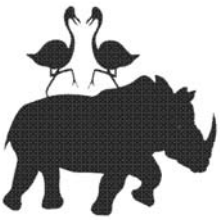

Джейми Сондерс:

КАК ИЗБЕЖАТЬ ЭСКАЛАЦИИ КОНФЛИКТОВ В КИБЕРПРОСТРАНСТВЕ?

Необходимы ли изменения российской концепции Конвенции ООН об обеспечении международной информационной безопасности? Возможно ли сегодня создание всеобъемлющего международно-правового режима безопасности киберпространства? Может ли Будапештская конвенция о киберпреступности рассматриваться в качестве потенциальной основы для глобального режима сотрудничества в борьбе с киберпреступностью? Какие терминологические и концептуальные обновления необходимо внести в текст Конвенции Совета Европы, чтобы адаптировать ее к текущей ситуации в области трансграничной киберпреступности? Каковы основные пункты в повестке дня британского МИД в части укрепления международного сотрудничества по вопросам безопасности киберпространства?

Джейми Сондерс, директор по вопросам международной политики в киберпространстве Министерства иностранных дел и по делам Содружества Великобритании, ответил на вопросы корреспондента журнала Индекс Безопасности.

ИНДЕКС БЕЗОПАСНОСТИ: Как Вы оцениваете российскую концепцию Конвенции ООН об обеспечении международной информационной безопасности, которая была представлена на Лондонской конференции по киберпространству в ноябре 2011 г.? Какие изменения необходимо внести в российский проект документа, чтобы он стал прочной основой для дальнейших дискуссий и переговоров о будущем режиме международной безопасности в киберпространстве?

СОНДЕРС: Во-первых, я бы хотел сказать, что мы приветствуем сам факт заинтересованности России в диалоге по данным вопросам. Россия активно участвует в работе Группы правительственных экспертов ООН по анализу ситуации в сфере информации и телекоммуникаций в контексте международной безопасности. Как Вы отметили, российское предложение было представлено год назад на Лондонской конференции по киберпространству, и я ожидаю в этом году двусторонних российско-британских обсуждений, которые были намечены министрами иностранных дел двух стран в мае 2012 г.

Мне кажется, основную озабоченность у нас вызывает вопрос о том, не является ли на данный момент преждевременным само предложение о принятии международного юридически обязывающего документа — это первое. Вторая область, которая вызывает у нас озабоченность — как подходить к решению данных проблем и как избежать эскалации конфликтов в киберпространстве. Нам необходимо найти способ привлечь к данной работе не только правительства, но и саму IT-индустрию, а также гражданское общество, поскольку у всех этих игроков существует серьезная заинтересованность в решении обозначенных вопросов. Они также могут вне-

сти очень важный вклад в плане укрепления доверия, обмена информацией, в том числе в кризисных ситуациях, и в других вопросах.

ИНДЕКС БЕЗОПАСНОСТИ: Не считаете ли Вы, что пришло время для установления юридически обязывающего режима в области информационной безопасности? Ведь мир уже столкнулся с целым рядом деструктивных вирусных атак (*Stuxnet, Flame*, *Duqu*), которые нанесли физический ущерб ключевым объектам инфраструктуры в таких странах, как Иран.

СОНДЕРС: Мы, безусловно, полагаем, что нормы международного права применимы к киберпространству. Я думаю, дальнейшие дискуссии должны сконцентрироваться на вопросе о том, нужны ли нам какие-то новые инструменты, или, может быть, задача состоит в более эффективном применении уже существующих международно-правовых документов (к примеру, законов о ведении вооруженных конфликтов) для решения проблемы кибератак. Я уверен, что существующие механизмы международного права релевантны таким задачам. Поэтому вопрос заключается в том, следует ли нам вести переговоры о создании новых инструментов или сконцентрироваться на более эффективном использовании уже существующих. Мы отдаем предпочтение именно второму варианту.

ИНДЕКС БЕЗОПАСНОСТИ: Может ли Будапештская конвенция о киберпреступности рассматриваться в качестве потенциальной основы для глобального режима сотрудничества в борьбе с киберпреступностью? Какие терминологические и концептуальные обновления необходимо внести в текст Конвенции, чтобы адаптировать ее к текущей ситуации в области трансграничной киберпреступности?

