсуждения современных тенденций в области кибербезопасности и развития сотрудничества в этой области между региональными организациями. Мы также принимали у себя в 2020 году 19-ю Совместную конференцию Республики Корея и Организации Объединенных Наций по разоружению и нераспространению, посвященную развитию и влиянию новых технологий, и будем сопредседательствовать на межсессионном совещании Регионального форума АСЕАН по безопасности ИКТ в 2021-2023 годах. Кроме того, в ноябре этого года Республика Корея будет проводить международный форум в целях дальнейшей активизации дискуссий по устранению возникающих угроз для безопасности, включая кибератаки и злонамеренное использование новых технологий в контексте международного мира и безопасности. В соответствии с принципами всеобъемлющего подхода, транспарентности и открытости этот форум станет гостеприимной международной площадкой, доступной для различных заинтересованных сторон.

В-четвертых, мы невозможно недооценивать тот факт, что кибербезопасность требует участия многих заинтересованных сторон, поскольку международное измерение безопасности киберпространства охватывает множество областей и дисциплин. Хотя правительства остаются в центре этих усилий, мы можем быть по-настоящему эффективными только тогда, когда вовлечем в этот процесс другие ключевые заинтересованные стороны, такие как частный сектор, научные круги, гражданское общество и технические специалисты. Мы также должны помнить о том, что сотрудничество с другими заинтересованными сторонами может внести большой вклад в достижение общего понимания и претворения в жизнь нормативно-правой базы ответственного поведения в киберпространстве.

В заключение я хотел бы, пользуясь этой возможностью, подтвердить приверженность Республики Корея сотрудничеству с Организации Объединенных Наций и всеми государствами-членами, направленному на создание открытого, безопасного, стабильного, доступного и мирного киберпространства.

Приложение LIII

Заявление Постоянного представительства Румынии при Организации Объединенных Наций

Мы высоко оцениваем инициативу Эстонии по организации первых открытых дебатов по кибербезопасности в качестве официального конкретного вопроса в повестке дня Совета Безопасности. Это своевременная инициатива по дальнейшему укреплению международного порядка, основанного на правилах, а также нашего многостороннего сотрудничества по вопросу, имеющему огромное значение для поддержания международного мира и безопасности.

Сегодняшние дебаты подтверждают большой прогресс, достигнутый государствами-членами в рамках подготовки последних одобренных консенсусом докладов Группы правительственных экспертов Организации Объединенных Наций и Рабочей группы открытого состава в консолидации нормативно-правовой базы ответственного поведения государств в киберпространстве — на основе существующего международного права, норм, мер укрепления доверия и наращивания потенциала.

В постоянно развивающейся среде международной безопасности информационно-телекоммуникационные технологии (ИКТ) являются источником как огромных благ, так и некоторых из наиболее заметных и острых угроз сегодняшнего дня. Такие угрозы исходят как от государственных, так и негосударственных субъектов и направлены на различные ключевые сферы, такие как энергетика, транспорт, финансы и здравоохранение, которые полагаются и на физические, и на цифровые важнейшие инфраструктуры для предоставления услуг на национальном, региональном или глобальном уровне. Цифровые технологии также могут использоваться не по назначению, а с тем чтобы попытаться ослабить наши демократические институты и подорвать доверие общества к демократическим принципам. Кроме того, их могут использовать для эксплуатации системных уязвимостей в геополитических целях. Пандемия коронавирусного заболевания (COVID-19) является недавним чудовищным примером губительных последствий кибероперaций, направленных на компрометацию или изменение стратегической информации об исследованиях и распределении вакцин.

В этой обстановке невозможно переоценить значение многостороннего сотрудничества между ответственными государствами, а также укрепления партнерских отношений между органами государственного управления, частным сектором, гражданским обществом и научными кругами. Нам надо работать сообща для обмена проверенной, точной, своевременной и достоверной информацией об угрозах и правильных мерах реагирования, а также для координации наших усилий и укрепления соответствующих превентивных механизмов на глобальном, региональном и национальном уровне. А самое главное, мы должны сосредоточить наши усилия на повышении стойкости нашего общества, которое сталкивается с последствиями угроз для наших важнейших объектов инфраструктуры — физических, цифровых или институциональных.

С учетом этого стоит отметить, что в рамках своего нынешнего председательства в Сообществе демократий Румыния активно продвигает тему взаимосвязи между технологиями и демократическими процессами в качестве одного из своих приоритетов. В качестве принимающей стороны недавно созданного в Бухаресте Европейского центра компетенций по кибербезопасности в промышленности и в сфере технологий и исследований Румыния приветствует и активно продвигает планируемые совместные партнерские инвестиции между государствами-членами Европейского союза и промышленностью. Как инициатор и принимающая сторона недавно созданного Евроатлантического центра по

вопросам устойчивости Румыния будет заниматься разработкой новых идей и стратегий по адаптации общества к новым угрозам для мира, безопасности и стабильности демократий.

В своем качестве государства-члена Европейского союза Румыния занимается продвижением и реализацией основных аспектов новой Стратегии кибербезопасности Европейского союза для цифрового десятилетия, особенно инструментария кибердипломатии, включая инструменты киберсдерживания и стратегической коммуникации Европейского союза против вредоносной кибердеятельности. Этот инструментарий кибердипломатии Европейского союза играет важную роль в предотвращении и пресечении киберинцидентов и принятии мер реагирования, учитывая, что эти киберинциденты влияют на безопасность Европейского союза и его государств-членов.

Для Румынии кибербезопасность является одним из ключевых аспектов национальной безопасности, и поэтому она прилагает усилия по разработке и адаптации надлежащей национальной правовой базы с целью содействия сотрудничеству и эффективному обмену информацией между компетентными органами, а также с целью выполнения своих международных обязательств. Ответственное поведение государств подразумевает ключевые позитивные обязательства: наличие современных и эффективных национальных законов, киберстратегий и институтов, развитие тесного международного сотрудничества и, что очень важно, транспарентность, соблюдение согласованных норм, продвижение демократических принципов и полное уважение человеческого достоинства.

Безопасность киберпространства является для Румынии одним из самых высоких политических и дипломатических приоритетов, который реализуется путем содействия ответственному поведению государства и укреплению превентивных и нормативных механизмов на глобальном, региональном и национальном уровне. Мы стремимся поддерживать глобальное, открытое, безопасное и надежное киберпространство, где в полной мере действуют права человека, основные свободы и верховенство права. Мы также придерживаемся мнения, согласно которому открытую, безопасную, стабильную, доступную и мирную Интернет-среду невозможно представить вне международной системы, основанной на правилах, в первую очередь на международном праве.

Румыния активно участвовала в обоих процессах Организации Объединенных Наций, направленных на укрепление нормативно-правовой базы кибербезопасности (Группа правительственных экспертов Организации Объединенных Наций и Рабочая группа открытого состава), которые успешно завершили свою работу, согласовав важные рекомендации по предотвращению конфликтов в киберпространстве (от укрепления понимания применимости международного права в киберпространстве до необязательных добровольных норм ответственного поведения государств, а также предложения по будущему институционализированному диалогу).

Румыния считает, что в дальнейшем разработка программы действий Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве будет способствовать принятию конкретных практических мер по укреплению потенциала и доверия, а также облегчит доступ к источникам финансирования на открытой, всеобъемлющей и транспарентной постоянной основе, тем самым содействуя усилиям всех государств-членов по предотвращению конфликтов, выработке общего восприятия угроз и повышению своей киберустойчивости.

