УДК 327.004

ПЕРСПЕКТИВЫ РАЗВИТИЯ СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В РАМКАХ ШОС

Cooperation Prospects for Cyber Terrorism Counteracting within SCO

Александра Камиловна Гайнетдинова
Студент Русско-китайского факультета
Байкальский государственный университет, г. Иркутск, Россия

Елена Юрьевна Сизых
Аспирант кафедры мировой экономики и экономической безопасности
Байкальский государственный университет, г. Иркутск, Россия

A.K. Gaynetdinova
Student, Russian-Chinese Department
Baikal State University, Irkutsk, Russia

E.Y. Sizykh
Postgraduate student, Department of World Economy and Economic Security
Baikal State University, Irkutsk, Russia

Аннотация. В статье дается определение понятию кибертерроризм, выделяются его виды и характерные особенности; обосновывается целесообразность международного сотрудничества в сфере противодействия кибертерроризму. Кроме того, в работе проанализированы, как существующие механизмы внутринациональной борьбы с кибертерроризмом на примере России и Китая, так и формы многостороннего сотрудничества в рамках деятельности ШОС, в заключении определены дальнейшие перспективы сотрудничества по данному вопросу.

Ключевые слова. Кибертерроризм, информационная безопасность, информационный терроризм, ШОС, Региональная Антитеррористическая Структура ШОС.

Abstract. The article defines the concept of cyber—terrorism, identifies its main types and characteristics. Then the paper proves the advisability of international cooperation in cyber—terrorism counteracting, analyzes both existing mechanisms of national measures (on the example of Russia and China) and main forms of multilateral cooperation within the framework of SCO. In conclusion, the future prospects on the matter are revealed.

Keywords. Cyber terrorism, information security, information terrorism, SCO, Regional Anti—Terrorist Structure of the SCO.

За последние несколько десятков лет обозначилась четкая тенденция проникновения информационных технологий во все сферы жизни общества. Помимо очевидных преимуществ технологического прогресса, следует отметить все больший интерес к использованию информационных технологий в деструктивных, преступных и антисоциальных целях, к числу которых следует отнести кибертерроризм.

Специфика кибертеррористической деятельности определяет целесообразность консолидации усилий государств в вопросе разработки практических мероприятий по борьбе с данным социально опасным явлением. Значительные успехи в этой сфере были достигнуты в рамках Шанхайской организации сотрудничества (ШОС). Целью настоящего исследования является определение существующих механизмов противодействия кибертерроризму в рамках ШОС, а также выявление дальнейших перспектив сотрудничества государств-членов в сфере информационной безопасности.

Термин кибертерроризм ввел в середине 1980-х гг. сотрудник американского Института безопасности и разведки Б. Коллин, и обозначал он террористические действия в виртуальном пространстве. В российском законодательстве понятие кибертерроризма не закреплено, тем не менее, в юридической науке существует множество определений кибертерроризма и родственных ему понятий.

Многообразие трактовок информационного терроризма связано с тем, что порой очень сложно идентифицировать кибертерроризм в проявлениях информационной войны, информационного криминала и прочих преступлениях, совершенных в киберпространстве [1, с. 132]. Главное отличие кибертеррориста от киберпреступника, действующего в хулиганских или корыстных целях, состоит в том, что совершаемое им деяние должно иметь опасные последствия, быть идеологически мотивированным, а также вызывать значительный общественный резонанс (более подробно характеристики кибертерроризма представлены на рис. 1).

Таким образом, в данной работе под кибертерроризмом понимается комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающая опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта [2].

Исходя из этого, можно выделить два вида кибертерроризма [3, с. 155]:

— непосредственное совершение террористических действий с помощью компьютеров и компьютерных сетей (в т.ч. управление террористическими актами через сеть Интернет, запуск вирусных программ, нарушение работы стратегически важных объектов и т.д.);

— использование киберпространства террористическими группами в организационно-коммуникационных целях и с целью шантажа, но не для непосредственного совершения терактов (в т.ч. открытие террористических сайтов, вербовка и изучение новых кандидатов, ведение пропаганды, неподконтрольной государственным надзорным органам).

