Организация Объединенных Наций S/2021/540

Совет Безопасности

Distr.: General
8 June 2021
Russian
Original: English

Письмо Постоянного представителя Эстонии при Организации Объединенных Наций от 8 июня 2021 года на имя Генерального секретаря

В качестве Председателя Совета Безопасности в июне Эстония намерена провести открытые прения высокого уровня на тему «Поддержание международного мира и безопасности в киберпространстве» по пункту «Поддержание международного мира и безопасности» во вторник, 29 июня 2021 года, в 8 ч 00 мин (по летнему североамериканскому восточному времени).

В качестве ориентира для обсуждения этой темы Эстония подготовила концептуальную записку (см. приложение).

Буду признателен за распространение настоящего письма и приложения к нему в качестве документа Совета Безопасности.

(*Подпись*) Свен **Юргенсон**
Посол, Постоянный представитель

21-07545 (R) 110621 150621

Просьба отправить на вторичную переработку

Приложение к письму Постоянного представителя Эстонии при Организации Объединенных Наций от 8 июня 2021 года на имя Генерального секретаря

Концептуальная записка для открытых прений Совета Безопасности на тему «Поддержание международного мира и безопасности в киберпространстве», которые состоятся 29 июня 2021 года

I. Цель

1. Цель этих открытых прений — способствовать лучшему пониманию растущих рисков, которые возникают в результате злонамеренной деятельности в киберпространстве, и их влияния на международный мир и безопасность, а также обсудить глобальные усилия по укреплению мира и стабильности в киберпространстве. У государств-членов будет возможность подтвердить свою приверженность международному праву и нормам ответственного поведения государств как ключевым элементам предотвращения конфликтов и поддержания мира и безопасности в киберпространстве.

II. Справочная информация

2. В соответствии с Уставом Организации Объединенных Наций главной обязанностью Совета Безопасности является поддержание международного мира и безопасности. Соответственно, Совет уделяет внимание меняющемуся характеру проблем международной безопасности, рассматривая ряд сложных новых факторов, способных дестабилизировать страны и обострить или продлить текущие конфликты. На протяжении многих лет Совет проводил как широкие тематические прения по новым угрозам международному миру и безопасности, так и заседания по конкретным вопросам, как то: изменение климата, природные ресурсы, пандемии, голод, транснациональная организованная преступность, незаконный оборот наркотиков и пиратство.

3. Совет уже обсуждал кибербезопасность на нескольких неофициальных заседаниях и в ходе прений, посвященных теме международной безопасности в целом, но эти открытые прения станут первым мероприятием, на котором Совет Безопасности рассмотрит ее отдельно. Как выяснилось в ходе этих совещаний, киберугрозы вызывают озабоченность у многих стран и представляют собой одну из главных угроз безопасности. Например, в декабре 2017 года Совет под председательством Японии провел открытые прения по сложным современным вызовам международному миру и безопасности. В ходе этих открытых прений Генеральный секретарь назвал кибербезопасность одной из растущих угроз международному миру и безопасности (см. S/PV.8144). В августе 2019 года Польша организовала открытые прения по вызовам миру и безопасности на Ближнем Востоке, предложив участникам обсудить вопрос о том, «как противостоять киберугрозам, включая угрозы энергетической инфраструктуре, в контексте продвижения механизмов сотрудничества в вопросах предотвращения серьезных инцидентов в киберпространстве на Ближнем Востоке и реагирования на них» (см. S/2019/643), и несколько участников затронули этот вопрос в своих выступлениях. В последний раз эта проблема обсуждалась в апреле 2021 года на проведенных под председательством Вьетнама прениях высокого уровня на тему «Защита гражданских лиц в вооруженном конфликте: жизненно необходимые гражданские объекты» (см. S/2021/415), где докладчики, а также некоторые

участники отметили угрозы, которые злонамеренные действия в киберпространстве создают для объектов критически важной инфраструктуры, в частности для медицинских учреждений.

4. Свободное, открытое и соответствующее требованиям совместимости киберпространство, управляемое и поддерживаемое многосторонним сообществом заинтересованных сторон, несомненно, позволяет государствам извлекать значительную экономическую выгоду и содействовать социальному прогрессу во всем мире. Цифровые технологии стали важным катализатором прогресса человечества и развития человеческого потенциала. Кроме того, технологии значительно способствуют уважению к правам человека, давая возможность высказаться уязвимым и маргинализованным группам общества. Устойчивое цифровое развитие также может внести весомый вклад в обеспечение постконфликтной стабильности в зонах региональных конфликтов.

5. К сожалению, в условиях растущей зависимости от цифровой сферы и наряду с различными преимуществами цифровых преобразований наблюдаются постоянный рост вредоносной деятельности в киберпространстве и усиление системных угроз нарушения функционирования критически важной инфраструктуры и цифровых сервисов. Неправомерное использование киберпространства может повлиять на жизненно важные отрасли экономики и основные услуги, оказываемые населению, такие как здравоохранение и энергоснабжение. Это может привести к разрушительным гуманитарным последствиям и дестабилизации, которые могут угрожать международному миру и безопасности. Пандемия, вызванная коронавирусной инфекцией (COVID-19), привела к дальнейшему усилению зависимости от критической цифровой инфраструктуры, и потому так важно ответственное поведение государств в киберпространстве в соответствии с принципами международного права.

6. Чтобы сократить масштабы злонамеренного использования возможностей киберпространства и добиться повышения стабильности в нем, крайне важно применять соответствующие превентивные механизмы на глобальном, региональном и национальном уровнях. За последнее десятилетие государства — члены Организации Объединенных Наций добились значительного прогресса в выработке свода норм ответственного поведения государств в киберпространстве на базе международного права и других норм и мер укрепления доверия и наращивания потенциала.

