Oleg Demidov
Project Coordinator, International Information Security and Global Internet Governance
12-12-05
Cyber Seminar Summary – October 31

Краткое изложение выступлений участников семинара ПИР-Центра «Информационно-коммуникационные технологии в контексте международной безопасности: поиск общих подходов» (Москва, 31 октября 2012 г.)

Приветственное слово и открывающие комментарии (М.В Якушев, Председатель Совета, ПИР-Центр; Дэнис Киф, Министр-советник, Заместитель Посла Её Величества, Посольство Великобритании в Российской Федерации)

Семинар открыл приветственным словом **Председатель Совета ПИР-Центра М.В.Якушев**, подчеркнувший, что в зале присутствуют ключевые в России эксперты по вопросам кибербезопасности и информационной безопасности. Мероприятие призвано помочь найти экспертные решения для конкретных и остро стоящих в России сегодня вопросов, связанных с киберпространством и кибербезопасностью, в том числе:

- Сближение подходов РФ и ее партнеров по вопросам международной информационной безопасности и кибербезопасности: в чем состоят ключевые противоречия и как их преодолеть?
- Укрепление мер доверия в киберпространстве: перспективные задачи для России и зарубежных партнеров.
- Международное сотрудничество в области борьбы с киберпреступностью: приоритеты России и интересы партнеров.

Заместитель Посла Её Величества в Российской Федерации Дэнис Киф в своей приветственной речи подчеркнул важность расширения международного сотрудничества в области киберпространства. Заместитель Посла отметил, что ответственность за управление киберпространством лежит на правительстве, представителях бизнеса и гражданском обществе. Господин Киф также изложил принципы сотрудничества правительств в киберпространстве, выдвинутые министром иностранных дел Великобритании Уильямом Хейгом на Лондонской конференции по вопросам киберпространства, которая прошла в ноябре 2011 г. Эти принципы, в частности, заключаются в необходимости расширения доступа к киберпространству, включая продвижение инноваций и свободы слова в Сети, защите прав граждан на конфиденциальную информацию, преодолению угроз киберпреступности и кибератак. Ключевой принцип сотрудничества в киберпространстве состоит в том, что одни лишь правительства не могут брать на себя эту задачу в отрыве от частного сектора и общественности – а значит, не могут и единолично регулировать и перекраивать киберпространство. ПИР-Центр делает очень правильное и позитивное дело, организуя обсуждение вопроса о сближении подходов между РФ и ее партнерами с участием экспертов IT-отрасли и «мозговых трестов».

Продолжая вступительное слово, **М.В. Якушев** отметил, что огромный интерес к проектам ПИР-Центра в области информационной безопасности и управления интернетом проявляют российские госструктуры, в том числе МИД РФ в лице Специального представителя Президента РФ по вопросам международного сотрудничества в борьбе с терроризмом и транснациональной организованной преступностью А.В. Змеевского. М.В. Якушев также подчеркнул, что важной особенностью семинара является то, что в его рамках проводится презентация тематического номера ИБ №1(104) 2013, посвященного вопросам МИБ и ГУИ. Журнал предлагает практически беспрецедентное для русскоязычных изданий по широте охвата рассмотрение проблем в названной области.

Первая сессия: Российский подход к обеспечению международной информационной безопасности: национальные интересы и глобальная повестка дня
(Модератор: Председатель Совета ПИР-Центра М.В.Якушев
Докладчики: директор Департамента международного сотрудничества Минкомсвязи РФ А.Ю. Муханов;
Директор Координационного центра национального домена сети Интернет А.В. Колесников)

Первая сессия открывала семинар с содержательной точки зрения, т.к. предыдущие выступления в значительной степени носили протокольно-приветственный характер. В целом, выступления и дискуссия в рамках сессии имели акцент на рассмотрение общих принципов и императивов российского подхода, причем по широкому спектру вопросов, в который попали не только проблемы информационной безопасности, но и де-факто вопросы глобального управления интернетом, поднятые представителями МИД в контексте декабрьской конференции МСЭ в Дубае.

