**ПЕТЕРБУРГСКИЙ МЕЖДУНАРОДНЫЙ ЭКОНОМИЧЕСКИЙ ФОРУМ**

**18–20 июня 2015**

# ПОСТРОЕНИЕ ЭФФЕКТИВНЫХ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ

**Арена**

**18 июня 2015 — 17:00–18:15, Мерседес Бар**

**Санкт-Петербург, Россия**

**2015**

**Модератор:**

**Сергей Плуготаренко**, Директор, «Ассоциация электронных коммуникаций» (НП «РАЭК»)

**Выступающие:**

**Эхуд Барак**, Премьер-министр Израиля (1999—2001 гг.)

**Фредерик Донк**, Региональный директор по Европе, The Internet Society

**Александр Жаров**, Руководитель, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (Роскомнадзор)

**Анджела Маккей**, Директор по вопросам политики и стратегии кибербезопасности в группе глобальной стратегии и дипломатии по безопасности, Microsoft

**Николай Никифоров**, Министр связи и массовых коммуникаций Российской Федерации

**Илья Сачков**, Основатель, генеральный директор, «Group-IB»

**Хоулинь Чжао**, Генеральный секретарь, Международный союз электросвязи (МСЭ)

**Светлана Шамзон**, Вице-президент, ЗАО «Компания ТрансТелеКом»

**Участники дискуссии в первом ряду:**

**Константин Долгов**, Уполномоченный Министерства иностранных дел Российской Федерации по вопросам прав человека, демократии и верховенства права

**Андрей Семериков**, Генеральный директор, АО «ЭР-Телеком Холдинг»

**С. Плуготаренко:**

Уважаемые коллеги, дамы и господа, мы можем начинать, поскольку у нас собрался полный состав докладчиков. Сессию мы ведем на русском языке. Те, кому требуется перевод, могут воспользоваться системой синхронного перевода.

Уважаемые дамы и господа, коллеги, представители экспертного сообщества, органов государственной власти, международные эксперты, представители бизнеса и общественных организаций! Я рад приветствовать всех вас на сегодняшнем мероприятии — на панели, которая называется «Построение эффективных систем кибербезопасности» и которая проходит в первый день Петербургского международного экономического форума здесь, в «Ленэкспо», в городе Санкт-Петербурге. Дополнительная расшифровка названия сессии, предложенная нами, звучит так: «Ожидание прорыва в вопросах кибербезопасности. Технологии, инновации и решения». Я призываю всех участников панели, тех, кто находится на сцене, в зале, всех, кто может подключаться к нашей дискуссии, мыслить в терминах этого самого прорыва. Есть представление, что мы сейчас находимся в точке принципиального фазового сдвига, перехода. Следующим этапом должен случиться некий прорыв, надеюсь, что в хорошем смысле.

Позвольте представиться. Меня зовут Сергей Плуготаренко, я директор российской «Ассоциации электронных коммуникаций». Наша организация работает на российском рынке с 2006 года и объединяет крупнейших игроков российской интернет-отрасли. Мы занимаем достаточно серьезные позиции в области экспертизы, аналитики, проведения собственных мероприятий и уделяем большое значение вопросам информационной безопасности и кибербезопасности. Целое направление внутри нашей ассоциации посвящено этим вопросам. Это подразделение является одним

из старейших эффективных образований, оно называется Комиссия по информационной безопасности и киберпреступности.

Среди спикеров сегодняшней панели — признанные эксперты международного и российского уровня, представляющие бизнес-сегмент, государство и общественные организации. Мы считаем, что состав нашей панели «крутой», мы сможем обсудить все вопросы за те час и пятнадцать минут, которые нам отвели организаторы, и постараемся сделать выводы по итогам сегодняшнего обсуждения.

Теперь о самой сути нашей сегодняшней панели. По данным Международного союза электросвязи, в мире сегодня насчитывается более трех миллиардов пользователей. При этом мы знаем, что доля активных, ежедневных пользователей растет и приближается к 70—80% от всех пользователей. Также растет и доля мобильных пользователей. Это новые вызовы, новые технологические тренды, которые мы сегодня наблюдаем. Интернет действительно стал доступным, вездесущим, незаменимым и незаметным. Об этом говорит факт проникновения Интернета в зону карманной доступности: сегодня он с нами дома, на работе и там, где мы даже не представляем.

При этом Интернет оказывает заметное воздействие и на офлайн. По данным нашей Ассоциации, только в России экосистема интернет-зависимых рынков уже составляет 10% от ВВП Российской Федерации. Постоянная динамика роста составляет 15—20% в год, и этот рост значительно больше офлайн-экономик. Наша ассоциация практикует экономический подход, связанный с оценкой угроз или, наоборот, возможностей, которые кибербезопасность несет нашей индустрии.

Такое мощное проникновение Интернета позволяет говорить о том, что кибербезопасность выходит на первые позиции в вопросах разработки национальных доктрин, корпоративных практик и, что немаловажно, в области пользовательской безопасности. Недавно Региональным

общественным центром интернет-технологий был предложен термин digital nation, или «цифровое гражданство». Он активно приживается и, как нам кажется, включает в себя гораздо больше, чем просто медиаграмотность или цифровая грамотность.

Сегодня кибербезопасность выходит на первый план и во многих офлайн-средах, таких как медицина, здравоохранение, экология, общественная безопасность, борьба с терроризмом. Нельзя не остановиться на последних разоблачениях, которые, как мы все понимаем, наверняка пошатнули веру пользователей в то, что их жизнь является приватной и что в Интернете все безопасно. Мы даже проводили ряд сессий на собственных недавних конференциях по кибербезопасности с хештегом «после Сноудена», и всем сразу становилось понятно о чем речь, не нужно было даже дополнительно что-то объяснять.

Если сегодня разные государства, разные нации вкладывают разные понятия в термин безопасности и кибербезопасности и не всегда могут договориться о том, какие общие подходы следует применять, то бизнес и общество, как нам кажется, могут договориться гораздо быстрее — у них больше точек соприкосновения. Я предлагаю нам делать акцент ровно на том, где мы можем сотрудничать, и постараться в ходе сессии ответить на некоторые вопросы, которые я на всякий случай обозначу. Естественно, можно от них отклоняться.

Вопрос первый: каков оптимальный баланс между профилактическими мерами безопасности на уровне государства и ответственностью частного сектора, между защитой персональных данных и безопасностью государства?

Второй вопрос: какие стратегии кибербезопасности в бизнесе и на государственном уровне наиболее успешны сегодня?

Третий: почему международное сотрудничество в вопросах киберугроз является обязательным условием успеха в борьбе с киберпреступностью, и почему мы хотим сделать на это ставку?

Пара слов о структуре сессии. Она будет разбита на три блока. В первом блоке прозвучит детальный обзорный доклад всех современных трендов в области кибербезопасности от руководителя Роскомнадзора Александра Александровича Жарова. Он расскажет про экономические показатели, статистику, частную и государственную информационную безопасность и про опыт Роскомнадзора. Во втором блоке я предоставлю слово всем спикерам для небольших пятиминутных выступлений, посвященных тем темам, в которых эти спикеры являются признанными экспертами. В третьем блоке, если у нас останется время, мы подключим представителей из зала к этакой Q&A-сессии. И резюмирует работу сегодняшней сессии министр связи и массовых коммуникаций Российской Федерации Николай Анатольевич Никифоров.

Кстати, я хотел бы, чтобы именно Николай Анатольевич выступил с коротким приветственным словом и задал тон сегодняшней дискуссии.

Николай Анатольевич, Вам слово.

**Н. Никифоров:**

Сергей, большое спасибо.

Уважаемые коллеги, дорогие друзья, я хотел бы поприветствовать вас на Санкт-Петербургском международном экономическом форуме. Сергей сказал, что у нас «крутая» панель. Я считаю, что она «суперкрутая» — здесь действительно много экспертов. Но я всё же хотел бы отдельно отметить присутствие и на Форуме, и на нашей секции генерального секретаря Международного союза электросвязи господина Хоулинь Чжао. Давайте его поприветствуем.

Многие в зале знают, что такое МСЭ (Международный союз электросвязи), или ITU, как эту организацию называют в англоязычном мире. Применительно к кибербезопасности мне вспомнилось мероприятие на площадке ITU, на котором мы обсуждали очень насущные вопросы. Это было в Дубае в 2012 году. Господин Чжао тогда работал заместителем генерального секретаря Международного союза электросвязи. Это была первая попытка публичной дискуссии по вопросу о том, что же такое Интернет, является ли он частью регламента электросвязи.

