4. Формирование собственного Тезауруса.

4.1. Переводы проекта «ИнфорЗиппер Нетворк»

4.1.1. Оливье Крепи-Леблан. Что произошло на WCIT и что делать дальше?

Что произошло на WCIT и что делать дальше?

Оливье Крепи-Леблан (Dr. Olivier MJ Crépin-Leblond)

2013.03.14

Часть 1: Что случилось на WCIT?

1.12 Эпилог по ITRs

2. **Рекомендуемые дальнейшие действия**

2.1. Внесение ясности

2.2. Общие рекомендации

2.2.1. Принятие активных мер по поддержанию действующей мультистейкхолдерной среды управления Интернетом в целом

2.2.1.1. Продвижение действующей мультистейкхолдерной модели Интернета в развитых странах мира

2.2.1.1. Продвижение действующей мультистейкхолдерной модели Интернета в развивающихся странах мира

2.2.2. Улучшение мультистейкхолдерной модели с целью обеспечения максимального охвата

2.2.2.1. Институонализация действуйющей мультистейкхолдерной модели

2.3 **Рекомендуемые дальнейшие действия для ICANN**

2.3.1. Организации поддержки и консультативные комитеты (SO и AC)

2.3.2. Рекомендуемые действия для сообщества At-Large и Консультативного Комитета At-Large (ALAC)

2.3.2.1. Наращивание потенциала

2.3.2.2. Проактивные действия по достижению действительного членства

2.3.2.2. Раскрутка способности сообществ At-Large найти общий язык со своим правительством

2.3.2.4. Больше поддержки - в обоих направлениях

2.3.3. **Достижения сообщества At-Large/историческая перспектива**

2.4. Заключение

Данный документ содержит личную интерпретацию автором событий, состоявшихся на Всемирной конференции по международной электросвязи («WCIT») в Дубае (Объединенные Арабские Эмираты) в декабре 2012 года,

а также их причин. Все мнения, высказанные в этом документе, мои собственные, хотя я признаю, что на них сказались годы веры в мультистейкхолдеризм. Поэтому читателю предлагается поинтересоваться мнениями других независимых источников информации для повышения сбалансированности общей картины.

Этот документ состоит из двух частей. Первая часть представляет собой реконструкцию событий, произошедших во время WCIT. Вторая часть содержит предложения по тем направлениям, которые Интернет-сообществу и, в частности, Консультативному Комитету сообщества At-Large при ICANN (ICANN At-Large Advisory Committee - ALAC) стоило бы проанализировать для того, чтобы, при поддержке ICANN, принять активные меры по продвижению модели многостороннего управления Интернетом (мультистейкхолдеризма) и преодолеть препятствия на пути ее имплементации. Эти предложения продиктованы насущными потребностями, ставшими очевидными в ходе WCIT – в том числе, но не только, потребностями в разъяснительной работе, образовательных программ, деятельности по наращиванию потенциала и активному вовлечению новых участников.

Часть 1: Что случилось на WCIT?

1.1 1.1 Предпосылки и закладка интриги

Большинство государств принадлежит к географическим группам, в которых они обсуждают свои позиции с целью выработки общей политики. Несколько таких подгрупп формируют блоки.

Основные блоки перечислены ниже:

APT – Asia Pacific Telecommunity – Азиатско-тихоокеанское сообщество телекоммуникаций

ATU – African Telecommunication Union – Африканский телекоммуникационный союз

CANTO - Caribbean Association of National Telecommunication Organizations – Карибская ассоциация национальных телекоммуникационных организаций

CEPT - European Conference of Postal and Telecommunications Administrations led by Portugal – Европейская конференция почтовых и телекоммуникационных администраций, управляемая Португалией

CITEL - Inter-American Telecommunication Commission – Межамериканская телекоммуникационная комиссия

CTU – Caribbean Telecommunications Union – Карибский телекоммуникационный союз

LAS – League of Arab States – Лига арабских государств

RCC – Regional Commonwealth in the Field of Communications – Региональное содружество в области коммуникации

Неприсоединившиеся – некоторые государства не входят в региональные организации и остаются полностью независимыми в своих решениях, хотя и принимали участие в небольших встречах, организованных Председателем.

Также подгруппой CEPT была группа Евросоюза (EU), включающая в себя только те страны, которые входят в Европейский Союз и управляемая Кипром (Президентом Евросоюза в то время) - (Европейские постсоветские страны в большинстве своем входят в РСС - прим. редактора).

