Александра Куликова
Координатор программы ПИР-Центра
«Глобальное управление интернетом и международная информационная безопасность»

GCCS 2015: Киберпространство по правилам и без

Четвертая Глобальная конференция по киберпространству (Global Conference on Cyberspace – GCCS2015), состоявшаяся в Гааге, Нидерланды, 16-17 апреля 2015 года, оставила двоякое ощущение. Голландское правительство, очевидно, приложило большие усилия, чтобы вынести на ее повестку дня самые актуальные вопросы кибербезопасности, радикальное расширив включенность в диалог заинтересованных сторон и пригласив к участию представителей гражданского сообщества. При этом, однако многие участники GCCS покинули Гаагу «с чувством недосказанности».

«Лондонский процесс» 4.0

Не уходя в подробности истории самого формата, стоит все-таки напомнить, что GCCS2015 – это четвертая конференция из серии «лондонского процесса», открывшегося в 2011 году первой Глобальной конференцией по вопросам киберпространства в Лондоне, в ходе которой проблемы кибербезопасности были впервые вынесены на повестку дня в глобальном масштабе. В рамках конференции Министр связи и массовых коммуникаций России Игорь Щеголев сделал акцент на российских инициативах по обеспечению международной информационной безопасности (МИБ), и в частности представленной осенью 2011 г. российской концепцией Конвенции ООН об обеспечении МИБ, цели которой в том числе состояли в ограничении злоупотребления информационными технологиями против интересов отдельных государств и современного мира в целом. Эта инициатива была воспринята в штыки как попытка легализировать инструменты борьбы с инакомыслием в глобальной сети.

Последующие конференции в Будапеште (октябрь 2012 г.) и Сеуле (октябрь 2013 г.) недалеко продвинулись в поисках реальных договоренностей, хотя рамочное соглашение по итогам Сеульской встречи о приверженности открытому и безопасному интернет-пространству прямо отражало достигнутое ранее в том же году заявление Группы правительственных экспертов ООН (UN GGE) о применимости норм международного права, включая Устав ООН, к киберпространству. Однако сложно было ожидать прорывных решений осенью 2013 года после разоблачений Сноудена: сессия британского Форума управлению Интернетом (IGF UK) по готовящейся Сеульской конференции в сентябре 2013 года выглядела довольно странно: насущная и острейшая тема электронной слежки и напряженность в отношениях правительственных партнеров была просто вынесена за скобки мероприятия. Неудивительно, что в 2014 году цикл не был продолжен.

Однако с ростом масштабов киберпреступности в мире и нарастанием геополитической напряженности, необходимость обсуждать и договариваться о поведении государств в трансграничном и неоднородно регулируемом киберпространтве стала очевидной. В 2015 году правительство Нидерландов предприняло большие усилия по «реанимации» несколько утратившего авторитет формата, организовав богатую программу мероприятий в преддверии конференции и на ее полях, в том числе открыв ее впервые для представителей гражданского общества.

Так, 14-15 апреля 2015 г. состоялось Подготовительное мероприятие для группы участников (около 40 человек), представляющих организации гражданского общества, особенно из стран Азии, Латинской Америки, Ближнего Востока, Африки (т.н называемые страны Глобального Юга). С учетом разной тематической подготовленности участников заранее была проведена серия вебинаров по основной проблематике GCCS; сам тренинг включал ролевые игры и секции в формате мозгового штурма в малых группах для лучшего понимания того, где и как «голос гражданского общества» встраивается в общий контекст Конференции (заявленные темы – свобода, развитие, безопасность). Это прежде всего тематика прав человека – защита права на частную жизнь и свободу самовыражения. Участникам была дана возможность сформулировать предложения для внесения в официальное заявление Председателя конференции; одно из заседаний Подготовительного мероприятия посетил министр иностранных дел Нидерландов Берт Кундерс, также одна из сессий GCCS была посвящена проблемам защиты права на тайну частной жизни онлайн.

