«РОССИЯ — КИТАЙ — США: ФОРМИРОВАНИЕ ГЛОБАЛЬНЫХ ПРАВИЛ ИГРЫ В КИБЕРПРОСТРАНСТВЕ»

Олег Викторович Демидов, эксперт Консультативной исследовательской сети при Глобальной комиссии по управлению интернетом (GCIG RAN), консультант ПИР-Центра

Стенограмма заседания Международного клуба *Триалог*

29 сентября 2015 г.

О. В. Демидов: Уважаемые коллеги, уважаемые участники клуба *Триалог*, всем доброе утро. Я бы хотел отметить, что я очень рад и горд выступать на площадке клуба *Триалог*. Раньше мне случалось бывать здесь в качестве гостя или в качестве сотрудника ПИР-Центра, но выступаю я здесь впервые. Я признателен за это.

В качестве вводного тезиса объясню, почему я хочу рассказать именно этой аудитории именно эту тему именно сейчас. Развитие международных дипломатических процессов, переговоров, выстраивание новых форматов сотрудничества, поведения государств в киберпространстве продолжается как минимум последние полтора десятилетия. Но только в этом году с помощью различных переговоров, с помощью документов, проведенных и подписанных за последние месяцы в разных форматах между государствами, сложились предпосылки для качественного прорыва в этой области на международном уровне. Ключевые события и прогресс в этой сфере происходят с подачи трех крупнейших кибердержав — России, Соединенных Штатов Америки и Китая. Один из парадоксов, на мой взгляд, состоит в том, что на фоне очень активных переговоров и достижения договоренностей в двустороннем формате — по линии Россия–Китай, Россия–США и США–Китай — складываются предпосылки, но пока нет ни международного правового механизма, ни соответствующей площадки, где эти государства могли бы в трехстороннем формате договориться о каких-то общих моментах своего видения политики в киберпространстве. Я постараюсь в своем выступлении показать и рассказать, какие моменты могли бы стать общими для трех этих государств, и какие могли бы быть пути к возникновению такого трехстороннего формата и взаимодействия в киберпространстве.

Я начну свое выступление с введения в то, что происходит сейчас на более широком уровне — на уровне ООН и других международных площадок с широким участием. Одним из ключевых событий этого лета стал выход очередного доклада Группы правительственных экспертов ООН (The UN Group of Governmental Experts) (ГПЭ), в котором впервые для международного сообщества, для государств-членов ООН предлагается конкретный набор политических норм, ограничивающих определенными рамками и подчиняющих

определенным правилам их поведение в киберпространстве. Ключевые положения доклада обобщены на слайде.

Сосредоточусь на вопросах и спорных моментах, которые возникают в отношениях этого доклада и задают вектор дальнейшей работы группы — ее очередной созыв произойдет уже в 2016 году.

Во-первых, несмотря на то, что группа в докладе дает ответ на принципиальный вопрос о том, применим ли устав ООН к киберпространству — ответ утвердительный — этот ответ, в свою очередь, порождает целую серию вопросов, связанных прежде всего с тем, что нет ясности, как именно положения Устава ООН применяются к киберпространству. В частности, это неясно в части трех ключевых определений, упоминаемых в Уставе ООН: использование силы либо угроза использования силы в международных отношениях, акт агрессии в отношении государства–члена ООН и вооруженное нападение в терминологии Устава ООН. Вопрос имеет практическое значение в связи с тем, что отдельные государства — в том числе, США и их партнеры по блоку НАТО — уже развивают собственные подходы в этой области и дают собственные интерпретации условий применения этих понятий к ситуациям или кризисам, возникающим в киберпространстве.

Одним из источников знаний, источником компетенций, на основе которых формируется подход НАТО к этому вопросу, являются экспертные документы Таллиннского центра передовых практик кибероборонь, в частности, документ,

известный как Таллиннское руководство по применению международного права в киберпространстве (The Tallinn Manual on the International Law Applicable to Cyber Warfare). В то же время, такие государства, как США, развивают и закрепляют в своих документах собственное видение, как развивается эта сфера. В частности, издание 2015 года, Руководство Пентагона по праву вооруженных конфликтов (Law of War Manual) перечисляет возможные условия, при которых кибератака может квалифицироваться как акт применения силы либо как вооруженное нападение.

