Основные проблемы обеспечения
международной информационной безопасности

(Доклад Президента Национальной Ассоциации
международной информационной безопасности В.П.Шерстюка)

Шестая Всекитайская международная конференция по безопасности Интернета
4 сентября 2018 года, г. Пекин (КНР)

Уважаемые организаторы Форума!
Уважаемые участники Форума!
Дамы и господа!

1. Мы весьма признательны организаторам Форума за возможность принять участие в столь значимом мероприятии, посвященном обсуждению проблем обеспечения безопасности Интернет.

Россию и Китай в деле обеспечения международной информационной безопасности (МИБ) связывают по-настоящему дружеские, братские узы. Межправительственное соглашение между нашими странами о сотрудничестве в области обеспечения МИБ, заключенное в 2015 г., перевело совместную работу в этой сфере на принципиально новый уровень. Не кривя душой, могу сказать, что позиции наших стран по вопросам обеспечения МИБ и борьбы с информационной преступностью практически совпадают, а российские и китайские делегации тесно координируют свою работу на международных площадках и форумах. Особый импульс данному сотрудничеству придают регулярные встречи лидеров наших стран Владимира Путина и Си Цзиньпина. Уверены, что эта тенденция продолжится и в ходе их предстоящей встречи во Владивостоке. Поэтому для меня особо приятно изложить позицию России по вопросам организации международного сотрудничества в этой области именно на китайской земле.

Как известно, Окинавская декларация 2000 года о формировании глобального информационного общества ознаменовала, по существу, начало новой эры развития человечества. Это эра интенсивного развития глобальной информационной среды информационно-коммуникационных технологий (ИКТ), основу которой составляет глобальная информационная инфраструктура и, в частности, Интернет. С какой надеждой на позитивные изменения, на безграничные перспективы развития человечества мы вступали в цифровую эру!

Однако сейчас приходит осознание того факта, что новая ИКТ-среда, обозначившая появление нового пространства общественных отношений как в национальном, так и в международном масштабе, не в силах изменить природу человека, закономерности международных отношений. Она лишь создает новые возможности для проявления как добродетелей, так и пороков, свойственных духовному миру человека.

Как отметил Президент Российской Федерации В.В.Путин, выступая в июле 2018 года на Международном конгрессе по кибербезопасности, организованном Сбербанком России, «сегодня активное внедрение цифровых технологий во многом определяет прогрессивное развитие каждого государства, да и, пожалуй, мира в целом. Искусственный интеллект, робототехника, «интернет вещей» становятся основой роста экономики, а цифровые платформы, электронный документооборот кардинально повышают открытость и эффективность работы органов власти, компаний, бизнеса, социальных и образовательных учреждений».

В то же время ИКТ-среда является не только новым фактором устойчивого развития общества, но и фактором усиления социальной опасности действий, связанных с реализацией преступных намерений, осуществлением террористической деятельности, новым пространством международных споров и конфликтов.

Опасный характер новых проблем обеспечения международной безопасности уже неоднократно отмечался как политическими лидерами различных государств мира, так и Генеральной Ассамблеей ООН.

Так, по мнению Президента Российской Федерации, «особого внимания, конечно, требует сегодня безопасность глобального информационного пространства. Мы видим, что количество угроз и рисков здесь только растёт. Так, по данным Всемирного экономического форума, в 2017 году потери только от кибератак в мире составили порядка триллиона долларов США, и, по мнению экспертов, если не предпринимать эффективных, результативных мер ущерб будет ещё больше. Как и другие страны, Россия также сталкивается с подобными вызовами. К примеру, в первом квартале 2018года по сравнению с аналогичным периодом прошлого года число кибератак на российские ресурсы увеличилось на треть». Президент Российской Федерации высказал уверенность в том, что нейтрализация этих угроз «и в целом обеспечение кибербезопасности – это государственная задача, и в её решении необходимо объединять усилия правоохранительных органов, деловых кругов, общественных организаций и самих граждан».

Политики и специалисты в Российской Федерации едины в том мнении, что обеспечение устойчивого функционирования и безопасного использования ИКТ-среды человеком, обществом и государством возможно лишь на основе международного сотрудничества в области противодействия существующим и будущим угрозам.