На самой Конференции прозвучали громкие заявления от представителей правительств стран-участниц, в частности, от главы МИД ЕС Федерики Могерини, о том, что государства должны принять на себя обязательства препятствовать использованию своих территорий для совершения кибератак на другие страны. Также была отмечена необходимость закрепить список критически важных объектов, в отношении которых было бы запрещено совершать компьютерные диверсии. Однако, в итоге призывы большинства выступавших министров о важности выработки договоренностей о нормах поведения в киберпространстве снова «повисли в воздухе». Одна из главных причин состоит в том, что достаточного продвижения вновь не получили ключевые понятия и правовые термины в области кибербезопасности. Также нюансы применения международного права (например, международного гуманитарного права) к киберпространству по-прежнему являются камнем преткновения и предметом непрекращающихся дебатов, а принципы ответственного поведения государств с целью предотвращения конфликтов в киберпространстве все так же остаются в неопределенной «серой зоне».

Хотели как лучше…

Конференция GCCSпрошла с размахом, многие участники отмечали масштаб технической и контентной подготовки. Впечатляет как число участников (около 1800 человек), так и количество мероприятий на полях конференции и за несколько месяцев до нее. СМИ сообщают, что на организацию и проведение мероприятия было затрачено около €15 млн. При этом экономический эффект от заключенных сделок на полях GCCS2015 еще предстоит оценить. Впечатления участников разнятся в отношении содержания конференции: при несомненно прекрасных возможностях пообщаться в кулуарах, завязать новые контакты, встретиться с партнерами, многие отмечали недостаточно глубокий уровень дискуссий на некоторых сессиях, сходство с форматом IGF в отношении отсутствия конкретных результатов дискуссий.

Основным посылом правительства Голландии на конференции стал призыв к странам мира начать договариваться о правилах поведения в киберпространстве, которые минимизировали бы риск киберконфликтов и роста киберпреступности. Необходимость в таких нормах уже назрела. Также была подчеркнута необходимость определить условия нового «социального договора» между правительствами и гражданами различных стран о балансе «безопасности» и «права на частную жизнь» в контексте информационного общества. Такой социальный контракт позволил бы развести понятия личной и национальной безопасности и обеспечить безопасность для пользователей в интернете. Для этого ставка делается на меры укрепления доверия между различными акторами в киберпространстве, а также укрепление потенциала в тех сообществах, которые сталкиваются с наиболее острыми киберугрозами.

Так, по итогам мероприятия был учрежден Глобальный форум по киберэкспертизе (Global Forum on Cyber Expertise), базирующийся в Гааге, – инициатива ряда государств (включая США, Великобританию, Канаду, Швейцарию, Вьетнам, Бангладеш, Мексику и проч.), частных компаний (в том числе Miscrosoft, HP, Huaiwei и др.) и международных организаций (ITU, Europol) по созданию площадки для обмена опытом и наращивания компетенций в сфере кибербезопасности по всему миру для противодействия киберпреступности и другим киберугрозам. Координатор Госдепа США по кибербезопасности Кристофер Пейнтер по итогам GCCS написал в своем блоге об уже заключенных США в рамках этого Форума договоренностях по развитию правовой базы для обеспечения кибербезопасности и повышению осведомленности о существующих рисках на африканском континенте и в Юго-Восточной Азии. Однако описание мандата этого проекта пока довольно схематичное, и не очень ясно, как Форум будет работать в реальности. Вместе с тем, можно предположить, что едва ли речь идет об обмене самым передовым опытом и технологиями в условиях дефицита доверия кибердержав друг к другу. Зато очевидно, что те технологии, которые будут «спущены» более слабым игрокам, будут «спонсированы» совершенно определенными субъектами, заинтересованными в продвижении своих продуктов на еще малоосвоенные рынки. Если же рассматривать эту инициативу в контексте всеобщей милитаризации киберпространства, едва ли она будет способствовать сдерживанию наращивания кибервооружений. Россия пока не присоединилась к инициативе Форума.