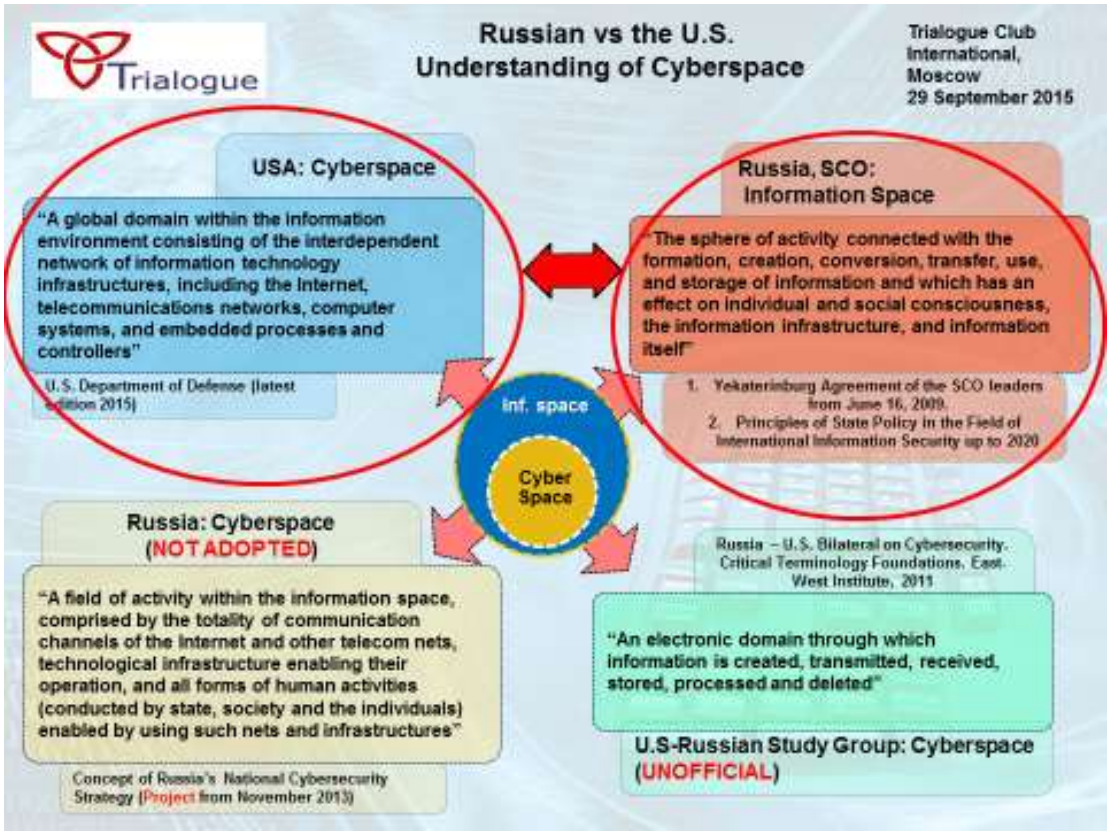
Стоит также отметить, что хотя такие документы как «Таллиннское руководство» и его вторая версия, готовящаяся к изданию в 2016 году, являются экспертными документами, они уже становятся краеугольным камнем для стратегий, которые на практике воплощает, в том числе, блок НАТО. В частности, на саммите НАТО в Уэльсе в 2014 году в рамках рассмотрения углубленной концепции кибероборонs НАТО было принято решение о том, что в киберпространстве могут возникать ситуации, инциденты, трактующиеся как нападения на страны-члены НАТО, и такие ситуации позволяют членам альянса задействовать Статью 5 Вашингтонского договора, которая дает им право коллективной кибероборонs.

Таким образом, в некоторых региональных форматах, в некоторых странах развитие теории и взглядов на условия и возможности применения механизмов международного права к кибероперациям и к кризисам в киберпространстве идет опережающими темпами по сравнению с наработками в этой сфере Группы правительственных экспертов ООН. С точки зрения отдельных участников Группы правительственных экспертов и с точки зрения некоторых членов международного сообщества, сам по себе этот факт не составляет проблемы. Однако позиция других государств, в частности, России, Китая и других участников Группы правительственных экспертов расходится с тем подходом, который заложен в Таллиннском руководстве и которым руководствуется НАТО в своей углубленной доктрине кибероборонs.

В случае с Россией сущность этих расхождений давно известна. Российская дипломатия полагает, что киберпространство в силу своих уникальных характеристик, трансграничности требует дополнительного международного правового регулирования. И основой международно-правового режима поведения государств в киберпространстве должны стать новые механизмы, договоры, конвенции, желательно выработанные и принятые на площадке ООН как наиболее представительной и легитимной международной площадке. В частности, Россия выступала с концепцией Конвенции об обеспечении международной информационной безопасности в 2011 году, а также совместно с государствами-членами Шанхайской организации сотрудничества дважды в 2011 и в 2015 году направляла Генеральному секретарю ООН письмо с проектом правил поведения в сфере международной информационной безопасности. Все эти упомянутые документы 2011 и 2015-го годов содержали в себе ключевые положения, которые Россия продвигает в своем внешнеполитическом курсе, и

которые Россия, а также в какой-то степени Китай пытались отстоять на площадке Группы правительственных экспертов ООН.

О каких положениях идет речь? **Во-первых,** право государств на суверенный контроль собственного сегмента киберпространства. В частности, информационной инфраструктуры, расположенной в его юрисдикции. **Во-вторых,** императив не прояснения правил, а вместо этого запрета и предотвращения конфликтов с использованием информационных технологий, в частности, кибервойн и наступательных кибероперация. **В-третьих,** тезис о недостаточности существующего инструментария международного права и необходимости выработки новых международно-правовых обязывающих инструментов для построения эффективного режима поведения государств в киберпространстве. **В-четвертых,** это сильный акцент на необходимости регулирования вопросов, связанных с контентом, с содержанием информации, передаваемый трансгранично через различные национальные сегменты киберпространства, и воздействие этой информации не только на информационную инфраструктуру, но и на социально-политическую стабильность в тех или иных странах. Последний тезис, кстати, хорошо иллюстрируется с терминологической точки зрения. На слайде можно посмотреть, насколько разные определения и понятия киберпространства, информационного пространства используют США и Россия, и ключевое отличие в их подходах как раз связано с вниманием к содержанию информации, к ее воздействию не только на инфраструктуру, но и на умы.