Сессию открывало выступление директора Департамента международного сотрудничества Минкомсвязи РФ **А.Ю. Муханова**. Как отметил г-н Муханов, семинар ПИР-Центра оказался актуален прежде всего в связи с приближением дубайских событий, которые могут либо «потрясти мир», либо надолго закрепить статус-кво, причем повестка Дубая может и должна рассматриваться именно в рамках проблематики информационной безопасности. Термин кибербезопасность, как было, отмечено, имеет право на жизнь в качестве обиходного понятия, но МИБ научнее, правильнее и уместнее на официально-дипломатическом уровне. Кибербезопасность следует рассматривать просто как органическую составную часть МИБ. А.Ю. Муханов отметил, что различные страны слишком в разной степени продвинулись в освоении киберпространства в тех или иных целях; и сегодня то, что США «заказывают музыку», уже не совсем справедливо. Нужны некие общие договоренности и подходы. Россия через МИД и Минкомсвязи предлагает комплексный подход, который увязывает воедино вопросы МИБ и ГУИ и нацелен на то, чтобы «информационные технологии не использовались против интересов безопасности государств» и не подрывали суверенные права государств. По словам г-на Муханова, Правила поведения в области обеспечения МИБ и концепция Конвенции об обеспечении

МИБ, суммирующие российский подход, не являются жесткой международно-правовой «офертой» - это гибкие предложения к диалогу всем странам, база для дальнейшей работы. На сегодня прогресс по ним тормозится по ряду направлений, в том числе – в плане доверия в сфере экономических транзакций в интернете (риски безопасности в сфере интернет-торговли). А.Ю. Муханов также затронул вопрос борьбы с глобальной киберпреступностью и кибератаками, отметив, что эффективный потенциал противодействия им заложен в российской концепции Конвенции о обеспечении МИБ. Но при этом нужно иметь виду проблему атрибуции - нельзя допустить, чтобы за действия отдельных хакеров страдали государства. Минкомсвязи также принимает участие в разработке соглашения о сотрудничестве стран СНГ в области обеспечения МИБ. Российские госорганы, включая Минкомсвязи сейчас активно продвигают на ряде площадок (ООН, АТЭС, СНГ, ШОС) вопросы МИБ; на острие повестки – в том числе создание систем совместного мониторинга киберугроз и интернационализация управления интернетом на базе площадки МСЭ. Но никто не собирается приватизировать ICANN – таких целей нет.

Комментируя выступления Дэниса Кифа и А.Ю.Муханова, М.В.Якушев отметил обозначившиеся терминологические шероховатости - неполное соответствие терминов «internet governance» и «управление интернетом» и сложность перевода на русский понятия «multistakeholderism». Слова влияют на концепции, которые отстаивают Россия и ее партнеры.

Следующий спикер, директор КЦ НДСИ **А.В.Колесников**, сделал акцент на том, как Координационный центр относится к российской позиции по МИБ и ГУИ, насколько привлекается к ее формированию. По словам А.В.Колесникова, интернет-сектор сегодня приносит России уже более 4% ВВП и стал наиболее быстрорастущим крупным сегментом национальной экономики, что нельзя не учитывать при выработки политик его регулирования на национальном и международном уровнях. Если говорить о МИБ, то необходим учетов интересов лидеров отрасли – таких гигантов как *Mail.Ru, Yandex* и т.д. В этой связи правомерен вопрос, отражает ли выбор РФ в вопросах МИБ таких партнеров как Таджикистан и Узбекистан интересы национального ИТ-сектора? Аудитория Рунета - 50 млн. россиян и 50 млн. носителей языка за рубежом, но узбеки и таджики нам ничего не дают в этом плане – ни денег, ни укрепления глобальных позиций Рунета. Интересы российского интернет-бизнеса – в Европе. А еще есть глобальная интернет-торговля, императив которой – сокращение барьеров и границ, и это надо поддерживать.