Следует отметить, что компьютерный терроризм — не является проблемой одного государства, он выходит далеко за его территории, это происходит по ряду причин:

Во-первых, многие телекоммуникационные сети, главным из которых является Интернет, являются едиными для жителей всех стран;

Во-вторых, поимка кибертеррориста составляет большую проблему, в том числе и потому, что законодательное ограничение на вмешательство во внутренние дела другого государства, защита граждан, пребывающих на его территории и др. являются значительным препятствием при осуществлении розыска киберпреступника.

В-третьих, в сравнении с ядерным или биологическим терроризмом, для организации террористической деятельности в киберпространстве требуются относительно небольшие финансовые затраты, чего нельзя сказать о мерах по противодействию кибертерроризму.

В связи с этим государства, объединяясь, создают межправительственные и иные международные организации, одной из целей которых, как правило, является сотрудничество в сфере информационной безопасности. К числу организаций с отлаженных механизмом противостояния информационному терроризму, безусловно, следует отнести Шанхайскую организацию сотрудничества.

Общеизвестно, что одной из первоначальных задач ШОС выступали взаимные внутрирегиональные действия по пресечению так называемых «трех зол» — актов терроризма, сепаратизма и экстремизма в Средней Азии. Кроме того, организация включает в свой состав 8 госу-

Рис. 1. Отличительные особенности кибертерроризма*
*составлено авторами

дарств, с общей площадью 34 млн. кв. км и населением более 3 млрд. чел. (43 % населения Земли), что позволяет ШОС стать ключевой платформой для активизации регионального и международного сотрудничества в сфере противодействия кибертерроризму.

В целях выявления перспектив развития сотрудничества в рамках ШОС мы проанализировали, как существующие механизмы внутренней борьбы с кибертерроризмом на примере России и Китая, так и формы двустороннего и многостороннего сотрудничества в рамках деятельности организации.

Законодательный опыт Китая в вопросах кибербезопасности имеет доостаточню долгую историю, регулирование происходит на основании следующих нормативно — правовых актов: Постановление ВСНП по защите интернет — пространства 2000 г., Антитеррористический закон КНР от 27 декабря 2015 г., закон КНР о кибербезопасности от 7 ноября 2016 г. Законотворческая работа в данной области в России началась несколько позднее (Закон Российской Федерации 27.07.2006 № 149—ФЗ «Об информации, информационных технологиях и о защите информации») и особенно активизировалась в последние годы (Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», Федеральный закона от 26 июля 2017 г. N 187—ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

Тем не менее, в настоящее время в уголовном законе обоих государств не закреплено понятие кибертерроризма, что влечет неоднозначные юридические трактовки при квалификации соответствующих преступлений. Это вызывает большие вопросы у правозащитников и работников в сфере информационной безопасности, поскольку кибертерроризм во всем мире признан антисоциальным, общественно опасным явлением [4].

К числу конкретных практических методов борьбы с проявлением киберпреступлений В России следует отнести создание единого территориально распределенного комплекса центров различного масштаба, обменивающихся информацией о кибератаках. Подразумевается создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Цель всей этой масштабной государственной инициативы — создать между важнейшими организациями страны систему обмена информацией о ведущихся кибератаках и тем самым обеспечить возможность превентивной защиты. 11 декабря 2018 г. заместитель директора НКЦКИ (Национальный координационный центр по компьютерным инцидентам) Николай Мурашов отметил, что в 2018 г. средствами ГосСОПКА было выявлено более 4,3 млрд компьютерных воздействий на критическую информационную инфраструктуру, из них более 17 тыс. наиболее опасных компьютерных атак. Данные показатели свидетельствуют об эффективности работы новой создающейся системы безопасности [6].