Мы все привыкли к классической связи — электросвязи, телефонам, и мы достаточно уверены в надежности их работы. Но мы совершенно не задумываемся над тем, насколько безопасна существующая Сеть с точки зрения надежности ее функционирования. Уже после этого мы все стали свидетелями разоблачений Сноудена. Кстати, любопытно, что на пленарной сессии прошлогоднего Санкт-Петербургского форума Президенту нашей страны пришлось комментировать очень многие обстоятельства, связанные с тем, как господин Сноуден оказался в России. После этого Российская Федерация столкнулась с беспрецедентными, на наш взгляд, фактами удаления доменов физических и юридических лиц, зарегистрированных в Крыму, под воздействием политических санкций. После этого мы проводили учения, связанные с надежностью функционирования российского сегмента сети Интернет, и намерены продолжать проводить эти учения каждый год.

Мы считаем, что кибербезопасность действительно присутствует в самых разных аспектах. И конечно, она трансгранична. Участие уважаемых спикеров в нашей сегодняшней дискуссии позволяет нам рассматривать этот важнейший вопрос в международном аспекте. Мы считаем, что различные страны мира, в том числе страны БРИКС (а Россия в этом году является председательствующей страной в БРИКС), действительно уделяют ему должное внимание. Наши страны разделяют опасения,

касающиеся защиты прав и свобод в Интернете, касающиеся стабильности работы самого Интернета, находящегося под управлением юрисдикции фактически одной страны, и касающиеся защиты персональных данных и соблюдения национального законодательства разных стран. Бессмысленно отрицать, что, несмотря на трансграничность Интернета, на территории каждой страны все-таки действует национальное законодательство, которое невозможно игнорировать и нельзя не уважать. Мы знаем ситуации, когда игнорирование и неуважение национального законодательства, равно как и исторических, культурных аспектов, приводило даже к гибели людей. Все эти истории очень свежи в нашей памяти.

Я считаю, что тема дискуссии и уровень участников чрезвычайно высоки, и не хотел бы отнимать время у господина Жарова, который представит детальный доклад. Пусть и остальные максимально компактно выскажут свои конкретные предложения относительно того, как нам нужно развивать ситуацию как с точки зрения и национального регулирования, так и в плане международной кооперации.

Большое спасибо.

**С. Плуготаренко:**

Спасибо, Николай Анатольевич.

Александр Александрович, теперь Ваша презентация, которую я бы назвал «Киберпреступность и кибербезопасность. Современное состояние». Пожалуйста.

**А. Жаров:**

Спасибо, господин председатель.

Господин Хоулинь Чжао, господин министр, дамы и господа, рад приветствовать вас на Санкт-Петербургском экономическом форуме.

Сегодня мы говорим о глобальной проблеме, поскольку живем в информационном обществе. Вопрос кибербезопасности и информационной безопасности настолько объемен и многогранен, что все аспекты охватить невозможно. Я постараюсь остановиться на основных из них.

Если еще несколько лет назад эти проблемы обсуждались на специализированных форумах интернет-специалистов и специалистов в области кибербезопасности, то сегодня мы должны констатировать, что кибербезопасность перестала быть проблемой, которая беспокоит только специалистов. Это проблема национальная, транснациональная, глобальная. Сообщения в СМИ о различных инцидентах, которые касаются вопросов кибербезопасности, так же часты, как прогнозы погоды. Эти инциденты сказываются на деятельности крупнейших транснациональных корпораций, оказывают влияние на принятие политических решений правительствами ряда государств. За последний год практически все сферы экономики во всем мире пострадали от киберугроз того или иного рода.

Поскольку на Петербургском международном экономическом форуме принято оценивать масштаб различных проблем в деньгах, приведу несколько цифр. По оценке PricewaterhouseCoopers, темп роста числа инцидентов в сфере информационной безопасности в мире опережают темп роста ВВП, и даже такого динамичного показателя, как рост количества смартфонов, приобретаемых населением. По итогам 2014 года он составляет 48%. Для сравнения, темп роста ВВП в номинальном выражении по итогам 2014 года всего 3,3%, а прирост приобретения смартфонов составил 22%.

Согласно исследованию компании Gartner, результаты которого были опубликованы в *The Wall Street Journal*, в 2014 году расходы на защиту от киберугроз в мире выросли на 7,9% и составили 71 миллиард долларов США. Прогноз на 2015 год — рост еще на 8,2%, в абсолютных цифрах —

более 77 миллиардов долларов США. Финансовые последствия инцидентов в сфере информационной безопасности также растут. Кроме прямого ущерба они могут включать в себя снижение доходов, сбои в работе бизнес-систем, штрафные санкции со стороны контролирующих органов и сокращение числа клиентов.

Кибербезопасность сегодня — это сфера притяжения масштабных инвестиций. Мы являемся свидетелями значительного притока венчурного капитала в компании, специализирующиеся на информационной безопасности, а также на предоставлении услуг в этой области. Лидеры этого рынка в последние годы организовали успешные IPO, нарастили капитализацию до миллиардов долларов. По данным исследований «Экономика Рунета», которые ежегодно проводятся российской «Ассоциацией электронных коммуникаций», которую возглавляет наш сегодняшний председатель Сергей Плуготаренко, в 2014 году связанные с Интернетом сегменты рынка в России оценивались совокупной цифрой пять триллионов рублей, или 8,2% ВВП России. Из них 1,3% ВВП — это чистая интернет-экономика, а 6,9% — отрасли, зависимые от киберпространства и, соответственно, зависимые от киберугроз.

В кибербезопасность в нашей стране активно инвестируют фонды и институты развития, такие как Фонд развития интернет-инициатив, Агентство стратегических инвестиций, «Российская венчурная компания», а также корпоративные и частные инвесторы. На пике бума венчурного финансирования стоимость некоторых компаний, занимающихся информационной безопасностью, в 5—10 раз превышала их годовой доход. Правда, по оценке PricewaterhouseCoopers, в последние месяцы 2014 года эти показатели демонстрировали тенденцию к снижению. Но никто не сомневается, что рынок программных средств, решений и услуг в сфере информационной безопасности будет только расти. Панацеи от этой беды нет, и очевидно, что угрозы требуют защиты.

Параллельно правительства и парламенты большинства развитых государств мира разрабатывают и воплощают в жизнь законодательные и нормативные требования, соответствующие современному уровню рисков и угроз, которые информационно-коммуникационное пространство продуцирует для государства, общества, бизнеса и гражданина.

Общемировые условия, в которых на текущий момент развивается рынок кибербезопасности, можно описать тремя характеристиками. Это усиление рисков, активизация участников рынка и ужесточение законодательных и нормативных требований в большинстве стран мира.

Россия не может оставаться в стороне от глобальных процессов в сфере обеспечения информационной и кибербезопасности. В последние несколько лет российская власть уделяет самое серьезное внимание этому вопросу. Государственной Думой был разработан и принят ряд законов, которые стали основой системы государственного регулирования процессов, происходящих в информационно-коммуникационном пространстве, в частности, в сети Интернет.

Регулирование Интернета в России началось с защиты от киберугроз самой незащищенной части населения — наших детей. Уровень вовлеченности современных детей и подростков в информационное общество абсолютен. Недаром их называют «поколением большого пальца», потому что именно большим пальцем они управляют тачпадами своих гаджетов. И в значительной степени гаджеты и информационное пространство им если не заменяют, то дополняют школу, семью и компанию сверстников. Это не плохо и не хорошо — это реальность сегодняшнего дня.

Риски и угрозы, с которыми сталкиваются дети в Интернете, имеют для них крайне нездоровые и разрушительные последствия. Поэтому они не могут оставаться вне зоны внимания родителей, педагогов и государства. Речь идет о сексуальном насилии в отношении детей, стимулированным распространением в Интернете детской порнографии, вовлечении

подростков в употребление наркотиков, различных формах виртуальной агрессии, которая все чаще становится причиной подростковых самоубийств и других негативных явлений.

Вы знаете, что в России в 2012 году и в последующие годы был принят комплекс законов, нацеленных на защиту детей от негативной информации. По новым законам, некоторые виды разрушительной информации, такие как детская порнография, призывы к употреблению и распространению наркотиков, призывы к самоубийству, были запрещены к распространению в Российской Федерации. Должен сказать, что законодатели в данном случае не изобретали велосипед, а интегрировали в российскую правовую систему те нормы, которые уже успешно применялись в других странах.

Вот несколько примеров. В Великобритании на уровне оператора связи или провайдера хостинга применяется блокирование доступа к сайтам, содержащим непристойные изображения несовершеннолетних, а также криминальный и разжигающий расовую ненависть контент. В США действует Федеральная комиссия по связи, которая осуществляет фильтрацию информации непристойного и порнографического характера, а также материалов, вредных для несовершеннолетних. Во Франции и в Германии, как и в Российской Федерации, ведут черные списки интернет-ресурсов и материалов. Стоит отметить, что фильтрация трафика во Франции находится под юрисдикцией правоохранительных и судебных органов, в Германии действует соглашение «Добровольный самоконтроль для мультимедийных сервис-провайдеров», что подразумевает самостоятельную фильтрацию трафика интернет-провайдерами.