Основной площадкой такого сотрудничества должна быть ООН, объединяющая практически все существующие государства мира и способная создать условия для поддержания международного мира и безопасности. Важную роль в содействии этому процессу играют такие региональные объединения как ШОС, БРИКС, ОДКБ и иные.

На наш взгляд, это является единственным средством снизить опасность тревожных тенденций, сложившихся в ИКТ-среде в последние годы и свидетельствующих о существовании весьма опасных угроз миру.

2. К числу таких угроз, по нашему мнению, относится, прежде всего, стремительное превращение **ИКТ-среды в пространство межгосударственного противоборства**, осуществляемого посредством враждебного использования информационно-коммуникационных технологий. Мы все понимаем, что в современных условиях противодействие данной угрозе является одним из важных аспектов предотвращения возникновения международных конфликтов.

Количество способов возможного использования информационных технологий для «силового» воздействия на противостоящую сторону постоянно возрастает. Еще недавно к числу таких способов эксперты относили, прежде всего, использование «вредоносного» программного и технического обеспечения для нарушения деятельности критически важных объектов информационной инфраструктуры, других объектов, оказывающих существенное влияние на жизнедеятельность общества, противоправного получения информации ограниченного доступа.

В настоящее время количество направлений использования информационных технологий для достижения военно-политических целей существенно расширилось. Все большее внимание специалистов привлекает исследование путей применения систем искусственного интеллекта в системах вооружения и военной технике. Активно исследуются способы и методы создания и боевого применения автономных боевых роботов на суше, на море, в воздухе и информационной инфраструктуре. Активно развиваются методы применения информационных технологий для повышения боевой эффективности средств ведения вооружённой борьбы на всех стадиях развития конфликта. Одновременно существенно расширяется количество объектов инфраструктуры государства, поражение которых способно привести к возникновению конфликта. Теперь к таким объектам часто относят не только объекты военной инфраструктуры государства, но и объекты экономического и социального характера.

По мнению экспертов Организации по безопасности и сотрудничеству в Европе, около 50 государств мира активно реализуют программы создания боевых вредоносных программ. В число этих стран входят 10 государств, обладающих самыми внушительными военными бюджетами. Особо следует подчеркнуть беспрецедентный рост военного бюджета США на 2019 г., достигший астрономической суммы 716 млрд. долл.

В этом контексте мы учитываем и неоднократные сообщения в СМИ о значительных объемах бюджетных инвестиций правительства США в исследование технологий создания вредоносных программ и методов их использования для оказания враждебного силового давления на противостоящие государства.

Как отметила Группа правительственных экспертов ООН по достижениям сфере информатизации и телекоммуникаций в контексте международной безопасности в докладе 2015 года, «ряд государств занимаются наращиванием потенциала в сфере ИКТ для военных целей. Использование ИКТ в будущих конфликтах между государствами становится более вероятным».

Как представляется, развитие средств ведения «силовых» действий в среде информационных технологий повышает риск возникновения конфликтов, способных нарушить международный мир и безопасность.

Данный тезис подтверждается рядом беспрецедентных решений, принятых в США в последнее время. В первую очередь, эта Стратегия национальной безопасности США (декабрь 2017 г.). Среди основных угроз в документе названы Китай и Россия, которые «стремятся бросить вызов американскому влиянию, ценностям и богатству», Иран и КНДР, которые «спонсируют террор и угрожают союзникам Америки».

Кроме того, 23 марта 2018 г. президент Трамп подписал закон «О доступе к персональным данным в других странах» (т.н. CLOUDAct). Его основное предназначение – обеспечить в ускоренном порядке правоохранительным органам и спецслужбам трансграничный доступ к персональным данным пользователей, подозреваемых в совершении преступлений, вне зависимости от места их хранения.

Данная инициатива Вашингтона – очередная попытка закрепить англосаксонское превосходство в цифровом пространстве и получить в нем полную «свободу рук». Легитимизировать любые силовые действия американо-британского альянса в этой сфере призван его «исключительный» статус. Тем самым декларируется принцип: «что позволено странам-основательницам Интернета – США и Великобритании – то не позволено другим».