А воз и ныне там

Что касается Гааги, то она, конечно, укрепила свои позиции не только как международный дипломатический и правовой хаб, но и теперь и глобальный центр компетенций в сфере кибербезопасности, что, безусловно, подкрепляет амбиции Нидерландов по получению

временного места в Совете Безопасности ООН в 2017-2018 гг. Возможно, этим в частности объясняется беспрецедентное внимание к деятельности Группы правительственных экспертов ООН по достижениям в области информатизации и телекоммуникаций (UN GGE/ ГПЭ ООН), к слову, изначально инициированной российской стороной. Впервые в рамках глобального формата GCCS, организованного прежде всего западными государствами, была высоко оценена работа UN GGE в области признания применимости Устава ООН и международного права к киберпространству, при необходимой при этом дальнейшей работы по адаптации их положений. Причем приоритет деятельности UN GGE был обозначен в качестве одного из центральных пунктов уже в предварительном проекте заявления Председателя конференции. Это своего рода веха, так как ранее роль работы UN GGE, мотором и идеологом которой всегда считалась Россия, если и признавалась, то не продвигалась открыто на глобальном уровне, тем более на западных площадках.

При этом очевидно, что к подписанию нового соглашения о нормах поведения в киберпространстве стороны пока не готовы. Имеющийся международный правовой инструментарий частично позволяет регулировать поведение государств в киберпространстве, но требует значительной доработки, прежде всего в области *jus ad bellum* и *jus in bello*. При этом «серой зоной» остается поведение государств в условно мирное время, непосредственно предшествующее эскалации конфликта (pre-threshold period). При этом обновленный проект Правил поведения в области обеспечения МИБ стран ШОС, внесенный в Генеральную Ассамблею ООН в январе 2015 года и выработанный как раз для предотвращения международных конфликтов в киберпространстве, старательно игнорировался участниками конференции. На сессиях GCCS документ был упомянут, пожалуй, лишь Владимиром Лапшиным, представителем Департамента новых вызовов и угроз МИД РФ, в его речи на пленарном заседании, а также послом Китая в Голландии на одной из сессий конференции.

То есть, если о применимости международного права к киберпространству уже можно говорить более-менее предметно, без фундаментальных разногласий в отношении правильности такого подхода, пусть и при необходимости доработки массы нюансов, то договориться о том, «что хорошо, и что плохо» в киберпространстве *до* эскалации конфликта по-прежнему не получается даже на уровне *мягкого права*. Это было очевидно как на основных сессиях GCCS2015, так и в обсуждениях представителей гражданского общества. Концептуальные разногласия относительно кибербезопасности и информационной безопасности до сих пор кажутся непреодолимыми, но не стоит упрощать их до противостояния условно авторитарных режимов с западным миром. Нормативные контексты в мире гораздо более разнообразны, и представления о том, что дозволено, а что нет, и где гражданские свободы ограничиваются соображениями национальной безопасности, различаются на национальном уровне в разных странах. Поэтому естественным образом меры по укреплению доверия и наращиванию киберпотенциала реально осуществимы именно на национальном уровне, работа на котором должна предшествовать гармонизации подходов на региональном и затем глобальном уровне. Этому переходу во многом сегодня мешает геополитическая напряженность в Европе вокруг Украины.

Однако можно предположить, что наличие другой растущей угрозы – Исламского государства (ИГИЛ) – и проблемы радикализации киберпространства в глобальном масштабе могли бы при наличии доброй воли участников подтолкнуть их к сближению позиций. При нежелании употребления термина «информационная безопасность», многие западные страны уже озабочены именно ее обеспечением в своем информационном пространстве – будь то заявления о противодействии российской пропаганде в социальных медиа или законы по

фильтрации экстремистского контента в Сети. По крайней мере, у России, как известно, в этой области уже наработан значительный опыт.