1.2 День открытия

В первый день конференции прозвучали вступительные речи. Без сомнения, ключевой речью, как по своим посылам, так и по символизму, стала речь г-на Фади Чехаде (Mr. Fadi Chehadé), президента и генерального директора ICANN. Ключевой она стала по двум причинам:

1. Приглашение от Генерального секретаря ITU доктора Хамадуна Туре (Dr. Hamadoun Touré) приехать в Дубаи и выступить на конференции. Оно состоялось в словах доктора Туре об Интернете и вопросах адресации и нумерации;
2. Призыв к умиротворению и диалогу, озвученный г-ном Чехаде в Дубае. Он был принят очень хорошо многими делегатами.

Далее, состоялся ряд двухсторонних встреч г-на Чехаде и Председателя правления ICANN доктора Стива Крокера (Dr. Steve Crocker) с официальными делегациями, включая нескольких министров, встречи с которыми в конечном счете могли покачнуть мнения некоторых стран (от их перечисления уклоняюсь). Неофициальные отзывы, полученные мной по личным каналам, состояли в том, что было жаль, что г-н Чехаде и д-р Крокер не провели еще день в Дубаи и не поговорили с большим количеством делегаций.

В дополнение к вышесказанному, визит руководителей ICANN на конференцию также открыл возможность для дальнейших дискуссий по привлечению новых действующих лиц в экосистему мультистейкхолдеризма, на которой построен Интернет. Наведение мостов с не-ICANN'овскими сообществами – это ключ к сохранению модели и ее росту. Больше об этом будет сказано в части «Следующие шаги».

Если бы руководство ICANN решило вообще не присутствовать на конференции, это усилило бы точку зрения большинства стран в ITU, что ICANN – это контролируемая США башня из слоновой кости инсайдеров

доменной индустрии, в управлении своими ресурсами не заинтересованных ни в расширении Интернет, ни в мировом общественном интересе. Визит г-на Чехаде противоречил этой точке зрения. Был ли он убедительным? Неофициальные источники заметили, что делегаты некоторых стран действительно оценили этот визит, особенно то обстоятельство, что г-на Чехаде сопровождал доктор Тарек Камел (Dr. Tarek Kamel), уважаемая личность в регионах Африки и Среднего Востока.

1.3 Методы работы

Метод работы Председателя был весьма незатейливым. Документы можно было скачать по одному из базы данных ITU, или можно было использовать программу для синхронизации собственной библиотеки данных со всеми опубликованными документами (правда, только для пользователей Windows).

Основной рабочий документ был поделен между несколькими рабочими группами. Некоторые, как, например, «Com 5», в дальнейшем были разделены на две рабочие подгруппы – Com 5-1 и Com 5-2.

Основной рабочий документ читался Председателем, строка за строкой, и во время сессии участвующие страны вносили в него предложения, которые заносились также в специальный рабочий документ, фиксирующий все предложения участников строка за строкой. В некоторых случаях таких предложений были десятки, в некоторых – были консолидированные предложения от регионов. После прочтения каждой строки основного рабочего документа Председательствующий открывал прения.

От стран-участниц поступало четыре вида отзывов:

а) отсутствие комментариев, считающееся согласием с обсуждаемым параграфом

б) положительная реакция всех участников

в) смешанные ответы от участников

г) отрицательные ответы от всех участвующих.

В случаях а) и б) Председатель фиксировал консенсус и больше никогда не возвращается к этой строке.

В случае г) Председатель спрашивал, не выступит ли какая страна против удаления этой строки.

В случае в) Председатель просил заключить текст и его заменители в [квадратные скобки], показывая все варианты, иногда в одну строку, и текст направлялся в [Com 2] [Com 5] [специальную рабочую подгруппу Com 5] [другой процесс], для каждой из которых Правление назначало Председателя.

Далее Председатель переходит к следующей строке Договора.

Процедура может быть многоуровневой, и Председатель Com 5, например, также имеет право запросить об организации специальных подгрупп, если на встрече Com 5 не достигается консенсус.

В результате было создано множество специальных рабочих групп, но только Пленарные заседания были открыты для публики и стенографировались. Рабочие группы сами по себе были открыты только для стран-делегатов с жестким фильтрованием физического доступа в комнаты для встреч и выдворением всех не-делегатов из комнат. То есть – без прессы, без гражданского общества, без членов секторов.