3. Второй опасной угрозой международной информационной безопасности является **использования глобальной медиасферы** и, в частности, социальных сетей, **для оправдания силовых подходов к разрешению межгосударственных споров и вмешательства во внутренние дела суверенных государств.**

Так это было в 1999 году в Югославии. Так это было в 2003 году в Ираке. Так это было в 2011 году в Ливии. Так это происходит сейчас в Сирии.

В последнее время проблема злоупотребления некоторыми государствами свободой массовой информации для пропаганды идеологического превосходства, особой исторической миссии становится все более серьезной. В средствах массовой информации достоверная информация, распространяемая этими государствами, активно перемешивается с ложной информацией («фэйками»).

Как это видно на примере мифического российского следа в так называемом «деле Скрипалей», заинтересованные государства создают

цепочки фэйковых новостей, образуя своеобразный «фэйк-чэйн». В этом «фэйк-чэйне» одни ложные новости подкрепляются другими ложными новостями. Создание «фэйк-чэйнов» имеет целью активное манипулирование международным и национальным общественными мнениями, что создает реальную угрозу международному миру и безопасности.

С этой точки зрения представляется весьма показательной попытка законодательной и исполнительной власти США преодолеть раскол американского общества, образовавшийся вследствие драматической борьбы кандидатов от демократической и республиканской партий за пост президента США, посредством формирования из Российской Федерации образа врага, нагнетания в своей стране и в мире антироссийской истерии. Отсутствие каких бы то ни было фактов не смущает американских политиков и даже придает им дополнительную уверенность в своей правоте.

Чтобы ощутить уровень деградации российско-американских отношений достаточно привести цитату из выступления одного из соавторов нового «драконовского» законопроекта об антироссийских санкциях - сенатора Линдси Грэма, - который, если верить Агентству Рейтер, сказал: «…Наша цель — изменить статус-кво и наложить сокрушительные санкции и принимать другие меры против России…».

Что здесь комментировать? Лишь отмечу, что именно для того, чтобы не допустить подобного развития событий и не создавать у таких американских политиков иллюзий возможности реализации этой откровенной, но не очень оригинальной мысли, Россия вынуждена активно заниматься совершенствованием средств ведения вооруженной борьбы, о которых говорил Президент Российской Федерации Владимир Путин в Послании Федеральному Собранию 1 марта 2018 года и укреплять международное сотрудничество со всеми здоровыми силами мира.

4. Завершая тему использования ИКТ для достижения военно-политических целей, хотел бы обратить Ваше внимание на то, что, по мнению российских экспертов, киберпространство не является каким-то особым аспектом стратегической стабильности. Оно тесно интегрировано с другими аспектами системы поддержания стратегической стабильности. В этой связи, представляется, что идеи о выделении киберстабильности в самостоятельное измерение стратегической стабильности, являются несколько надуманными. Поддержание стратегической стабильности - это комплексная задача, в выполнении которой учитываются все факторы и используются разнообразные средства.

Поддержание стратегической стабильности является важным направлением обеспечения международного мира и безопасности. Выполнение данной задачи должно базироваться на применении принципов и норм международного права для регулирования международных отношений в области использования ИКТ.

В докладах Группы правительственных экспертов 2013 и 2015 годов отмечалось, что международное право применимо к ИКТ-среде, но в

реализации данного вывода в международной практике имеются определённые трудности.

Эти трудности, на наш взгляд, обусловлены, прежде всего, особенностями ИКТ-среды, отличающими ее от традиционных сред международных отношений - земли, воздуха, водных пространств, недр и космоса.

Данные отличия заключаются в следующем.

Прежде всего, в искусственном характере ИКТ-среды, существование которой целиком зависит от активности человека, частных организаций и государственных структур. Эти субъекты совместно создают условия для функционирования и развития ИКТ-среды, для ее использования во всех сферах общественной жизни. Одним из следствий искусственности ИКТ-среды является отсутствие в ней государственных границ. Это обстоятельство создает определенные трудности в применении международного права для регулирования международных отношений по поводу использования ИКТ. Как отметил Генеральный секретарь ООН в предисловии к Докладу Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 года «обеспечение стабильности и безопасности в киберпространстве может быть достигнуто лишь по линии международного сотрудничества, причем основой такого сотрудничества должны являться нормы международного права и принципы, провозглашенные в Уставе Организации Объединенных Наций».