В рамках всех будущих процессов Организации Объединенных Наций Румыния будет активно продвигать свою позицию, согласно которой международное право применимо к киберпространству. Мы твердо убеждены в том, что нет никаких оснований считать, будто действующее международное право не может надлежащим образом регулировать межгосударственные отношения, поддерживаемые в киберпространстве или через него. Это включает международное гуманитарное право в контексте кибероперации, проводимых в рамках вооруженного конфликта (как международного, так и немеждународного). В таких условиях планирование и проведение кибероперации должно осуществляться в соответствии с принципами, регулирующими ведение военных действий, а именно: разграничение, соразмерность, необходимость и предосторожность.

Тем не менее расширение диалога и обмена мнениями между государствами может помочь прояснить некоторые конкретные обстоятельства применения международного права к киберпространству. С учетом этого мы отмечаем, что предварительное мнение Румынии по этой теме было опубликовано с целью внести вклад в работу Группы правительственных экспертов в соответствии с резолюцией 73/266 Генеральной Ассамблеи.

Приложение LIV

Заявление Постоянного представительства Сенегала при Организации Объединенных Наций

[Подлинный текст на французском языке]

Мы хотели бы прежде всего поблагодарить Каю Каллас, Премьер-министра Эстонской Республики, за ее председательство на этих важных виртуальных открытых дебатах на высоком уровне по теме кибербезопасности — теме, которая приобретает все большее значение в системе Организации Объединенных Наций в связи с угрозами безопасности в киберпространстве. Мы благодарим также Высокого представителя по вопросам разоружения г-жу Идзуми Накамицу, выступление которой было выслушано нашей делегацией с большим интересом.

Факты предельно ясны: распространение вредоносной деятельности в киберпространстве представляет собой реальную угрозу международному миру и безопасности и требует внимания Совета Безопасности. Дискуссия, которую мы ведем сегодня, представляет собой попытку обеспечить понимание Советом этой угрозы и является продолжением беспрецедентных усилий, предпринятых более чем за десятилетие Генеральной Ассамблеей по вопросам кибербезопасности.

С этой точки зрения, различные процессы обсуждений, проводимые в рамках четырех составов Группы правительственных экспертов и Рабочей группы открытого состава, соответственно, по поощрению ответственного поведения государств в киберпространстве и по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, являются полезными и недвусмысленно сигнализируют о стремлении государств достичь консенсуса в отношении методов регулирования киберпространства.

В знак признания применимости нескольких существующих принципов и норм международного права к киберпространству и провозглашения ответственности государств за противоправные деяния, совершенные ими в этой сфере на международном уровне, выводы докладов Рабочей группы открытого состава и последней Группы правительственных экспертов, принятые, соответственно ,в марте и мае 2021 года, представляют собой дополнительный вклад в понимание применимости международного права в киберпространстве.

Кроме того, по примеру ряда стран, Сенегал считает, что меры доверия и транспарентности необходимы для обеспечения ответственного поведения государств в киберпространстве и должны быть поэтому усилены.

По сути, регулярно обмениваясь информацией о своей кибердеятельности, государства могут способствовать предотвращению ошибочного восприятия и злоупотреблений, предупреждению и регулированию кризисов, возникающих в результате использования киберпространства, и в ряде случаев созданию основ для плодотворного сотрудничества в вопросах цифровизации.

Тем не менее в связи с огромными изменениями в этом секторе и появлением новых киберугроз Сенегал считает, что правил международного позитивного права и мер доверия и транспарентности недостаточно для того, чтобы должным образом регулировать киберпространство. Поэтому они должны быть дополнены международными юридически обязывающими документами.

Таким образом, общий подход, включающий в себя добровольные меры доверия и транспарентности и международную конвенцию обязывающего харак-

тера, является актуальным не только для установления правил использования киберпространства, но и для учета позиций и интересов всех государств-членов. Именно на этот подход должны быть направлены усилия новой Группы открытого состава по вопросам безопасности информационных и коммуникационных технологий на период 2021–2025 годов.

Со своей стороны, правительство Сенегала активно участвует в позитивном содействии реализации этого процесса, который является для него приоритетным с момента принятия в ноябре 2017 года Национальной стратегии кибербезопасности. Этот документ, в котором говорится о создании в 2022 году в Сенегале киберпространства доверия, безопасности и устойчивости для всех, включает в себя оценку стратегического контекста кибербезопасности в Сенегале с учетом существующих и будущих угроз и содержит определение пяти стратегических целей, а именно: укрепление правовой и организационной базы кибербезопасности; защита критически важных информационных инфраструктур и государственных информационных систем; продвижение культуры кибербезопасности; укрепление потенциала и повышение уровня технических знаний в области кибербезопасности во всех отраслях экономики, а также участие в региональных и международных усилиях по вопросам кибербезопасности.

В соответствии с последней целью Сенегал стал первой страной, присоединившейся к Конвенции Малабо о кибербезопасности и защите персональных данных (Конвенция Малабо). Он также присоединился к Будапештской конвенции о киберпреступности (Будапештская конвенция) и к Конвенции 108 Совета Европы о защите лиц в связи с автоматической обработкой досье, касающихся персонала (STE no. 108), а также к ее Дополнительному протоколу о контролирующих органах и трансграничных потоках данных (STE no. 181). Кроме того, он принял директиву Экономического сообщества государств Западной Африки (ЭКОВАС) от 19 августа 2011 года, касающуюся борьбы с киберпреступностью, и одобрил Парижский призыв от 12 ноября 2018 года о доверии и безопасности в киберпространстве и Крайстчерчский призыв от 15 мая 2019 года о противодействии терроризму и насильственному экстремизму в Интернете.

В своей стране мы располагаем правовой системой регулирования использования цифровых технологий. Помимо закона № 2008-08 от 25 января 2008 года об электронных транзакциях можно упомянуть закон об ориентации № 2008-10 от 25 января 2008 года об информационном обществе, законы № 2008-11 и № 2008-12 от 25 января 2008 года о киберпреступности и защите персональных данных, а также закон № 2018-28 от 28 ноября 2018 года о кодексе электронных коммуникаций. Был также пересмотрен Уголовно-процессуальный кодекс, с тем чтобы учесть процедуру рассмотрения нарушений, совершаемых с помощью ИКТ.

Наряду с этим была обновлена организационная структура в результате создания Центральной технической службы по статистике и безопасности информационных систем, Специального отдела по борьбе с киберпреступностью и Комиссии по защите данных. Эта структура в скором времени будет укреплена благодаря учреждению Национального консультативного комитета по кибербезопасности и Национального управления по вопросам кибербезопасности для целей реализации Национальной стратегии по кибербезопасности — 2022 год.

Кроме того, усиление киберпотенциала представляет собой еще один вызов, с которым необходимо справиться, особенно развивающимся странам. Поэтому в Сенегале было многое сделано для организации обучения в сфере информационной безопасности. Так, сейчас в нашей стране есть несколько учебных заведений по данному направлению, среди которых больше всего известны Национальная школа кибербезопасности и регионального образования в Дакаре,

открытая в ноябре 2018 года, и Профессиональный институт информационной безопасности, созданный в октябре 2015 года.

Кибербезопасность не должна препятствовать инновациям и возможностям развития, которые обеспечивают новые информационно-коммуникационные технологии, и не должна использоваться в целях сдерживания их развития.