В России в качестве уполномоченного органа по ведению Единого реестра запрещенной информации определен Роскомнадзор. Как я уже сказал, в этот реестр вносятся страницы сайтов, содержащих, по мнению экспертов, запрещенную к распространению информацию — детскую порнографию,

информацию о суициде и наркотиках. Кроме того, в него может вноситься информация, признанная запрещенной по решению судов.

Механизм достаточно прост. Мы уведомляем администрацию ресурса или хостинг-провайдера о том, что данная информация должна быть удалена, и ждем три дня. Если информация не удаляется, то ресурс выгружается через Реестр запрещенной информации более чем 4,5 тысячам операторам связи, предоставляющим доступ в Интернет гражданам Российской Федерации, и информация блокируется.

Я не буду углубляться в эту тему, она предельно публичная, о ней много писали и пишут в СМИ и она представлена в Интернете достаточно широко. Цифры вы можете увидеть на слайде: к нам на горячую линию Реестра запрещенной информации поступило более 188 тысяч обращений, более чем по 30% из них информация была признано запрещенной. Подавляющее большинство — это сайты-наркоторговцы, и мы их эффективно блокируем.

Когда закон вступал в силу, со стороны интернет-сообщества были самые апокалиптические ожидания: якобы из-за досудебного принятия решений будут блокироваться добропорядочные ресурсы и что государство будет использовать его для запрещения политической информации. Эти прогнозы не оправдались. У нас четко блокируются три темы, о которых я сказал, а постоянно заблокированными остаются порядка 14% ресурсов. В подавляющем большинстве это сайты-наркоторговцы или иной бизнес, который по своей сути абсолютно криминален.

Парадоксальная ситуация: введение досудебной блокировки сайтов привело к активизации правоохранительных органов и судов. За этот период было инициировано достаточное количество судебных процессов. На слайде вы видите, что за два года показатель внесения в реестр запрещенной информации по решению судов увеличился фактически в три раза.

Если мы обратимся к следующему слайду, то увидим специфику этой информации. Это экстремистские материалы (почти две тысячи судебных решений), заблокировано более четырех тысяч страниц интернет-казино (почти тысяча решений), две тысячи URL-страниц и так далее. Пропаганда проституции, пропаганда наркотиков, информация о даче взяток, способы производства взрывчатых веществ — в общем, самая разнообразная негативная информация. Из этого слайда можно сделать вывод, что Единый реестр запрещенной информации в сочетании с широким применением судами правовых норм, связанных с законодательным ограничением на доступ к противоправной информации в Интернете, постепенно становится универсальным инструментом противодействия и профилактики правонарушений в России, а уж в Сети — совершенно точно.

Уважаемые коллеги, необходимо помнить, что за удобством, простотой, скоростью и легкостью использования информационных технологий скрывается обратная сторона медали. Зачастую пользователю приходится жертвовать такими понятиями, как приватность, неприкосновенность частной жизни, личная и семейная тайна, деловая репутация. Персональные данные — часть личного пространства любого человека. Именно на защиту этого пространства и направлены усилия Роскомнадзора как уполномоченного органа по защите прав субъектов персональных данных.

Основными киберугрозами в Сети в контексте защиты прав субъектов персональных данных являются: распространение сведений, порочащих честь, достоинство и деловую репутацию; нарушение неприкосновенности частной жизни, личной или семейной тайны и тайны переписки; несанкционированное и непрозрачное для пользователей использование личной информации для аккумулирования массива больших данных для изучения корпорациями потребительских предпочтений людей. Для многих людей эти моменты звучат абсолютно абстрактно, кажутся чем-то далеким

от реальности. Сегодня модно говорить о том, что Интернет нивелировал понятие неприкосновенности частной жизни, что Интернет — это свободная среда, его нельзя регулировать и контролировать, но ровно до тех пор, пока конкретные люди не сталкиваются с вполне конкретными последствиями киберугроз. Тогда они начинают искать защиты. В 2014 году мы получили 20 тысяч обращений граждан России с жалобами на нарушение их прав как субъектов персональных данных, которые были загружены в интернет-сети. Потребность граждан в защите растет ежегодно минимум в два раза, и, безусловно, эта цифра будет и дальше расти.

Я остановлюсь подробнее на некоторых последствиях киберугроз, которые сказываются на личном пространстве гражданина. Это, во-первых, монетизация пользователей сети, когда пользовательское внимание становится товаром особого рода, что находит свое отражение не только в новых моделях таргетированной рекламы, приобретающей все более адресный характер. Это касается и случаев воровства клиентских баз и их продажи недобросовестным коммерческим структурам.

Во-вторых, это агрессивный маркетинг. Навязчивые рекламные сообщения, как назойливые насекомые, находят всё новые и новые способы проникать через всевозможные антиспам-фильтры и заполнять собой пространство наших персональных коммуникаций: электронную почту, SMS- и MMS-сообщения, сервисы личных сообщений и текстовые мессенджеры.

Они не только засоряют это пространство. Зачастую они являются способом мошеннического отъема денег, когда автоматическое списание денег со счета происходит в момент открытия сообщения или в результате неосознаваемой абонентом активации каких-либо функций гаджета, которые дают доступ к его электронным кошелькам.

Использование персональных данных для совершения уголовно наказуемых преступлений — это, наверное, самая тяжелая часть. Незаконное владение и использование сугубо персональных данных и

информации оставляют широкий простор для совершения различных уголовно наказуемых деяний. Это и шантаж, и мошенничество, и грабеж, и даже убийство. Например, в прошлом году в Роскомнадзор массово поступали обращения от девушек, которые, надеясь получить позиции в индустрии красоты, участвовали в пикантных сессиях и обнаружили свои фотографии совсем на других ресурсах, которые предлагали интим-услуги и где были выложены их фотографии, сопровождавшиеся полным набором персональных данных. Более того, администраторы этих сервисов предлагали девушкам удалить эти фотографии за определенное вознаграждение. Нам удалось по решению суда эти сервисы заблокировать, но это лишь один из примеров распространенной истории.

Четвертое — это доведение до самоубийства. Это касается в основном подростков. Вы знаете, что появилось такое понятие, как кибербуллинг, или агрессия в виртуальной среде. На подростка оказывается психологическое воздействие со стороны его сверстников, которые заставляют его совершать унизительные действия, которые снимаются и публично выкладываются в сеть. Такие действия могут, в конечном итоге, привести к самоубийству.

Пятое — это репутационные риски, бесконтрольное распространение персональных данных, когда фотографии, фамилия, имя и отчество, точное место жительства сопровождаются ложной информацией, порочащей честь, достоинство и деловую репутацию.

И отдельно стоящая тема — это манипулирование общественным мнением, когда авторитет отдельных публичных личностей используется для придания значимости конструируемому мнению в продвижении какого-либо товара или с целью опорочить эту публичную личность. Публичность граждан и открытость тех или иных сведений о них не должны восприниматься свободными для любого способа использования информации. Данная информация может быть использована любым

способом, но только или субъектом персональных данных, или исключительно для достижения общественно значимых целей.

Новелла последнего времени — это персональные кибератаки. Дело в том, что Интернет вещей — это реальность сегодняшнего дня. Существует экосистема устройств, таких как холодильники, чайники и иные устройства, и они абсолютно не защищены. И реальностью сегодняшнего дня становится проникновение хакеров внутрь таких устройств. Ладно, когда это чайник. Но они сами описывают в интернете случаи, когда удавалось проникнуть в компьютерную систему автомобиля и перехватить управление автомобилем или самолетом. Один их хакеров произвел и описал в интернете эксперимент, в котором он смог проникнуть в программное обеспечение кардиостимулятора, смог отключить его и даже вызвать разряд в 850 Вольт, который, безусловно, убил бы человека с таким устройством в груди.

Зачастую целью хакеров является не атака на вещи, но атака с помощью этих вещей, создание ботнетов-вещей. Буквально несколько дней назад один из моих знакомых, руководитель крупнейшей корпорации, рассказал мне о сильнейшей атаке — пожалуй, самой сильной за последние несколько лет. Когда его специалисты по компьютерной безопасности ее отражали, они начали разбираться и выяснили, что она велась с ботнета, созданного с помощью холодильника. Это серьезная история, поскольку количество таких устройств огромно, и организовать из них ботнет — не такая сложная задача для специалиста. Это серьезный вызов сегодняшнего дня.

