А.А. Стрельцов, А.И.Смирнов[1]

Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям

Возможная повестка дня российско-американского сотрудничества в области международной информационной безопасности (МИБ) определяется, прежде всего, реальным состоянием российско-американских отношений, а также возрастающей ролью продолжающейся научно-технической революции в мировой политике в целом.

Как отметил Президент Российской Федерации В.В.Путин, выступая на итоговой сессии XIV ежегодного заседания Международного дискуссионного клуба «Валдай»: «Раньше, оценивая роль и влияние государств, говорили о значении геополитического фактора, о размерах территории, обладании военной силой, природными ресурсами. Безусловно, это и сегодня важнейшие факторы. Однако теперь другим важнейшим фактором, без всяких сомнений, становится научно-технологический, и его значение будет только усиливаться. Собственно говоря, так было всегда, но сегодня это будет иметь прорывной характер и очень быстро будет решающим образом влиять на сферу политики и безопасности».[2]

По оценкам ведущих экспертов мира в области внешней политики, отношения между Россией и США в настоящее время достигли критически низкого уровня. Эта оценка совпадает с мнением Министра иностранных дел России С.Лаврова, который полагает, что «двусторонние связи остаются заложником разборок в американском истеблишменте…. Это прямое следствие политики администрации Б.Обамы, которая разрушала фундамент сотрудничества, а перед уходом заложила под него мины долгосрочного действия, чтобы осложнить жизнь своим преемникам»[3].

---

[1] Анатолий Александрович Стрельцов – Заслуженный деятель науки Российской Федерации, действительный государственный советник Российской Федерации 3 класса, д.ю.н., д.т.н., проф., зам. Директора ИПИБ МГУ им. М.В.Ломоносова; Анатолий Иванович Смирнов – д.и.н., проф., Гл.науч. сотрудник Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России, Президент Национального института исследований глобальной безопасности, Чрезвычайный и Полномочный Посланник в отставке

[2] URL: http://kremlin.ru/events/president/news/55882

[3] https://ria.ru/politics/20171004/1506134984.html

Определенные надежды на потепление в российско-американских отношениях, которые порождались решениями президентов Российской Федерации и США (2009 г.) о начале «перезагрузки» этих отношений[4], о сокращении стратегических наступательных вооружений, подписанием совместного заявления о новой области сотрудничества в укреплении доверия (2013 г.)[5] и другими, достаточно быстро исчезли.

Анализ событий современной внешней политики США предоставляет достаточно аргументов в поддержку предположения о том, что в последние годы американский истеблишмент в стратегическом плане готовится к реализации «силового» сценария разрешения противоречий с Россией. С этой целью оказывается масштабное информационно-психологическое давление на международное общественное мнение, которому навязывается образ России как главного виновника всех проблем внутренней и внешней политики США и Запада в целом.

В этот сценарий вписываются попытки голословно обвинить Россию во влиянии на результаты американских выборов 2016 г., в доступе к закрытым данным в американских государственных информационных системах, в ведении «фейковой» пропаганды и в других случаях якобы недобросовестного поведения России.

Предположение экспертов о подготовке США «силового» сценария взаимодействия с Россией объясняет многие факторы американской внешней политики. В частности:

- продавленное конгрессом США подписание 2 августа 2017 г. закона «О противодействии противникам Америки посредством санкций», предусматривающего ужесточение режима санкций в отношении России, Ирана и КНДР[6];
- решение Б.Обамы о закладке в объекты критической информационной инфраструктуры России так называемых «кибербомб», которые можно привести в действие[7] для подрыва экономической и социальной стабильности российского общества;
- разработка ЦРУ маскировочных программных средств проведения компьютерных атак, в том числе под «чужим флагом»[8];
- усиление информационной составляющей американского потенциала ведения «гибридной» войны и создание системы глобальной

---

[4] URL: https://ria.ru/politics/20090401/166744761.html
[5] URL: http://kremlin.ru/supplement/1479 (дата обращения: 6.10.2017)
[6] URL: http://tass.ru/politika/4458190 (Дата обращения 03.08.2017).
[7] URL: https://www.kommersant.ru/doc/3335422 (дата обращения 6.10.2017)
[8] URL: http://tass.ru/mezhdunarodnaya-panorama/4077772 (дата обращения 6.10.2017)

электронной слежки и роботроллинга в социальных сетях, направленного на инспирирование «кибербунта» в России;

- открытие под надуманным предлогом ряда киберцентров передового опыта НАТО, т.ч. с Евросоюзом в Хельсинки в сентябре 2017 г. Центра по противодействию так называемым «гибридным угрозам» (в первую очередь из России)[9];
- целый ряд иных действий США, в том числе с российским дипломатическим имуществом, грубо нарушающих международное право, и создающих угрозу национальным интересам Российской Федерации.