СОНДЕРС: Во-первых, очень важно, чтобы в государствах по всему миру существовало современное законодательство в области противодействия киберпреступности. Во-вторых, необходимы механизмы, обеспечивающие международное сотрудничество в борьбе с компьютерными преступлениями. Мне кажется, большинство государств согласятся с такой постановкой вопроса. На наш взгляд, в Будапештской конвенции даны четкие ответы на вопрос о том, как государствам необходимо действовать. Мы продолжаем поддерживать этот документ и рассматриваем его как хороший образец того, на каких принципах должно основываться качественное национальное законодательство в сфере борьбы с киберпреступностью.

Конечно, Конвенция была принята более 10 лет назад и, согласно распространенному сегодня мнению, нуждается в определенном обновлении. На самом деле механизм для такого обновления заложен в самом тексте Конвенции — а именно в Статье 44. На сей момент никаких обновлений текст конвенции не претерпел. С моей точки зрения, если мы считаем необходимым вносить изменения и поправки в текст Конвенции, нам следует сделать их настолько технологически нейтральными, насколько это вообще возможно. Аналогичный процесс происходит на уровне национального законодательства по борьбе с киберпреступностью — но чем более всеобщим является правовой документ, тем более он долговечен. Хотя, на мой взгляд, очень важен сам факт наличия механизма обновления Будапештской конвенции, притом что такой механизм прописан в Статье 44 самой конвенции, любопытно, что Великобритания до последнего времени не обнаруживала потребности в использовании этого механизма.

ИНДЕКС БЕЗОПАСНОСТИ: Существуют ли какие-то другие потенциальные документы или инициативы, которые, могли бы заменить Будапештскую конвенцию в качестве основы глобального режима по борьбе с киберпреступностью? Способна ли российская глобальная инициатива по борьбе с киберпреступностью, которая может быть обнародована в ближайшее время, заменить собой Будапештскую конвенцию?

СОНДЕРС: Я думаю, важно само содержание Будапештской конвенции, то есть те ее положения, которые обеспечивают основу заложенного в ней механизма трансграничного сотрудничества. Любые будущие предложения в данной сфере будут рассматриваться в сопоставлении с этим базовым уровнем, поэтому если какая-

либо новая инициатива не будет содержать определенных положений, которые на данный момент отсутствуют в Конвенции, но важны с нашей точки зрения, нам будет очень трудно поддерживать такую инициативу. Другими словами, мы рассматриваем Будапештскую конвенцию в качестве действующего стандарта международного сотрудничества по борьбе с киберпреступностью.

Естественно, если будет предложено всеобъемлющее соглашение или другой инструмент, который предложит востребованные на сегодня нормы и более эффективные меры сотрудничества по сравнению с Будапештской конвенцией, мы поддержим такой инструмент. Именно в этом состоит ключевой вопрос: если новые предложения способны предоставить более эффективные механизмы по сравнению с уже имеющейся конвенцией, мы всерьез будем их рассматривать. Если же они попросту не дотягивают до уровня существующих положений Конвенции, у нас возникнут серьезные вопросы в их отношении.

Хочу подчеркнуть, что мы не считаем Будапештскую конвенцию совершенным документом. В этой области есть еще над чем работать, и именно с этой точки зрения мы будем рассматривать все новые инициативы. Хотелось бы также добавить, что между Россией и Западом существует не так уж много противоречий касательно того, как добиться желаемого результата в области борьбы с киберпреступностью на международном уровне. Однако я полагаю, что соглашение с Россией должно содержать акцент на совершенствование системы международного сотрудничества по борьбе с киберпреступностью и обеспечивать соответствующую среду для поддержания стабильности всего киберпространства. Не думаю, что у нас есть какие-то фундаментальные разногласия по поводу того, какими мы видим желаемые плоды нашего сотрудничества.

ИНДЕКС БЕЗОПАСНОСТИ: Камнем преткновения между Россией и ее западными партнерами при обсуждении проблем киберпространства являются существенные терминологические и концептуальные расхождения. Российские эксперты предпочитают вести речь об *информационной безопасности*, а не о *кибербезопасности.* Какой из этих двух подходов Вам представляется более рациональным для целей международного регулирования киберпространства? Есть ли шансы на то, что российская концепция информационной безопасности будет понята и принята на Западе, в частности в Великобритании?