Я резюмирую, к чему удалось прийти, о чем удалось договориться всем 20 участникам Группы правительственных экспертов с учетом этих противоречий и с учетом разницы в подходах ключевых участников группы — а США и Россия всегда были наиболее активными и наиболее принципиально различными по своим взглядам участниками группы. Основным предметом, по которому удалось достичь согласия, стало обязательство не нападать на объекты критической инфраструктуры, а также оказывать друг другу помощь в расследовании и пресечении инцидентов, связанных с атакой на объекты критической инфраструктуры в киберпространстве. Это важный шаг и большое достижение, но проблема здесь заключается в том, что не прояснены ключевые понятия, и не прояснены детали такого взаимодействия. Понятия и классификация объектов критической инфраструктуры у всех 20 стран, особенно у Китая, России и США, очень сильно различаются. Составление единой международной классификации объектов критической инфраструктуры было бы важной задачей, и я заранее выношу это в резюме своего выступления, как одну из будущих задач для Китая, России и США в киберпространстве. Однако прогресс в этом направлении потребует хотя бы минимального повышения уровня доверия между участниками этого потенциального *треугольника*. Например, сейчас стратегический диалог по киберпространству между Россией и США заморожен, несмотря на предшествующие значительные достижения.

Последнее, что следует сказать про итоги работы нынешнего созыва Группы правительственных экспертов: с одной стороны, России и ее единомышленникам удалось пронести в доклад положения о том, что концепция государственного суверенитета применима к национальной ИКТ-инфраструктуре и объектам такой инфраструктуры, находящимся в национальной юрисдикции; с другой стороны, одна из ярких идей, предложенных российской делегацией, не прошла в итоговый текст доклада — вынести в качестве отдельного положения обязательства государств воздерживаться от кибернападений на объекты банковской информационной и телеинфраструктуры. Забегая вперед, нужно сказать, что ровно такая же норма обсуждалась в СМИ в преддверии визита китайского лидера Си Цзиньпина в США, когда было достигнуто нынешнее соглашение между Китаем и США. Также якобы предлагалось внести в соглашение норму о ненападении на киберинфраструктуру банков, однако в итоговом коммюнике этого не оказалось. Я постоянно заостряю на этом внимание потому, что выделение какого-либо конкретного класса объектов критической инфраструктуры было бы радикальным шагом вперед с точки зрения международно-правового режима. Пока государства говорят о ненападении на критическую инфраструктуру в целом, их обязательства во многом остаются абстрактными — пока неясно, о каких объектах идет речь. Выделение конкретных типов инфраструктуры: банковской, телекоммуникационной, ядерной, неважно какой — сразу бы создало более четкие обязательства и помогло бы найти общий язык техническим специалистам всех стран, участвующих в таком соглашении. Последнее любопытное положение в докладе ГПЭ — положение о том, что государствам следует прилагать меры по обеспечению контроля над цепочками

поставок ИКТ-продукции, чтобы избежать бэкдоров, «закладок» в них, и чтобы избежать их использования не в декларированных целях.

Теперь от обзора доклада Группы правительственных экспертов я хотел бы перейти к двустороннему сотрудничеству по линиям Россия–Китай, Россия–США и США–Китай по тем же самым вопросам о нормах поведения в киберпространстве. Прежде всего я напомню, чего удалось достичь России и США на двустороннем направлении на данный момент. Ключевым прорывом стала серия соглашений, подписанных президентами двух стран в 2013 году. Они обеспечивали пакет мер доверия в киберпространстве и выводили отношения двух государств в этой сфере на новый уровень. В частности, в пакет мер доверия входило соглашение о создании канала обмена информацией между высокопоставленными представителями обеих сторон в случае серьезного кризиса в киберпространстве. Таким кризисом могла быть атака, запущенная в отношении объекта критической инфраструктуры на территории России с территории США — или наоборот. То есть, киберинциденты, кибероперации и кибератаки, в которые так или иначе была бы вовлечена инфраструктура участников соглашения. В дополнение к каналу срочной связи между высокопоставленными представителями сторон был также организован круглосуточный канал информирования и обмена данными на базе инфраструктуры национальных Центров по уменьшению ядерной опасности. Таким образом, инфраструктура времен «холодной войны» оказалась востребована для задач поддержания стратегической стабильности в киберпространстве. Кроме того, в соглашение вошло положение об обмене данными и сотрудничеству в обмене информацией о киберинцидентах между российским и американскими Центрами реагирования на киберинциденты (Computer Emergency Response Teams, CERTs). В соглашение также был заложен механизм двусторонней рабочей группы по развитию соглашений, по расширению их положений и дальнейшей эволюции — укреплению и расширению пакета мер доверия. Следует отметить, что российская дипломатия в лице Андрея Крутских, специального представителя президента России по вопросам международного сотрудничества в области информационной безопасности, официально признала и подтвердила огромную практическую пользу, которую эти соглашения принесли Российской Федерации. Господин Крутских в интервью заявил, что механизм соглашения, в частности, механизм канала срочного обмена информацией, оказался востребован во время проведения Олимпийских игр в Сочи в феврале 2014 года, когда каналы были задействованы во время отражения кибератак на инфраструктуру Олимпиады. К сожалению, как раз вскоре после Олимпийских игр сначала рабочая группа, а потом и весь пакет мер, прописанных в соглашениях, оказались фактически заморожены из-за крымского, а потом украинского кризиса. Этот факт отражен и в свежем издании стратегии Пентагона по операциям в киберпространстве. Оно вышло весной 2015 года. Там сообщается, что диалог по вопросам стратегической стабильности в киберпространстве с Россией заморожен до тех пор, пока не позволит международная ситуация, а с Китаем такой диалог продолжается. То есть, на сегодняшний день, по сути, стратегической задачей в двустороннем треке Россия–