Некоторые рабочие группы добились существенного прогресса. Например, рабочая группа по Статье 6 провела много длительных сессий, но в результате интенсивных переговоров сумела продвинуться вперед. Другие рабочие группы быстро заходили в глухое противостояние, так как аргументы ни одной из сторон не достигали «линии противостояния» и не пересекали ее.

Когда через пару часов временами весьма очень жарких споров, похожих на перетягивание каната, рабочая группа не могла достичь консенсуса, Председатель Рабочей группы подводил итоги и закрывал ее. В дальнейшем предоставлялся отчет более широкой Коммуникационной группе, например, Com 5-1, Com 5-2, Com 2 и т.п. Этот вопрос далее обсуждался в более широкой группе Com, нередко с тем же тупиковым результатом, что и рабочая группа, но с большей «огневой мощью», задействованной всеми заинтересованными государствами. Если консенсус не находился, вопрос передавался пленарному заседанию нерешенным. И так страсти накалялись, вопрос обсуждался два, три, четыре раза и больше, с теми же самыми аргументами, предъявляемыми через переговорные столы, только в разных форумах. Это в самом деле было как попасть в фильм «День сурка» и наблюдать, как в повторяющихся «дежавю» растет раздражительность персонажей.

С другой стороны, любой консенсус на уровне рабочих групп (и было бы справедливо отметить, что по большинству статей в Регламент международной электросвязи - ITR - т достигли консенсуса) передавался в соответствующую группу Com и быстро выносился на пленарное заседание. Это давало Председателю конференции столь необходимый для вдоха воздух и способ смягчить атмосферу при нарастании напряженности в аудитории. Через несколько дней работы Председатель мог уже набирать комбинацию трудных вопросов и легких побед для того, чтобы показать прогресс зрителям веб-трансляции и наблюдателям.

1.4 Первые выходные

На последней сессии в пятницу вечером, казалось, шел обычный поток докладов специальных рабочих групп, консенсуса не удавалось достичь по многим пунктам. За пять минут до конца вечернего пленарного заседания Объединенные Арабские Эмираты объявили, что они намерены

представить новый документ, консолидирующий предложения от нескольких стран Африки и арабского региона.

Это тут же подняло температуру на несколько уровней:

Во-первых, объявление о новых документах было спорным, поскольку, согласно Уставу ITU, все документы Конференции необходимо было получить, по крайней мере, за месяц до начала конференции.

Во-вторых, этот документ был описан как вносящий значительное количество требований, касающихся управления Интернетом.

В-третьих, он был представлен принимающей страной – Объединенными Арабскими Эмиратами, и Председатель конференции г-н Мохамед аль-Ганем (Mr. Mohamed Al-Ghanem) казался весьма удивленным существованием такого документа.

Предложения ОАЭ сразу же поддержали Алжир, Иран, Россия, Китай, Камерун... и опротестовали США, Великобритания, Швеция, Португалия, что по понятным причинам вызвало настоящий переполох.

Сессия вскоре после этого закрылась, а в зале пленарных заседаний осталось множество озадаченных лиц, с нетерпением ожидавших возможности прочитать это предложение как можно скорее – будет ли оно принято ITU (так как были сомнения на счет своевременности его подачи), и когда оно будет представлено?

1.5 Игра в прятки с предложением

Не прошло и суток после окончания первого пятничного пленарного заседания, как на веб-сайте WCITLeaks появилась версия просочившихся неаутентифицированных документов, претендующих быть этим предложением. В этом тексте вновь оказались ратифицированными самые сильные предложения от африканских и арабских делегаций, и обнаружилось предложение России, ратифицированное ОАЭ, Китаем, Саудовской Аравией, Алжиром, Суданом и Египтом. Затем через несколько часов, драматизма добавилось: Дина Кабиил (Dina Kabeel), PR-представитель Египта, отмежевалась от этого заявления в своем аккаунте в Twitter, объявив, что Египет никогда даже не слышал об этом документе и не хочет иметь к нему никакого отношения.