Вернемся к персональным данным. Следует сказать, что мы двигаемся в этом вопросе в европейском фарватере. Наш Закон «О персональных данных» был полностью написан на основании Конвенции Совета Европы №108. Сейчас мы внимательно наблюдаем за изменениями в европейском законодательстве и будем думать о том, как модифицировать наше

законодательство о персональных данных, чтобы оставаться в этой европейской экосреде по защите персональных данных.

Еще одна тема. Сейчас идет достаточно широкая дискуссия вокруг законопроекта о праве на забвение. Я с удовлетворением отметил, прочитав сегодняшние СМИ, что диалог между депутатами, авторами этого закона, и интернет-отраслью активизировался. Безусловно, граждане имеют право на защиту своего личного пространства. Но безусловно и то, что интернет-компании, работающие в области поиска и сбора информации, должны иметь адекватный инструмент для того, чтобы этот закон работал. Закон нужен. Уверен, что обе стороны друг друга слушают и слышат, и финальный вариант будет приемлем и для государства, и для граждан страны, и для интернет-компаний.

Следует сказать, что на почве информационной безопасности и защиты от киберугроз запускается очень важный процесс — диалог внутри отрасли. Поскольку тема очень многогранная, я не коснулся ряда вопросов, таких как страшные вирусы-трояны типа Stuxnet. Я уверен, что руководитель Group-IB об этом скажет. Проблема трансгранична и настолько глобальна, что только объединение усилий всех участников процесса может привести к результату.

Думаю, что на этом я закончу, благодарю за внимание. Прошу прощения, если я о чем-то не упомянул.

**С. Плуготаренко:**

Александр Александрович, большое спасибо. Доклад действительно получился всеобъемлющим, хотя отмечу, что ряд аспектов кибербезопасности, таких как международные и бизнес-аспекты, будет раскрыт следующими спикерами. У нас для этого представлены представители всех этих сегментов.

Сейчас я хотел бы напомнить всем докладчикам, что мы переключаемся в режим более динамичных пятиминутных выступлений (плюс-минус, естественно).

Следующий спикер для нас очень важен. Я предоставляю слово Хоулинь Чжао, генеральному секретарю Международного союза электросвязи, который, совершенно очевидно, обладает огромным количеством экспертиз в области кибербезопасности, в вопросах управления и использования Интернета, в вопросах обмена информацией о киберпреступлениях (известная система ИМПАКТ и так далее). Господин Чжао, Ваш взгляд на современное состояние вопроса кибербезопасности и некий международный подход, международный vision.

**Houlin Zhao:**

Thank you very much. Good afternoon, ladies and gentlemen. It is a real pleasure to be here with you at this afternoon session. I have prepared a speech, but if I read my speech, five minutes may not be long enough! It is better not to read my speech.

This is not my first visit to St. Petersburg. My first visit to St. Petersburg was 15 years ago, in 2000, when I visited Russia for the first time. The second time was in 2003, after the G8 Summit in St. Petersburg, to which I was invited by former Minister Raymond. The third time I was here was in May this year, with my good friend Oleg, to mark the 120th anniversary of Popov's invention of a radio device – the first radio device in the world – and also the ITU's 150th anniversary, so we jointly celebrated that.

As you might have noted, the ITU celebrates its 150th anniversary this year. Russia is a founding member of the ITU and has therefore been with the ITU since the very beginning. I found that Russia is different to the standard founding members. While many of the founding members contributed to activities, Russia contributed many technological developments, including television and satellite

communications developments. Russia and Russia's experts have also contributed a lot as far as cyber security is concerned.

On June 12 of this year in Geneva, President Putin received several heads of agencies and I was lucky enough to be received by him at that time. President Putin also referred to this very important cyber security work. I visited Russia at the beginning of this year, after my new term started as Secretary General, and met with Prime Minister Medvedev, who also highlighted the importance of cyber security. Last week, I was in South Africa and met with President Zuma of South Africa; a couple of days earlier, I met the Prime Minister of Singapore, Mr. Lee Hsien Loong, and he spoke of cyber security issues as well.

Hence I see these very important observations everywhere, being made by top-level leaders. And today, I see that Mr. Barak has joined us. That is another sign of the importance of cyber security in our world.

We had our meeting in Davos at the beginning of this year, where we talked about Internet governance, and noted that the World Economic Forum was exploring a new initiative called the Internet Initiative. At the meeting, I shared that in my view none of these cyber security issues and questions are anything new to the ITU.

The ITU has always been a United Nations specialized agency. We have been working on this issue for many years. For example, twelve years ago, in 2003, I came to Moscow to talk about cyber security issues with the former Chairman of ICOMM. Before we came to Moscow, we looked at the newspaper and it said, "These two guys are fighting each other". Yet in reality we talked to each other and have utmost respect for each other; we did not fight.

There was a misperception that the ITU should be kept away from Internet governance and cyber security issues, even though we have worked in that field for a long time. It was actually the ITU who initiated the approach of inviting the United Nations to organize the World Summit on the Information Society at the Plenipotentiary Conference Meeting in Minneapolis in the United States in 1998.

Why? Because 12 years before, the ITU picked up this important issue and lobbied very intensively for technical standards and for a lot of market issues, but we found this was not sufficient. We were talking to ourselves: engineers talking to engineers, and Ministers for Communications talking to Ministers for Communications. That was not enough.

We therefore invited the United Nations to organize the World Summit on the Information Society. This was the ‘modest approach’, and it was initiated and supported by the ITU. As a result of this process, the ITU was recognized and nominated as the only facilitator for cyber security. However, even some of our Ministers from European Member States, whom I met with at the Pasadena meetings in March this year, did not know that the ITU was recognized as the only facilitator for cyber security. We had worked very hard to establish the first Impact Project. I am very pleased to see that my friend on my left is also deeply engaged with this project. And still there is a perception that the ITU should be kept away from this.

That was one of the reasons why our World Conference on International Telecommunications was held in Dubai in December 2012. We tried to develop new telecommunications regulations to help operators in the industry achieve further sustainable development. Yet this was misinterpreted as the ITU wanting to take over Internet governance. There was a very big dispute, after which not even the expression ‘cyber security’ could be put in our telecommunications regulations text. We worked for almost two days to find a name to replace ‘cyber security’. All this even though the ITU was recognized as the only facilitator for cyber security.

We tried to work out some other way. The ITU focused on the protection of minors in cyberspace, because we had heard a lot about child online protection. We believed that this might be a topic that could be easily accepted by everyone, to try to establish an international framework to protect children from abuse

online. However, we have worked on this for almost 10 years now and have still not made any significant progress toward an international framework.

When we talk about cyber security, we have already heard a lot of information from our speakers. At the national level, there is a lot of progress, but at the international level it is not developing that easily.

What I would like to highlight now is that it has indeed not been easy to make progress in the past. We started in May 2013, when we organized our ITU Telecom Policy Forum in Geneva, specifically for Internet governance issues, and Minister Nikolay was there. Everyone was very constructive, and supportive of this policy forum and supported the idea of ITU playing an active role. Then things began to change. That has continued up until now, especially this year.

At the Davos meeting, for example, when we organized our Broadband Committee Meeting, we attracted several ministers, and were also pleased to see the President of Estonia joining us. In my office in January, I received the Minister of Defence from Finland. I was very pleased and also surprised, and said, “Why have I received you? Usually I receive Ministers of Communications.” He told me that in Finland, national security is coordinated by the Minister of Defence and that nowadays they consider national security to also include cyberspace.

I am therefore very pleased to see Mr. Barak here today. Before becoming the Prime Minister (1999-2001), Mr. Barak was Defence Minister of Israel; now he is also showing an interest in cyber security. In February of this year, I was in Germany, where the German Foreign Minister told me that the issue of cyber security in Germany is now coordinated by the Foreign Ministry, as well as the Communications Ministry. These kinds of things show a positive development; people are realizing that cyberspace should not be left only to the experts and should not be left to policy debate.

I am particularly pleased to note the statement made by the French Interior Minister before the famous march in Paris on January 11, 2015, after the

abhorrent terrorist attack. He made a public statement that this terrorist attack in Paris has alerted European members to the fact that they have to pay attention to cyberspace for national security.

Now, why did I pick this particular issue? Because in the past, people polarized the debate, linking China, Russia, South Africa, and other countries with Internet censorship under the guise of national security. In that debate, it seems to some that these countries have never cared about freedom of expression or privacy, while other countries are very much promoting those values of freedom of expression or privacy.

After the terrorist attack in Paris in January 2015, we now have the statement by the French Interior Minister on national security issues, and a Minister of Defence coming to my office to talk about the defence of his country by cyber coordination on security issues. Recently, in The Hague in the Netherlands, another conference on cyber security was organized.