В предположение о подготовке «силового» сценария, как представляется, вписывается и позиция США по отказу от взаимодействия с Россией в сфере предотвращения инцидентов в ИКТ-среде, предусмотренного совместным заявлением президентов Российской Федерации и Соединенных Штатов Америки (2013 г.), а также принятие в 2015 г. Стратегии кибербезопасности США, позволяющей вести наступательные кибервойны.[10]

Вышеизложенное стимулирует активизацию усилий экспертов по поиску рациональных направлений двустороннего сотрудничества в ИКТ-сфере.

Среди множества работ, так или иначе посвященных обсуждению возможных направлений двустороннего сотрудничества, привлекает внимание аналитическая записка РСМД (П.Шариков, М. Смекалова) и американского Института Восток-Запад (Б.МакКонелл)[11], в которой предпринята попытка анализа ситуации в области МИБ и выработки предложений на определенную перспективу.

Поддерживая стремление вышеуказанных экспертов к всестороннему анализу основных факторов, влияющих на выбор направлений такого сотрудничества, можно согласиться с исходной позицией авторов о том, что «текущее состояние российско-американских отношений отличается высоким уровнем недоверия», равно как и с предложением продолжать контакты на уровне экспертного, дипломатического и бизнес-сообществ для достижения компромисса.

Однако нельзя согласиться с тем, что при формулировании предложений по направлениям российско-американского сотрудничества

---

[9] URL: https://goo.gl/rDCwkQ (дата обращения 6.10.2017)
[10] URL: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения 16.10.2017)
[11] МакКоннелл. Б., Шариков.П., Смекалова.М.. Предложения по российско-американскому сотрудничеству в сфере кибербезопасности. РСМД. 2017, сентябрь, № 11. URL: http://russiancouncil.ru/papers/RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-ru.pdf

авторы оставляют без внимания позицию Российской Федерации, изложенную в целом ряде документов стратегического планирования, принятых в последнее время.

Так, по существу, проигнорирована позиция Российской Федерации по вопросу об основных внешних угрозах государственной, экономической и общественной безопасности России, а также угрозах международному миру и безопасности, исходящих из глобального информационного пространства, изложенная в Концепции внешней политики России[12]. Осталась за рамками исследования закреплённая в этом же документе позиция российского политического руководства по вопросу о необходимости выработки под эгидой ООН универсальных правил ответственного поведения государств в области обеспечения МИБ, в том числе посредством интернационализации на справедливой основе управления информационно-телекоммуникационной сетью "Интернет".

Остались незамеченными многочисленные инициативы России и её партнеров в сфере МИБ, например, представленная Секретарем Совета Безопасности России Н.Патрушевым еще в 2011 г. концепция универсальной Конвенции об обеспечении международной информационной безопасности[13].

Кроме того, вызывает недоумение попытка соавтора рассматриваемой работы Брюса МакКоннелла, вице-президента по глобальным вопросам Института Восток-Запад, критиковать российский подход к определению «информационной безопасности», который, по его мнению, является излишне широким. «…Российское видение кибербезопасности включает защиту от использования информационного пространства для нанесения ударов по России. Так, например, действия госсекретаря США Хилари Клинтон по защите права на свободу слова и продвижению социальной сети «Твиттер» для высказывания своих политических настроений, были восприняты как попытка стимулирования «цветной революции» в России» (данный тезис резко контрастирует с истерией в американском истеблишменте по поводу «мифического» влияния России на американские выборы 2016 г.).

