Организация Объединенных Наций A/70/127

Генеральная Ассамблея

Distr.: General
2 July 2015
Russian
Original: English

Семидесятая сессия
Пункт 93 первоначального перечня*
Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности

Вербальная нота Постоянного представительства Бангладеш при Организации Объединенных Наций от 26 июня 2015 года на имя Генерального секретаря

Постоянное представительство Народной Республики Бангладеш при Организации Объединенных Наций в Нью-Йорке свидетельствует свое уважение Генеральному секретарю Организации Объединенных Наций и в своем качестве Председателя Руководящего совета Межпарламентского союза имеет честь настоящим препроводить Генеральной Ассамблее текст (на английском и французском языках) резолюции, озаглавленной «Кибервойна: серьезная угроза миру и глобальной безопасности» и принятой 132-й Ассамблеей Межпарламентского союза, проходившей в Ханое 31 марта 2015 года (см. приложение).

Постоянное представительство Народной Республики Бангладеш при Организации Объединенных Наций просит Канцелярию Генерального секретаря распространить настоящую вербальную ноту и приложение к ней в качестве документа семидесятой сессии Генеральной Ассамблеи по пункту 93 первоначального перечня.

* A/70/50.

Приложение к вербальной ноте Постоянного представительства Бангладеш при Организации Объединенных Наций от 26 июня 2015 года на имя Генерального секретаря

[Подлинный текст на английском и французском языках]

Кибервойна: серьезная угроза миру и глобальной безопасности

Резолюция, принятая консенсусом* 132-й Ассамблеей Межпарламентского союза

(Ханой, 1 апреля 2015 года)

132-я Ассамблея Межпарламентского союза (МПС),

сознавая, что информационно-коммуникационные технологии (ИКТ) являются средством интеграции и развития и не должны использоваться государствами или негосударственными субъектами в нарушение норм международного права, в частности положений и принципов Устава Организации Объединенных Наций, касающихся суверенитета, невмешательства, суверенного равенства государств, мирного разрешения споров и запрещения угрозы силой или ее применения,

признавая работу, проделанную Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности,

считая, что доступ человека к киберпространству включает, в частности, широкое использование цифровой спутниковой связи, оптоволоконных сетей и современных компьютерных программ, систематический обмен информацией, графическими, аудиовизуальными и компьютерными данными, интеллектуальными аппаратными и техническими средствами, программным обеспечением и операционными системами, а также возможность их использования в своих собственных целях,

признавая, что ненадлежащее использование технологий может иметь пагубные последствия на национальном, региональном и даже глобальном уровне и что поэтому необходимо создать международные регулирующие правовые вопросы органы и документы, касающиеся назначения и использования технологий,

будучи убеждена в том, что, поскольку киберпространство приносит всем гражданам во всех странах мира колоссальную социально-экономическую пользу, обеспечение в киберсреде предсказуемости, информационной безопасности и стабильности имеет исключительно важное значение,

* Делегация Боливарианской Республики Венесуэла высказала оговорку в отношении использования термина «кибервойна».

рассмотрев резолюции Генеральной Ассамблеи Организации Объединенных Наций 31/72 от 10 декабря 1976 года (о конвенции о запрещении военного или любого иного враждебного использования средств воздействия на природную среду), 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года (о борьбе с преступным использованием информационных технологий), 69/28 от 2 декабря 2014 года (о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности) и 57/239 (о создании глобальной культуры кибербезопасности),

учитывая важное значение международных и региональных соглашений о борьбе с киберпреступностью и транснациональной организованной преступностью, об обмене информацией и административной помощи, включая Конвенцию 1977 года о запрещении военного или любого иного враждебного использования средств воздействия на природную среду, Конвенцию Совета Европы 2001 года о киберпреступности и Дополнительный протокол к ней (касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы), Конвенцию арабских государств 2010 года о борьбе с преступлениями, связанными с информационно-коммуникационными технологиями, и Соглашение Шанхайской организации сотрудничества 2009 года о сотрудничестве в области обеспечения международной информационной безопасности; *учитывая также* важное значение международных договоров в деле предотвращения кибервойны,