Тем временем среди делегатов ЕС сложился консенсус на счет того, чтобы полностью игнорировать документ в течение выходных, пока он не появился официально в архиве документов ITU, чтобы не привлекать к нему внимание и не придавать ему значения. Это оказалось хорошей тактикой, так как на понедельник, 10 декабря, вместо того, чтобы представить документ, Объединенные Арабские Эмираты объявили, что он снят. Ради исторической точности, а также для того, чтобы передать уровень путаницы и политического маневрирования в игре, нужно отметить, что документ появился в базе данных ITU во вторник, 11

декабря, зарегистрированным, но без какого бы то ни было указания на его легитимность в качестве временного документа, и его автором была указана Россия. Такова была политическая игра, всегда с дамокловым мечом в воздухе, готовым нанести удар, если страны, не согласные с рассмотрением Интернета как части ITR, продолжат сопротивляться включению любого текста, упоминающего Интернет, хоть в Правила, хоть в Резолюции. Угроза начала обсуждения этого документа еще несколько раз возникала в течение остальной части конференции с тем, чтобы оказать давление на ЕС. Его использовали в качестве противовеса варианту, в котором в *резолюцию* было бы внесено включение Интернета в ITR примерно как «...или вы соглашаетесь с этой резолюцией об Интернете или мы будем настаивать на обсуждении этого документа, который означает возврат к нашей жесткой позиции от доброжелательной позиции компромисса, в которой мы находимся сейчас.»

Тактика была ясна: масса новых предложений, затем – обсуждение, и одна за другой предметы торга уступались фронту «западных демократий» под прелогом необходимости идти на уступки «другой стороне» тоже.

Личный комментарий: это как начать печатать свои деньги и менять их на твердую валюту, по курсу 1:1. Через некоторе время обменный пункт начнет жаловаться, но при этом половина монопольных денег и так уже будет находиться на его счету... отнюдь не к его радости. Тем не менее при попытках отказа принимать монопольные деньги в дальнейшем обменный пункт приобретет репутацию "злоумышленника", так как отвергает предлагаемые ему деньги, не смотря на то, что и так уже получил их целую кучу. Аналогично, у сторонников существующей экосистемы Интернета были только кусочки этой экосистемы, которыми они могли торговаться, кирпичик за кирпичиком, в то время как сторонники двухсторонней системы выдвигали предложения только для того, чтобы расплатиться за кирпичики здания мультистейкхолдеризма.

1.6 Основные камни преткновения

Предлагаемый Договор содержит более 20 статей, некоторые из которых содержат по несколько правил. Если бы он содержал только несколько разногласий, возможно, недели было бы достаточно, чтобы их решить. Увы, к концу выходных стало ясно, что между всеми сторонами обнаружились очень серьезные разногласия и четыре дня будут очень плотно заполнены попытками найти консенсус по всем этим пунктам, тем более, что не все делегации были такого размера, как делегация Великобритании (более 25 человек) что позволяло нам и участвовать в нескольких параллельных секциях, а также, по очереди, и отдохнуть, и проанализировать позиции, и пообщаться. Конечно, Председателю конференции за выходные напомнили несколько раз, чтобы он ограничил количество создаваемых специальных рабочих групп. Одновременно

проводилось два (редко – три) параллельных рабочих семинара. Другим ограничением стало проведение двух наборов семинаров в день. Обычно, типичный день состоял из блока семинаров, блока рабочей группы по коммуникации и пленарного заседания, что позволяло выносить нерешенные вопросы на пленарное заседание.

Вопросы взаиморасчетов оказались вполне решаемыми в рабочих группах. При этом другие вопросы оказывались просто неразрешимыми ни на уровне семинаров, ни на уровне Com 5, и выносились на пленарное заседание... и снова... и снова... и снова, и каждый раз Председатель помнил о прямой веб-трансляции и передвигал вопрос на более позднюю дату или отправлял его обратно в рабочую группу.

Конечно, к воскресенью уже стало понятно, что, так как специальные рабочие группы не вели веб-трансляций, и не допускали на заседания неправительственных делегатов, все инакомыслие держалось за закрытыми дверями, потому серьезность ситуации и отсутствие прогресса были скрыты от внешнего мира.

Основными камнями преткновения оказались:

- Преамбула: права человека
- Статья 1.1a: телекоммуникации / информационные и коммуникационные технологии
- Статья 1.2: Эксплуатационные организации и Признанные эксплуатационные организации
- Статья 3.7: Доступ к телекоммуникационным сетям (предложение Кубы)
- Статья 3.8: Управление ресурсами Интернета (Россия, арабская группа, затем опять Россия)
- Статья 5A – Безопасность
- Статья 5B – Спам
- Статья 6: Взаиморасчеты
- Резолюция: Содействие созданию благоприятных условий для быстрейшего роста Интернета

1.6.1 Преамбула: права человека

Предложение о включении формулировки, касающейся прав человека, внес Тунис, сразу после начала конференции. Изначально ее предлагалось внести как часть Статьи 1 ITRs, но такое предложение было отклонено многими странами. Позднее на той же неделе Тунис предложил взамен включить формулировку о правах человека в преамбулу, так, чтобы она применялась к документу в целом, но не была «*регламентом*».