Задача глобального нормотворчества также осложняется тем, что даже при лидирующей роли государств решать проблемы борьбы с киберпреступностью и нераспространения кибероружия невозможно без участия частного сектора, генерирующего необходимые технологии и заинтересованного в непрерывности бизнес-процессов. В этом плане бизнес мог бы стать гораздо более значимым союзником государственных акторов, чем можно было бы предположить, причем именно в части скорейшей выработки договоренностей о поведении в «серой зоне», предшествующей прямому конфликту. В этом контексте следует отметить шесть норм поведения государств для предотвращения конфликтов в киберпространстве от Microsoft – проект, который компания презентовала еще в декабре 2014 года и с тех пор активно продвигает на всех площадках, включая GCCS. Отношение к нему как прецедентной инициативе, адресованной именно государствам и исходящей при этом от негосударственного актора, в экспертной среде может быть неоднозначное. Компания, безусловно, решает и свои бизнес-задачи на фоне продолжающейся тяжбы с правительством США, особенно что касается нормы №1 о недопущении внедрения закладки в продукты частных компаний ИТ-отрасли. Однако в случае поддержки этой инициативы коалицией других крупных частных игроков она может получить интересное развитие.

В такой ситуации наиболее реалистичными кажутся соглашения о выработке международных норм поведения в киберпространстве для обеспечения безопасности и отказоустойчивости глобальной инфраструктуры Интернета как наименее политизированного пласта в данной проблематике. В качестве возможной цели можно было бы обозначить достижение договоренности между РФ, США, КНР и другими ведущими кибердержавами о невмешательстве в работу системы уникальных идентификаторов Интернета (DNS, системы распределения IP-номеров и номеров автономных систем). Например, в рамках экспертного круглого столе в Гаагском институте глобальной безопасности (The Hague Institute for Global Security) на полях GCCS д-р Деннис Бредерс, научный сотрудник голландского научного совета государственной политики (Netherlands Scientific Council for Government Policy) и профессор университета Эразмуса в Роттердаме, высказался за присвоение глобальной инфраструктуре сети Интернет статуса глобального общественного блага (‘global public good’) и необходимость выработки правил поведения, которые гарантировали бы ее неприкосновенность и позволяли бы отделить решение вопросов безопасности самого интернета от политик по обеспечению национальной безопасности в цифровую эпоху. Подобные идеи неоднократно звучали в разных интерпретациях на полях GCCS: и в общей формулировке упомянута в итоговом заявлении Председателя конференции.

Помимо уже упомянутых моментов, в итоговом заявлении Председателя стоит отметить следующие положения:

- GCCS выражает поддержку процессу передачи ответственного управления функциями IANA глобальному сообществу заинтересованных сторон и призывает уделить первостепенное внимание поддержанию стабильности, безопасности и отказоустойчивости интернета.
- Всемирный Форум по управлению интернетом (IGF), мандат которого будет пересмотрен в декабре2015 года на итоговой Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО +10), следует сохранить как зарекомендовавшую себя площадку для диалога по вопросам управления интернетом (правда, нет упоминания о создании механизма реализации принимаемых на нем

решений). Саму встречу рекомендовано провести с максимально широким вовлечением различных заинтересованных сторон, включая общественные организации.

- особое внимание уделяется сотрудничеству государств и частного сектора (ГЧП) в области поддержания безопасности критических инфраструктур и глобальной инфраструктуры интернета как на национальном, так и на глобальном уровне через механизмы обмена лучшими практиками, в том числе через созданный в рамках конференцииGlobal Forum on Cyber Expertise. Отмечена важность уже отработанных механизмов выработки технических стандартов интернета и их успешного применения (IETF стандарты)
- возлагается большая ответственность на правительства в области создания и развития национальных систем обеспечения безопасности критических инфраструктур и укрепления потенциала защитных мер, а также и в плане обмена опытом и взаимопомощи.
- отдельно была отмечена необходимость уважать и охранять права человека при реализации политик в сфере национальной безопасности в контексте киберпространства. Тем не менее, правозащитники не были удовлетворены уровнем дискуссии вокруг темы защиты права на тайну частной жизни и ее невнятной формулировкой в итоговом документе Конференции.

Следующая конференция GCCS 2017 состоится в Мексике. За два года, работа созданного форума GFCE должна как минимум дать первые результаты. Определенный импульс к реальному сближению позиций можно ждать от Группы правительственных экспертов ООН при условии, если не снижения, то по крайне мере стабилизации геополитической напряженности. Наконец, ключевым условием для какого-либо прогресса в области кибербезопасности и информационной безопасности остается банальное доверие сторон друг к другу, которое пока остается в большом дефиците.