в полной мере сознавая то, что некоторые понятия, определения и стандарты политики в киберпространстве, особенно те, которые касаются кибервойны и международного мира и безопасности, не имеют единого толкования и до сих пор проясняются на национальном, региональном и международном уровнях, а также то, что по некоторым вопросам международный консенсус до сих пор не достигнут,

с удовлетворением отмечая прогресс в формировании общего понимания относительно приемлемого поведения государств в киберпространстве, достигнутый на международных форумах, в частности Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и в рамках других двусторонних, региональных и многосторонних инициатив,

признавая, что определенные принципы международного публичного права, включая, в частности, принципы, закрепленные в Уставе Организации Объединенных Наций, Женевских конвенциях 1949 года и Дополнительных протоколах к ним, Всеобщей декларации прав человека, Международном пакте о гражданских и политических правах и Конвенции о ликвидации всех форм дискриминации в отношении женщин, касаются киберпространства и распространяются на него, а также имеют важное значение для поддержания мира и международной стабильности и создания открытой, безопасной и мирной ИКТ-среды, доступной как для женщин, так и для мужчин,

считая, что киберпространство не ограничивается Интернетом, что последствия использования компьютерного оборудования, программного обеспечения, данных и информационных систем могут выходить за пределы сетей и информационно-технологической инфраструктуры и что оно считается одним из инструментов содействия экономическому росту, а также считая, что неравенство, включая гендерное неравенство, существует и в ИКТ-среде,

сознавая тот факт, что разные аспекты политики в киберпространстве, отличаясь друг от друга, все же неразрывно друг с другом связаны и могут оказывать воздействие на деятельность в киберпространстве, имеющую отношение к международному миру и безопасности, и наоборот,

считая, что скрытое и незаконное использование частными лицами, организациями и государствами компьютерных систем других стран для целей совершения нападений на третьи страны является поводом для серьезного беспокойства, поскольку оно может привести к возникновению международных конфликтов,

считая также, что киберпространство может быть использовано в качестве нового измерения конфликта, равно как и нового поля деятельности, где многие киберресурсы, если не большинство из них, могут применяться как в гражданских, так и в военных целях,

сознавая, что киберпространство не является изолированной средой и что осуществляемая в нем дестабилизирующая деятельность может иметь серьезные последствия для глобальной общественной жизни, привести к нарушению безопасности и возникновению конфликтов в других — традиционных — сферах или породить новый вид конфликта, и *будучи убеждена* в необходимости налаживания регионального и международного сотрудничества для противодействия угрозам, обусловленным злонамеренным использованием ИКТ,

будучи также убеждена в том, что государствам следует содействовать тому, чтобы частный сектор и гражданское общество играли надлежащую роль в повышении безопасности ИКТ и их использования, включая безопасность всей системы производства и сбыта ИКТ-продукции и услуг,

сознавая, что военные системы ИКТ, используемые для развертывания и применения сил, могут стать объектом враждебных действий в киберпространстве, в результате которых третьи стороны могут захватить такие системы и использовать их для несанкционированного, незаконного и разрушительного применения силы, а также *будучи обеспокоена* тем, что полностью автономные военные системы («роботы-убийцы») особенно подвержены риску такого несанкционированного использования, поскольку окончательные решения относительно выбора цели не требуют участия оператора, и *будучи особенно обеспокоена* тем, что взлом систем командования и управления ядерными силами может привести к несанкционированному применению и подрыву ядерных боеприпасов и вызвать беспрецедентную катастрофу,

отмечая, что использование ИКТ привело к изменению национальной и международной обстановки в плане безопасности и что технологии могут быть использованы в злонамеренных целях и для нарушения прав человека и гражданских прав; *отмечая также*, что за последние годы опасность применения ИКТ государствами и негосударственными субъектами для совершения преступлений, в том числе актов насилия в отношении женщин и девочек, и для осуществления деструктивной деятельности существенно возросла,