Второй важный вопрос – терминология. В РФ не прижились понятия киберугроз и кибербезопасности, но они куда понятнее и конкретнее с технической и практической точки зрения – по сравнению с расплывчатым понятием информационной безопасности. Например, оборот киберпреступности в РФ достигает сегодня 4 млрд. долл., и киберкриминал уже способен подкупать госструктуры, что крайне опасно. Давайте акцентировать российский подход и на эту проблему, это важно – и это именно *кибер*преступность. Еще один принципиальный момент – Россия традиционно занимает реактивно-

оборонительную позицию в борьбе с кибервызовами. К примеру, РФ вступает в коалицию с партнерами в Средней Азии и с КНР для того, чтобы противостоять неким угрозам, реагировать на них. С точки зрения А.В. Колесникова, интернет являет собой среду, которая не приемлет оборонительного подхода. России необходимо действовать в этой области проактивно. Нельзя занимать круговую оборону против кого-либо – необходимо наступать, разрабатывая собственные кибертехнологии и иные разработки в информационной сфере при серьезном бюджетном финансировании и внимании государственных органов. Нужна российская DARPA, по примеру подходов США, Великобритании и других стран. Западные страны исповедуют прагматичный подход – они развивают проекты, отвечающие их собственным интересам, что правильно – РФ следует поступать так же вместо попыток запретить все и вся.

Сессию продолжил комментарий **Э.В. Чернухина**, первого секретаря-помощника начальника ДНВ МИД РФ. Как отметил представитель МИД, ДНВ активно сотрудничает с частными структурами в вопросах МИБ – включая *Group-IB* и *Лабораторию Касперского*, по таким темам как кибератаки, киберпреступность. Тема вообще очень востребована, министр С.В.Лавров часто поднимает ее на совещаниях. МИД с интересом воспринял октябрьскую инициативу министра иностранных дел Великобритании Уильяма Хейга по созданию Глобального центра киберугроз в Великобритании, сюжет будет внимательно отслеживаться. По поводу позиции РФ в области МИБ и киберпреступности – рост возможностей ИКТ ведет к росту угроз, в ближайшем будущем эта тенденция необратима, с этим никто не спорит. Проблема МИБ комплексна, ее нельзя решать, дробя на отдельные сегменты – хотя российский подход признает ее многогранность, выделяя триаду угроз информационного терроризма, преступности и военно-политического характера, причем одна легко перетекает в другую в зависимости от целей и масштаба. Один из важных шагов в практическом продвижении российского подхода – Екатеринбургское соглашение ШОС от 19 июня 2009 г.. Но центральной площадкой для РФ остается ООН, через которую продвигается идея разработки универсального документа, кодифицирующего киберпространство.

Краткий комментарий также сделал координатор проекта ПИР-Центра **О.В. Демидов,** изложив идею возможного использования опыта строительства режима ядерного нераспространения и контроля над ОМУ применительно к киберпространству. Первый урок, который можно извлечь из этого опыта – формирование международного режима никогда не начинается с глобальных всеобъемлющих механизмов. Консенсус между ключевыми игроками изначально возникает по весьма узким и наиболее острым вопросам; постепенно набор точечных соглашений формирует «каркас» для всеобъемлющего режима – но режим безопасности киберпространства еще не прошел эту стадию. Второй урок – каждый элемент международного режима безопасности должен быть обеспечен инструментами имплементации и (применительно к нормам контроля) верификации, что отсутствует применительно к концепции Конвенции о МИБ. Именно по этим причинам инициативы РФ и стран ШОС буксуют.

Вопросы и ответы, дискуссия:

Вопрос М.В.Якушева к Э.В.Чернухину:

Какие аргументы приводит РФ своим западным партнерам в пользу включения вопросов мер доверия и обеспечения безопасности в области использования ИКТ в международно-правовые соглашения?