Стоит отметить, что Тунис предложил эту формулировку отчасти из-за нестабильной политической ситуации в стране. Тунис, как лидер в событиях «арабских весны», попытался показать, как идейный лидер, что новые режимы могут быть построены на таких ценностях, как уважение прав человека - и это уважение прав человека распространяется на все виды деятельности. В связи с этим стоит отметить, что для Туниса включение его предложения по формулировке прав человека в преамбуле представляется большим, чем просто желание - оно является ключевым элементом для его будущего. Это стало известно по прошествии дней. Мнение Запада, который, возможно, изначально полагал, что о формулировке прав человека не может быть и речи в техническом документе, опасаясь, что это приведет к политике и вопросам управления, смягчилось и Европейский Союзом (ЕС), в частности, благодаря своим сильным позициям по правам человека, проддержал идею.

По иронии судьбы, именно эта тема, войдя на арену через черный ход, привела к крушению консенсуса и голосование по ней прошло только в конце конференции. Вопрос привел к странным пертурбациям, когда все страны соглашались уважать права человека в принципе и абсолютно поклялись уважать все аспекты прав человека, но некоторые яростно сопротивлялись включению формулировки о правах человека.

1.6.2 Статья 1.1a: телекоммуникации / информационные и коммуникационные технологии

Это проблема была красной чертой для многих стран. В соответствии с глоссарием ITU, термин «*Телекоммуникации*» определен в Уставе и Конвенции ITU как:

> 1012 Телекоммуникации: Любая передача, излучение или прием знаков, сигналов, письменного текста, изображений и звуков или сообщений любого рода по проводной, радио, оптической или другим электромагнитным системам.

В то же время, термин «*Информационные и коммуникационные технологии*» («Information and Communication Technology», ICT) не определен, при том, что в течение нескольких лет он использовался в WSIS (Всемирном саммите по вопросам информационного общества) и других публикациях ITU, таких как в ITU-D и т.п. Проблема состоит в том, что многие правительства в отношении использования термина ICT в регламентах исходят из того, что ICT относятся не только к телекоммуникационной инфраструктуре, но и к терминалам конечных пользователей, а также к данным, иначе известным как контент. Замена термина «*Телекоммуникации*» на «*Информационные и коммуникационные технологии*» по всему документу позволит значительно расширить сферу действия регламента за рамки полномочий ITU. В конце концов, это

«Международный Союз телекоммуникаций (электросвязи)», а не «Международный Союз информационных и коммуникационных технологий».

Это было трудное сражение, в итоге закончившееся в пользу сохранения статуса-кво в «Телекоммуникациях», так как не нашлось никаких убедительных аргументов, почему мандат ITU должен быть расширен. Несколько европейских стран дали понять, что это последний рубеж, и они готовы выйти из переговоров, если термин будет изменен на ICT. Генеральный Секретарь ITU д-р Туре, видя рост напряженности в самом начале первой недели конференции и явно обеспокоенный тем, что создался потенциал для раннего крушения конференции, сообщил всем, что ничто в регламентах не будет относиться к контенту. Хотя многие документы в МСЭ и в целом в Организации Объединенных Нации говорят об ICT, в правилах останутся «Телекоммуникации».

Эта ранняя дискуссия выглядит как основной компромисс, на который пошли африканская, арабская и российская группы, и он послужил только ужесточению позиций в других разногласиях.

1.6.3 Статья 1.2: Эксплуатационные организации и Признанные эксплуатационные организации

Термины «Эксплуатационные организации» (Operating Agency, OA) и «Признанные эксплуатационные организации» (Recognized Operating Agency, ROA) определены в уставе ITU:

1007 Эксплуатационная организация: Любое частное лицо, компания, корпорация или правительственная организация, которая эксплуатирует оборудование электросвязи, предназначенное для обеспечения службы международной электросвязи или способное причинять вредные помехи такой службе.