В качестве превентивного средства и средства борьбы с вредоносным использованием киберпространства инициативы по кибербезопасности должны преследовать в качестве своей главной цели содействие созданию доступной, безопасной, спокойной и процветающей цифровой среды, в которой никто не будет обделен, в соответствии с пунктом 9c цели 9 Повестки дня в области развития на период до 2030 года.

Следуя этим устремлениям, правительство Сенегала разработало Стратегию цифровой экономики Сенегала на 2016–2025 годы в соответствии с Планом развития Сенегала. Этот документ, отражающий стремление Сенегала сохранить позицию лидера инноваций в Африке в области цифровизации, сформулирован под лозунгом «Цифровизация для всех, в том числе для всех пользователей к 2025 году в Сенегале с участием динамичного и инновационного частного сектора в рамках эффективной экосистемы».

Приложение LV

Заявление Постоянного представителя Сингапура при Организации Объединенных Наций Бурхана Гафура

Благодарю Вас за созыв этого важного заседания, на котором впервые Совет Безопасности будет официально рассматривать вопросы безопасности в киберпространстве.

Это своевременная тема. Ускорение темпов цифровизации, вызванное пандемией коронавирусного заболевания (COVID-19), по-новому позитивно повлияло на нашу жизнь. Но у нас появились и новые факторы уязвимости. Киберугрозы и злонамеренная кибердеятельность становятся все более частыми и изощренными и имеют более серьезные последствия. Согласно оценкам, в 2020 году ущерб от вредоносной кибердеятельности составил почти 1 трлн долл. США. Недавний всплеск такой деятельности является суровым напоминанием о том, что международное сообщество должно продолжать защищаться и должно быть готовым реагировать на эти глобальные и трансграничные угрозы. В связи с этим я хотел бы выделить пять важных аспектов.

Во-первых, мы должны признать, что тема киберпространства в основе своей относится к вопросам управления глобальным общим достоянием. Будучи небольшим государством, Сингапур всегда поддерживал многостороннюю систему, основанную на правилах и на уважении международного права. Наш подход ничем не отличается и применительно к киберпространству. Чтобы киберпространство оставалось безопасным, надежным, открытым и совместимым, мы должны применять глобальный подход, основанный на глобальных правилах и нормах и на соблюдении международного права. Сделать это будет непросто, учитывая нестабильный и раздробленный глобальный ландшафт, что вызвано растущей геополитической напряженностью. Однако у нас нет иного выхода, кроме как продолжать пропагандировать и поддерживать применимость международного права и норм, с тем чтобы поощрять ответственное поведение государств в киберпространстве. Нам надо удвоить масштабы международного сотрудничества для повышения киберустойчивости и стабильности.

Сингапур привержен роли Организации Объединенных Наций как единственного универсального, всеобъемлющего и многостороннего форума в деле разработки правил, регулирующих киберпространство. Нас воодушевляет то, что дискуссии по кибербезопасности, которые происходят в Организации Объединенных Наций, становятся все более зрелыми. С тех пор как в 1998 году безопасность информационно-коммуникационных технологий (ИКТ) впервые была включена в повестку дня Организации Объединенных Наций, шесть составов Группы правительственных экспертов изучали угрозы, возникающие в результате неправомерного использования ИКТ в контексте международной безопасности, и способы борьбы с этими угрозами. Четыре из них согласовали доклады по вопросам существа, включая последний, который ознаменовал собой завершение работы этой Группы.

Дискуссии по кибербезопасности впервые были вынесены на более широкое обсуждение государствами-членами на сессии Генеральной Ассамблеи. Этому способствовало создание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Нас вдохновляет недавно состоявшееся успешное принятие консенсусом ее доклада. Этот доклад является вкладом в наше общее понимание многих вопросов и определяет области, в которых надо провести дополнительные обсуждения.

Сингапур активно участвовал в деятельности как Рабочей группы открытого состава, так и последней Группы правительственных экспертов. Сингапур также имеет честь быть избранным Председателем новой Рабочей группы открытого состава по безопасности и использованию информационно-коммуникационных технологий в 2021-2025 годах. Как Председатель этого органа Сингапур твердо намерен продолжать открытые, всеобъемлющие и транспарентные дискуссии по кибербезопасности, происходящие в Организации Объединенных Наций. Мы надеемся, что работа новой Рабочей группы открытого состава будет способствовать установлению многостороннего порядка в киберпространстве на основе правил и вселит во все государства, большие и малые, уверенность, предсказуемость и стабильность, которые необходимы для экономического прогресса, создания рабочих мест и внедрения технологий. Мы надеемся на тесное сотрудничество со всеми государствами-членами в этой области.

Во-вторых, все государства уязвимы перед лицом злонамеренной кибердеятельности, которая становится все более масштабной и изощренной. Однако особенно уязвимы малые государства, прежде всего развивающиеся и наименее развитые страны. Если мы действительно серьезно воспринимаем глобальный подход к кибербезопасности, мы должны уделять большое внимание наращиванию потенциала стран, которые нуждаются в помощи. Это одна из областей, в которой Организация Объединенных Наций может помочь путем координации усилий. Сингапур в партнерстве с Управлением Организации Объединенных Наций по вопросам разоружения разработал учебный Интернет-курс, открытый для всех государств-членов, с целью способствовать более глубокому пониманию использования ИКТ и их последствий для международной безопасности. Мы по-прежнему готовы сотрудничать с Организацией Объединенных Наций и оказывать ей поддержку, предлагая дальнейшие программы по наращиванию потенциала.

В-третьих, Сингапур считает, что можно сделать больше для содействия повышению осведомленности и реализации существующих 11 добровольных, необязательных норм ответственного поведения государств при использовании ИКТ. Мы поддерживаем обмен передовой практикой и опытом в вопросах соблюдения норм. Это поможет выявить проблемы, которые мы должны решить, и пробелы, для устранения которых могут потребоваться дополнительные нормы. Сингапур поддерживает дальнейшую работу по совершенствованию существующих норм. Например, злонамеренная кибердеятельность, направленная против любой трансграничной очень важной информационной инфраструктуры, такой как облачные и банковские системы, может вызвать широкомасштабные сбои в работе основных служб в нескольких государствах, включая те, которые связаны с международной торговлей, транспортом и коммуникациями. Государствам следует рассмотреть вопрос о том, как улучшить трансграничное сотрудничество с соответствующими владельцами и операторами инфраструктуры для усиления мер безопасности ИКТ, принимаемых в рамках такой инфраструктуры.

Это подводит меня к четвертому вопросу о более активном взаимодействии с другими заинтересованными сторонами, в том числе с частным сектором. Поскольку значительная часть важнейших информационных структур принадлежит частному сектору, международное сообщество должно найти пути тесного сотрудничества с частным сектором для предотвращения и смягчения последствий таких сбоев. Сингапур поддерживает совместный подход государственного и частного секторов к обмену передовым опытом для поддержки надежной системы кибербезопасности.

