Секция «Международная безопасность: новые вызовы и угрозы»

Сотрудничество России и Китая в борьбе с кибертерроризмом

Научный руководитель – Васецова Елена Сергеевна

Чжэн И
Аспирант
Московский государственный университет имени М.В.Ломоносова, Институт стран Азии и Африки, Кафедра политологии стран Востока, Москва, Россия
E-mail: zdiamor@gmail.com

Прежде всего, отметим, что РФ и КНР являются мишенями для международных террористических группировок исламистского толка, которые стремятся дестабилизировать ситуацию внутри страны, осложнить развитие региона в целом. В Китае, на территории Синьцзян-Уйгурского автономного округа (СУАР), проживают уйгуры. В данном районе активно действует вооруженная исламистская суннитская группировка, признанная террористической рядом стран, это «Исламское движение Восточного Туркестана». Организация поставила цель создать независимое исламское государство на землях СУАР и Южного Казахстана. Также серьезную опасность представляет террористическое квазигосударство «Исламское государство», с которым б**о**рется РФ. В свою очередь, КНР не принимает активного участия в боев**ы**х действиях, направленных против ИГ. В то же время, Пекин тесно координирует свою позицию по сирийскому кризису, в том числе, и по противодействию радикальным исламистским группировкам, с Москвой. Китай поставляет в Сирию нелетальное военное имущество, прежде всего, военную технику и обмундирование. Таким образом, и Россия, и Китай воспринимаются ИГ как враги, против которых применяются механизмы информационного противодействия.

ИГ отличается налаженной пропагандистской системой, а его студии «Аль-Фарукан» и «Аль-Хайят» создают продукцию высокого качества. В 2015 г. ИГ распространило обращение на уйгурском языке с призывами к мусульманам Китая отправиться на войну в Сирии.

Очевидно, что призывы нашли благодатную п**о**чву, так как в рядах ИГ активно воюют граждане КНР. По утверждению сирийского посла в Пекине в феврале 2017 г., около 5 тысяч боевиков-граждан КНР (преимущественно уйгуры) проникли в Сирию через турецкую границу для участия в войне на стороне ИГ или другой радикальной исламистской суннитской группировки, признанной террористической многими государствами, - «Джебхат ан-Нусре». В 2015 г. выходцы из Китая были на первом месте по количеству задержанных иностранных боевиков на турецкой границе (324 из 913 человек) .

ИГ активно вербует россиян и русскоязычное население центральноазиатских республик вступить в свои ряды. По данным ФСБ РФ, на осень 2015 г. свыше 5 тыс. граждан из РФ и государств Центральной Азии воевали на стороне ИГ, из них 2400 составляли граждане РФ. По словам представителя ведомства, вербовка граждан из разных стран, в том числе входящих в ШОС, представляет собой одну из наибольших опасностей со стороны ИГ.

Помимо активной пропагандистской работы во всемирной паутине, ИГ выступает с угрозами в адрес властей РФ и КНР. Так, в 2017 г. члены ИГ выложили видеоролик собственного производства, в котором обратились к властям КНР с угрозой пролить реки крови, и в котором председатель КНР Си Цзиньпин превратился в поток пламени. Боевики ИГ несколько раз брали на себя ответственность за крушение самолета А321 российской авиакомпании «Когалымавиа» над Синаем, произошедшее 31 октября 2015 г.

Также ИГ обнародовало видеообращение с угрозой совершения кровавых террористических актов на территории России. В данном обращении содержатся угрозы взять Кремль и «вернуть» Кавказ.

Необходимость дать отпор кибертеррористам предопределила совершенствование антитеррористического законодательства РФ и КНР. В российское законодательство постоянно вносятся поправки, направленные, в том числе, и на борьбу с кибертерроризмом. Антитеррористический закон КНР, принятый в 2015 г., представляет собой детально разработанный документ, содержащий 10 глав и предусматривающий различные меры по противодействию терроризму во всех его проявлениях. В соответствии со статьей 19 главы 3 Антитеррористического закона КНР, Интернет-провайдеры и мобильные операторы обязаны оказывать техническую поддержку органам государственной безопасности для предотвращения и расследования террористической деятельности. Их обязывают участвовать в разработке и реализации упреждающих мер по укреплению информационной безопасности, включая отслеживание информации, распространяемой террористами. По решению органов государственной безопасности, информация должна быть удалена. Для предотвращения случаев распространения во всемирной паутине террористических идей власти Китая проводят политику ограничения свободы слова в Интернете. Также иностранные кампании, работающие на территории двух государств, обязаны передавать государственным органам КНР конфиденциальную информацию. Данная практика широко критикуется различными международными неправительственными правозащитными организациями за нарушение прав человека и создание условий для шпионажа за теми или иными лицами и организациями.

Автор статьи считает, что принимаемые властями КНР и России меры в целом обоснованы и своевременны в свете повсеместного распространения идеологии крайнего исламизма, активизации деятельности террористических группировок на Ближнем Востоке, в сопредельных с КНР и РФ государствах, и общего усиления террористической угрозы. Законодательство КНР и РФ предоставляет большие возможности для развития как двустороннего, так и международного сотрудничества в сфере борьбы с кибертерроризмом.