Отвечая на вопрос, Э.В.Чернухин отметил, что мнения РФ и ее партнеров – западных и не только, - на самом деле, в основном сходятся по вопросам противодействия киберпреступности и кибертерроризму. Кроме того, комментатор выразил несогласие с тезисом О.В. Демидова, что международное сообщество находится на самом начальном отрезке в плане формирования режима МИБ, подчеркнув наличие обширного пласта международного гуманитарного права, который может быть применим в киберпространстве. Вопрос в том, как 192 государствам мира развивать международное сотрудничество в сфере МИБ, при отсутствии адекватной международно-правовой базы. Будапештская Конвенция пытается закрыть пробел в части киберпреступности, но, во-первых, не может претендовать на роль глобального механизма, во-вторых, она серьезно устарела. Все это лишний раз подтверждает востребованность инициатив РФ.

Вопрос М.В.Якушева к А.Ю. Муханову и А.В. Колесникову:

Насколько российские внутренние, национальные нормы, а также практика их применения в части противодействия киберпреступности и расследования кибератак соответствует потребностям самой РФ и международно-правовым нормам в этой сфере?

Ответ А.Ю.Муханова:

Вопросы в большой степени взаимосвязаны; например, в РФ международное законодательство обладает приоритетом над национальными правовыми нормами. Поэтому, МИД по крайней мере в части внутриведомственных норм ориентируется прежде всего на международные документы в области связи и телекоммуникаций, так что одно без другого невозможно. Кроме того, выполнение российских законов в части противодействия киберугрозам также ориентировано на международные нормы и стандарты с учетом трансграничных последствий угроз в этой области.

Ответ А.В.Колесникова: РФ не хватает, к примеру, перенятия международных норм, криминализирующих спам. Большинство мировых *спам-баронов* родом из России, особенно те из них, кто зарабатывает миллионы долларов на фармацевтическом спаме – что является уголовным преступлением в законодательстве США, Канады и ряда других стран. Преступники пользуются в тем, что в РФ нет закона, криминализирующего из деятельность, и остаются недосягаемы для зарубежного правосудия, находясь в России.

Вторая сессия: Диалог России с ключевыми партнерами по вопросам киберпространства: укрепление доверия, борьба с киберпреступностью и кибертерроризмом
(Модератор: Директор Координационного центра национального домена сети Интернет А.В. Колесников
Докладчики: Председатель Совета ПИР-Центра М.В. Якушев;
советник Секретариата ОДКБ В.О. Шушин;
генеральный директор Group-IB И.К. Сачков)

Сессию открыло выступление **М.В.Якушева** на тему укреплению доверия в киберпространстве. Докладчик отметил специфику современных киберугроз, а именно их глобальные последствия, трансграничный характер, комплексное воздействие на многие сферы жизни и отсутствие консенсуса по поводу противодействия им на международном уровне. Более того, темпы развития ИКТ обуславливают быстрое устаревание мер противодействия киберугрозам. Есть проблемы подмены фундаментальных подходов соображениями текущей политической целесообразности, а также отсутствие согласия по поводу баланса между обеспечением международной безопасности и соблюдением прав человека. Какие решения и меры просматриваются? Во-первых, совершенно очевидна необходимость ГЧП в вопросах обеспечения МИБ. Реальный пример сегодня действующее с 2011 г. партнерство ИМПАКТ-МСЭ, в рамках которого *Лаборатория Касперского* выявила и обезвредила в ближневосточных сетях вирусы *Flame, Gauss* и др. РФ в отличие от 144 стран мира не является участником партнерства, хотя это сулит нам явные преимущества. Еще одна область, требующая действий – регулирование голосового интернет-трафика. Пример – ситуация со *Skype*, который ФСБ потребовала запретить в 2011 г., и это не только российская проблема. Здесь вряд ли нужен отдельный международный акт, скорее востребованы нормы *мягкого права*.

