Организация Объединенных Наций S/2023/364

Совет Безопасности

Distr.: General
22 May 2023
Russian
Original: English

Письмо Постоянного представителя Албании при Организации Объединенных Наций от 19 мая 2023 года на имя Председателя Совета Безопасности

Имею честь сообщить Вам, что Постоянное представительство Республики Албания при Организации Объединенных Наций, совместно с представительством Соединенных Штатов при Организации Объединенных Наций, организует заседание по формуле Аррии на тему «Ответственность и меры реагирования государств в связи с кибератаками на жизненно важные объекты инфраструктуры».

Заседание состоится в четверг, 25 мая, с 15 ч 00 мин до 17 ч 30 мин в зале Совета по опеке в Центральных учреждениях Организации Объединенных Наций и будет проведено при поддержке постоянных представительств Эквадора и Эстонии при Организации Объединенных Наций в качестве совместных организаторов.

В качестве ориентира для обсуждений по этой теме мы подготовили концептуальную записку (см. приложение).

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

(*Подпись*) Ферит **Ходжа**
Посол
Постоянный представитель

Приложение к письму Постоянного представителя Албании при Организации Объединенных Наций от 19 мая 2023 года на имя Председателя Совета Безопасности

Концептуальная записка для заседания по формуле Аррии на тему «Ответственность и меры реагирования государств в связи с кибератаками на жизненно важные объекты инфраструктуры», которое состоится 25 мая 2023 года

Введение

Стремительное развитие цифровых технологий привело к изменению мироустройства, повлияв на все аспекты современной жизни. Несомненно, такое развитие несет в себе преимущества для всех— от государств и отдельных лиц до правительств, промышленных предприятий, систем здравоохранения и финансовых систем, региональных и международных организаций, специальных политических миссий и миссий по поддержанию мира.

Хотя развитие цифровых технологий имеет множество преимуществ, оно достается ценой подверженности широкому спектру угроз. Эти угрозы возникают в результате злонамеренной кибернетической деятельности, осуществляемой как государственными, так и негосударственными субъектами, и могут угрожать поддержанию международного мира и безопасности. В результате эти угрозы могут подорвать целостность, безопасность, экономический рост и стабильность международного сообщества. Ненадлежащее использование технологий может привести к эскалации существующих конфликтов или возникновению новых. Набор киберугроз постоянно расширяется с появлением новых технологий, таких как искусственный интеллект. Такие киберугрозы значительно возрастают, и в этой связи вопрос кибербезопасности становится как никогда актуальным. Это включает не только злонамеренную кибернетическую деятельность, осуществляемую в целях получения финансовой выгоды, но и приводящие к инцидентам подрывные мероприятия в киберсфере, направленные против государств и их жизненно важной инфраструктуры.

К деятельности государств в киберпространстве применимы нормы международного права, и в частности положения Устава Организации Объединенных Наций. Все государства-члены обязаны соблюдать Устав, включая его положения о соблюдении прав человека и основных свобод, а также другие нормы международного права, включая международное гуманитарное право, и должны содействовать установлению глобального, открытого, стабильного и безопасного киберпространства. Все государства также обязались руководствоваться рамочными основами ответственного поведения государств в киберпространстве, включая 11 добровольных норм (резолюция 70/237 Генеральной Ассамблеи). При использовании информационно-коммуникационных технологий государствам-членам необходимо также руководствоваться положениями докладов Группы правительственных экспертов, включая ее доклад за 2021 год, и доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2021 год.

Значительную обеспокоенность вызывает злонамеренная деятельность в киберсфере, нацеленная на объекты жизненной важной инфраструктуры и критической информационной инфраструктуры, которые имеют определяющее значение для предоставления основных государственных услуг в затрагиваемых государствах. В докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2015 год (A/70/174) эта обеспокоенность была отражена в одной

из 11 норм, но несмотря на это, кибератаки на жизненно важную инфраструктуру в последние годы постоянно усиливаются.

В то время как государства несут ответственность за осуществление некоторых из наиболее серьезных кибератак, затрагивающих жизненно важную инфраструктуру, в большей мере эта деятельность может быть отнесена на счет негосударственных субъектов, добивающихся получения финансовых выгод. Однако и в последнем случае следует ожидать, что государства не будут спокойно на это смотреть. Суверенитет государств и принципы, проистекающие из суверенитета, применимы к осуществлению государствами деятельности, связанной с информационно-коммуникационными технологиями, и к их юрисдикции над инфраструктурными объектами в области информационно-коммуникационных технологий, находящимися на их территории. Соответственно, следует ожидать, что если государство знает или будет добросовестно уведомлено о том, что международно-противоправное деяние, совершаемое с применением информационно-коммуникационных технологий, происходит из инфраструктурного объекта на его территории или осуществляется со сквозным использованием такого объекта, оно будет принимать все соответствующие разумно доступные и возможные меры для обнаружения, расследования и урегулирования такой ситуации.