Среди внутренних мер борьбы с кибертерроризмом в Китае следует отнести так называемый Golden Shield («Золотой щит») — общенациональный электронный барьер, фильтрующий

и контролирующий информационные потоки таким образом, что все интернет—данные пользователей в Китае проходят через определенное количество контрольно—пропускных пунктов (шлюзов), управляемых ограниченным числом компаний, предоставляющих доступ в Интернет [5, с. 610]. Это вызывает вопросы у многих западных правозащитников, так как подобная мера нарушает свободы человека (свобода информации и средств массовой информации, свобода мысли и слова) и может использоваться властями в целях слежки за частными лицами и компаниями. Тем не менее, следует отметить, что позиции России и Китая по вопросу предпочтения национальной безопасности частным правам и свободам, во многом схожи (в качестве подтверждения можно привести пакет антитеррористических поправок в законодательство Ирины Яровой и Виктора Озерова, активно обсуждаемый законопроект об устойчивой работе Рунета и т.д.).

Безусловно, невозможно накрыть «золотым щитом» все информационное пространство ШОС. Тем не менее, несмотря на различия в особенностях национальной борьбы за безопасность своего киберпространства, не исключаются и общие универсальные методы, которые реально реализовать в рамках международного сотрудничества.

Основным регулирующим документом в вопросе борьбы с кибертерроризмом в рамках ШОС является «Соглашение между правительствами государств—членов ШОС о сотрудничестве в области международной информационной безопасности» от 2009 г. (вступило в силу 2 июня 2011 г.), его ратифицировали четыре участника ШОС: Россия, Китай, Казахстан, Таджикистан. Участники соглашения сумели согласовать систему определения понятий, относящихся к IT—сфере. В рамках данного документа была заложена общая платформа для продвижения в ООН и других международных организациях и диалоговых структурах согласованных идей в области международной информационной безопасности. Уникальность документа заключается в том, что он впервые на международно—правовом уровне зафиксировал наличие конкретных угроз в области информационной безопасности, а также определил основные направления, принципы, формы и механизмы сотрудничества в этой сфере. Как в рамках ШОС, так и в широкой международной практике вступившее в силу Соглашение стало первым договорным актом, охватывающим весь спектр проблем международной информационной безопасности — от противодействия кибирпреступности и кибертерроризму до вопросов разоружения [8, с. 123].

Масштабная работа в сфере противодействия кибертерроризму проводится в рамках постоянно действующего органа ШОС — региональной антитеррористической структурой (РАТС ШОС) государств—участников Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г. [7]. Его основными задачами и функциями являются:

1. поддержание рабочих контактов с компетентными органами государств—членов и международными организациями, занимающимися вопросами борьбы с терроризмом, сепаратизмом и экстремизмом; 2. содействие взаимодействию государств—членов в подготовке и проведении антитеррористических учений по просьбе заинтересованных государств—членов, подготовке и проведении оперативно—розыскных и иных мероприятий по борьбе с терроризмом, сепаратизмом и экстремизмом; 3. участие в подготовке проектов международно—правовых документов, затрагивающих вопросы борьбы с терроризмом, сепаратизмом и экстремизмом; 4. сбор и анализ информации, поступающей в РАТС от государств—членов, формирование и пополнение банка данных РАТС; 5. подготовка и проведение научно—практических конференций, семинаров, содействие в обмене опытом по вопросам борьбы с терроризмом, сепаратизмом и экстремизмом и т.д.

Кроме того, на настоящем этапе, любая из сторон может инициировать проведение внеочередных консультаций, предлагая время и место, а также повестку дня для последующего согласования со всеми сторонами и Секретариатом ШОС [9]. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств сторон могут заключать соответствующие договоры межведомственного характера.