В-пятых, Сингапур считает, что региональные организации играют важную роль в поддержке дискуссий в Организации Объединенных Наций и

реализации правил и норм, разработанных в Организации Объединенных Наций. Кибербезопасность была одним из приоритетов председательства Сингапура в Ассоциации государств Юго-Восточной Азии (АСЕАН) в 2018 году. В том же году АСЕАН стала первой региональной организацией, которая приняла принципиальное решение присоединиться к 11 добровольным, необязательным нормам ответственного поведения государств при использовании Службы информационно-коммуникационных технологий (СИКТ). В настоящее время АСЕАН разрабатывает план действий по реализации этих норм. В рамках АСЕАН Сингапур также поддерживает программы по наращиванию потенциала. Центр передового опыта АСЕАН–Сингапур в области кибербезопасности был создан в 2019 году как многопрофильный центр по наращиванию потенциала в таких областях, как меры укрепления доверия, политика, стратегия, законодательство и операции. Мы надеемся на совместную работу с государствами-членами для укрепления наших коллективных усилий по наращиванию киберпотенциала.

В заключение позвольте мне сказать, что безопасная и надежная цифровая инфраструктура должна лежать в основе наших амбиций в области цифровой экономики. Сегодня как никогда важно, чтобы государства-члены решали проблему кибербезопасности сообща, настойчиво, комплексно и скоординированно. Сингапур готов работать со всеми странами для налаживания партнерских отношений и сотрудничества в целях создания безопасного, пользующегося доверием, открытого и совместимого киберпространства.

Приложение LVI

Заявление Постоянного представителя Словакии при Организации Объединенных Наций Михаля Млинара

Словакия присоединяется к заявлению Европейского союза. Мы хотели бы высказать дополнительные замечания от своей страны.

Я хотел бы поблагодарить Председателя за проведение этой своевременной дискуссии, которая дает возможность поразмышлять о растущих рисках, связанных со злонамеренной деятельностью в киберпространстве, и их влиянии на международный мир и безопасность, а также рассмотреть вопрос о глобальных усилиях по укреплению мира и стабильности в киберпространстве.

В связи с кризисом, вызванном пандемией коронавирусного заболевания (COVID-19), стала еще более актуальной и насущной необходимость укрепления безопасности и стабильности киберпространства. Кризис показал, что цифровые возможности стали решающими для предоставления основных услуг, а также для дальнейшего эффективного управления. Нарушение функционирования важнейших объектов инфраструктуры может привести к серьезным последствиям. Вредоносные кибердействия против жизненно важных секторов и служб ведут к дестабилизации и в итоге могут создавать угрозы международному миру и безопасности.

Поскольку киберугрозы в значительной степени носят транснациональный характер, важно поддерживать международное сотрудничество и диалог между государствами, а также между государствами и многосторонним сообществом заинтересованных сторон. Благодаря прежде всего нашей общей ответственности и совместным усилиям правительств, частного сектора и гражданского общества мы можем эффективно поддерживать международный мир и безопасность в киберпространстве и защищать права человека.

Объединенных Наций играет важную роль в проведении международных дискуссий, направленных на повышение осведомленности о кибервызовах международному миру и безопасности и на достижение прогресса в поощрении ответственного поведения государств в киберпространстве.

Словакия решительно поддерживает многосторонний подход, который призван помогать регулировать и решать текущие и будущие проблемы в киберпространстве. Мы убеждены в том, что стабильность киберпространства должна основываться на действующем международном праве, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека. Словакия полностью поддерживает применимость действующего международного права к поведению государств в киберпространстве, как это признано в трех одобренных консенсусом докладах групп правительственных экспертов, принятых Генеральной Ассамблеей в 2010, 2013 и 2015 годах. Наши усилия будут направлены на проведение транспарентных и конструктивных дискуссий, с тем чтобы все мы могли извлечь пользу из опыта, передовой практики и знаний друг друга.

Словакия также является коспонсором программы действий по поощрению ответственного поведения государств в киберпространстве в рамках Рабочей группы открытого состава. Мы верим во всеобъемлющий и конструктивный институциональный диалог, ориентированный на результаты, регулярность и консенсусный подход. На наш взгляд, предложение относительно этой программы действий закладывает основу для такого диалога между всеми государствами-членами Организации Объединенных Наций.

По мнению Словакии, два вида мер — меры по укреплению доверия и наращиванию потенциала в киберпространстве — имеют наибольшее значение для поддержания стабильности в киберпространстве. Региональные организации, такие как Организация по безопасности и сотрудничеству в Европе, являются очень полезными инструментами предотвращения конфликтов и укрепления сотрудничества между государствами. Регулярное общение и взаимодействие между государствами в киберпространстве помогает избегать конфликтов и добиваться деэскалации потенциально растущей напряженности, создавая в то же время площадку для диалога.

Международное право является одним из основных столпов стабильности и предсказуемости в отношениях между государствами. Словакия решительно поддерживает тех, кто подтверждает, что существующее международное право — особенно Устав Организации Объединенных Наций во всей его полноте и международное гуманитарное право и право в области прав человека — применимо к действиям государств в киберпространстве. В Уставе Организации Объединенных Наций изложены нормы и принципы международного права, имеющие особое значение для поддержания мира и стабильности. Нет сомнений в том, что права человека применяются как в Интернете, как и вне его, и государства должны уважать и отстаивать эти права.

Приложение LVII

Заявление Постоянного представительства Словении при Организации Объединенных Наций

Словения приветствует первые открытые дебаты Совета Безопасности, посвященные конкретному тематическому вопросу — вопросу кибербезопасности. Рассмотрение вопроса о кибербезопасности является своевременным и полезным для всех государств-членов. Открытые дебаты в Совете Безопасности по этой теме способствуют повышению осведомленности в рамках международного мира и безопасности. В связи с этим Словения приветствует недавно одобренные консенсусом доклады Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве.

Словения присоединяется к заявлению Европейского союза, и мы хотели бы высказать дополнительные замечания нашей страны.

Мы живем во взаимосвязанном и быстро меняющемся мире. Глобальное, открытое, свободное, стабильное и безопасное киберпространство способствует получению социально-экономических выгод. Однако существуют и злонамеренные кибердействия. Неправомерное использование киберпространства может негативно повлиять на жизненно важные отрасли экономики и основные услуги населению в таких областях, как здравоохранение и энергетика, а также на другие базовые объекты инфраструктуры. Злонамеренные цели использования ИКТ государственными или негосударственными субъектами могут подорвать доверие между правительствами и вызвать негативные последствия, ведущие к дестабилизации международного мира и безопасности.

Для смягчения существующих и возникающих угроз, по твердому убеждению Словении, киберпространство должно регулироваться в полном соответствии с действующим международным правом, в частности Уставом Организации Объединенных Наций во всей его полноте, международным гуманитарным правом и правом в области прав человека, а также путем выполнения норм и правил ответственного поведения государств. Для этого нашей первой целью должно стать содействие применению существующего международного права и сосредоточение наших коллективных усилий на продвижении применения существующих норм ответственного поведения государства, включая уголовное преследование частных организаций, действующих с территории страны, законам которой они должны подчиняться.

Нормы ответственного поведения государства находятся в соответствии с политикой укрепления доверия и мерами по наращиванию потенциала. Именно в этой сфере мы можем добиться реальных результатов. Словения решительно поддерживает — вместе с 53 государствами-членами — предложение об учреждении программы действий по поощрению ответственного поведения государств в киберпространстве. Эта программа действий будет основана на принятых решениях Генеральной Ассамблеи. Программа действий даст возможность поддерживать проекты по наращиванию потенциала и станет своего рода институциональным механизмом Организации Объединенных Наций для сотрудничества и обмена передовым опытом и для сотрудничества с другими заинтересованными сторонами.

Кроме того, применяя нормы ответственного поведения государств, Словения будет продолжать продвигать и поддерживать важную роль гендерной

перспективы для сокращения «цифрового гендерного разрыва» и обеспечения эффективного и конструктивного участия женщин в процессах принятия решений, связанных с использованием ИКТ в контексте международной безопасности.