принимая во внимание негативные последствия, которые может иметь незаконное использование ИКТ для объектов инфраструктуры, национальной безопасности и экономического развития государств, и *сознавая*, что единственным надежным способом недопущения появления новых проблем и их урегулирования, обеспечения наиболее широкого использования достижений

ИКТ, предотвращения их потенциального негативного влияния, содействия их мирному и законному использованию и обеспечению того, чтобы научный прогресс был направлен на поддержание мира и содействие достижению благополучия и развития народов, является сотрудничество между государствами, которое будет также препятствовать превращению киберпространства в театр военных действий,

считая, что средства ведения кибервойны могут, в частности, включать направление на конкретный компьютер или компьютерную систему потоков данных, которое является средством и методом ведения войны и цель которого состоит в получении оперативной информации, пригодной к использованию для дестабилизации экономического, политического и социального положения или, согласно разумным предположениям, способной привести к гибели людей, причинению людям телесных повреждений, разрушениям и нанесению ущерба, в том числе в ходе вооруженных конфликтов,

сознавая, что меры кибероборонs и борьбы с киберпреступностью дополняют друг друга, и *отмечая* в этой связи, что Конвенция Совета Европы о киберпреступности (Будапештская конвенция), которая является единственным международным договором, касающимся преступлений, совершенных с использованием сети Интернет и других компьютерных сетей, открыта для присоединения, в том числе для третьих стран,

отмечая, что четкого понимания в отношении использования киберпространства в военных целях и последствий конкретных видов деятельности еще не сложилось; *отмечая также*, что многие виды деятельности в киберпространстве в зависимости от их природы, масштабов, потенциальных последствий и других обстоятельств могут привести к дестабилизации ситуации в плане безопасности,

будучи обеспокоена предложением специалистов по военному планированию сохранить средства ядерного сдерживания в качестве одного из инструментов противодействия связанной с кибернападениями смертельной угрозе,

признавая, что отсутствие стратегической связи между государствами, неспособность оперативно установить источник нападения и ограниченность понимания приоритетных задач союзников и противников могут привести к просчетам, недоразумениям и недопониманию в киберпространстве и что в связи с этим важно принять меры по укреплению доверия, направленные на повышение транспарентности и предсказуемости и развитие сотрудничества между государствами,

считая, что ввиду разработки и распространения государствами и негосударственными субъектами сложных вредоносных инструментов и средств усиливается угроза для международного мира и безопасности,

признавая неприемлемой практику использования государствами киберпространства в качестве средства применения экономических, ограничительных или дискриминационных мер по отношению к другому государству с целью ограничения его доступа к информации или услугам,

осуждая использование ИКТ в нарушение норм международного права и вопреки целям и принципам Устава Организации Объединенных Наций и признанным на международном уровне правилам сосуществования государств,

осуждая также использование ИКТ преступными и террористическими группами для обмена сообщениями, сбора информации, вербовки сторонников, организации, планирования и координации нападений, пропаганды своих идей и деятельности и сбора финансовых средств и памятуя о том, что при этом такие группы зачастую пользуются уязвимостью конкретных социальных групп, и осуждая далее использование киберпространства в целях дестабилизации и создания угрозы для международного мира и безопасности,

отмечая необходимость добиться заключения международной конвенции, касающейся Интернета, в целях недопущения использования Интернета террористами и террористическими организациями для незаконной деятельности, в том числе для сбора финансовых средств, привлечения сторонников и распространения идей, побуждающих людей к насилию и разжигающих ненависть,

напоминая о том, что совершение актов сексуального насилия во время войны или конфликта считается военным преступлением, и считая в этой связи, что распространение информации о таких актах посредством ИКТ для целей запугивания, устрашения и угнетения людей, общин и стран и принуждения их к подчинению, является военным преступлением в киберпространстве;

считая необходимым установить баланс между обеспечением безопасности в киберпространстве и уважением частной жизни, конфиденциальности и интеллектуальной собственности, а также приоритетных задач в области развития электронного правительства и электронной торговли,

считая также необходимым разработать практические меры укрепления доверия в области ИКТ на национальном, региональном и международном уровнях,