Б.МакКонелл пытается не замечать инспирированных с участием бывшего госсекретаря США Х.Клинтон «арабской весны», а также целого ряда других «цветных революций», несмотря на то, что публикация дипломатической переписки в Wikileaks убедительно раскрывает технологию этой, по существу, подрывной работы США в ИКТ-среде. Вряд ли можно

---

[12] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации 30 ноября 2016 г., http://kremlin.ru/acts/bank/41451/page/2

[13] URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения 7.10.2017)

прийти к другому выводу, анализируя текст шифртелеграммы посольства США в КНР от 25 января 2010 г.[14]

Трудно согласиться и с тем, что образование так называемой «Глобальной комиссии по стабильности киберпространства»[15] является средством решения всех проблем создания, оценки и разработки рекомендаций, касающихся применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, а также выдвижения предложений по обсуждениям в более широком формате.

Ни процедура образования Комиссии, ни ее состав не создают оснований для подобных иллюзий. При этом остаются «за кадром» многочисленные инициативы России и её партнеров в ООН по организации работы по исследованию глобальных аспектов стратегической стабильности, в том числе в ИКТ-сфере.

Вызывает сожаление, что российские соавторы записки РСМД не высказали своего мнения на сей счет.

Искусственность данного подхода к выстраиванию повестки дня российско-американского сотрудничества в области МИБ вынуждает авторов настоящей работы предложить свой взгляд на основные проблемы обеспечения МИБ и возможные приоритетные направления сотрудничества России и США в данной области.

По мнению авторов, в современных условиях укрепление российско-американского сотрудничества по-прежнему является одним из ключевых факторов обеспечения международной безопасности вообще и в информационной сфере в частности.

Как показала работа Группы правительственных экспертов ООН по достижениям в области информатизации и телекоммуникации в контексте международной безопасности, в международном экспертном сообществе, усилиями, в том числе Российской Федерации и её партнеров, сложилось общее понимание необходимости соблюдения международных обязательств, вытекающих из признанных государствами источников международного права: общих и специальных международных конвенций; международного обычая; общих принципов права, признанных цивилизованными народами; судебных решений[16].

---

[14] См. Смирнов А.И., Кохтюлина И.Н. "Глобальная безопасность и мягкая сила 2.0" – М.; ВНИИГеосистем. 2012 г. с. 55, 219-226 URL: https://mgimo.ru/upload/iblock/60a/60ad847142af15b58c4b7ce272d9607c.pdf

[15] URL: http://cyberstability.org/commissioners/ (дата обращения 7.10.2017)

[16] Статут Международного Суда. Ст.38, п.1

Существует согласие[17] и в том, что ИКТ-среда является новым пространством международных отношений. Основными признаками, отличающими ИКТ-среду от традиционных пространств реализации отношений суверенных государств (суши, моря, воздушного пространства), являются:

искусственный характер ИКТ-среды, образуемой совокупностью средств телекоммуникаций, вычислительной техники, программного обеспечения, функционирующих в системе глобальных цифровых идентификаторов, работоспособность которой поддерживается усилиями, прежде всего, негосударственных организаций, находящихся в различных юрисдикциях;

виртуальность процессов применения ИКТ, следствием которой является невозможность непосредственного наблюдения условий возникновения инцидентов в ИКТ-среде;

трудность определения источников инцидента в ИКТ-среде;

дестабилизирующие последствия злонамеренного или враждебного использования ИКТ против критически важной инфраструктуры общества, совершения террористических нападений на объекты ИКТ-среды и связанную с ИКТ инфраструктуру;

использование ИКТ террористическими организациями для вербовки сторонников, финансирования, обучения, подстрекательства и проведения терактов.

Озабоченность американских политиков «мифическим» влиянием других государств на развитие политических процессов в США приближает время признания угрозой МИБ использование ИКТ для вмешательства во внутренние дела суверенных государств, о необходимости противодействия которой Россия и ее партнеры по Шанхайской организации сотрудничества не только заявили в совместном соглашении[18], но и дважды – в 2011 и в 2015 гг. вносили проекты соответствующих резолюций в ООН[19].

Из возможных способов обеспечения применимости международного права к ИКТ-среде США выбирают толкование международных обычаев и принципов, не накладывающие на государства дополнительных обязательств по международному сотрудничеству в области предотвращения использования ИКТ в военных целях, а также в области сотрудничества по

---

[17] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. 22 июля 2015 г., A/70/174

[18] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 г.

[19] URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/916241

проблемам предотвращения преступной, в том числе террористической, деятельности.