Словения как будущий Председатель Совета Европейского союза с 1 июля 2021 года будет укреплять сотрудничество в области кибербезопасности и содействовать рациональному принятию решений кибервопросов Европейским союзом и регионом Западных Балкан. Сближение региона Западных Балкан и европейской киберэкосистемы является важным элементом создания пользующейся доверием и безопасной среды для цифрового развития, усиления взаимосвязанности и доступа к цифровой экономике и обществу. Это также станет вкладом в поддержание глобальной стабильности в киберпространстве.

С этой целью Словения планирует организовать неформальный саммит Европейского союза и региона Западных Балкан в начале октября 2021 года. Словения также проведет конференцию по кибербезопасности — мероприятие на Западных Балканах в сотрудничестве с ИССЕС. Кроме того, мы внесем свой вклад в проведение обзора и достижение прогресса — в сотрудничества с государствами Западных Балкан — в области предотвращения и расследования случаев сексуального насилия и эксплуатации детей.

Как будущий Председатель Совета Европейского союза Словения также будет содействовать усилиям европейских регуляторов по укреплению киберустойчивости и управлению киберкризисами, пересмотру Директивы о безопасности сетевых и информационных систем (Директива NIS-2), определяющей меры по обеспечению высокого общего уровня кибербезопасности в рамках Союза, а также усилиям по активному внедрению Инструментария кибердипломатии Европейского союза как средства содействия предотвращению конфликтов, смягчению угроз кибербезопасности и повышению стабильности международных отношений. Мы будем добиваться расширения международного сотрудничества, снижения риска неправильного восприятия, эскалации и конфликтов.

В заключение позвольте мне еще раз подчеркнуть, что Совет Безопасности играет центральную роль в поддержке усилий в области кибербезопасности, которые имеют огромное значение для поддержания международного мира и безопасности. Организуя эти открытые дебаты, вы уже активно содействуете созданию среды, которая ведет к развитию сотрудничества, укреплению доверия, связанного с ИКТ, а также к глобальному, открытому, свободному, стабильному и безопасному киберпространству.

Приложение LVIII

Заявление Постоянного представительства Южной Африки при Организации Объединенных Наций

Южная Африка с интересом отметила созыв этих открытых дебатов Совета Безопасности, чтобы впервые рассмотреть в качестве отдельного тематического вопроса поддержание международного мира и безопасности в киберпространстве. Мы также благодарим Высокого представителя по вопросам разоружения г-жу Накамицу за проведенный ею брифинг. Мы также приняли к сведению ориентировочные вопросы, представленные для сегодняшнего обсуждения, на которые мы постараемся отреагировать в своем заявлении.

Прежде всего Южная Африка хотела бы подчеркнуть, что вопрос о мире и безопасности в киберпространстве — это постоянно возникающий сложный вопрос, который требует активного участия всех государств-членов Организации Объединенных Наций. Именно по этой причине мы считаем, что надлежащим местом для рассмотрения этого вопроса является Первый комитет Генеральной Ассамблеи, который уже им занимался этим вопросом.

В этой связи можно отметить, что государства-члены участвовали в работе Группы правительственных экспертов нескольких составов, последняя из которых уделяла основное внимание поощрению ответственного поведения государств в киберпространстве и подготовила одобренный консенсусом доклад в конце мая 2021 года под умелым руководством посла Бразилии Гильерми ди Агиар Патриоты.

Кроме того, с 2019 года отмечается широкое участие всех государств-членов в Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, которая приняла консенсусом доклад в конце марта 2021 года, а также в недавно созданной Рабочей группе открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ в 2021–2025 годах под руководством посла Бурхана Гафура, Постоянного представителя Республики Сингапур, в качестве ее Председателя.

Таким образом, члены Организации Объединенных Наций прошли долгий путь в обсуждении возникающих угроз международному миру и безопасности в киберпространстве, международно-правовой базы, регулирующей этот аспект международного мира и безопасности, норм, правил и принципов ответственного поведения государств-членов, практических мер укрепления доверия, необходимых мер по укреплению потенциала, а также путей продолжения диалога в этой области.

Позвольте мне вкратце поделиться в связи с этим следующими соображениями.

Южная Африка считает, что множество возникающих угроз требует участия всех соответствующих субъектов, включая гражданское общество и частный сектор.

Это будет необходимо как для понимания природы этих угроз, так и для сотрудничества всех слоев общества в целях выявления угроз, исходящих от государственных и негосударственных субъектов в киберпространстве, и их адекватного устранения.

Южная Африка хотела бы подчеркнуть необходимость преодоления цифрового и гендерного разрыва, а также превращения цифрового разрыва в цифровые возможности, что будет иметь ключевое значение для повышения

устойчивости и в то же время будет способствовать более активному развитию. Однако растущая изощренность вредоносных инцидентов в сфере ИКТ вызывает озабоченность у развивающихся стран, таких как Южная Африка.

Южная Африка по-прежнему обеспокоена растущей угрозой кибератак на важнейшие объекты инфраструктуры, включая информационную инфраструктуру. Хотя мы считаем, что противостоять этим угрозам следует путем расширения сотрудничества и разработки механизмов передовой практики, эти усилия следует направить на поддержку национальных приоритетов и деятельности по выявлению и обозначению такой инфраструктуры. Мы также осознаем, что, несмотря на подверженность угрозам, положительные социально-экономические возможности, которые могут быть получены благодаря ИКТ, не должны быть омрачены злонамеренным использованием этих технологий. Поэтому опасения вызывают не сами технологии, а попытки их неправильно использовать.

Что касается регулирования использования киберпространства и особенно пресечения угроз, создаваемых для международного мира и безопасности, то Южная Африка выступает в поддержку применимости к этой среде международного права, особенно Устава Организации Объединенных Наций во всей его полноте.

С учетом уже проделанной значительной работы мы считаем, что нам следует сосредоточиться на внедрении действующих норм, правил и принципов. Основополагающий принцип, поддерживаемый развивающимися странами, заключается в необходимости признания нами того факта, что все мы подвергаемся рискам в различной степени, учитывая различные возможности государств по защите от угроз, создаваемых злонамеренными действиями в киберпространстве. Поэтому наша делегация хотела бы подчеркнуть необходимость программ по наращиванию потенциала со стороны как государств, так и других заинтересованных кругов, чтобы помочь странам в борьбе с дестабилизирующими угрозами злоумышленников в киберсфере. Южная Африка считает, что наращивание потенциала имеет решающее значение для объединения усилий государств в целях повышения безопасности глобального киберпространства, поскольку речь идет о действительно глобальном вызове, требующем глобальных решений.

Наконец, Южная Африка сохраняет свою приверженность продолжению сотрудничества в целях решения этих вопросов, особенно в рамках Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, которая начнет свою основную работу в декабре. Она будет служить всеобъемлющей, единой структурой для обсуждения вопросов о том, как мы сообща можем противостоять возникающим сложным и всепроникающим угрозам международному миру и безопасности в киберпространстве.

Приложение LIX

Заявление Постоянного представительства Швейцарии при Организации Объединенных Наций

[Подлинный текст на французском языке]

Мы хотели бы поблагодарить Эстонию за организацию этих открытых дебатов, а Высокого представителя — за ее брифинг. Киберпространство стало неотъемлемой частью нашего общества и создает огромные возможности для социально- экономического развития. В то же время злонамеренные кибероперации порождают риски нестабильности и угрозы международному миру и безопасности. Мы обеспокоены тем, что киберпространство используется для проецирования силы и становится все более фрагментированным и дестабилизированным.