Кибератаки, которые преднамеренно наносят ущерб жизненно важной инфраструктуре или иным образом препятствуют использованию такой инфраструктуры для предоставления услуг населению, оказывают заметное влияние на поддержание международного мира и безопасности. Неспособность государства справиться с чреватой эскалацией кибернетической деятельностью, исходящей с его территории, также может иметь дестабилизирующие последствия. В этой связи следует отметить, что в сложившихся условиях на глобальном уровне Совет Безопасности должен играть определенную роль в оценке сопутствующих рисков, и прежде всего в предотвращении конфликтов, возникающих в результате использования информационно-коммуникационных технологий для кибератак. Он должен также добиваться ответственного поведения государств в киберпространстве и настаивать на соблюдении Устава Организации Объединенных Наций и норм международного права.

Цель

Во взаимосвязанном мире, в котором государства, государственные и частные организации, а также отдельные лица все больше полагаются на услуги и операции, предлагаемые в киберпространстве, аспекты кибербезопасности оказываются неразрывно связанными с международным миром и безопасностью. Цель этого заседания— сосредоточить внимание на важности и актуальности решения вопросов, связанных с ответственным поведением государств в области использования информационно-коммуникационных технологий, в качестве темы, имеющей отношение к главной ответственности Совета Безопасности за поддержание международного мира и безопасности.

В целях выполнения своих обязанностей по Уставу Совет Безопасности должен взять на себя ведущую роль в продвижении норм ответственного поведения государств и обратить внимание на применимость норм международного права к использованию информационно-коммуникационных технологий государствами-членами. Выявляя и осуждая противоречащее нормам или противоправное поведение государств и поощряя позитивные меры по укреплению безопасности и стабильности киберпространства, Совет Безопасности может снизить риск возникновения конфликта в результате злонамеренных действий или бездействия. В частности, Совету Безопасности необходимо рассмотреть вопрос

о росте числа кибератак на критическую инфраструктуру и о том, какие дальнейшие шаги необходимо предпринять для сдерживания этой деятельности и смягчения причиняемого ею ущерба.

Заседание по формуле Аррии предоставит возможность осветить вклад не только государств, но и других заинтересованных сторон, а также заслушать докладчиков из международных организаций, которые представят информацию и подкрепят знаниями наши действия по преодолению текущих проблем, связанных с кибербезопасностью. С учетом того, что весьма значительная часть жизненно важной инфраструктуры принадлежит предприятиям частного сектора и эксплуатируется ими, как на внутреннем, так и на международном уровне необходимо налаживать действенные партнерские связи между государственным и частным секторами в целях борьбы с киберугрозами.

Наводящие вопросы

- Какие возможные действия может предпринять Совет Безопасности для борьбы с киберугрозами и кибератаками в отношении жизненно важной инфраструктуры государств?
- Какую роль может сыграть Совет Безопасности в обеспечении безопасного и мирного киберпространства, в укреплении доверия между государствами в этом отношении и в предотвращении конфликтов, возникающих в результате использования каким-либо государственным или негосударственным субъектом информационно-коммуникационных технологий в злонамеренных целях?
- Какие механизмы имеются в распоряжении государств для уведомления другого государства о злонамеренной деятельности, исходящей с его территории? Какова ответственность вышеупомянутого другого государства, получившего такое уведомление?
- Какие механизмы имеются у пострадавших государств для запроса помощи у других государств в ответ на серьезную кибератаку?
- Какие возможные способы и механизмы имеются для установления более тесных партнерских связей между государственными и частными структурами в целях обеспечения согласованной и слаженной защиты от кибератак и реагирования на них?

Докладчики

- Заместитель Генерального секретаря и Высокий представитель по вопросам разоружения
- Мариетье Шааке, директор по вопросам международной политики Стэнфордского центра киберполитики
- Молиехи Макумане, аналитик по вопросам кибербезопасности в рамках Программы по безопасности и технологиям Института Организации Объединенных Наций по исследованию проблем разоружения

Формат

Заседание по формуле Арриа организуется постоянными представительствами Албании и Соединенных Штатов при Организации Объединенных Наций и проводится при поддержке постоянных представительств Эквадора и Эстонии при Организации Объединенных Наций в качестве совместных организаторов. Данное заседание является открытым для всех государств — членов

Организации Объединенных Наций, постоянных наблюдателей, представителей неправительственных организаций и средств массовой информации. Устный перевод будет обеспечиваться на все шесть официальных языков Организации Объединенных Наций.

Совместные организаторы, государства-члены и постоянные наблюдатели будут приглашены выступить с заявлениями после выступлений докладчиков и членов Совета Безопасности. Приоритет будет отдаваться совместным организаторам и тем, кто выступает от имени групп из двух и более делегаций.

Чтобы зарегистрироваться для выступления с заявлениями, пожалуйста, сообщите название государства-члена и имя и должность выступающего по адресам электронной почты andris.stastoli@mfa.gov.al и garelleka@state.gov до 16 ч 00 мин 23 мая. Приветствуется участие на уровне постоянного представителя или поверенного в делах.

Делегациям предлагается ограничивать продолжительность своих выступлений тремя минутами.