США остается хотя бы восстановление того уровня доверия и того уровня сотрудничества, который сложился к февралю 2014 года. Более того, сама логика и наполнения пакета мер доверия, который был выработан между Россией и США, служит отличной матрицей, примером для других двусторонних и многосторонних форматов. Во-первых, потому что из итогового варианта соглашений вычищены, исключены почти все вопросы, по которым у сторон были непримиримые противоречия: контент, контроль, влияние информации на политические процессы и т. д. Оставлены вопросы инфраструктуры, там, где технические специалисты отлично понимают друг друга, там, где есть понимание угрозы. Кроме того, принципиально важно, что соглашения предусматривали именно круглосуточную постоянную работу каналов обмена информацией. Поскольку, как только вы организуете постоянное взаимодействие технических групп экспертов, капитал доверия между ними начинает непрерывно нарабатываться автоматически. Пока они работают, их взаимодействие укрепляется. Это радикально отличается от тех договоров, в которых на бумаге прописаны некоторые меры взаимодействия, но они используются от случая к случаю. В качестве иллюстрации моей предыдущей фразы рассмотрим недавнее соглашение между Россией и Китаем от 8 мая 2015 года. Соглашение содержит очень обширный и разветвленный перечень мер сотрудничества двух стран по вопросам кибербезопасности и регулирования киберпространства — порядка 15 пунктов. Основные, но далеко не все из них перечислены на слайде.

Соглашение включает в себя сотрудничество по обмену информацией между правоохранительными органами, выработку подходов к регулированию в

киберпространстве и на международной арене, защиту объектов критической инфраструктуры, борьбу с киберпреступностью, борьбу с кибертерроризмом и т. д. Таким образом, с формальной точки зрения механизм сотрудничества между Россией и Китаем гораздо шире и разветвленнее аналогичного механизма, появившегося в отношениях России и США 2013 года. Однако на деле майский документ остается по сути рамочным соглашением, которое не наполнено и не предусматривает технических механизмов сотрудничества, которое само по себе не обязывает стороны к организации конкретного взаимодействия и не указывает, как технически такое взаимодействие должно быть организовано. Этим оно принципиально отличается от российско-американского пакета мер доверия в киберпространстве. Второе радикальное отличие российско-китайского документа в том, что он насыщен идеологическими положениями. Он транслирует совместное видение сторонами-подписантами того, на какие принципы должен опираться международно-правовой режим регулирования киберпространства. Один из таких принципов — это интернационализация управления инфраструктурой интернета, то есть, подчинение контроля над ключевой инфраструктурой глобальной сети межправительственной организации. Таким образом, можно заключить, что пока в значительной степени российско-китайский механизм сотрудничества, заключенный в майском соглашении, служит скорее декларацией единства взглядов двух стран в отношении подходов к формированию международно-правового режима поведения в киберпространстве, нежели является практическим механизмом по защите инфраструктуры. Однако все предпосылки для развития практических мер взаимодействия в документе, в принципе, заложены. Просто они должны будут развиваться и прописываться уже отдельными документами в рамках этого широкого соглашения. Это длительный процесс, и, в отличие от российско-американского пакета мер доверия, он не укладывается в одно соглашение. Это будет происходить поэтапно.

Мы рассмотрели российско-китайское и российско-американское взаимодействие по вопросам регулирования киберпространства и кибербезопасности. Остается третий элемент этого потенциального *большого треугольника* — китайско-американское взаимодействие. Достигнутая буквально на днях договоренность между лидерами двух стран договоренность считается прорывной, и присутствующая здесь аудитория, я думаю, понимает, почему. До этого всегда считалось, что Соединенные Штаты четко разделяют вопросы шпионажа в киберпространстве и вопросы кибероперациий, проводимых с целью обеспечения национальной безопасности или осуществляемых с экономической мотивацией. То есть, похищение, присвоение торговых, экономических, интеллектуальных секретов и активов и их последующее использованием корпоративным сектором или государством в зависимости то того, в чьих интересах таким операции велись. Конечно, для США наиболее болезненным в отношениях с Китаем оставался вопрос экономического кибершпионажа. Неоднократно озвучивалась статистика о том, что китайцы стоят за похищением 80% данных из американских сетей, что Китай является ключевым бенефициаром деятельности хакеров, похищающих торговые секреты у американских компаний