Открытое, безопасное, стабильное, доступное и мирное киберпространство выгодно всем. Организация Объединенных Наций играет важную роль в этом отношении. Швейцария приветствует недавнее принятие консенсусом докладов Группы правительственных экспертов Организации Объединенных Наций и Рабочей группы открытого состава. Эти доклады представляют собой важные шаги на пути к обеспечению ответственного поведения государств в киберпространстве.

Что касается укрепления мира и стабильности в киберпространстве, то я хотел бы выделить следующие элементы.

Во-первых, международное право применимо к киберпространству. Соблюдение международного права является важнейшим условием предотвращения конфликтов и поддержания международного мира и безопасности. Обязательство разрешать споры мирными средствами распространяется и на деятельность государств в киберпространстве. Кроме того, международное гуманитарное право применимо, когда вооруженный конфликт, будь то международный или немеждународный, реально существует. Швейцария приветствует тот факт, что в последнем докладе Группы правительственных экспертов об этом ясно сказано. Это крупное достижение. Международное гуманитарное право и его основные принципы накладывают важные ограничения на проведение кибероперациий в условиях вооруженного конфликта.

Во-вторых, Швейцария озабочена гуманитарными последствиями злонамеренных кибероперациий, число которых со времени начала пандемии растет, причем зачастую такие кибероперации затрагивают медицинские учреждения. Швейцария подчеркивает, что такие учреждения находятся под защитой, что было продемонстрировано в ходе открытых дебатов в апреле. В докладах Группы правительственных экспертов заложена основа для защиты важнейших объектов инфраструктуры от злонамеренных кибердействий. Кроме того, должны подлежать защите данные, собранные в гуманитарных целях. Мы также призываем государства соблюдать добровольные нормы ответственного поведения в киберпространстве и дополнительные указания Группы правительственных экспертов по их применению, с тем чтобы избежать нанесения ущерба важнейшим объектам инфраструктуры, смягчить гуманитарные последствия и обеспечить защиту гражданского населения.

В-третьих, для предотвращения атмосферы недоверия в киберпространстве важны меры укрепления доверия. На региональном уровне Швейцария стремится повысить роль Организации по безопасности и сотрудничеству в Европе в обеспечении киберстабильности: совместно с Германией Швейцария

разрабатывает предложение по внедрению мер укрепления доверия, предусматривающее проведение консультаций в случае серьезного киберинцидента. Швейцария также стремится к транспарентности и наращиванию потенциала: наш Национальный центр по вопросам кибербезопасности оказывает техническую помощь другим государствам в случае инцидента и обменивается данными и информацией о возможных угрозах. Совет Безопасности и организации системы Организации Объединенных Наций должны принимать во внимание региональные инициативы и меры укрепления доверия, которые оказались полезными для обеспечения мира и стабильности в киберпространстве.

Наконец, организации гражданского общества, научные круги и технические специалисты, а также частный сектор играют важную роль в поддержке международной киберстабильности, особенно в связи с соблюдением прав человека и основных свобод в Интернете и вне его. Швейцария, являясь членом Коалиции за свободу в Интернете, сотрудничает с более чем 30 правительствами и сетью заинтересованных сторон для продвижения свободы выражения мнений в Интернете. Мы призываем Совет Безопасности и государства-члены привлекать различных участников к реализации нормативно-правовой базы ответственного поведения государств в киберпространстве.

Многостороннее сотрудничество и соблюдение норм международного права, включая права человека и международное гуманитарное право, необходимы для обеспечения мира и безопасности в киберпространстве. Швейцария призывает к дальнейшей работе над этими темами, в том числе в рамках новой Рабочей группы открытого состава и будущей программы действий по поощрению ответственного поведения государств в киберпространстве. Как один из кандидатов в члены Совета Безопасности Швейцария надеется на продолжение многостороннего конструктивного диалога с опорой на существующую нормативно-правовую базу.

Приложение LX

Заявление Постоянного представительства Таиланда при Организации Объединенных Наций

Таиланд высоко оценивает усилия Эстонии по организации открытых дебатов на высоком уровне в Совете Безопасности по теме: «Поддержание международного мира и безопасности в киберпространстве», которые проводятся своевременно в нужный момент. Мы также высоко оцениваем лидерство Эстонии, которая первой провела официальное заседание Совета по теме кибербезопасности. Мы надеемся, что обеспечение безопасности и предотвращение неправомерного использования киберпространства и информационно-коммуникационных технологий (ИКТ) по-прежнему будут занимать важное место в повестке дня Совета, приветствуя при этом участие более широкого круга государств-членов Организации Объединенных Наций в этих важных обсуждениях.

Таиланд считает, что киберпространство принесло блага человечеству, как это было видно во время пандемии, обеспечив связь людей с основными социальными службами и, что самое главное, друг с другом, а также способствовало выполнению Повестки дня в области устойчивого развития на период до 2030 года. Однако использование ИКТ государствами и негосударственными субъектами, включая террористов, в злонамеренных целях, таких как нападения на важнейшие объекты гражданской инфраструктуры, не только подрывает международный мир и безопасность, но и негативно сказывается на безопасности нашего населения. Поэтому ответственность за решение этих вопросов лежит на государствах согласно соответствующим нормам международного права.

По мнению Таиланда, Организация Объединенных Наций может играть важную роль в поддержке усилий по созданию стабильного и безопасного киберпространства. Действительно, вопрос о безопасности киберпространства стоит в повестке дня государств-членов уже более двух десятилетий. Наиболее очевидным достижением стало недавнее поистине историческое принятие консенсусом доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2019–2021 годы) и доклада Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (2019–2021 годы).

Таиланд приветствует новую Рабочую группу открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы). Мы уверены в том, что под умелым руководством г-на Бурхана Гафура, Постоянного представителя Сингапура, Председателя Рабочей группы открытого состава, государства проведут плодотворные обсуждения, в том числе по вопросам укрепления доверия, сотрудничества и транспарентности в отношениях между государствами и дальнейшей разработки норм ответственного поведения государств в киберпространстве.

Таиланд надеется, что в рамках новой Рабочей группы открытого состава будут решены или разъяснены следующие вопросы: дальнейшая разработка руководящих указаний и рекомендаций по практическому применению норм ответственного поведения государств; достижение общего понимания того, как международное право применяется в киберпространстве и существуют ли пробелы; разработка долгосрочных и основанных на потребностях мер укрепления доверия и принятие документа «Регулярный институциональный диалог».

Таиланд также принимает к сведению успешные усилия других межправительственных органов, частного сектора и организаций и процессов граждан-

ского общества, которые внесли свой вклад в наши коллективные усилия по созданию безопасного и защищенного киберпространства. Таиланд поддерживает многосторонний подход к нашей работе, с тем чтобы обеспечить конструктивное участие соответствующих заинтересованных сторон и партнеров в обществе, в том числе женщин и молодежи.

С этой целью Таиланд ратует за укрепление нормативной базы путем активизации практической реализации согласованных норм, устранения существующих расхождений и удовлетворения потребностей в потенциале, а также обеспечения того, чтобы существующие многосторонние и двусторонние каналы оставались открытыми для дальнейшего диалога. Все государства должны продолжать совместную работу по сохранению нашего общего видения открытого, безопасного, доступного и мирного киберпространства и среды ИКТ для всех.