Следующая область, требующая скорейшей проработки - идентификация в социальных сетях. Опять же, нормы международного права могли бы быть удобны, однако нельзя ущемлять права пользователей. Необходимое условие для разрешения этих вопросов – следование принципу мультистейкхолдеризма., причем нужно очень четко отличать этот механизм от многосторонней дипломатии, электронной демократии и т.д. Кроме того, надо различать вопросы политической дискуссии и практические вопросы, которые не надо политизировать. Развивать международно-правовое регулирование, однако, нужно прямо сейчас; самое главное - избежать конфронтации на политическом уровне, чем сейчас грешит российский МИД. Дискуссия о том, что лучше - ICANN или МСЭ, - неверна в принципе – организации просто предназначены для выполнения разных функций. Проводя аналогии с МИБ, уместно сослаться на опыт регулирования космической деятельности – прошло 50 лет, а единого договора нет, и все работает на основе ряда точечных соглашений. Возможно, в ООН имеет смысл создать комитет по использованию интернета по аналогии с Комитетом по использованию космического пространства в мирных целях. В

целом, развитие ИКТ и диалог международного сообщества в целом достигли той стадии, когда возможно развитие практических механизмов.

Сессию продолжил доклад советника Секретариата ОДКБ **В.О. Шушина** на тему роли ОДКБ в борьбе с киберпреступностью в региональном формате. Организация начинала проработку этой тематики с нуля, не опираясь на какую-либо готовую правовую базу; принципиальное решение было принято в 2006 г. В 2008 г. была подписана Комплексная программа о формировании системы информационной безопасности ОДКБ, включающая отдельное соглашение о борьбе с преступлениями в информационной сфере. В рамках реализации были созданы специальные подразделения полиции. Помимо киберпреступности ИКТ активно используются и для раскачивания ситуации в различных странах и регионах, что несет угрозу и странам ОДКБ; поэтому сегодня подготовлен проект Концепции коллективной безопасности ОДКБ с очень высоким приоритетом МИБ.

Специфической проблемой в этой сфере для Организации стало то, что по вопросам МИБ ни у одной из ее стран нет единого целевого ведомства – повестка размазана по десяткам структур и органов; в итоге непонятно, с кем следует говорить. Решением стало подписание в 2010 г. Положения о сотрудничестве в области ИБ в развитие Программы 2008 г. В результате, в странах-членах Организации определены национальные координирующее органы по этим вопросам, создана рабочая группа по информационной политике и информационной безопасности при Комитете секретарей Советов безопасности. Кроме того, еще с 2009 г. ОДКБ проводятся ежегодные операции ПРОКСИ, нацеленные на выявление и пресечение преступной деятельности в информационном пространстве стран Организации. Региональные проблемы не могут ждать достижения глобальных договоренностей, поэтому ОДКБ действует сейчас.

Последним из докладчиков в рамках сессии выступал генеральный директор Group-IB **И.К.Сачков**, осветивший вопросы борьбы с киберпреступностью в РФ в свете глобальной составляющей этой проблематики. В РФ 80% компьютерных преступлений с особо крупными суммами ущерба расследуют эксперты Group-IB, поэтому уровень осведомленности о ситуации очень высок. В 2010 г. рынок российской киберпреступности составил 1,3 млрд. долл., в 2011 г. – уже 2,3 млрд., а русский рынок, включающий жителей и выходцев из СНГ - уже 4,5 млрд. долл.; включая суммы фактического прямого ущерба и объем нелегальных услуг на рынке. По большей части преступники оставались безнаказанными, т.к. в российском законодательстве имеется ряд пробелов и уловок, не устраненных даже последними изменениями УК РФ в декабре 2011 г. В сочетании со сверхприбылями это служит мощным стимулом для роста рынка, который вырос до размеров рынка каннабиатов или рынка оружия, и многие криминальные элементы перетекают в него из других ниш. Программисты крупных преступных групп в РФ получают до 35 тыс. долл. в месяц.