и американского государства, и что сумма ущерба от их действий исчисляется многими десятками миллиардов долларов ежегодно. Вместе с тем, в силу крайней трудности сбора технических и юридических доказательств того, кто именно стоит за кибератакой, кибероперацией, считалось, что надавить на Китай в достаточной степени, чтобы заставить отказаться от таких действий, невозможно. По этой причине ожидалось, что переговоры двух лидеров, поиск общего языка по поведению в киберпространстве не закончится договоренностью в отношении коммерческого шпионажа. Ожидалось, что стороны скорее договорятся воздерживаться от атак на критическую инфраструктуру, от активных военных операций и т. п. Тем удивительнее, что Бараку Обаме и Си Цзиньпину удалось достичь взаимопонимания в вопросе о коммерческом, экономическом кибершпионаже. Возможно, ключевой предпосылкой к тому, что Китай изменил свою позицию тотального отрицания участия в таких операциях и пошел на серьезный компромисс, стала угроза санкций, которые президент США пообещал ввести в отношении китайских компаний и граждан за кибершпионаж с экономическими мотивами. Информация о возможном скором введении санкций появилась в августе этого года. В юридическом смысле механизм санкций был основан на приказе Обамы о введении такого рода санкций в отношении американских граждан. Только теперь он был пересмотрен так, чтобы его можно было применить к зарубежным гражданам и компаниям — в частности, к китайским. Этот механизм предполагал четыре основания для их введения:

1) Участие в атаках на объекты критической инфраструктуры США.
2) Участие в атаках на ключевые компьютерные сети США.
3) Участие в похищении торговых и интеллектуальных секретов американских компаний и американского государства.
4) Прямое выгодоприобретение от похищения американских торговых секретов с помощью кибероперациий.

Последний пункт является самым интересным и был самым действенным с практической точки зрения.

Судя по всему, реальная перспектива введения такого механизма против китайских компаний, которые американские спецслужбы подозревают в экономическом кибершпионаже, смогла повлиять на китайское руководство и создать достаточно пугающую перспективу для того, чтобы Китай пошел на принятие нормы, положения, которое обязывает его воздерживаться от крупномасштабного кибершпионажа по экономическим мотивам. Конечно, сейчас очень много споров и разных точек зрения о том, какова реальная ценность этой сделки. Ведь, по сути, речь идет о декларации о намерениях, которая не подкреплена, опять же, никакими механизмами мониторинга, нет и реальных механизмов верификации того, как китайцы будут ее исполнять. Однако я позволю себе предположить, что даже в текущем виде — в виде простой декларации о намерениях — это соглашение является большой победой для Белого дома и шагом вперед, поскольку, на самом деле, оно обеспечено не механизмом мониторинга, а механизмом экономического сдерживания в

киберпространстве — той самой перспективой санкций против китайских компаний. Я хотел бы еще раз зафиксировать на этом внимание. Долгое время аналитики и правительственные эксперты считали, что в киберпространстве может работать механизм военного сдерживания. То есть, государства будут воздерживаться от масштабных кибероперациий друг против друга, поскольку будут уязвимы их военные объекты, управляющие инфраструктурой, командные сети, сети, принадлежащие вооруженным силам. Этого типа сдерживания как раз не происходит в достаточной степени. А вот экономическое сдерживание, возможно, даже эффективнее. Приведу небольшой пример: еще в 2012 году сообщалось, что каждый день сети одного лишь Пентагона выдерживают до 8-10 миллионов попыток тестирования их на наличие брешей в защите. Это были не атаки, а именно постоянное автоматическое тестирование неизвестными хакерами на наличие уязвимостей в защите периметра. Эти цифры растут с каждым годом. То же самое происходит в обратную сторону: кто-то тестирует слабости американских военных сетей, а американцы тестируют стратегические командные сети других государств аналогичным образом. То есть, противостояние военных и спецслужб государств ведется очень активно, просто оно скрыто от постороннего взгляда и не доходит до точки реального разрушения критической инфраструктуры. В то же время, атаки на компании и государственные сети с целью экономического шпионажа более легко отследить по их последствиям. Уже накануне и во время встречи Барака Обама и Си Цзиньпина международные копании, занимающиеся информационной безопасностью, и эксперты зафиксировали резкое снижение такого рода атак. То есть, уже сейчас, несмотря на отсутствие технического обеспечения, китайско-американская договоренность начала реально влиять на обстановку.

Таким образом осуществляются разные варианты двустороннего сотрудничества между участниками *большого треугольника* Россия-Китай-США, но трехстороненнго взаимодействия здесь пока нет. Почему вообще тогда стоит выделять этот *треугольник*? Почему стоит говорить о нем? Потому что вместе Китай, Россия и США сейчас как участники международного диалога по урегулированию в киберпространстве обладают таким весом, что любое решение и любая норма, которая будет согласована этими тремя государствами сообща станет прецедентом и станет безусловным сигналом для всего международного сообщества. Эти три государства — минимальный достаточный состав игроков для того, чтобы сообща трансформировать весь международно-правовой режим, связанный с поведением в киберпространстве и с международной кибербезопасностью. К сожалению или к счастью, ни Индия, ни Япония, ни Евросоюз столь же влиятельными, столь же необходимыми в этом смысле не являются. В отношении Европейского союза следует сделать оговорку — это не совсем так, когда речь заходит об обеспечении privacy, защиты персональных данных, но по вопросам военной стратегии в киберпространстве трех игроков достаточно.