Приложение LXI

Заявление Постоянного представительства Турции при Организации Объединенных Наций

Мы хотели бы поблагодарить Эстонию за организацию этих открытых дебатов, которые посвящены важнейшей теме, особенно в нынешних условиях, вызванных пандемией. Мы также благодарим г-жу Накамицу, Высокого представителя по вопросам разоружения, за ее брифинг.

Использование информационно-коммуникационных технологий (ИКТ) оказывает влияние на экономику и развитие во всем мире. Пандемия показала, насколько сильно мы зависим от цифровых технологий. Обеспечение свободного, открытого и безопасного доступа к ИКТ, безусловно, имеет огромное значение.

Турция озабочена растущим числом кибератак. Вредоносная кибердеятельность, направленная на важнейшие объекты инфраструктуры, терроризм, цифровой шпионаж, мошенничество, надругательство над детьми и их эксплуатация в Интернете, а также неправомерное использование персональных данных входят в число современных угроз, которые также создают риски для международного мира и безопасности.

Вследствие развития техники кибератаки стало легче осуществлять, а негативные последствия и издержки для жертв быстро растут. Кибератаки также становятся все более «адресными» по своему характеру. Ежегодные потери от кибератак растут в геометрической прогрессии. Для защиты от этих атак нужны новые современные методы и инструменты.

Турция приветствует одобренные консенсусом доклады Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и недавно созданной Группы правительственных экспертов Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве. Эти доклады являются ценным вкладом в текущую работу по кибербезопасности под эгидой Организации Объединенных Наций. Не менее важно то, что доклады как Рабочей группы открытого состава, так и Группы правительственных экспертов являются совместимыми и дополняют друг друга с целью повышения стабильности, устойчивости и международного сотрудничества в киберпространстве. Мы надеемся увидеть более высокий уровень взаимодействия в таких начинаниях в будущем.

В связи с быстрыми темпами цифровизации Турция уделяет особое внимание принятию необходимых мер для укрепления национальной кибербезопасности. Сейчас в стадии реализации находятся Национальная стратегия кибербезопасности и План действий, рассчитанный на период 2020-2023 годов. Основными стратегическими целями данного Плана действий являются защита важнейших объектов инфраструктуры и повышение устойчивости, наращивание потенциала, создание собственной системы кибербезопасности, обеспечение безопасности технологий нового поколения (а именно: Интернет вещей, пятое поколение мобильной связи, облачные вычисления и т.д.), борьба с киберпреступностью, развитие и стимулирование локальных и национальных технологий, включение кибербезопасности в систему обеспечения национальной безопасности, а также развитие международного сотрудничества.

Кроме того, Национальная группа экстренного реагирования на киберугрозы в Турции играет важную роль в реализации и координации превентивных мер против киберугроз.

Наши усилия дополняют учебные программы, а также национальные и международные учения по кибербезопасности. Агентство по информационно-коммуникационным технологиям Турции предлагает государственные учебные Интернет-программы по кибербезопасности и другим смежным областям. За последние четыре года более 5000 человек прошли обучение в различных областях кибербезопасности.

Ежегодно организуемый «День безопасного Интернета» является одним из мероприятий вышеупомянутого Агентства, направленных на повышение осведомленности о продуманном и безопасном использовании Интернета. Кроме того, Турция предпринимает шаги по противодействию повышенным рискам для кибербезопасности и в сотрудничестве с соответствующими заинтересованными сторонами принимает меры, чтобы гарантировать устойчивость бизнеса, доступность и защиту потребителей во время пандемии.

Мы также предприняли шаги по укреплению нашей национальной законодательной базы.

Поскольку риски в киберсфере имеют трансграничный характер, расширение международного сотрудничества имеет огромное значение. Сознавая это, Турция участвует в обмене разведданными о киберугрозах и вносит свой вклад в политику и стратегии сотрудничества в рамках региональных и международных организаций, включая Организацию по безопасности и сотрудничеству в Европе, Группу двадцати и ОЭСР. Турция также участвует в международных учениях, в том числе в рамках МСЭ и НАТО.

Организация Объединенных Наций играет центральную роль в усилиях по развитию стратегического и эффективного сотрудничества в использовании ИКТ государствами. Турция поддерживает применимость международного права в киберпространстве. Настало время опираться на результаты предыдущей работы, выполненной в системе Организации Объединенных Наций, и найти правильные способы практической реализации правил, норм, принципов и рекомендаций по ответственному поведению государств в киберпространстве.

Одной из главных областей нашей будущей работы является выработка общего понимания путей и средств применения международного права в киберпространстве. Это действительно необходимо для устранения недопонимания и повышения ответственности в киберпространстве.

Надо также установить каналы связи между государствами-членами для чрезвычайных ситуаций и обмениваться через них информацией и ресурсами. Это станет большим вкладом в укрепление доверия и ускорит нашу работу по наращиванию потенциала.

Кроме того, нам надо также срочно пересмотреть и укрепить существующие международные инструменты для расширения сотрудничества в рамках новых технологий, таких как «облачные» вычисления, Интернет вещей, пятое поколение мобильной связи и искусственный интеллект.

Полезными инструментами могут стать проведение исследования национальных нормативных подходов к обеспечению безопасности новых технологий и подготовка кодекса поведения для руководства и информирования национальных структур. Кроме того, нам надо выработать общее понимание и определения угроз.

В контексте наращивания потенциала мы считаем, что Организация Объединенных Наций, а также региональные организации могут продвигать программы обмена экспертами по кибербезопасности и создавать общие учебные платформы. Надо поощрять проведение международных учений, с тем чтобы

повысить готовность к киберинцидентам и потенциал реагирования на них на национальном уровне.

Поскольку киберпространство не имеет границ, а кибербезопасность — это вопрос, затрагивающий много заинтересованных сторон, национальным властям надо работать с пользователями, частным сектором, НПО и международными партнерами для борьбы с киберугрозами. Глобальные поставщики, поставщики услуг и компании, занимающиеся вопросами безопасности, также должны более эффективно сотрудничать с правительствами и международными организациями, с тем чтобы внести свой вклад в обеспечение глобальной кибербезопасности.

Турция намерена продолжать сотрудничество и диалог в целях содействия региональной и глобальной кибербезопасности.

Приложение LXII

Заявление Постоянного представительства Украины при Организации Объединенных Наций

Мы благодарим Эстонию за инициативу проведения столь важного заседания Совета Безопасности, а также благодарим Высокого представителя по вопросам разоружения г-жу Накамицу за ее брифинг.

Быстрое развитие информационно-коммуникационных технологий постепенно привело к «переформатированию» Интернет-пространства: сегодня это уже не удобная площадка для общения, а настоящее оружие, которое становится все более опасным в руках хакеров, преступников, некоторых государственных субъектов и их ставленников.

К сожалению, несмотря на существующие правовые нормы и институциональные механизмы, созданные для борьбы с киберпреступностью на национальном, региональном и международном уровне, благами современного цифрового мира слишком часто злоупотребляют, а кибератаки происходят все чаще и превращаются в новый метод гибридной войны.

Международная политика постепенно становится уязвимой для киберугроз. За последние несколько лет некоторые государства стали удобными мишенями кибератак.