All of this shows a very positive development. Countries are now considering cyber security to be priority security issues. This encourages me, and I believe we are making progress now.

Last year, I heard from the European Commissioners that they supported Brazil's NETmundial Initiative, because there was little progress on cyber security in Brazil. This question is now being repeated everywhere: why is there so little progress? I think that people are indeed frustrated by that, but I also see a very positive development in that. I see possibilities of working together to make progress and improve the cyber security situation. The ITU would like to make a contribution in this.

The ITU has made technical contributions. We have a Technical Standardization Group, led by our Russian experts. This group has developed famous recommendations such as X509, which was developed in 1988, and is still valid today. We have made a lot of technical contributions. We have also worked on

market issues, and we have worked on security development issues. ITU is picking up and focusing on priority items, including cyber security.

As the new Secretary General of the ITU, I am committed to making progress and to facilitate international cooperation. Here, again, I will count on Russian support, including the support of the Russian administration, support from the experts, and also support from the media. I am very confident that we will make very good progress. Thank you.

**С. Плуготаренко:**

Большое спасибо, господин Чжао.

Мы получили даже больше, чем просили. И более того, мне кажется, очень важно, что господин Чжао, говоря об экспертах, партнерах, использует термин «друзья». У нас получается этакое заседание друзей, что кажется мне очень приятным и показывает открытость и Союза электросвязи, и его генерального секретаря.

Продолжая международную линию, я хотел бы передать слово премьер-министру Израиля до 2001 года Эхуду Бараку, которого неоднократно упоминал господин Чжао. Совершенно очевидно, что Израиль, как страна, уделяющая повышенное внимание вопросам безопасности и кибербезопасности в том числе, обладает большим количеством экспертиз в этой области. Я понимаю, что уложить в пять минут то, что Вы знаете и, может быть, хотели бы рассказать, невозможно, но все-таки прошу постараться это сделать. Ваш подход к тем темам, которые мы сегодня обсуждаем.

**E. Barak:**

Mr. Zhao, distinguished members on the stage and distinguished guests: I will be brief, because I assume that most people in the room are familiar with cyber security.

Firstly, “we ain’t seen nothing yet”. We experienced many types of attacks last year. They are now moving from simple DDOSs into APTs, used not only by nation states. Extremely advanced DDOSs are still awaiting us, very sophisticated new tools that have not yet trickled down into the community of attackers beyond nation states.

We are dealing with a variety of attackers. There are, first of all, rogue nations, such as Iran and North Korea. Then there is organized crime, whether narco-trafficking or money-laundering, followed by the main players in areas such as the hacking community, hacking activists and hacking monetizers. In addition, of course, we also have recognized terrorist groups, as well as attacks by corporate business, IP claims, or even cyberspace blackmail.

We need to therefore brace ourselves for something much worse than we have seen up until now. What we have witnessed in regard to Lockheed Martin or Sony is nothing compared to what awaits us downstream.

Secondly, offence is light years ahead of defence, and will remain so in the foreseeable future. There are many reasons for this; it is the very nature of the game. It is infinite and can be compared to scoring in a basketball match. In basketball, the better the two parties are, the higher the scores. In soccer, on the other hand, the more evenly matched both sides are, the lower the score – it tends to be 0-0 or 1-0, and it will remain so.

There are far greater budgets and R&D capacity behind offensive strategies, financed by nation states and heavily financed by organized crime, which is highly motivated. In spite of all the talk in the business communities, there is little real action. Business is a long way away from seeing cyber security as ‘mission critical’ for the success of their companies. The challenge of cyber security applies to national security, business transactions, the economy, IP, even law and order, and it needs action. So, what should be done?

After Edward Snowden and after recent events, especially in North America, we have to rebuild trust between government authorities, the cyber security

community, and the providers in the Internet community. There is a need for an unbiased look at the nature of the problem, including the fact that we are moving slower than the attackers in cyber security. We have to be equipped with a sense of urgency about action. So I ask again, what should be done?

First of all, I believe that the ITU, the American NIST, the FCC, and their equivalents in all other countries, should establish a coordinated effort to deal with standards, protocols, interfaces, and similar aspects. Otherwise, you cannot weave together the different fragments of cyber security that are now widely dispersed around what can still be perceived as a perimeter – although that perimeter seems to be growing ever wider – and the deeper layers of cyber security. It is extremely easy nowadays for any attacker to identify which providers are giving security services to certain entities, sometimes directly, just by reading publicly available material, sometimes by launching a simple attack. We need to understand what should be done and what should be avoided in order to penetrate cyber attack networks.

There is a need for this first level of cooperation; there is a need to establish a deep cooperation with a series of operators in the private sector, both the providers of content – the Googles and the Amazons of the world – as well as with the ISPs, with the likes of Verizon, with the hardware and software producers such as Microsoft or IBM, and with the security providers, such as the RSAs and MacAfees of this world.

Without this kind of coordination, nothing will move. No player, neither government nor private businesses, can do this job on their own.

There is a need to coordinate certain activities, to join hands with the private sector, to finance the necessary R&D and to establish forensic labs for cyber security together, as well as monitor cloud computing in a cooperative way.

Cyberspace attackers have evolved from breaking through anti-virus protection and firewalls, and have now reached Big Data and anomaly detection. All parties need to protect data centres where everything is virtual. We are talking about

software-defined networks, there is not even any kind of physical perimeter anymore.

Our assumption should be that any entity or operation with any connection to the Web has already been penetrated, even if you are unaware of it. Anyone who does not assume this is blinding himself to reality

The threat thus has moved from ‘intrusive’ to ‘disruptive’, but we have not yet been exposed to destructive efforts by major players – to destroy certain entities or capacities of a rival – though we will surely live to see that.

In the cyber security industry, I detect confusion more than anything else. The leading players feel that they are left behind, that in a way they are all losers, and they do not know what to do. When people do not know what to do, they usually do what they know. That is as true in cyber security as it is on the battlefield. So now we double the height of firewalls or make them a little bit more complicated, ignoring the fact that they can all be bypassed somehow – over, under, through, or a myriad of other tricks.

It might sound strange to most of you, but if you checked now where enterprises are spending their IT Development money, you will see that it is still going into firewalls and anti-virus software, which are extremely ineffective by any standard. Yet this kind of confusion is also an opportunity to create a better way, a better organization. I think the next system will look as follows.

There is a need to monitor, on a massive scale, everything that moves through the Net, at least at Mega Data level, and in real time. Nothing short of this will establish the foundation for effective cyber security systems.

There is a need for a central repository where everything is frozen for at least two years, in order to be able to identify post-factum what happened and prevent further attacks.

There is a need to run this centralized repository with very deep real-time inspection and deep intelligence, including intelligence tips from nation-level sources of intelligence. This cuts through the massive work to be done and

reduces it by two or three orders of magnitude. With that many zettabytes of information available right now, even Big Data practices are facing a huge challenge in dealing with these amounts of information.

When I use the words ‘deep intelligence’ and ‘inspection’, I mean the use of deep learning and advanced machine learning practices for Big Data treatment and anomaly detection. There is a need to draw consequences from all of these analyses and translate it, using intelligence tips, not just for defence but also for offence.

I am involved in several extremely advanced, small cyber security companies in Israel, dealing with future solutions for major data centres. The treatment is more than just blocking something. When you have high-value information of a critical nature, it is not enough to block attacks. Even if you block attacks at a rate of $10^{-6}$, you will experience $10^{7}$ attacks and security will be breached. You want to know who the attacker is, what he is trying to achieve, and what to do in order to trap him. To do that, you need something that we call ‘dynamic honeypots’. When a dangerous attacker is identified, do not tell him that he has been identified. Let him believe that he is still operating, and follow what he is doing. Find out why he is there and who he is, without him being aware of it. We are working on this very intensively and many such developments will be needed.

What is the problem with what I have just described? It has a disturbing similarity to what the NSA was doing, which has just now been blocked. The problem is that a real struggle against cybersecurity threats will not work without these repositories, with keeping Big Data and being able to work with Mega Data in this way.

The solution is cooperation, teamwork with national authorities, with government and private entities. We need to rebuild the trust that has been lost over the last few years. We need direct, intensive inspection by the two other branches of governance, by the law and justice system. In any country, there should be a group of judges who are allowed to see highly classified information. The

authorities that operate the national repositories should report to them, and they should judge whether it is legitimate or not. There should be a continuous inspection by the legislative, by the parliament, the duma, the congress, or the Knesset. A team of legislators who are authorized to see everything, and it should pass their criteria, otherwise we cannot do it.