Таким образом, есть шанс договориться о каких-то критически важных и минимальных нормах поведения в киберпространстве этим узким составом в том

случае, если это не получается сделать более широким составом — например, составом Группы правительственных экспертов. А эффективным посредником, который сглаживает межгосударственные противоречия и разницу в подходах разных государств может выступить частный сектор. Я хочу заострить внимание на том, что в 2015 году радикально выросла активность представителей частного сектора в международных дискуссиях о поведении государств в киберпространстве. Перед вами набор норм, которые в своей публикации весной 2015 года предложила компания *Microsoft*, и я хочу заметить, что это хорошие нормы, заслуживающие обсуждения.

Важно то, что частный сектор действительно имеет право на участие в подобного род дискуссиях. В сентябре этого года на саммите по сотрудничеству в киберпространстве в Нью-Йорке (Global Cyberspace Cooperation Summit) топ-менеджер *Microsoft* заметил, что во многих случаях, связанных с кибероперациями, связанных с использованием в интересах государств продвинутого, сложного, вредоносного программного обеспечения все издержки по ликвидации последствий таких операций в глобальном масштабе нес частный сектор — в том числе, *Microsoft.* Так, именно *Microsoft* пришлось практически на всех соответствующих компьютерах, рабочих станциях в мире переустанавливать програмное обеспечение, чтобы закрыть, залатать уязвимость нулевого дня, которую использовал вирус *Stuxnet.* Такие инциденты стоят *Microsoft* и другим игрокам корпоративного сектора сотни миллионов долларов. Поэтому они действительно являются правомерными участниками этой дискуссии.

Я думаю, что в итоге мы получаем довольно скромную композицию международного диалога. У нас есть члены *большого треугольника*, которые пока сотрудничают друг с другом в двустороннем формате, и есть отдельный участник этого диалога — частный сектор — который способен выступать посредником.

В заключение я хотел бы предложить свое экспертное видение того, о чем и как США, Россия и Китай могли бы попытаться договориться в трехстороннем формате при помощи представителей частного сектора. **Во-первых,** как я уже упоминал очень ценной была бы попытка выработать классификацию объектов критической инфраструктуры и устранить все разногласия в этом. **Во-вторых,** было бы оправданным запустить трехстороннюю инициативу по решению проблемы атрибуции кибератак, то есть, попытаться выяснить, кто стоит за кибератакой, если она проходит через несколько стран, если кибероперация управляется через каскад командных серверов и невозможно в итоге понять, кто стоит в исходной точке, кто является автором. В этом смысле есть особая причина именно для такого состава взаимодействия: Россия, Китай и США. Эти государства обладают очень серьезными техническими компетенциями, высоким уровнем технической экспертизы в сфере расследования, установления авторства кибератак, идентификации субъектов в киберпространстве. Эти же три государства являются источниками очень многих киберинцидентов. Очень многие кибератаки осуществляются предположительно с участием инфраструктуры или лиц, находящихся на территории этих стран. Кроме того, сотрудничество в сфере атрибуции кибератак и их авторов предполагает сотрудничество на уровне национальных Центров реагирования на киберинциденты. Такое взаимодействие было налажено по линии Россия–США, сейчас оно активно налаживается по линии США–Китай, а также по линии Россия–Китай, но от объединения этого взаимодействия в трехстороннем формате польза будет значительно больше. **Наконец,** пожалуй, самой долгосрочной и амбициозной целью для этих государств в киберпространстве мог бы стать выход за рамки договоренностей о совместных мерах защиты инфраструктуры и о мерах легитимной обороны в киберпространстве. Могла бы последовать стадия добровольных переговоров о самоограничении проактивных наступательных кибероперациий. Именно потому, что перед нами три ведущие в военном смысле кибердержавы, и именно потому, что военный потенциал этих кибердержав в значительной степени направлен друг против друга. Здесь я должен оговориться: существует некое представление о том, что Россия и Китай являются в этом смысле идеальными партнерами, не предпринимают друг против друга никаких действий в киберпространстве, но это не совсем так. По крайней мере, от экспертов *Лаборатории Касперского* неоднократно поступала информация о том, что им приходится бороться с китайскими зловредными программами и с постоянными сетевыми атаками, источником которых является Китай.

Итак, каждому участнику этого *треугольника* есть о чем договариваться с другими в этой сфере в том смысле, чтобы ограничить себя в том, как и на кого они могут наападть в киберпространстве.

На этом я хотел бы свои тезисы завершить. Я был бы рад ответить на ваши вопросы, и я думаю, что вопросов здесь может быть больше, чем ответов, которые я дал, но такова ситуация в принципе. Задавайте вопросы, а я попытаюсь на них ответить.

Томаш Зипфел: Я представляю посольство Чешской Республики. Я хотел бы спросить, проявляют ли другие страны активность по теме кибербезопасности, кроме этих трех ключевых игроков? Участвуют ли в переговорах, достигают ли соглашений, предпринимают ли какие-либо другие действия в этой сфере на международной арене? Спасибо.