Неопределенность пространственных пределов государственного суверенитета в ИКТ-среде существенно затрудняет практическое применение принципа суверенного равенства государств. Одновременно это препятствует объективному контролю выполнения государствами в ИКТ-среде международных обязательств.

Здесь речь не столько о границах в традиционном смысле слова, сколько о зонах ответственности государств в ИКТ-среде за выполнение международных договоров, соблюдение международных обычаев и общих принципов права, признанных цивилизованными народами.

Важным отличием ИКТ-среды от традиционных сфер международных отношений является, также виртуальность процессов передачи, обработки и хранения информации, осуществляемых с использованием средств вычислительной техники и коммуникационных устройств и сетей. Виртуальность данных процессов делает невозможным визуальный контроль заинтересованных субъектов международного права за возникновением опасных событий в ИКТ-среде, сбор на основе презумпции доверия к правоохранительным органам государства, считающего себя жертвой, достоверной информации об инцидентах, способных привести к нарушению международного мира и безопасности. В свою очередь, отсутствие такой информации становится существенным препятствием на пути реализации

требований ст.2 п.3 Устава ООН, касающихся мирного разрешения международных споров.

Наконец, в качестве особенности ИКТ-среды необходимо отметить двойственный характер ИКТ. С одной стороны, ИКТ, которые, по определению, представляют собой совокупность методов и средств обработки и передачи информации, не являются оружием. С другой стороны, как это признается специалистами, враждебное использование ИКТ способно при определенных условиях превратить устройства и механизмы невоенного назначения в оружие и причинить значительные страдания как гражданам отдельных государств, так и человечеству в целом.

По существу, мы пытаемся применить международное право для регулирования отношений в принципиально новой среде существования человечества. Отсутствие механизмов применения международного права для регулирования международных отношений в ИКТ-среде, само по себе создает дополнительную угрозу сохранению стратегической стабильности.

5. На наш взгляд, единственным выходом из сложившегося положения, является активизация международного сотрудничества, направленного на адаптацию, приспособление международного права к ИКТ-среде.

В этой связи Российская Федерация в 2003 году выступила инициатором образования при Генеральном Секретаре ООН Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Практическая полезность этих инициатив сейчас осознается практически всеми государствами мира.

Многолетние усилия экспертов были отмечены в 2015 году консенсусным принятием доклада Генеральному Секретарю ООН, который по многим параметрам можно назвать историческим.

Стороны договорились о целом спектре прорывных идей:

во-первых, о приоритетном предотвращении использования ИКТ в военно-политических целях;

во-вторых, об отказе от обвинений государств в кибератаках без серьезных доказательств, как это сейчас нередко происходит;

в-третьих, об использовании ИКТ исключительно в мирных целях;

в-четвертых, о запрете использования вредоносных закладок в ИКТ-продукты, способных превратить устройства и механизмы различного назначения в оружие;

в-пятых, о суверенном праве государств распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности.

К глубочайшему сожалению Группа правительственных экспертов, работавшая в 2016-2017 гг, не смогла поддержать набранный темп и достичь консенсуса по проекту итогового доклада Генеральному Секретарю ООН.

Это печальное обстоятельство, которое, тем не менее, не должно давать повода для пересмотра роли ООН в обеспечении международной информационной безопасности и перевода обсуждения данной проблематики на региональный уровень либо на двухсторонний формат.

Сейчас, когда международная обстановка существенно обострилась, эксперты многих государств мира полагают, что продолжение работы в направлении принятия норм, правил и принципов ответственного поведения государств в среде информационных технологий будет способствовать снижению опасности возникновения конфликтов, связанных с враждебным и злонамеренным использованием информационных технологий государствами для разрешения межгосударственных противоречий.

Российская Федерация и другие государства-члены Шанхайской Организации Сотрудничества предполагают на предстоящей сессии Генеральной Ассамблеи ООН выступить с новым проектом резолюции. Этот проект будет содержать новую редакцию норм и правил, которые в большей степени отражают реалии современных международных отношений в ИКТ-среде.