Несмотря на значительные успехи в совместной работе государств—членов ШОС по противодействию кибертерроризму, необходимо продолжать активизацию работы по данному вопросу, так как на лицо разрыв между ускоряющимся темпом технологических инноваций, с одной стороны, и запаздывающей реакцией политических и законотворческих институтов — с другой. Очевидно, что сотрудничество в данной области будет интенсифицироваться, в том числе по следующим направлениям:

— совершенствование соответствующей законодательной базы, дальнейшая гармонизация законов стран—участниц ШОС, в том числе и по вопросу экстрадиции киберпреступников;

— закрепление в законодательстве необходимых понятий, введение и конкретизация в уголовном законодательстве стран—участниц состава преступления и соответствующей ответственности за совершение преступлений информационного терроризма;

— расширение единой базы данных информационных атак;

— создание соответствующих исследовательских центров;

— совместная подготовка кадров;

— углубление сотрудничества в вопросах диверсификации поставок оборудования, включая системы хранения данных и телекоммуникационное оборудование и т.д.

Кроме того, имеет смысл расширять международное сотрудничество по данному вопросу. В настоящее время РАТС взаимодействует не только с компетентными органами стран—участниц ШОС, но и с международными организациями. Однако сотрудничество с ООН началось относительно недавно. Так, 22 февраля 2018 РАТС ШОС впервые приняла участие в заседании комитетов Совбеза ООН по противодействию терроризму в Нью—Йорке, стороны обсудили конкретные формы и направления практического взаимодействия [10]. По нашему мнению, несмотря на существующие политические разногласия между странами, совместная консолидация усилий государств по обеспечению защиты киберпространства является самым действенным способом борьбы с проявлением информационного терроризма.

Список использованной литературы

1. Туронок С. Г. Информационный терроризм: выработка стратегии противодействия / С.Г. Туронок // Общественные науки и современность. — 2011. — №. 4. — С. 131-140.

2. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУР. 2010. №1-1 (21) [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya (02.04.2019).

3. Морозова А.П. Кибертерроризм и информационный терроризм как новые формы проявления терроризма / А.П. Морозова // Научные труды Северо-Западного института управления. — 2017. — Т. 8. — №. 2. — С. 154-163.

4. Мухаметов А.Ф. Процесс формирования законодательного обеспечения национальной безопасности государства: а как у них? [Электронный ресурс]. — Режим доступа: http://repository.kazguu.kz/handle/123456789/532 (01.04.2019).

5. Дремлюга Р.И., Коробеев А.И., Федоров А.В. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты / Р.И. Дремлюга, А.И. Коробеев, А.В. Федоров // Всероссийский криминологический журнал. — 2017. — Т. 11. — №. 3.

6. За 2018 год на россию совершили более 4 миллиардов компьютерных атак [Электронный ресурс]. — Режим доступа: http://gossopka.ru/2018/12/12/%D0%B7%D0%B0-2018-%D0%B3%D0%BE%D0%B4-%D0%BD%D0%B0-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D1%8E-%D1%81%D0%BE%D0%B2%D0%B5%D1%80%D1%88%D0%B8%D0%BB%D0%B8-%D0%B1%D0%BE%D0%BB%D0%B5%D0%B5-4-%D0%BC%D0%B8%D0%BB%D0%BB/ (01.04.2019).

7. Соглашение между государствами — членами Шанхайской организации сотрудничества о Региональной антитеррористической структуре от 6 июня 2002 г. [Электронный ресурс]. — Режим доступа: http://kremlin.ru/supplement/3864 (02.04.2019).

8. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? [Электронный ресурс]. — Режим доступа: https://en.riss.ru/images/pdf/journal/2012/4/10_.pdf (02.04.2019).

9. Копытова Е.А. ШОС как инструмент поддержания международной безопасности [Электронный ресурс]. — Режим доступа: https http://elar.uspu.ru/handle/uspu/9287 (02.04.2019).

10. РАТС ШОС и Контртеррористический комитет СБ ООН активизируют сотрудничество [Электронный ресурс]. — Режим доступа: https://ria.ru/20180222/1515106577.html (02.04.2019).