О. В. Демидов: Целый ряд европейских государств очень активно участвует в диалоге о киберпространстве и кибербезопасности. Они выставляют высочайшие стандарты технического сотрудничества между Центрами реагирования на киберинциденты. Их национальные стратегии по борьбе с киберпреступностью постоянно обновляются, кроме того, они открыты для международных инициатив, международного сотрудничества. Они обмениваются данными для борьбы с киберпреступностью. Российские дипломаты, в том числе, господин Крутских, которого я выше упоминал, утверждают, что не так давно вели переговоры с европейскими странами о киберсотрудничестве, о заключении двусторонних соглашений, аналогичных тому, что было заключено в этой области с США. В числе потенциальных партнеров, если я не ошибаюсь, упоминалась Франция, например. Кроме того, в Европе, в рамках Совета Европы, идет сотрудничество в соответствии с Будапештской конвенцией по киберпреступлениям. А с 2015 года идет работа в рамках ОБСЕ относительно установления мер доверия в киберпространстве.

Что касается других, неевропейских, регионов, в последние годы Индия стала значительным глобальным игроком в сфере киберполитики. В 2013 году был принят меморандум о взаимопонимании в сфере кибербезопасности между Россией и Индией. Правительство Индии продвигает свой подход и свои взгляды в том, что касается политики в информационной сфере, в рамках ООН. Также с 2013 года Бразилия стала активным участником международного диалога. Она предлагает свое видение защиты приватности в Интернете, свои подходы к шифрованию данных. Бразилия в 2013 году поддержала резолюцию Генеральной ассамблеи ООН «Право на приватность в цифровую эпоху», а также выступает на международных конференциях в поддержку справедливого и прозрачного управления интернетом. В настоящее время в Бразилии действует собственный пакет законов, известный как Marco Civil da Internet, регулирующий управление интернетом, защиту персональных данных, кибербезопасность и противодействие киберпреступлениям.

На самом деле, многие государства стали активными участниками диалога по киберпространству, и даже предпринимают упреждающие действия в этой области. Но не всегда достаточно быть просто активно, иногда нужно еще и иметь значительный военный, экономический и технический потенциал в ИКТ-сфере. И

такое сочетание значительных потенциалов мы можем видеть у России, Китая и США.

Нурлан Алькенов: Я представляю посольство Казахстана. Хотел бы поблагодарить Олега за очень полезное выступление. На прошлой неделе я участвовал на научно-практической конференции в Белгороде. Тема этой конференции — «Ограждение молодежи от влияния экстремистской террористической идеологии». Там прозвучал такой тезис: из России за последние годы 1900 молодых людей выехали в Сирию для участия в военных действиях на стороне так называемого ИГИЛ под влиянием различных деструктивных сайтов. Я отмечу, что население Казахстана в десять раз меньше, а у нас уехали около 400 человек, так что для нас это тоже очень актуальная проблема. На конференции также упомянули, что на этих сайтах применяются очень высокие технологии, которые воздействуют на психику людей. Я хотел бы узнать, возможно ли им противостоять, и что делается, чтобы искоренить это явление.

О. В. Демидов: Во-первых, пока на международном уровне отсутствуют эффективные механизмы сотрудничества, которые позволяли бы закрывать сайты, использующиеся экстремистами для вербовки новых сторонников. Существуют некоторые ограниченные по своему охвату механизмы, затрагивающие вопросы контента. Например, если не ошибаюсь, в середине 2000-х годов был принят дополнительный протокол о ресурсах, распространяющих экстремистскую и ксенофобскую информацию, к Конвенции Совета Европы о киберпреступности. Но договориться о понятии расизма и ксенофобии и его криминализации было легче, чем договориться о криминализации и запрещении контента, оправдывающего экстремистскую и террористическую идеологию. Это вопрос трактовок и определений в национальных законодательствах. Я бы не стал исключать, что в случае угрозы, которую вы отметили, в том числе, колоссально возросшей интернет-активности таких структур, как Исламское государство, Совет Европы начнет развивать механизмы конвенции именно в эту сторону. Не знаю, правда, насколько это будет успешно.

Есть другие региональные форматы, в которых меньше разногласий по поводу определения экстремизма и терроризма. Например, это формат ОДКБ, где правоохранительные органы ежегодно проводят совместные операции по выявлению и закрытию сайтов, распространяющих противоправный контент, в том числе, экстремистский. Такие усилия предпринимают в рамках ежегодных операций «Сорняк» и «ПРОКСИ». Но здесь проблема в том, что регионального охвата недостаточно, чтобы эффективно бороться с проблемой. Большинство ресурсов и большинство людей, отвечающих за создание ресурсов, позволяющих экстремистским структурам вести вербовку и распространять свою информацию, находятся вне стран ОДКБ. Поэтому эффективность таких операций сильно ограничена.

Здесь можно было бы пойти двумя путями, причем один не исключает другого. Можно прилагать дипломатические усилия к тому, чтобы соглашения о противодействии распространению экстремистской и террористической информации были приняты в более широких международных рамках, возможно даже на площадке ООН. Второй путь — как можно быстрее и эффективнее создавать подразделения информационной борьбы, которые вели бы контрпропаганду, используя те же самые каналы, например, социальные сети, против вербовщиков Исламского государства.