I am talking about the next step here, but we can already see on the horizon what comes after that. If I may make one remark about the real long-term future of cyber security, it is that it will help if we start almost from scratch into a totally new paradigm.

The human immune system is a good metaphor for this paradigm, in terms of cyber security. Our immune system is a biological system that evolved over millions of years. The solution for our cyber security problem should also be something which is modular, developing, evolving, Linux-like, not the old Microsoft- or Apple-like systems, but open systems that respond and learn along the way.

What characterizes the human immune system? Identification of self. Assuming mistakes – the human immune system assumes that mistakes will come anyhow. Correction mechanisms for mistakes. Continuous vigilance, all around the system, with the blood system which reaches every cell individually. Immediate attack on any kind of aggressor, either by the macrophage if it is bacteria or the T-cells if it is a virus. While you attack, you learn from what you face and immediately start to produce the unique antibodies for this specific new attack, until it is defeated.

This kind of approach, which is open, adaptable and learning, is the kind of paradigm that will help us improve our position vis-a-vis the dramatically evolving threat. Thank you very much.

**С. Плуготаренко:**

Многое хочется прокомментировать, но я вижу, что мы выбиваемся из тайминга, и прошу всех последующих спикеров все-таки его придерживаться. Более того, сокращается время на выступление каждого.

Господин Барак, большое спасибо за выступление. Продолжая тему международных экспертов, я хотел бы предоставить слово Фредерику Донку, The Internet Society.

**F. Donck:**

That would be me, thank you. Thank you, Chairman, for inviting me through the Internet Society to participate in this great panel with very distinguished members.

I have listened to many interesting perspectives today. I would like to start by saying that maybe we do not have a consensus yet on what cyber security means. Each time I address a conference on cyber security, I understand there are so many angles. That might be a first obstacle, this lack of a common shared understanding of the concept.

To clarify this, we ought to define the objective: what is it that we are trying to protect here, or to secure? Devices, applications, infrastructures, data, users, children, or even essential services such as electricity. Every panelist has said that there are different perspectives; whether you are a business, a user, or a government – each has different interests and different angles they want to protect and secure.

Yet we all have something in common. Any time we discuss and try to framework cyber security, we need to work back from an understanding of the different ways that the Internet is valuable. I believe that nobody will dispute the fact that the Internet is a communication tool, an engine for economic growth, and an enabler of social and even political change.

This is because, even though the Internet is evolving, it is based on very strong building blocks, very strong characteristics. It is still evolving, but there are elements that will not change. In our community, we call these The Environs of the Internet. Let me briefly describe them, because whatever we try to do on the Internet will ultimately have to be consistent with these environs. That will be the real challenge, even when we speak about cyber security.

Firstly, one of the critical characteristics of the Internet is its global reach. The Internet is composed of endpoints that communicate with other endpoints. This is relevant to integrity: wherever the endpoints start connecting to the Internet, they need to receive the information the sender has sent to them. In other words, whether I am in Belgium, my home country, or here in Russia, I should be able to access www.internetsociety.org.

Permissionless innovation is another strong characteristic or environ. Needless to say, I believe the explanation is in the term itself. If Tim Berners-Lee had had to ask permission of a telecommunications operator or a government to launch the World Wide Web, I am not sure that we would have the World Wide Web right now. An environ of the Internet is that everybody is able to launch and develop lawful activities on the Internet.

Accessibility is not just the ability to access the Internet, but is also the ability to share content and to contribute.

Collaboration is another environ – the Internet is based on collaboration between different stakeholders.

Last but not least, openness. This includes open standards, SMTP or HTTP for the Web, and SMTP for e-mail, among many others. Open standards means they are being adapted to different levels.

Those are the environs of the Internet. None of them are the cause or the origin of malicious activities. However, let us recognize that the strength of the Internet, which is its openness, might also be its weakness. Bad guys can also access the Internet, and they do not ask permission to launch viruses on the Internet.

Hence the real challenge for any cyber security framework would be consistency with the environs of the Internet. This includes the fact that we might need to preserve the openness and the global nature of the Internet. We might need to establish the right balance between factors that enable trust and that allow communications between users. It is based on confidence, it is based on privacy, and it is based on security.

We need to find the right balance between security and economic growth, development and innovation. And finally, we need to recognize that different security solutions are needed for different types of interactions.

With this in mind, what would be the global strategy, or the global framework, for cyber security? It might be based on managing risk in a collaborative way. There might be many definitions of risk. I love the one used by the OECD, “The effect of uncertainties on objectives”, and as the OECD states, “This is a combination of threats and vulnerabilities”. There will always be vulnerabilities. A 100% level of security might not be achievable; we need to take that into account.

Risk is a naturally dynamic concept. It depends significantly on different aspects of the digital environment, the people involved, and your organizational processes.

There is a traditional approach to security which is based on identifying external as well as internal threats; identifying or trying to assess their impact on the organization, and trying to build or invent or craft measures to prevent the perceived harm. More and more these days, however, there is a growing recognition of a new paradigm. This new paradigm is about protecting opportunities for economic and social prosperity. So this is the role of cyber security, and security needs have to be considered in the ecosystem of the Internet.

The new perspective on managing risk is to first take into account inward risk, the risk that exists to the assets of an organization, of the state, or the user. Secondly, and this is quite new, is managing outward risk. This is the recognition

of the risk that your organization itself presents, by its action or inaction, to the Internet's ecosystem.

An example would be poor security practices allowing a compromised computer to join a long-life botnet. Or poor maintenance of what we call the open DNS resolver, which is used as a reflector in case of a Denial of Services (DoS) attack. Those are examples that show that accounting for those outward risks is not evident, because they do not represent an immediate threat to the organization in question. There is no direct business case for the organization in question. One of the difficulties with cyber security is that there is little incentive for some businesses or organizations to deal with it.

Lastly, when managing risk collaboratively, there is also the consistent idea of shared risk management. Because we are in an interconnected world, one network acting alone can make little difference; there is a collective responsibility.

What will the role of governments be here? Governments have a very important leadership role in this. The role of government is to foster open, transparent, collaborative development, deployment of security solutions, and to engage in a truly multi-stakeholder way.

The reason I am saying this, is because what we have to avoid at all costs is a top-down approach to security, both by regulations and by government. We should even try to avoid deals within or between business leaders that would impose specific protocols. Similarly, we should avoid engineers inventing something without the engagement of governments and businesses. We really need a multi-stakeholder effort here.

International cooperation is key. First of all, this means that when we have these conversations at an international level, we need to use a common terminology on what it is that we mean by cyber security. Governments need to share Best Practices; they need to facilitate the sharing of information and, of course, translate policy into technical solutions that work with what I call the environs of the Internet.

It should be based on open technical standards, and it should be flexible enough to deal with the different future threats. This has already been touched on by several speakers today, that cyber threats change rapidly. Compliance-driven regulation might prove ineffective or even counterproductive. We need flexibility in any policy and any approach, and that applies to public-private partnerships, information sharing, and voluntary industry adoption of Best Practices.

I could continue for much longer on this topic. We, the Internet Society, would like to promote a vision of collaborative security. I like both words here, ‘collaborative’ and ‘security’. This is not a top-down approach, it really is a grassroots, bottom-up approach with different stakeholders. I would like to continue speaking about that if I get some time later in the conversation. Thank you.

**С. Плуготаренко:**

Большое спасибо.

Закончить этот международный блок я попрошу Константина Долгова, уполномоченного Министерства иностранных дел Российской Федерации по вопросам прав человека, демократии и верховенства права. Константин, я вынужден сказать, что у нас две минуты, и все остальные спикеры тоже ускоряются.

**К. Долгов:**

Сергей, спасибо, я постараюсь уложиться.

Есть два измерения проблемы всё более активного использования ИКТ — информационно-коммуникационных технологий — в негативных подрывных целях. Соответствующий список угроз прозвучал и у Николая Анатольевича, и у Александра Александровича. Безусловно, это и содействие терроризму и экстремизму, о чем говорил господин Барак, — использование ИКТ в подрывных политических целях.

Я приведу только один пример, который сегодня, по-моему, предметно не звучал. В последние недели мы столкнулись (это произошло раньше, но попало в СМИ и очень активно обсуждается только сейчас) с проблемой вербовки российских граждан со стороны ИГИЛ. Что с этим делать? Проблема, в общем-то, не новая, и не только Россия с этим сталкивается. Еще в прошлом году всеми 15 государствами принята специальная Резолюция Совета Безопасности ООН, которая направлена на то, чтобы пресечь рекрутирование боевиков, террористов. Это очень хорошая, замечательная резолюция. Есть адекватное международное сотрудничество по этому вопросу? Нет. Многие об этом говорят, но многие государства, к сожалению, живут и действуют по принципу «если не наших граждан рекрутируют, посмотрим, как дальше пойдет». А рекрутируют уже граждан и Европы, и США, и многих других стран, не говоря уже про ближневосточные государства.