1008 PP-98 Признанная эксплуатационная организация: Любая отвечающая вышеприведенному определению эксплуатационная организация, которая эксплуатирует службу общественной корреспонденции или радиовещания и на которую обязательства, предусмотренные в статье 6 настоящего Устава, налагаются Членом Союза, на территории которого расположен орган управления этой организации, или Членом Союза, разрешившим этой эксплуатационной организации установить и эксплуатировать на своей территории службу электросвязи.

Северная Америка и Европа хотели, чтобы термин ROA, использованный в

ITRs 1988 года, оставался и в новом регламенте. Некоторые другие страны были непреклонны в своем ст ремлении это положение изменить. У России, например, была серьезная проблема с использованием ROA, поскольку часть ее эксплуатационных организаций не признана, и они, следовательно, избегают какого-либо регулирования, тем самым имеют потенциал дестабилизировать телекоммуникационный рынок России. Некоторые другие страны в Африке столкнулись с аналогичной проблемой. Кое-кто в европейских странах понимал эту проблему, хотя было высказано общее мнение, что это внутренние проблемы, которые нужно решать внутри, а не прибегать к Международным регламентам для ремонта у себя в доме.

По состоянию на выходные было выдвинуто промежуточное предложение использовать термин «Эксплуатационная организация» в основном тексте, каждый раз сопровождая его звездочкой со сноской, говорящей «*уполномоченным или признанным государством-членом для построения, деятельности и участия в предоставлении международных телекоммуникационных услуг для общественности*». Эта идея «не взлетела», когда возник вопрос, будут ли сноски и звездочки обязательными или нет, и юридический персонал ITU отвечал на этот вопрос уклончиво. Затем дискуссия сосредоточилась на том, включать ли этот текст в основной текст, и, наконец, на том, определить ли его как «уполномоченный орган по эксплуатации», как это предложил ЕС. Соединенные Штаты настаивали на более жестком термине для этого определения, где была использована «Общественная корреспонденция», в терминах Устава ITU:

> 1004 Общественная корреспонденция: Любое сообщение электросвязи, которое предприятия и станции, предназначенные для обслуживания населения, должны принимать для передачи.

Сторонники ОА хотели термин «услуги населению», избегая «корреспонденцию», чтобы не ограничивать определение в соответствии с определением ITU. И дело опять шло по кругу.

Последним вариантом стали «Уполномоченные органы» в Регламенте 1.1a-bis, и Соединенные Штаты собирались возражать против этого, но, как мы знаем, обсуждение до этого пункта не дошло, так как окончательно застопорилось еще на преамбуле. ЕС, в то время не вполне удовлетворенный "уполномоченными органами", был скорее склонен использовать эту позицию в торговле.

1.6.4 Статья 3.7: Доступ к телекоммуникационным сетям (предложение Кубы)

Это предложение было повторно внесено Кубой в Документ 26, основываясь на Резолюции 69 конференции Всемирной ассамблеи стандартизации телекоммуникаций, прошедшей за неделю до WCIT в

Дубаи. Это был повтор кубинского предложения, изложенного во Временном Документе 25, опубликованном в начале декабря.

ADD CUB/26/4

31D 3.8 Члены Союза должны воздерживаться от односторонних и/или дискриминационных действий, могущих препятствовать доступу другого Члена Союза к публичным Интернет-сайтам.

Обсуждение в рамках специальной рабочей группы, встреча которой состоялась в начале конференции, было безрезультатным из-за отсутствия четкого понимания того, чего именно Куба (при поддержке Ирана, Судана, Китая и России и вмешательстве Бразилии и Уругвая) на самом деле хотела. Всякий раз как Интернет-сайты понимались как контент, нас уверяли, что это не так. В ходе обсуждения также была добавлена идея использования ресурсов. Но чтобы избежать использования термина «Интернет» и не коснуться контента, никакого консенсуса достигнуто не было, хотя были проведены некоторые работы по замене «доступа к публичным Интернет-сайтам» на «доступ к телекоммуникационным сетям».

Так как в специальной рабочей группе консенсус достигнут не был, вопрос был передан обратно в Com 5. Там тоже к консенсусу прийти не удалось, так что вопрос был направлен на обсуждение на пленарном заседании. Противники этого предложения привели тот аргумент, что оно предотвращает возможность отрезать государство от телекоммуникационных сетей, если против него вводятся санкции. Возник также вопрос о применимости такого регламента, так как было неприемлемым допустить, что, если кто будет блокировать контент, Член Союза сможет отрезать физические связи с такой страной, при той степени развития сети телекоммуникаций, какая наблюдается сегодня сегодня.