Вы сказали, что вербовщики экстремистских и террористических структур используют крайне продвинутые сайты для своих целей. Это не совсем так. Они используют очень активный, быстрый функционал: социальные сети, микромессенджеры, сервисы онлайн-обмена видео, стриминга видео. То есть, каналы, во-первых, наиболее востребованы молодежью, во-вторых, позволяющие в течение нескольких секунд распространять любой мультимедийный контент. Это быстрые каналы. Исламское государство просто научилось законам жанра интернет-медиа. Оно научилось создавать и распространять привлекательный шок-контент, делать это адресно — этим и отличается функционал социальных сетей от функционала Web 1.0. Одним только правоохранительным органам, действительно, сложновато с этим бороться, потому что контрпропаганда такому стилю работы требует вовлечения молодежи, изучения целевой аудитории и некоторой изобретательности. Хороший пример, на мой взгляд: в США какие-то ребята сняли смешные ролики, пародирующие Исламское государство, высмеивающие те привлекательные идеи, которые распространители экстремистского контента пытаются доносить до своей аудитории. Высмеять — значить, разрушить.

Повторюсь, такие вещи должны следовать рука об руку с государственной политикой, дипломатическими усилиями для создания механизмов сотрудничества, правовых каналов, для криминализации и уголовного преследования таких людей. Одно не замещает другое.

А. Ф. Зульхарнеев: Известно, что Запад ни в какую не принимал предложения властей Китая по ограничению контента. Есть ли признаки того, что эта ситуация меняет позицию американских или европейских экспертов и официальных лиц в отношении контента?

О. В. Демидов: Спасибо, это очень интересный и непростой вопрос. Я бы сказал, что происходит переосмысление потребностей и приходит понимание необходимости каких-то формально закрепленных совместных усилий по борьбе с явно противоправным, экстремистским контентом. Уже присутствует понимание того, что узких региональных мер и договоренностей будет недостаточно. Придется идти на диалог с теми государствами, которые не обязательно придерживаются тех же подходов. Они понимают, что внутри Евросоюза или внутри ОДКБ, в узких региональных группах, решить этот вопрос не получится. Вместе с тем, конкретного понимания, как продвинуться в этой

сфере, не изменяя собственным принципам — в частности, принципу, который исповедуют государства Европы и США, свободы доступа к информации, свободы распространения информации, свободы высказывания в интернете. Как криминализовать и эффективно преследовать экстремистский и террористический контент, не отступая от этих принципов, пока не совсем понятно. В значительной степени все это скатывается к тому самому проклятому вопросу определений. Чудовищно сложно вывести такое определение экстремистского и террористического контента, которое одновременно бы удовлетворяло правоохранительные органы России, США и ЕС, и при этом никем бы не воспринималось, как посягательство на свободу связи. Я ожидаю, что колоссально возросшая активность идеологов террористических и экстремистских движений в интернете подтолкнет и Россию, и Европу, и США к тому, что преодолеть свои разногласия и засесть за болезненную, кропотливую, долгую работу по выведению таких определений.

Джефри Вальдез: Я представляю экономический отдел посольства Филиппин. Во время презентации я хотел задать вопрос, но ответ на него уже прозвучал — об этом спрашивал представитель Чехии. И ответ заключался в том, что в основном технические возможности реагирования и потенциального ответа на атаки в военном секторе делают Россию, США и Китай *большим треугольником.* Мы видим, что в Соединенных Штатах зарегистрировано большинство провайдером интернета и большая часть сайтов, в Китае — самое большое число пользователей интернета. Россия обладает значительными техническими возможностями, в том числе, военными. Здесь есть какая-то опасность в вопросах об интеллектуальной собственности, контенте? Ведь США и ЕС считают, что вопросы контента должны регулироваться определенным образом.

О. В. Демидов: Спасибо за вопрос. Я соглашусь с тем, что, когда я привожу концепцию *большого треугольника* в киберпространстве, этот треугольник построен, прежде всего, на техническом и на военном потенциале своих трех участников. Если мы будем выстраивать другие проекции *большого треугольника* или другой композиции государств на основе их вклада в производство объектов интеллектуальной собственности или вклада в глобальную интернет-экономику, то состав скорее всего будет другим. Конечно, добавится и вытеснит Россию Европейский союз, а если мы будем говорить о вкладе в разработку программной продукции, сюда добавится Индия. Можно продолжать этот ряд дальше — при каких-то параметрах добавится Япония, при каких-то параметрах выпадет Россия. Но все-таки такой состав *большого треугольника* не случаен, потому что, когда государства говорят о добровольных нормах и правилах поведения, то вопросы согласования и введения этих норма прежде всего упираются в основы международного права. В частности, в Устав ООН. Там первоочередную роль играет оценка таких понятий, как силовой потенциал, применение силы, вооруженное нападение — то, что отсылает нас к техническому и военному потенциалу, необходимости его оценки, интерпретации и ограничения применительно к киберпространству. То, в чем эти три государства занимают ведущие позиции.