7. Международное право, в частности Устав, содержит достаточные ориентиры для деятельности государств в киберпространстве. Принципы международного права, которые успешно регулируют поведение государств в других областях, также являются первичными ориентирами для поведения государств в киберпространстве. Помимо международного права, важную роль в обеспечении ориентиров для поведения государств в киберпространстве играют добровольные, не имеющие обязательной силы нормы ответственного поведения государств в мирное время и меры укрепления доверия, которые повышают прозрачность, ясность намерений и предсказуемость. Государства должны выполнять свои международные обязанности в соответствии с международным правом в связи с вменяемыми им международно-противоправными деяниями.

8. Вопрос о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности обсуждался сменявшими друг друга составами групп правительственных экспертов при Первом комитете Генеральной Ассамблеи, которые подготовили в 2010, 2013, 2015 и 2021 годах

консенсусные доклады на эту тему[1]. В Генеральной Ассамблее государства-члены путем консенсуса договорились руководствоваться при использовании информационно-коммуникационных технологий нормами ответственного поведения государств, а также нормами международного права и мерами укрепления доверия[2]. Успех посвященных киберпространству процессов в Первом комитете в 2021 году придает импульс дальнейшей имплементации норм ответственного поведения государств в киберпространстве. В консенсусном докладе, принятом рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и одобренном Генеральной Ассамблеей, подтверждается необходимость применения в киберпространстве международного права, других соответствующих норм, мер укрепления доверия и наращивания потенциала[3]. Этот консенсусный доклад, подготовленный по итогам последнего заседания Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, стал значительным вкладом в углубление понимания того, как международное право применимо к использованию государствами информационно-коммуникационных технологий, и содержит дополнительные рекомендации по имплементации норм, а также по укреплению доверия в киберпространстве и наращиванию потенциала.

9. Региональные организации, такие как Организация американских государств, Организация по безопасности и сотрудничеству в Европе, Африканский союз, Ассоциация государств Юго-Восточной Азии (АСЕАН) и Региональный форум АСЕАН, также добились значительных успехов, приняв региональные соглашения по кибербезопасности и разработав и приняв меры по укреплению доверия в киберпространстве, направленные на повышение стабильности и снижение вероятности конфликта. В то же время особо важную роль в повышении устойчивости к потрясениям в киберпространстве играют усилия по наращиванию потенциала и целый ряд глобальных и региональных программ. Кроме того, поскольку государства, как правило, не сами управляют всей своей критической инфраструктурой, а полагаются на сотрудничество с частным сектором, возник ряд государственно-частных инициатив по кибербезопасности. С учетом многостороннего характера киберпространства следует и далее поощрять любые возможности привлечения частного сектора, научных кругов и гражданского общества к обсуждениям на глобальном, региональном и национальном уровнях.

III. Вопросы для обсуждения

10. Государствам-членам предлагается в их выступлениях на заседании уделить внимание следующим вопросам:

a) Каковы нынешние и назревающие киберугрозы международному миру и безопасности? Как злонамеренное использование киберпространства может повлиять на конфликты в будущем?

b) Какие глобальные, региональные и национальные политические механизмы имеются для снижения киберугроз и поощрения ответственного поведения государств и как государства — члены Организации Объединенных Наций могут способствовать их реальному применению?

---

[1] Доклады A/65/201, A/68/98 и A/70/174 были одобрены Генеральной Ассамблеей; доклад, обсуждавшийся 28 мая 2021 года, готовится к изданию.

[2] Резолюция 70/237 Генеральной Ассамблеи.

[3] Решение 75/564 Генеральной Ассамблеи.

c) Как улучшить соблюдение международного права и норм ответственного поведения государств в киберпространстве, согласованных государствами — членами Организации Объединенных Наций?

d) Как укрепить доверие, уменьшить недопонимание и не допустить развития событий, которые могут привести к разрушительным гуманитарным последствиям в результате злонамеренной деятельности в киберпространстве?

e) Как во время вооруженных конфликтов уменьшить возможные гуманитарные последствия вредоносного использования информационно-коммуникационных технологий?

f) С учетом многостороннего характера киберпространства какую роль может играть более широкое сообщество, в том числе частный сектор, гражданское общество и научные круги, в содействии предотвращению конфликтов, достижению взаимопонимания и повышению устойчивости в киберпространстве?

g) В случае серьезных ситуаций, которые возникают в результате действий в киберпространстве, способных привести к международному конфликту или вызвать спор, каковы возможные варианты реагирования и пути поиска мирного решения?

IV. Докладчики

11. Для выступления в Совете приглашена Высокая представительница по вопросам разоружения.

V. Формат

12. Открытые прения высокого уровня состоятся 29 июня 2021 года в формате открытой видеоконференции. На заседании будет председательствовать премьер-министр Эстонской Республики Кая Каллас.

13. Всем государствам — членам Организации Объединенных Наций, которые не являются членами Совета, и постоянным наблюдателям при Организации Объединенных Наций предлагается принять участие посредством представления письменных заявлений через модуль e-Speakers. Государствам-членам следует направить свои заявления в формате Microsoft Word с сопроводительным письмом, надлежащим образом подписанным Постоянным представителем или временным поверенным в делах, на имя Председателя Совета Безопасности не позднее даты проведения заседания, т. е. 29 июня 2021 года. Эти заявления будут опубликованы как часть официального сводного документа, содержащего представленные тексты выступлений на этой открытой видеоконференции.