Украина — это государство, где кибератаки с 2014 года стали одним из основных элементов предпринимаемых извне попыток подорвать наш суверенитет. В 2014-2021 годах Украина столкнулась с беспрецедентным количеством кибероперций против жизненно важных объектов нашей инфраструктуры. Большинство этих атак было совершено хакерскими группами, управляемыми из Российской Федерации.

Кибероперации против крупных объектов важнейшей инфраструктуры, энергетического, транспортного и нефтегазового сектора являются вызовами и угрозами международному миру и безопасности. Недавно трубопровод «Колониал» стал объектом кибератаки, которая нанесла серьезный ущерб компьютерам, управляющим трубопроводом, что привело к тяжелым последствиям.

Во времена пандемии коронавирусного заболевания (COVID-19) губительные последствия злонамеренных кибероперций стали очевидными. Некоторые государственные и негосударственные субъекты используют глобальный кризис для проведения кибероперций, в том числе против сферы здравоохранения, что вызывает серьёзную озабоченность международного сообщества.

Однако не только важнейшая инфраструктура, но и международная политика становится все более уязвимой в условиях злонамеренного использования все более сложных и изощренных возможностей ИКТ, что подтверждают громкие случаи вмешательства кремлевских хакеров в крупные избирательные кампании и биографии кандидатов.

Поэтому киберстабильность стала важнейшим компонентом обеспечения всеобщего мира и безопасности, требующим строгого соблюдения международного права, применимость которого в киберпространстве была недавно подтверждена в докладах Рабочей группы открытого состава и Группы правительственных экспертов, требующим также надлежащего выполнения норм, правил и принципов ответственного поведения и укрепления международного сотрудничества для сохранения свободного, открытого, стабильного и безопасного киберпространства.

Мы подчеркиваем, что особое внимание следует уделять разработке единых стандартов борьбы с киберугрозами, обмену передовым опытом, укреплению взаимного доверия в области кибербезопасности, предотвращению использования киберпространства в политических, террористических и военных целях, а также оказанию финансовой и технической помощи для увеличения национальных возможностей противостоять киберугрозам, уменьшения рисков и повышения устойчивости.

На сегодняшний день кибероперации против важнейших объектов инфраструктуры и государственных учреждений, а также дезинформационные кампании, способные подстрекать к терроризму, являются широко используемым методом вмешательства во внутренние дела суверенных государств, включая Украину.

Нет сомнения в том, что Россия использует высокие технологии для достижения собственных политических и геополитических целей, в том числе поощряя и усиливая конфликты в соседних государствах и проводя агрессивные информационные войны.

Мы настоятельно призываем международное сообщество тщательно рассмотреть вопрос об ответственности в случаях выявления конкретного государства или государственных субъектов, стоящих за подготовкой или осуществлением целенаправленного злонамеренного использования ИКТ или распространения лжи во враждебных целях.

В конце концов международные усилия, предпринимаемые в этой области, будут просто напрасными, если не будет надежных механизмов для выявления, наказания и привлечения к ответственности отдельных лиц и соответствующих государств, ответственных за координацию и финансирование незаконной деятельности в глобальном киберпространстве.

Приложение LXIII

Заявление Постоянного представительства Объединенных Арабских Эмиратов при Организации Объединенных Наций

Пандемия коронавирусного заболевания (COVID-19) высветила зависимость мира от информационно-коммуникационных технологий, которые были необходимы для того, чтобы мы могли получать информацию и поддерживать связь друг с другом, даже если мы сами были на расстоянии друг от друга.

В течение последних восемнадцати месяцев мы наблюдали тенденцию к увеличению числа злонамеренных кибероперaций, направленных против медицинских учреждений, включая организации, занимающиеся исследованиями и разработкой вакцин для борьбы с COVID-19. Мы живем в нестабильном регионе, и Ближний Восток не застрахован от риска, связанного с вредоносной киберактивностью: он часто становится объектом крупных кибероперaций и шпионажа. За последние несколько лет в нашем регионе произошли серьезные инциденты, затронувшие телекоммуникационный, банковский и государственный секторы. Объектами нападения также стали нефтегазовые объекты, что привело к ущербу в сотни миллионов. Такая злонамеренная кибердеятельность, направленная против важнейших объектов инфраструктуры региона, может вызвать конфликт в условиях и без того напряженной обстановки и создать угрозу международному миру и безопасности.

Объединенные Арабские Эмираты намерены создать необходимую инфраструктуру и механизмы для укрепления своего потенциала в области кибербезопасности, как для защиты от киберугроз, так и для более эффективного сотрудничества с другими странами в целях решения общих проблем. В ноябре 2020 года мы учредили Совет по кибербезопасности Объединенных Арабских Эмиратов, который будет разрабатывать комплексную национальную стратегию кибербезопасности и национальный план реагирования на киберинциденты. Мы проводим крупнейшие конференции по вопросам кибербезопасности и цифровой трансформации, включая «Гитекс», «Гисек» и «Кибертех», для наращивания внутреннего потенциала, а также разработали платформу для государственно-частного партнерства, с тем чтобы облегчить обмен информацией. Мы также сотрудничаем с государствами, международными организациями и структурами частного сектора для обмена информацией как на политическом, так и на техническом уровне. Например, Объединенные Арабские Эмираты участвуют в работе региональных организаций, таких как новая совместная платформа анализа вредоносных программ Совета сотрудничества стран Персидского залива, и являются активным членом Группы реагирования на связанные с компьютерами чрезвычайные ситуации Организации исламского сотрудничества. Эти меры укрепления доверия на основе сотрудничества и транспарентности входят в число методов, с помощью которых Объединенные Арабские Эмираты вносят свой вклад в снижение киберрисков для международного мира и безопасности.

Объединенные Арабские Эмираты приветствуют рекомендации, содержащиеся в докладах как Рабочей группы открытого состава по ИКТ, так и Группы правительственных экспертов. Они подчеркивают важность поддержки усилий по дальнейшему внедрению добровольных норм ответственного поведения государств в киберпространстве, а также необходимость выработки общего понимания применимости международного права к деятельности в Интернете. Однако надо сделать еще больше как для поощрения и поддержки усилий государств по выполнению нынешних рекомендаций, так и для разработки новых рекомендаций в быстро меняющихся условиях. Программа действий по ответственному поведению государств в киберпространстве представляет собой

идеальную «дорожную карту» для дальнейшей работы и будет способствовать устранению киберрисков для международного мира и безопасности.

Минимизация киберрисков для международного мира и безопасности будет оставаться сложной задачей. Объединенные Арабские Эмираты предлагают две рекомендации, которые могут помочь в решении этой задачи.

Во-первых, государства должны обеспечить обучение и наращивание потенциала на двустороннем, региональном и международном уровнях, в том числе с помощью учебных программ и разработки рекомендаций для оказания помощи в реализации норм ответственного поведения государства. Эти действия могут стать мерами по укреплению доверия и реакцией на недоверие и недопонимание между государствами в киберпространстве, которые могут угрожать международному миру и безопасности.

Во-вторых, государствам следует продолжать делиться своими мнениями и оценками с Генеральным секретарем и активно участвовать в международных форумах и межрегиональных форматах, связанных с киберпространством. Обмен передовой практикой и опытом может помочь государствам адаптироваться к меняющимся нормам и стать ответственными участниками киберпространства.

Все государства несут ответственность за укрепление международного мира и безопасности как в Интернете, так и вне его. Соблюдение норм ответственного поведения государств и выполнение своих обязательств по международному праву — наилучшая точка отсчета.