Кроме того, в России есть ситуация *гонки вооружений* – государство и частный сектор ежегодно вкладывают огромные средства в системы защиты, но это не работает, так как хромает главное – привлечение киберпреступников к ответственности. Еще одна проблема – мягкость и толерантность общественного мнения к киберкриминалу; параллельно с этим – необъяснимо мягкие приговоры: частой практикой стали условные сроки за кражу миллионов долларов. Бурно растущий сегмент рынка – мошенничество в сфере электронного банкинга; объем платежей растет в России на 200% в год, киберпреступная ниша растет соответствующими темпами. Раньше российские киберпреступники воровали деньги на Западе, теперь «вернулись» в Россию. В этом году *Group-IB* помогла арестовать несколько крупных групп киберпреступников и их участники могут получить реальные сроки. Члены этих групп – поголовно долларовые миллионеры возрастом в среднем 23-25 лет. В 2012 г. с участием *Group-IB* впервые реализованы уголовные дела по фишингу. О международной стороне вопроса: необходимо укрепление международного сотрудничества, т.к. есть трансграничный аспект проблематики, но в ряде стран, правовой аппарат хуже, чем в России, надо развивать международно-правовые механизмы. Помимо этого, требуется ужесточение уголовной ответственности и выправление массового сознания в отношении киберпреступников, искоренение толерантности к ним.

После выступлений спикеров слово перешло к комментаторам, начиная с программного директора «Инфофорума-2012» **Е.К. Волчинской**. Возвращаясь к вопросам первой сессии, г-жа Волчинская подчеркнула, что российские инициативы в сфере МИБ и ГУИ своевременны, и «ничего не вырастет само» из локальных или двусторонних соглашений. Аналогии с опытом режима ядерного нераспространения и даже с космосом в данном случае неуместны, так как ИКТ имеют принципиально иную природу – и в их использование вовлечено совсем иное количество акторов. Для охвата этой реальности необходимо изменение существующих механизмов международного права, и российские инициативы должны стать «кузницей» для выработки таких новых механизмов. При этом не надо конфронтационных акцентов – например, не нужно предлагать что-то как *альтернативу* Будапештской конвенции. Она была неплоха и выполнила свою роль – но концептуально устарела, нужна не альтернатива ей, а следующий уровень и поколение правовых механизмов.

Есть вопрос терминологии – она не состыкована в договорах и документах различных международных структур; более того, вопросы вызывает практика рассмотрения терроризма и экстремизма в информационном пространстве отдельно от вопросов информационной преступности – ведь терроризм и экстремизм также являются преступлениями. Есть вообще опасная тенденция выделять все новые виды информационных преступлений. На деле, сегодня речь идет зачастую об обычных преступлениях, но совершаемых посредством или при помощи ИКТ – если обособлять их все как информационные преступления, половину международного законодательства можно выбрасывать; на самом деле, нужна адаптация имеющихся норм к реалиям информационных угроз. Е.К. Волчинская также отметила, что акцент на военный аспект проблемы МИБ в

российских инициативах оправдан – соответствующие императивы равным образом прописаны в документах НАТО, США и т.д. Мы не можем ждать, пока что-то вызреет само по себе, иначе будем полностью не готовы к использованию против нас «информационного оружия». Другое дело, что наша политика в сфере МИБ куда внятнее и адекватнее на международном уровне, чем на национальном. На национальном уровне это повестка не обеспечена ни доктринально, ни кадрово, ни концептуально что необходимо срочно исправлять.