осуждая любое умышленное несанкционированное использование технологий, включая, в частности, осуществляемый при поддержке государства шпионаж,

1. *рекомендует* парламентам укреплять свой потенциал, с тем чтобы лучше понимать сложный характер национальной и международной безопасности в киберпространстве, и учитывать взаимосвязи между различными аспектами развития политики в киберпространстве;

2. *призывает* парламенты работать с другими органами государственной власти, гражданским обществом и частным сектором в целях формирования целостного представления о зависимости от киберпространства и рисках и угрозах на национальном уровне; призывает также правительства уменьшить обусловленные зависимостью от киберпространства негативные последствия, в особенности в сфере развития электронного правительства и национальной безопасности, и способствовать принятию национальных стратегий кибербезопасности;

3. *обращается с призывом* ко всем парламентам провести анализ своей нормативно-правовой базы, с тем чтобы определить оптимальные способы учета в ней потенциальных угроз, связанных с преступностью, терроризмом и войной, которые могут возникнуть ввиду меняющегося характера киберпространства;

4. *обращается также* с просьбой к парламентам принять законы о борьбе с применением сексуального насилия в отношении женщин и девочек во время войны и конфликта, которое является военным преступлением, а также о борьбе с распространением информации о таких актах с использованием ИКТ, которое является военным преступлением в киберпространстве;

5. *призывает* парламенты взять на себя обязательство тщательно проанализировать государственные финансы, с тем чтобы обеспечить выделение достаточных ресурсов на кибербезопасность;

6. *призывает также* парламенты использовать все имеющиеся в их распоряжении механизмы надзора для обеспечения строго контроля за деятельностью в киберпространстве и принять основанные на положениях их соответствующих конституций национальные законы, предусматривающие более суровые меры наказания за кибернападения, а также использование надлежащих защитных мер, механизмов управления и существующих структур для защиты свободы выражения мнений и обеспечения гражданам возможности беспрепятственно использовать средства ИКТ;

7. *рекомендует* парламентам государств, которые еще не сделали этого, обратиться к их соответствующим правительствам с просьбой однозначно заявить, что нормы международного права, включая право вооруженных конфликтов, должны распространяться в том числе на враждебные действия в киберпространстве, с тем чтобы обеспечить наличие ограничений на использование кибероперации как средства и метода ведения войны, но отмечает при этом, что вопрос о конкретном способе их применения по-прежнему обсуждается на международном уровне;

8. *призывает* парламенты работать с другими органами государственной власти и гражданским обществом над созданием комплексной стратегии кибербезопасности, которая предусматривала бы меры обеспечения кибероборонны, укрепления потенциала и борьбы с кибертерроризмом;

9. *предлагает* парламентам способствовать распространению информации и передового опыта в области кибербезопасности среди всех национальных заинтересованных сторон;

10. *обращается с призывом* ко всем парламентам обеспечить конструктивное участие всех заинтересованных сторон, включая частный сектор, академические круги, техническое сообщество, гражданское общество и женские организации и ассоциации, в усилиях по устранению киберугроз, связанных с использованием ИКТ;

11. *рекомендует* парламентам обладающих ядерным оружием государств призвать свои правительства отказаться от политики «запуск по предупреждению», вывести ядерные вооружения из состояния высокой боевой готовности и увеличить период времени, отводящийся на принятие решений относительно использования ядерного оружия, с тем чтобы не допустить несанкционированной активизации или использования систем ядерного оружия в результате кибернападения, в соответствии с теми целями, которые ставятся на переговорах по соглашениям о запрещении применения ядерного оружия и обеспечении его ликвидации;

12. *обращается с призывом* ко всем парламентам обеспечить, чтобы их национальные законы и регламенты не допускали преступного использования кибертехнологий в целях разжигания конфликтов между государствами и не позволяли нарушителям получать иммунитет и убежище;

13. *призывает* национальные парламенты содействовать налаживанию тесного сотрудничества и партнерских отношений между государственным и частным секторами в целях повышения эффективности стратегий кибербезопасности и кибероборонына национальном уровне;