Двустороннее межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (МИБ) ознаменовало новый уровень российско-китайского взаимодействия в сфере МИБ. Соглашение, отражающее стратегическую близость подходов России и Китая по МИБ, имеет прикладной характер и ориентировано на совместное решение задач, связанных с обеспечением национальной и международной информационной безопасности. Соглашение предусматривает создание правовых рамок для диалога заинтересованных ведомств России и Китая по всему спектру вопросов МИБ.

Прежде всего, документ подчеркивает важность совместного реагирования на наиболее острые угрозы в указанной области, включая противодействие использованию информационно-коммуникационных технологий (ИКТ) в нарушение общепризнанных принципов международного права, в том числе для вмешательства во внутренние дела государств, подрыва суверенитета, политической и экономической стабильности, разжигания межнациональной и межконфессиональной вражды, террористических целях.

Принятое Соглашение предполагает реализацию мер по обмену информацией о существующих и потенциальных рисках и угрозах в сфере МИБ, взаимодействие по совершенствованию международно-правовой базы сотрудничества в данной области и др..

На международной арене РФ и КНР совместно с Таджикистаном и Узбекистаном выступают инициаторами разработки и принятия международного кодекса по обеспечению информации в сфере безопасности. Данный документ является уникальным сводом

продуманных предложений по введению и совершенствованию международных норм в области информационной безопасности. Цель кодекса заключается в определении прав и обязанностей государств в информационном пространстве, правил конструктивного и ответственного поведения, а также условий их сотрудничества с учетом общих рисков и угроз в информационном пространстве для того, чтобы информационные и коммуникационные технологии были использованы исключительно на благо социального и экономического развития и населения государств в соответствии с задачей по поддержанию международной стабильности и безопасности.

Сближение России и Китая на почве развития сотрудничества в сфере кибербезопасности воспринимается крайне негативно властями США. В 2015 г. Пентагон обнародовал новую версию стратегии вооруженного ответа на киберугрозы. Как и в предыдущей версии, стратегия приравняла кибератаки к военным действиям и утвердила право реагировать на них как на акт агрессии. Однако, в новой версии предусмотрены не только оборонительные, но и наступательные меры противодействия кибератакам. Документ прямо указывает на главных потенциальных противников США в киберпространстве. Прежде всего это Россия и Китай. В стратегии сказано, что китайцы нацелены на промышленный кибершпионаж и подрыв конкурентоспособности США, а вот «намерения русских иногда сложно понять» [16]. В июне 2017 г. в конгрессе США обсуждалось предложение изменить киберстратегию стран НАТО, чтобы защититься от потенциальных угроз со стороны России. На фоне происходящих событий, китайско-американский диалог по противодействию киберугрозам приостановлен.

По мнению автора статьи, усиливающееся сотрудничество России и Китая в сфере борьбы с кибертерроризмом не направлено против третьих сторон и не представляет опасности для информационного пространства США. Что действительно вызывает резкое неприятие США и их союзников, так это становление многополярного мира, центрами силы которого являются Россия и Китай. Именно этим объясняется желание представить РФ и КНР в неприглядном виде, подрывая их авторитет на международной арене.

Двустороннее сотрудничество сторон в сфере борьбы с кибертерроризмом также развивается на платформе Шанхайской организации сотрудничества (ШОС). Региональный антитеррористический центр Шанхайской организации сотрудничества (РАТС ШОС) создал механизм сотрудничества по борьбе с террористической деятельностью в сети Интернет. Разработаны законодательные и нормативные акты, наращивается взаимодействие для противодействия деятельности террористических сил в информационном пространстве, развивается сотрудничество государств-членов ШОС в борьбе с кибертерроризмом.

Таким образом, в настоящий момент между Россией и Китаем накоплен значительный опыт противодействия кибертерроризму, результатом которого является значительная нормативно-правовая база, охватывающая различные аспекты борьбы с данной угрозой. Россия и Китай развивают сотрудничество в области борьбы с кибертерроризмом в ШОС, что расширяет фронт борьбы с терроризмом в целом. Стороны предлагают ряд инициатив по противодействию кибертерроризму на международной арене. Сотрудничество в сфере борьбы с кибертерроризмом планируется осуществлять по следующим направлениям: разработка и проведение совместных мер по борьбе с кибертерроризмом, совершенствование нормативно-правовой базы в данной сфере; регулярное проведение мониторинга и общего реагирования на киберугрозы; противодействие распространению материалов соответствующей направленности; совершенствование законодательной базы государств-членов ШОС по борьбе с кибертерроризмом. В целом, относительно сотрудничества в сфере борьбы с терроризмом в информационном пространстве между Россией и Китаем наблюдается полное единодушие. Выскажем предположение, что дальнейшее развитие сотрудничества в указанном направлении может быть затруднено прежде всего

из-за нежелания США и их союзников терять лидирующие позиции на мировой арене.