Основной упор в этом проекте сделан на предложение о закреплении норм, правил и принципов ответственного проведения государств в следующих областях:

соблюдение прав и свобод человека;

обеспечение стабильности функционирования и безопасности использования глобальной информационной инфраструктуры, посредством интернационализации управления Интернетом, укрепления безопасности критической информационной инфраструктуры, запрета злонамеренного и враждебного использования ИКТ;

укрепление гарантий невмешательства во внутренние дела суверенных государств, в процессы их политического и социального развития;

обеспечение безопасности использования продуктов ИКТ;

использование мирных способов разрешения споров в ИКТ-среде;

реализация мер доверия.

Как показало исследование, проведенное в Институте проблем информационной безопасности МГУ в 2016 г., имплементация в правоприменительную практику норм, правил и принципов ответственного поведения государств в ИКТ-среде, рекомендованных к рассмотрению государствами в докладе Группы правительственных экспертов 2015 года, может потребовать приложения дополнительных усилий.

По существу, к такому же выводу пришла международная группа экспертов, завершившая аналогичное исследование в 2017 году. По результатам этих исследований в 2018 году подготовлен и издан при поддержке департамента разоружения ООН Сборник комментариев к нормам, принципам и правилам ответственного поведения государств в ИКТ-среде. Все это, как нам представляется, создает условия для следующего

шага - выявления проблем практического применения норм «мягкого права» в этой области и подготовки рекомендаций по их решению.

В 2018 году Международным консорциумом информационной безопасности, созданным по инициативе МГУ имени М.В.Ломоносова, начат международный проект, направленный на исследование вопросов реализуемости норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Проект осуществляется международной группой экспертов, включающей представителей организаций Российской Федерации, США, Эстонии, Южной Кореи и Швейцарии. Предварительные результаты этой работы планируется представить на рассмотрение Международного консорциума в декабре 2018 г.

6. Все более проблемной для международного сообщества предстает и тематика противодействия использованию ИКТ в преступных целях, которая по своему масштабу и всеохватности давно превратилась в глобальную угрозу, от которой страдают как развивающиеся, так и развитые страны.

Неудивительно, что главной темой последней сессии Комиссии ООН по предупреждению преступности и уголовному правосудию (Вена, 14-18 мая с.г.) впервые за всю ее историю стала борьба с киберпреступностью. Тогда, в ходе своего выступления, Генеральный секретарь ООН А.Гутерреш оценил потери мировой экономики от этой угрозы в 1.5 трлн. долл. США в год. По оценкам профильных экспертов, ожидаемый ущерб мировой экономике от компьютерной преступности в 2021 году составит 6 трлн. долл. США в год, что будет сопоставимо с объемом всей прибыли от использования ИКТ.

В настоящее время у мирового сообщества, к сожалению, нет единого подхода к решению этой задачи. Ситуация осложняется отсутствием полноценной международно-правовой базы сотрудничества и даже единой терминологической базы.

На региональном уровне соответствующие документы разработаны и приняты в рамках ряда организаций. В качестве примеров можно привести Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (от 1 июня 2001 г.), Конвенцию Совета Европы по киберпреступности 2001 г. (23 ноября 2001 г.; т.н. Будапештская конвенция), Соглашение между правительствами государств-членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности (от 16 июня 2009 г.), подписанную государствами-членами Лиги арабских государств Конвенцию по борьбе с правонарушениями в области информационных технологий (от 21 декабря 2010 г.), Конвенцию Африканского союза о кибербезопасности и защите персональных данных (от 27 июня 2014 г.).

Результатом такой «регионализации» стала фрагментация позиций на международном уровне, препятствующая выработке общего понимания ключевых аспектов противодействия незаконным действиям в информационной сфере. Мы твердо убеждены, что проблема столь глобального масштаба требует запуска политической дискуссии на соответствующем уровне – в ООН.

По этой причине Российская Федерация и другие государства Шанхайской организации сотрудничества планируют внести на предстоящей 73-й сессии Генассамблеи ООН проект резолюции «Противодействие использованию ИКТ в преступных целях». Его суть крайне проста и во многом носит технический характер. Постановляющая часть содержит три пункта.