14. *рекомендует* использовать стратегический информационный план, предполагающий участие сектора образования, организованных общин и граждан, в целях повышения уровня осведомленности населения о преимуществах и практической ценности активного использования киберпространства и потенциальных пагубных последствиях его ненадлежащего использования;

15. *рекомендует также* государствам при использовании ИКТ соблюдать нормы международного права и положения Устава Организации Объединенных Наций и рассмотреть на законодательном и исполнительном уровнях вопрос о принятии совместных мер, которые могли бы способствовать укреплению мира и международной стабильности и безопасности и обеспечить формирование общего понимания в отношении применения соответствующих норм международного права и вытекающих из них стандартов, правил и принципов, которые определяют ответственное поведение государств;

16. *призывает* парламенты способствовать тому, чтобы к Конвенции Совета Европы о киберпреступности (Будапештской конвенции) присоединилось как можно больше стран, поскольку она является одним из инструментов укрепления национального законодательства и повышения эффективности международного сотрудничества в борьбе с киберпреступностью;

17. *рекомендует* парламентам добиваться создания и внедрения на региональном и международном уровнях соответствующих регламентов и механизмов надзора, обеспечивающих использование киберпространства в соответствии со всеми нормами международного права, положениями Всеобщей декларации прав человека, Международного пакта о гражданских и политических правах и признанными на международном уровне правилами сосуществования, а также практических мер укрепления доверия в целях содействия повышению транспарентности и предсказуемости, укреплению сотрудничества и устранению недоразумений и понизить тем самым риск возникновения конфликта в связи с использованием киберпространства;

18. *предлагает* парламентам содействовать использованию инструментов оказания помощи и ресурсов для создания потенциала противодействия киберугрозам;

19. *настоятельно призывает* МПС совместно с соответствующими международными организациями поддерживать межпарламентское сотрудничество в целях достижения международных соглашений, гарантирующих более эффективное применение ИКТ странами и надлежащее и безопасное использование киберпространства, в целях обмена передовым опытом в отношении мер укрепления доверия, способствующих обеспечению мира и международной стабильности и безопасности посредством уменьшения риска нарушения без-

опасности, связанного с использованием ИКТ, а также в целях разработки совместных механизмов;

20. *призывает* парламенты играть позитивную роль в создании безопасной среды для содействия мирному использованию киберпространства и обеспечения того, чтобы при реализации принципов свободного выражения мнений и обмена информацией надлежащим образом учитывались вопросы общественной безопасности;

21. *призывает также* парламенты работать с их правительствами над созданием международных соглашений в целях предотвращения кибервойны, обеспечения применения правовых норм, касающихся международного мира и безопасности, в киберпространстве, а также установления глобальных стандартов и обеспечения того, чтобы принимаемые при кибернападениях национальные и международные меры реагирования отвечали положениям таких соглашений и таким стандартам;

22. *призывает далее* укреплять международное сотрудничество в целях оказания развивающимся странам технической помощи и помощи в создании потенциала в таких областях, как предупреждение, проведение расследований, осуществление судебного преследования и наказание правонарушителей, а также в целях повышения безопасности сетей для защиты от враждебных действий в киберпространстве;

23. *предлагает* МПС настоятельно призвать Организацию Объединенных Наций принять резолюцию, запрещающую осуществлять незаконный контроль за такими важнейшими объектами инфраструктуры, как водопроводные и электрические сети и больницы, и использовать их в качестве объектов для кибернападений;

24. *призывает* Организацию Объединенных Наций повысить кибербезопасность путем создания глобального реестра кибернападений;

25. *рекомендует* проанализировать и обновить правовые документы, договоры и соглашения о сотрудничестве, касающиеся в том числе киберпространства, кибербезопасности, технологий и телекоммуникаций;

26. *предлагает* МПС, руководствуясь положениями настоящей резолюции, предложить Генеральной Ассамблее Организации Объединенных Наций провести конференцию по предотвращению кибервойны в целях формирования единой позиции по соответствующим вопросам и разработки международной конвенции о предотвращении кибервойны.