Я полностью согласен с господином Бараком в том, что нужен мегаконтроль, или метаконтроль (можно по-разному говорить) за интернет-пространством. Вопрос, на который он сам постарался ответить — кто будет это осуществлять? Сегодня это пытается осуществлять одна сторона — США, и Николай Анатольевич очень правильно об этом говорил. Агентство национальной безопасности США и другие соответствующие спецслужбы делают это сугубо в своих интересах, нарушая права как американских граждан, так и граждан других стран (об этом в Вашингтоне предпочитают особо не говорить). Доходит до того, что в нарушение Венской конвенции прослушивают дипломатов!

Информация, которую предоставил Сноуден, довольно красноречива, но это только верхушка айсберга. Россия выступает за создание «правил дорожного движения» в плане регулирования и управления Интернетом. Господин Чжао, Международный союз электросвязи — это usual suspect в том, что касается выполнения соответствующих функций от имени

международного сообщества. Но давайте не будем забывать, что хотя правила дорожного движения международные, на практике они сильно отличаются, например, в Европе и в США. Поэтому правила будут хороши только в том случае, если мы выработаем их коллективно, если все государства проявят политическую волю и будут жить по этим правилам, способствуя осуществлению того самого мегаконтроля, о котором говорил господин Барак.

Что касается США, то, безусловно, там есть определенные подвижки, принят новый закон. Но этот новый закон (я имею в виду «Акт о свободе») вносит косметические изменения. Я не хотел бы вступать в полемику с господином Бараком, но Вы сказали про суд. Суд, конечно, нужен. В Соединенных Штатах Америки он есть и сейчас. Этот новый закон даже увеличивает полномочия суда в плане разрешения на прослушку, на перлюстрацию электронных сообщений и так далее. Но суд-то закрытый, суд абсолютно не публичный. О существовании этого суда 99,99% американцев не знают вообще. Это закрытый суд, который работает в области борьбы со шпионажем, и он непосредственно взаимодействует с президентом и со спецслужбами. То есть это такой пул из спецслужб и своего собственного суда, которые решают вопросы между собой. Если суд будет таким, то, конечно, он не будет работать, и никакого управления Интернетом не получится.

Вот самый последний конкретный пример, с которым мы сталкиваемся в нашей непосредственной работе. Американцами развязана охота за российскими гражданами за рубежом. Если посмотреть, кого в последний год поймали в третьих странах, добились экстрадиции и так далее (не буду сейчас подробно говорить о противоправных методах, которые США для этого задействуют), то в основном это специалисты в области IT. Хакеры они или не хакеры — это еще надо доказать. Презумпцию невиновности пока никто не отменял, но об этом, к сожалению, американцы частенько

забывают. И мы знаем о случаях, когда потом с нашими гражданами проводится работа: их пытаются заставить работать уже на американское правительство. Вот такой сбор мозгов идет по миру.

Если США борются с преступностью, тем более организованной, в области ИКТ — это прекрасно. Но тогда бороться надо вместе. Есть двухсторонние механизмы, есть соответствующие многосторонние механизмы. Хотя многосторонних и не хватает, но они есть, и здесь Россия готова к полнейшему взаимодействию. Не буду об этом долго говорить, так как помню о времени.

Есть инициатива по линии ШОС — Шанхайской организации сотрудничества. Это замечательная инициатива, к которой присоединились и Китай, и Россия, и другие страны ШОС. Она как раз посвящена правилам поведения в области обеспечения международной информационной безопасности. Пользуясь случаем, призвал бы всех коллег посмотреть на эту инициативу и по возможности оказать ей содействие.

То же самое в рамках Организации по безопасности и сотрудничеству в Европе. Первый шаг сделан: согласован какой-то первоначальный перечень мер доверия в этой области. Но надо идти дальше, надо развивать многостороннее сотрудничество и создавать механизмы, тем более что главный механизм — Международный союз электросвязи — у нас уже имеется.

Хочу в заключение подчеркнуть, что любое сотрудничество в этой области будет эффективным только тогда, когда оно будет осуществляться на основе доброй воли и баланса интересов, а не в целях продвижения своих корыстных геополитических или каких угодно других интересов. К сожалению, это та реальность, с которой мы сегодня сталкиваемся.

Большое спасибо.

**С. Плуготаренко:**

Спасибо.

На этом высоком политическом градусе я хотел бы остановить дискуссию в международной плоскости и на оставшееся время переключить ее в плоскость корпоративную, плоскость бизнеса. Наш следующий спикер — представитель компании Microsoft Анджела Маккей. Она директор по вопросам политики и стратегии кибербезопасности корпорации Microsoft. У Анджелы выступление с неким vision по проблематике кибербезопасности на некоторое количество лет вперед.

Анджела.

**A. McKay:**

Good afternoon, thank you. I am honoured to be at the Forum and on this distinguished panel.

Microsoft has a long-standing commitment to security, privacy, and transparency for our customers. By that I mean all of our customers around the world: consumers, enterprises and governments.

We have seen through experience that continuous risk management is the best strategy for managing cyber security, with efforts to protect against threats, detect the threats that occur, and respond effectively to them. Also, note that I said ‘continuous risk management’, by which I mean continually learning over time. Microsoft has a role in that.

We take action with technical innovations, such as reducing the number and severity of vulnerabilities in our software; operational efforts, helping to take down the botnets that have been talked about by several of the other panelists. Also in the policy domain, we are working to advance cyber crime law and protect critical infrastructures.

Our customers and enterprises also have a role, and governments do as well. In particular, I would like to talk about private-to-private collaboration and government-to-industry collaboration. Both of those are very important.

Here in Russia, we, along with others in the security community, have worked to share information on threats that helps to reduce the overall threat in the ecosystem through an effort called Netascope. Along with the Russian government and other governments around the world, we have something called the Government Security Programme, which helps governments see source code directly so that they can know with confidence that there are no backdoors in our products and services. This is done around the world.

And finally, one of the other areas of cooperation I would like to note is a focus on capacity-building around the world through the ITUD. While 3 billion users are already online, we have another 2.5 billion users coming online over the next few years. It is the responsibility of my organization, as well as the others up here on this panel today, to make sure that they are coming online and reaping the benefits of the global economy. Thank you.

**С. Плуготаренко:**

Я попрошу продолжить выступление нашего коллегу Илью Сачкова. Group-IB — организация, которая не понаслышке знает, что такое киберпреступность и каким образом с ней можно и нужно бороться.

Илья, тоже не более пяти минут.

**И. Сачков:**

Большое спасибо.

У меня есть пять минут, и, как ни странно, я начну с рассказа про лошадей. Человечество использовало лошадей для кавалерийских атак более двух тысяч лет, и в несколько недель или месяцев Второй мировой войны человечество полностью от этой идеи отказалось. И вообще, если

обратиться к истории, человечество от чего-то отказывается или производит революцию в чем-либо, когда, к сожалению, гибнут многие и очень многие люди. В течение 12 лет мы помогаем разным государствам искать преступников, понимаем, как они думают, как они выглядят, какие они используют методы. И как человек, который не понаслышке знает, что такое компьютерная преступность, я боюсь, что если прорыва не произойдет естественным образом, то в ближайшее время нас ждут человеческие жертвы.

Поясню свою мысль. В последние годы у классической компьютерной преступности было две цели: либо деньги, либо информация. Это изменилось после появления и усиления Исламского государства. Для примера скажу, что Исламское государство атаковало в России более тысячи ресурсов абсолютно безо всякой причины. У этих людей нет мотивации украсть информацию или украсть деньги — у них есть мотивация получить, как бы странно или страшно это ни звучало, мировое господство. И человечество должно понять, что нужно кардинально изменить подход к управлению информационной безопасностью и действительно выработать единые правила игры, потому что компьютерное преступление — это единственное преступление в мире, которое можно совершить за одну секунду, находясь в одной стране, во всех остальных странах мира. И таких примеров тысячи.

Вторая причина — это наш пассивный подход к информационной безопасности. Я двумя руками за то, что сказал господин Барак. Представляете, 35 крупнейших российских банков в течение нескольких месяцев были заражены вирусом. Банки использовали самые современные средства информационной безопасности, потратили на это кучу денег, на каждом зараженном компьютере были антивирусы лучших мировых производителей. А злоумышленники за декабрь 2014 года украли один миллиард рублей. Поэтому сейчас, внимательно глядя на Исламское

государство и используя тот опыт, который у нас есть, я могу сказать: то, что было сказано сегодня, нужно сделать в этом году. Иначе, к сожалению, в ближайшие годы может произойти катастрофа, которая приведет к гибели большого количества людей. И только после этого, используя свой исторический опыт, мировое сообщество сделает какие-то изменения. Большое спасибо.