Соглашаясь с принятием ответственности за предотвращение «использования их территории для совершения международно-противоправных деяний с использованием ИКТ»[20], американские эксперты пока не видят необходимости договариваться об установлении границ зон ответственности государств в ИКТ-среде, о процедуре объективизации данных о нарушении международных обязательств государствами, о порядке расследования международных инцидентов в ИКТ-среде на основе взаимодействия национальных Групп реагирования на инциденты информационной безопасности.

Исходя из безусловного приоритета поддержания международного мира, безопасности, создания открытого, безопасного, стабильного, доступного и мирного глобального информационного пространства, крайне важно сосредоточить усилия государств на предотвращении конфликтов в ИКТ-среде и использования ИКТ для достижения военных целей, а не на их легализацию.

В условиях бурного роста преступности в компьютерной сфере, а также с учетом уязвимостей Industry 4.0 (ожидаемый ущерб от их использования в преступных целях возрастет, как ожидается, с 400 млрд. долларов в 2016 г. до 3 триллионов долларов суммарно к 2020 г.)[21] не менее важным становится принятие универсальной Конвенции по противодействию информационной преступности, проект которой представлен Россией в мае 2017 г. на Восьмой международной встрече высоких представителей, курирующих вопросы безопасности, а также «на полях» 26-й сессии Комиссии по предупреждению преступности и уголовному правосудию ООН[22].

Международное сообщество могло бы сосредоточить усилия на прогрессивном развитии международного права, на адаптации его к особенностям ИКТ-среды как новой сферы международного сотрудничества.

В основу предложений по приоритетным направлениям российско-американского сотрудничества в области международной информационной безопасности можно было бы положить идею совместного выполнения следующих мероприятий.

1. Подготовка проекта Конвенции по обеспечению международной

---

[20] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. 22 июля 2015 г., A/70/174, п.13 c)

[21] URL: https://goo.gl/Bg4bnY (дата обращения 6.10.2017)

[22] URL: http://www.un.org/russian/news/story.asp?NewsID=27991# (дата обращения 6.10.2017)

информационной безопасности, закрепляющей основные подходы к прогрессивному развитию международного права применительно к ИКТ-среде посредством принятия норм, уточняющих содержание международных обязательств государств в ИКТ-среде, процедуру выявления нарушений этих обязательств, определения субъектов, нарушивших международные обязательства, а также процедуры мирного разрешения международных споров, связанных с инцидентами в ИКТ-среде.[23]

2. Подготовка проекта руководства по применению принципов, норм и правил ответственного поведения государств в ИКТ-среде.

3. Подготовка проекта Конвенции по противодействию информационной преступности.

4 Подготовка проектов дополнений к существующим международным договорам, уточняющих содержание международных обязательств в ИКТ-среде, и, прежде всего, в контексте предупреждения возникновения международных конфликтов и мирного разрешения международных споров.

5. Подготовка универсального международного договора о порядке отграничения зон ответственности государств в ИКТ-среде и правового закрепления границ этих зон ответственности (пространственных пределов суверенитета государств в ИКТ-среде).

6. Подготовка международных соглашений о порядке расследования международных инцидентов в ИКТ-среде на основе взаимодействия национальных центров реагирования на опасные события в данной среде, а также порядка приписывания субъектам международного права ответственности за возникновение таких инцидентов.

7. Создание международного органа для рассмотрения международных споров по вопросам безопасности продуктов, реализующих функции ИКТ, а также по вопросам использования ИКТ для вмешательства во внутренние дела суверенных государств.

Для организации работы по перечисленным направлениям стоило бы создать при одной из международных организаций или Комиссии международного права при Генеральной Ассамблее ООН специализированную рабочую группу по подготовке предложений по проектам международных договоров. В состав такой рабочей группы могли бы войти юристы, инженеры и представители силовых структур заинтересованных государств.

Экспертизу проектов документов, подготовленных специализированной рабочей группой, можно было бы осуществлять с использованием потенциала Группы правительственных экспертов ООН по достижениям в сфере

---

[23] Крутских А.В., Стрельцов А.А. Международное право и проблемы обеспечения международной информационной безопасности. Международная жизнь. 2014, № 11.

информатизации и телекоммуникации в контексте международной безопасности, созываемой Генеральным секретарем ООН по рекомендации Генеральной Ассамблеи ООН, а также в формате двусторонних и многосторонних консультаций.