В первом пункте Генассамблея просит все государства-члены информировать Генерального секретаря о своей точке зрения и об оценках по проблемам в сфере противодействия использованию ИКТ в преступных целях. Во втором – просит Генерального секретаря ООН представить доклад Генеральной ассамблее на ее семьдесят четвёртой сессии. В третьем пункте – постановляет включить в предварительную повестку дня своей семьдесят четвёртой сессии пункт, озаглавленный «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

Надеемся, что данный проект резолюции придаст импульс международной дискуссии по борьбе с информационной преступностью, будет способствовать формированию транспарентного переговорного процесса в этой сфере с учетом равной географической представленности в рамках Генассамблеи ООН. Таким образом, все страны смогут высказаться по этому вопросу и будут созданы условия для достижения глобального компромисса.

На наш взгляд, одним из решений этой проблемы может стать подготовленная под эгидой ООН Конвенция по противодействию преступлениям в сфере использования ИКТ, которая учитывала бы реалии всех без исключения стран и основывалась бы на принципах суверенного равенства сторон и невмешательстве во внутренние дела государств. Идея разработки подобного документа впервые была отражена в итоговой декларации 12-го Конгресса ООН по предупреждению преступности и уголовному правосудию (Бразилия, апрель 2010 г.). В ее основу могут лечь положения как действующих региональных инструментариев, так и, например, российского проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности, который 28 декабря 2017 г. получил статус официального документа ООН и отвечает современным требованиям.

7. Четвертой опасной угрозой международной информационной безопасности является **кибертерроризм**, который постепенно сращивается с компьютерной преступностью и начинает серьезно угрожать безопасности использования критической информационной инфраструктуры.

В докладе Группы правительственных экспертов ООН отмечалось, что «угрозы частным лицам, компаниям, национальной инфраструктуре и государственным органам приобретают все более острый характер, и соответствующие инциденты имеют все более тяжелые последствия». Группа пришла к выводу, что «к числу наиболее пагубных нападений с использованием информационных и коммуникационных технологий относятся нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств. Опасность вредоносных нападений с использованием информационных и коммуникационных технологий на критически важную инфраструктуру является реальной и серьезной».

С этой точки зрения представляется важным совершенствование механизмов реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры, безопасности использования ИКТ для реализации прав и свобод человека, осуществления экономической, социальной, политической, культурной и иных видов деятельности.

С учетом многоаспектности проблематики международной информационной безопасности, усилия государственных органов, предпринимаемые в области противодействия кибертерроризму, необходимо согласовывать с деятельностью заинтересованных негосударственных организаций.

Заслуживают серьезного внимания инициативы в области обеспечения безопасности использования ИКТ-среды, выдвигаемые организациями бизнеса. Так, на Одиннадцатом Форуме в г. Гармиш-Партенкирхен (Германия, 2017 год) российская компания «Норильский Никель» выступила с инициативой разработки Хартии информационной безопасности критических объектов промышленности. «Норильский никель» является глобальной и системообразующей компанией Российской Федерации. Она вносит значительный вклад в социально-экономическое развитие регионов России. За прошедший год представителями компании проделана большая работа по подготовке проекта Хартии, организации его обсуждения с заинтересованными лицами и учету поступающих замечаний. Известна аналогичная инициатива компании Майкрософт и Сбербанка России. Представляется важным определить механизм использования потенциала организаций частного бизнеса, негосударственных организаций, граждан для консолидации усилий всего общества для противодействия угрозам устойчивого функционирования глобальной информационной инфраструктуры и безопасного использования ИКТ.

8. В целях содействия развитию частно-государственного партнерства в области безопасности использования ИКТ в Российской Федерации в апреле 2018 года образована Национальная Ассоциация международной информационной безопасности.

Предполагается, что Ассоциация будет в упреждающем режиме проводить проработку проблемных вопросов обеспечения международной информационной безопасности в интересах формирования переговорных позиций государственных органов.

В рамках выполнения уставных задач Ассоциация готова к взаимодействию с заинтересованными организациями Китайской Народной Республики, других государств в интересах укрепления мира и безопасности.

Спасибо за внимание!