**С. Плуготаренко:**

Илья, большое спасибо.

И еще одно выступление — Светлана Шамзон, «Компания ТрансТелеКом». Светлана, я знаю, что у Вас есть несколько тем, которые Вы хотели бы раскрыть. И мне сейчас дали сигнал, что у нас еще есть время — порядка десяти минут с учетом завершающего слова министра. Поэтому Вы можете взять до пяти минут.

**С. Шамзон:**

Большое спасибо.

Я хочу пойти от общего. Мы сегодня говорим о стратегии кибербезопасности. Очень важно поговорить о тех уровнях, на которых эта стратегия должна будет действовать. Один уровень — это то, что касается непосредственно бизнеса, и то, что касается экономики. Сегодня большинство российских компаний, особенно инфраструктурных компаний, предоставляющих магистральные услуги, предоставляют своим клиентам еще и комплекс услуг, связанных с такими вещами, как межсетевые экраны, защита от DDoS-атак, шифрование траффика. Это направление сейчас очень активно развивается.

Для того чтобы перейти на следующий уровень, очень важно сказать о следующей вещи. Если в предыдущие периоды основой кибербезопасности была автономность систем, то на сегодняшний день это практически

невозможно. Это возможно, но на уровне подписания указа о государственном сегменте Интернета. Это фактически выделенная корпоративная сеть, которая имеет максимальную защиту. Для таких сетей берутся цифровые каналы, объединяются в свою сеть, а какая там будет защита, уже решает непосредственно сам заказчик. Эта сеть практически автономна.

Говоря о том, что сегодня мы пользуемся глобальной системой, я приведу для примера небольшую статистику о том, где хранятся данные. Аналитики компании IDC посчитали, что в 2013 году объем мирового рынка облачных сервисов составил 45,7 миллиарда долларов. Совокупный рынок облачных услуг в 2013 году в России вырос более чем на 70%, и в последующие с 2013 по 2017 годы прогнозируется рост этого рынка на 27%, что говорит о том, что все наши данные, вся наша информация фактически хранится в облаках. Поэтому о каких автономных системах сейчас можно говорить?

Первый уровень, о котором я сказала — это уровень бизнеса. Второй уровень, о котором, наверное, тоже нужно сказать, — это тот уровень, на котором сейчас в России принимаются очень серьезные меры. Это то, что касается российского законодательства. Это те акты, о которых говорил Александр Александрович, это то, что касается защиты личных данных, это то, что касается защиты детей. И на сегодняшний день Россия принимает достаточно серьезные законодательные документы, которые позволяют эффективно защищать самый незащищенный сегмент — наших детей.

При этом есть еще более высокий уровень. Поскольку система международная и все мы пользуемся одним Интернетом и храним данные в облаках, здесь необходим следующий уровень — международный. Очень важно обратить внимание на то, что в своей презентации показал Александр Александрович. Все, что касается защиты детей — реестр запрещенных сайтов для детей и работа операторов по сохранению этой информации, — есть в Великобритании, во Франции, в России и еще в

целом ряде стран. Обобщение таких практик и создание пусть даже не регламентов, а рекомендаций на уровне Международного союза электросвязи могло бы стать первым шагом к тому, чтобы систематизировать это пространство.
На этом я остановлюсь. Спасибо.

**С. Плуготаренко:**
Большое спасибо.
И у нас есть еще один эксперт — Андрей Семериков, «ЭР-Телеком Холдинг».

**А. Семериков:**
Спасибо.
Действительно, получилась очень «крутая» дискуссия, содержательно добавить нечего. Хотел бы только сказать, что, как говорится, «не хочешь язву желудка — не ешь плохие продукты». Поэтому нужно думать и о личной гигиене с точки зрения пользования услугами. Я уверен, что сегодня многие, абсолютно не задумываясь, пользуются услугами бесплатного провайдера Wi-Fi со странным названием «Форум 2015». Что это за провайдер? Всем понятно, что он одноразовый, но он бесплатный, и поэтому мы смело отправляем в эту сеть все самые конфиденциальные данные, которые у нас есть. А об этом надо думать.

**С. Плуготаренко:**
Понятно, это такое хорошее напутствие по окончании первого дня работы Форума. Есть еще два дня, и можно сделать выводы.
Я хотел бы предоставить слово Николаю Анатольевичу Никифорову для некоторого резюме нашей сегодняшней дискуссионной панели. Николай

Анатольевич, основные выводы, которые Вы могли бы сделать по итогам всего услышанного.

**Н. Никифоров:**

Уважаемые коллеги, дорогие друзья, хотел бы поблагодарить всех за очень интересную дискуссию.

Многие спикеры говорили о разных аспектах кибербезопасности. И это хорошо, потому что мы рассмотрели ее с разных сторон. Но мне кажется, дискуссию объединила одна фраза (по крайней мере, мне она почему-то очень хорошо запомнилась), которую произнес господин Барак. Из его уст она прозвучала как resume trust. Одна из проблем, к которой мы подходили с разных сторон, заключается в восстановлении доверия. Очень много наломали дров. Я не знаю, как это переведут на английский язык, но именно из-за этой проблемы, из-за тех дров, которые наломали государства, из-за тех рисков и угроз, с которыми мы реально столкнулись и из-за которых уже гибли люди, — из-за всего этого нам нужно восстанавливать доверие.

Российская Федерация, как и многие наши зарубежные партнеры, высказывается о том, что это доверие нужно восстанавливать на основе международного права. В конце концов, именно право делает нас цивилизацией. Это общие легитимные правила игры. Мы считаем, что это должно происходить под эгидой ООН, потому что именно на уровне ООН мы сегодня видим финализацию международного права. Угрозы стали глобальными. Государства должны объединить свои усилия. Должны быть выработаны новые правила игры. Как Министерство, мы также концентрируемся на правах граждан, которые, на самом деле, даже шире, чем понятие «кибербезопасность».

Мы считаем, что и управление Интернетом, и другие правила игры должны основываться на многосторонней модели управления, но, еще раз повторю,

*правовой* модели управления. У нас есть такие примеры по многим другим направлениям, но нет какой-либо конвенции и действительно утвержденных общепринятых международных правил жизни в киберпространстве и, соответственно, соблюдения кибербезопасности. Мы выступаем за то, чтобы на площадке ООН продолжалась дискуссия в формате встреч на высшем уровне по управлению информационным обществом. Очень важно, что в цели десятилетия были включены ключевые показатели по развитию инфокоммуникационных технологий. Давайте вместе добиваться, чтобы в задачи нового десятилетия мы обязательно включили и задачи, связанные с кибербезопасностью.

Сегодня идет обсуждение этих вопросов. Что-то делает Форум по управлению Интернетом. Но этого недостаточно, у него нет полномочий, у него нет мандата. Многие страны выступали за такой подход именно в формате тех или иных конвенций. Мы высоко оцениваем работу, которая проходит на площадке ШОС — Шанхайской организации сотрудничества. Мы считаем, что нужно именно под эгидой ООН выработать новые правила международной игры. Эти правила будут касаться работы государств и определят правовые механизмы для взаимодействия бизнеса и защиты наших прав и свобод.

Мне кажется, что мы с вами живем в очень интересное время и становимся свидетелями не просто истории, а, по сути, нового качественного перехода нашего цивилизационного развития. Это происходит не в эти десятилетия, а буквально в эти годы. И мне кажется, для всех нас большая честь жить в эту историческую эпоху и внести свой посильный вклад в то, чтобы новые возможности, которые дали нам технологии, принесли только позитивное. А весь негатив мы смогли бы вовремя обуздать и принять такие правила игры, чтобы человечество развивалось дальше, получало позитивные созидательные импульсы. Давайте работать для этого. Эта миссия, эта задача достойна того, чтобы мы вкладывали в нее свое время, ресурсы,

финансы, усилия государств. И тогда от этого выиграем мы все, выиграет наша планета, выиграет вся наша цивилизация.

Большое спасибо.

**С. Плуготаренко:**

Большое спасибо, Николай Анатольевич.

Не поверите, у меня была такая ремарка. Я написал себе: в том случае, если останется время для вопросов и ответов, главный вопрос, который нужно поднять, — это восстановление доверия. Я думаю, что всем нам — отрасли, государству, разным странам и, наверное, самим пользователям — действительно нужно над этим работать.

Давайте на этой ноте и объявим завершившейся нашу дискуссионную панель. Огромное спасибо всем докладчикам и большое спасибо всем слушателям.