СОНДЕРС: Здесь нужно различать два отдельных аспекта. Первый аспект — это вопрос языка и терминологии. Я согласен с тем, что этот аспект уже привнес определенные трудности, способные затормозить развитие международного диалога. Я думаю, чтобы добиться определенного прогресса, нам — то есть Великобритании, России и другим игрокам — нужно четко объяснить друг другу то значение, которое мы вкладываем в наши определения и термины. Конечно, здесь также существуют определенные трудности перевода, так что нужно постараться прийти к единому набору определений и терминологии.

В данный момент нам часто приходится лишь догадываться о том, что же на самом деле имеет в виду наш партнер. Чем более четко мы сможем объяснить смысл наших идей и предложений, тем меньше мы будем зацикливаться на терминах и тем лучше мы сможем понять глубинный смысл этих предложений. Не думаю, что нам удастся выработать общий набор определений и терминов в краткосрочной перспективе — но мы можем, по крайней мере, понять, какой смысл мы вкладываем в разные термины. Это поможет нам определить, где именно между нами на самом деле существуют разногласия, а где каждый из нас просто не до конца понимает, о чем ведет речь партнер.

Нужно, однако, отметить, что за разной терминологией иногда скрываются и реальные разногласия. Это, в частности, касается предлагаемой тематики международной дискуссии по вопросу безопасности. Если британские политики и эксперты не истолковали превратно смысл российской фразеологии, можно утверждать, что термин *информационная безопасность*, который широко используется рос-

сийской стороной, включает само по себе информационное наполнение коммуникаций. Поэтому основной вопрос в рамках международного диалога на эту тему сводится к тому, что российский подход предполагает такие ограничения свободы слова в киберпространстве, которые, на наш взгляд, противоречат обязательствам, взятым на себя обеими нашими странами в рамках Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах. Эти документы подписали и Великобритания, и Россия. Поэтому важно понять смысл, который мы вкладываем в используемые термины, и постараться определить, действительно ли мы говорим о различающихся подходах, или все дело в том, что мы неправильно поняли друг друга. При этом не следует преуменьшать различия в наших взглядах, которые на самом деле существуют — особенно это касается вопроса информационного наполнения коммуникаций.

ИНДЕКС БЕЗОПАСНОСТИ: Считает ли британское правительство новые крайне сложные виды вредоносных программ типа *Stuxnet* и *Flame* угрозой национальной безопасности? Какие шаги предпринимает британский МИД для продвижения дискуссии по данной проблеме на международном уровне?

СОНДЕРС: Во-первых, Вы отдельно выделили в своем вопросе вирусы *Stuxnet* и *Flame.* Я бы не сказал, что мы считаем именно эти киберинструменты отдельной угрозой для нашей национальной безопасности. Но мы осознаем, что вредоносные программы в целом представляют собой угрозу, или потенциальную угрозу, и в этом смысле их можно воспринимать как угрозу национальной безопасности. Современные вредоносные программы действительно способны нанести весьма существенный ущерб критическим объектам национальной инфраструктуры. Великобритания пока не сталкивалась с вирусами типа *Stuxnet* или *Flame*, нацеленными конкретно против ее систем и объектов. Но это не отменяет того факта, что вредоносные программы могут нанести серьезный ущерб нашей критической инфраструктуре. Мы хорошо осознаем этот факт.

Что касается необходимых мер реагирования на такие угрозы, то мы, естественно, очень активно участвуем в работе Группы правительственных экспертов ООН по вопросам безопасности в киберпространстве. Мы также поддерживаем деятельность в этом направлении в рамках ОБСЕ и Регионального форума АСЕАН (АРФ). Что касается мер по укреплению доверия, мы считаем, что это очень важная и нужная тема для межправительственных дискуссий. С моей точки зрения, перед нами стоит общая цель: предотвратить наращивание разрушительного потенциала вредоносных программ и не допустить нанесения ущерба критической национальной инфраструктуре.