С комментарием также выступил **член Совета НДСИ М.А.Медриш**, отметив, что российский подход, возможно, выиграл бы от изменения философии – от *борьбы с* угрозами к *борьбе за* укрепление интернет-экономики, расширение информационного общества и т.д. *вопреки* тем факторам, которые этому позитиву мешают. Речь идет не просто о перестановке слов - такая смена акцентов повлекла бы и пересмотр приоритетов финансирования, включая расширения финансирования образования в сфере кибербезопасности и информационной безопасности, начиная со школьного уровня и т.д. Надо переходить от реактивного действия к проактивному, прежде всего в образовании. Законодательство объективно всегда будет запаздывать по сравнению с бурным развитием ИКТ – но ведь есть *best practices* разных стран, например, сообщества CERT – негосударственные площадки, которые действуют и работают. Возможно, именно содействие государств таким механизмам стоит вынести в центральную тему очередных переговоров по МИБ.

По терминологии: понятие «информационной безопасности» очень неудачно, так как ссылается на морально устаревшую Доктрину информационной безопасности от 2000 г., которая не отвечает сегодняшним реалиям. Кибербезопасность - это нечто другое, ее рамки четко очерчены проблематикой компьютерных сетей. Если мы будем и далее говорить на разных языках, мы будем лишь меньше понимать друг друга, поэтому целесообразнее изменить российскую терминологию и перейти к более четкой и распространенной терминологии кибербезопасности. Наконец, России необходима стратегия кибербезопасности, а также поправки в Стратегию национальной безопасности, которая полностью опускает эту проблематику.

Отвечая на комментарий М.А.Медриша, **Е.К. Волчинская** отметила, что важны на термины, а общее понимание их содержания. Сегодня даже западные страны включают в понятие кибербезопасности вопросы контента, чего не было прежде, тем самым приближая смысл этого термина к «информационной безопасности» в российской трактовке. Если договориться о включении вопросов контента в оба термина, мы сможем придти к их общему согласованному пониманию. До этого момента переходить к использованию терминологии кибербезопасности нецелесообразно.

С комментарием также выступил Советник по правовым вопросам Посольства США в РФ **Люк Дембоски**, работавший в США федеральным прокурором по расследованию компьютерных преступлений. По мнению г-на Дембоски, одной

из проблем, которая выявилась в ходе дискуссии, является отсутствие четкого разведения в национальном и, возможно, международном масштабе, «обычных» компьютерных преступлений, преследующих цели обогащения, и действий, направленных непосредственно против национальной безопасности. Если эти понятия не отделять друг от друга, государственный *Левиафан* будет тормозить сотрудничество по всем направлениям, насаждая проблематику защиты национальной безопасности. Нельзя согласиться с российским тезисом о неразделимом характере триады угроз террористического, криминального и военно-политического характера. Если киберпреступность помещается в рамки дискурса национальной безопасности, то вместо сотрудничества происходит «задраивание люков», а киберпреступники остаются безнаказанными. Для успешного развития интернета и национальных экономик эти сегменты проблемы должны быть четко разведены.

Далее стороны перешли к дискуссии.
Вопрос М.В. Якушева Люку Дембоски:

Как «разводить» киберпреступность и вопросы национальной безопасности в реальности, если, к примеру, группа хакеров крадет деньги из банка, затем за вознаграждение атакует сетевые ресурсы политической оппозиции, а после по заказы устраивает кибератаку на ресурсы другого государства? Ведь это одни и те же люди, которые используют примерно одни и те же средства.

Реакция Е.К.Волчинской на вопрос М.В.Якушева:

Сама деятельность различается по целям и по объектам, но методы противодействия и расследования все равно практически одинаковы, так что на каком уровне их стоит «разводить» на практике, действительно неясно.

Ответ Люка Дембоски:

В США используется совершенно разное законодательство для расследования и ведения дел, связанных с «обычной» киберпреступностью, и инцидентов, которые представляют угрозу для национальной безопасности. В связи с этим проблема «разведения» типа деструктивного действия в киберпространстве не стоит так остро, как в России.