Наконец, стоит также упомянуть, что мы принимали проведенную в 2011 г. Лондонскую конференцию по киберпространству. Один из основных вопросов, обсуждавшихся на конференции, касался именно угрозы, которую представляют собой разрушительные вредоносные программы для наших критических объектов и систем. Данный вопрос вновь был вынесен в повестку Будапештской конференции по киберпространству (4–5 октября 2012 г.), равно как и всех основных мероприятий в области кибербезопасности, запланированных на будущий 2013 г. Я не утверждаю, что это единственная проблема, заслуживающая серьезного рассмотрения, но ее важно обсуждать именно на уровне правительств, чтобы привлечь к этим вопросам внимание политического руководства наших стран.

ИНДЕКС БЕЗОПАСНОСТИ: Вы отметили, что вредоносные программы считаются серьезной угрозой для критической национальной инфраструктуры. Какие сегменты этой инфраструктуры наиболее уязвимы? Энергосети, банковские информационные системы или какие-либо иные объекты?

СОНДЕРС: Это очень сложный вопрос, в котором сочетаются два аспекта: степень уязвимости самих систем и роль этих систем в обеспечении общественных процессов. Поэтому невозможно составить какой-то список наиболее уязвимых или наиболее важных сегментов критической национальной инфраструктуры.

Но очевидно, что есть определенные сегменты, в том числе электрические сети и энергосистемы, системы обеспечения страны продовольствием, которые требуют наиболее прочных гарантий того, что система обладает должным уровнем безопасности и надежно защищена. Мы анализируем состояние нашей критической инфраструктуры по отдельным секторам, чтобы определить, где существует наибольшая вероятность возникновения проблем и где перед нами стоят самые сложные задачи. Я также считаю, что важно не пытаться рассматривать киберугрозы в отрыве от всех остальных угроз. Нам нужно защищать такие системы, как электросети, от широкого спектра угроз — как стихийного, так и техногенного характера, как компьютерных, так и всех остальных. Поэтому мы стремимся к целостному и всестороннему анализу ситуации.

ИНДЕКС БЕЗОПАСНОСТИ: Когда речь идет о массированных и хорошо спланированных кибератаках, ключевой проблемой является анонимность их авторов. Подвергались ли британские правительственные компьютерные сети таким атакам и удавалось ли определить их источник? Обвиняло ли когда-либо британское правительство какие-либо конкретные государства в том, что они несут прямую ответственность за кибератаки?

СОНДЕРС: Во-первых, Великобритания, как и многие другие страны, регулярно подвергается попыткам вторжения в ее компьютерные сети. Я полагаю, что ранее уже звучали конкретные цифры, характеризующие атаки на сети государственного сектора — сети некоторых ведомств подвергались тысячам атак. Так что, как видите, объем вредоносной сетевой деятельности весьма велик, и определить, кто стоит за такими атаками, трудно, однако эта задача не является принципиально невыполнимой. Пока что мы решили не обвинять какие-либо конкретные страны в том, что они несут ответственность за кибератаки. На официальном уровне мы таких публичных заявлений не делаем. Однако нужно понимать, что если мы имеем основания подозревать какую-либо страну в подобной деятельности, то у нас есть право предпринять ответные меры, в соответствии с нашими правами и обязанностями, закрепленными в международном праве. Если мы полагаем, что наши системы подверглись нападению, то мы, естественно, предпринимаем соответствующие шаги.

ИНДЕКС БЕЗОПАСНОСТИ: Входят ли в число таких ответных шагов дипломатические или военные меры?

СОНДЕРС: Реагирование будет происходить на самых разных уровнях и, естественно, будет включать определенные шаги на дипломатической арене. Наша реакция на кибернападение не будет ограничиваться лишь принятием каких-либо технических мер, направленных на устранение уязвимости компьютерных систем. Речь будет идти и о других ответных мерах, в том числе дипломатического характера, если это будет целесообразно.

ИНДЕКС БЕЗОПАСНОСТИ: Каковы основные пункты в повестке дня британского МИД в части укрепления международного сотрудничества по вопросам международной информационной безопасности? Планирует ли сама Великобритания в ближайшее время представлять какие-то новые глобальные инициативы или перспективные стратегии в данной сфере?

СОНДЕРС: Я бы хотел особо отметить два момента в данном случае. Первый из них состоит в том, что, с моей точки зрения, необходимо проделать большую работу над повышением уровня информированности общественности и конкретных социальных групп по поводу проблем, связанных с киберпространством. Такая работа, в частности, должна вестись на высшем уровне государственного руководства и бизнеса, а также среди гражданского общества в различных странах. Естественным сегментом целевой аудитории являются бизнес-лидеры по всему миру. Все мы хорошо понимаем, что столкнулись с серьезной угрозой в данной области. Как я уже упоминал, наша прошлогодняя конференция в Лондоне стала практической площадкой для отработки подобного подхода. Мы регулярно обсуж-

даем эту проблему с партнерами, чтобы повысить их информированность о ситуации, предложить им свою помощь и т. д. На самом деле такой стране, как Великобритания, есть что сказать своим партнерам во всем мире, чтобы подтолкнуть их к осознанию того, что киберугрозы представляют собой серьезный вызов и этот вызов необходимо сдерживать сообща.

Второе направление, которому мы уделяем внимание, включает передачу уже накопленных нами опыта и знаний другим странам, с тем чтобы помочь им в развитии собственного потенциала в данной области. Мы уже финансируем целый ряд инициатив, в рамках которых передаем другим странам не только финансовые средства, но и собственный опыт. Однако мы считаем, что должны делать в данном направлении еще больше, поэтому в сентябре-октябре 2012 г. нам предстоит провести анализ того, какой дополнительный вклад мы можем внести в программы по развитию собственного национального потенциала других стран, как сделать эти масштабные программы укрепления потенциала борьбы с киберугрозами более эффективными. Для нас также важно удостовериться в том, что мы оказываем необходимое влияние на глобальную повестку в области укрепления потенциала противодействия киберугрозам.

ИНДЕКС БЕЗОПАСНОСТИ: Существуют ли у Великобритании какие-либо конкретные региональные приоритеты в международном сотрудничестве по укреплению кибербезопасности?

СОНДЕРС: Выделить подобные приоритеты непросто, поскольку различные сценарии в регионах требуют разных шагов и подходов. Естественно, высшим приоритетом для нас является обеспечение безопасности *наших собственных* информационных систем. Однако мы также уделяем значительное внимание тем странам, которые больше всего нуждаются в нашей помощи. Некоторые из них — и здесь я, в частности, привожу тот случай, когда мы выделяем финансирование на программы в данной области — расположены в Юго-Восточной Европе, и мы сотрудничаем с ними через механизмы Евросоюза. Мы также финансируем работу Совета Европы по оказанию содействия тем странам, которые стремятся укреплять свое национальное законодательство в области кибербезопасности. Мы поддерживаем работу в рамках Содружества наций, направленную на укрепление потенциала и расширения возможностей правоприменительной практики применительно к сфере кибербезопасности. Но это лишь начало, и нам предстоит сделать намного больше, в том числе предпринимать более энергичные усилия именно в тех областях, где они способны принести максимальную отдачу, на которую мы рассчитываем. Нас, в частности, беспокоит, что ведется довольно много различных программ, которые не приносят ожидаемых результатов.

Я бы также хотел вернуться к Вашему предыдущему вопросу относительно международных обсуждений на тему законов и глобальных соглашений в области кибербезопасности. Такие обсуждения уже ведутся, однако есть еще одна область, играющая важную роль в развитии международного сотрудничества в данной сфере. Речь идет об укреплении доверия, повышении прозрачности и подобных мерах, которые создают благоприятный климат для международного сотрудничества в борьбе с общими киберугрозами.

ИНДЕКС БЕЗОПАСНОСТИ: Каковы ключевые приоритеты британского МИД в сфере сотрудничества с Россией по вопросам кибербезопасности?

СОНДЕРС: Во-первых, мы весьма искренне приветствуем участие в этих дискуссиях российских неправительственных организаций, а также российского бизнеса. Мы считаем, что их роль и вклад очень важны. Мне кажется, чем больше мы говорим друг с другом и чем шире круг совместно обсуждаемых проблем и сюжетов, тем больше вероятность того, что нам удастся найти точки соприкосновения и добиться прогресса. И я надеюсь, что ПИР-Центр воспримет этот посыл как всестороннюю поддержку своей работы в рамках проекта по информационной безопасности и управлению интернетом.