При отсутствии консенсуса по Статье 3.8 Куба далее предложила внести эту формулировку в Преамбулу. Это вызвало крупный конфликт на вечернем пленарном заседании в среду, когда переговоры зашли в тупик из-за того, что «недискриминационный доступ к телекоммуникационным сетям» некоторые страны приравняли к правам человека. К этому мы еще вернемся.

1.6.5 Статья 3.8: Управление ресурсами Интернета (Россия, арабская группа, затем опять Россия)

Это предложение вызвало настоящий переполох, когда оно было

внесено Россией до начала конференции, в Документ 37, 17 ноября 2012 года. Генеральный секретарь ITU д-р Туре продолжал отмечать, что ни один из регламентов не касается Интернета и что ITU не пытается «захватить Интернет», хотя это предложение обосновывает свои требования на итогах Тунисской программы для информационного общества Всемирного встречи на высшем уровне по вопросам информационного общества (WSIS, Женева-2003 – Тунис-2005).

– Цитата – Документ 37 –

ADD RUS/27/8

31B 3A.2 Члены Союза имеют равные права по управлению Интернетом, в том числе в отношении выделения, назначения и отзыва ресурсов нумерации, наименования, адресации и идентификации в Интернете и поддержки обеспечения функционирования и развития базовой инфраструктуры Интернета.

Основания: §§ 38, 52 и 53 Тунисской программы для информационного общества, WSIS, Женева-2003 – Тунис-2005.

ADD RUS/27/9

31B 3A.3 Члены Союза имеют суверенное право разрабатывать и осуществлять государственную политику, в том числе международную политику, по вопросам управления Интернетом, а также регулировать национальный сегмент сети Интернет, так же как и деятельность эксплуатационных организаций, предоставляющих доступ к Интернет или передачу Интернет-трафика в пределах их территории.

Основания: Преамбула Устава ITU и §§ 35a, 58, 64, 65, 68 и 69 Тунисской программы для информационного общества, WSIS, Женева-2003 – Тунис-2005.

– Конец цитаты –

Эти две статьи сами по себе взрывают нынешнюю экосистему Интернета, базирующуюся на мультистейкхолдерном взаимодействии на различных форумах и заменяют ее многосторонними отношениями между странами. Они используют набор точек зрения из повестки дня WSIS, вырванных из контекста.

Это предложение было основой неуловимых ОАЭ, потом – российским предложением, закончившимся игрой в прятки, как описано выше.

Интересно отметить, что сам документ никогда не обсуждался в рабочих группах или на пленарных заседаниях, а, скорее, использовался его авторами как угроза. Поскольку было известно заранее, что США и ЕС будут против содержания этого документа, его можно было бы назвать «ядерной бумагой» - сдерживающим фактором, который будет использоваться только в отчаянных случаях, но которым можно размахивать для того, чтобы удержать оппозицию «в стойле».

Так как любое упоминание этого документа действительно несколько раз накаляло обстановку в помещении и добавляло стресса делегатам, пытающимся договориться о консенсусе, было ясно, что любое использование этого документа приведет к краху конференции в целом.

Вспомним однозначные заверения: «Эта конференция не об Интернете».

В результате, председатель конференции, г-н аль-Ганим никогда не ставил обсуждение этого документа ни в одну повестку дня WCIT.

1.6.6 Статья 5A – Безопасность и надежность сетей

Обе статьи – 5A и 5B – шли за довольно всеобъемлющим заголовком Статьи 5: «Безопасность жизни и приоритетность телекоммуникаций». В регламентах 1988 года была только Статья 5, и, соответственно, Статей 5A и 5B не было.

Статья 5A обсуждалась с разных сторон, некоторые из которых могли дублироваться – «Все дороги ведут в Рим», вначале в контексте, а далее смешиванием предложений, адресованных вопросам качества обслуживания (quality of service — QoS).

Статья 5A – касается «Безопасности и надежности сетей». Другие называли ее «Сетевой безопасностью», «Надежностью», «Эластичностью» и т.п. Некоторые страны, в основном входящие в RCC, APT, арабские страны и Африка настаивали на использовании слова «Безопасность».

Проблема с использованием этого слова состоит в том, что оно имеет очень широкое значение и может охватывать многие аспекты работы сети. Оно может включать безопасность на физическом уровне (замки на кабинетах и телекоммуникационных комнатах), но также и на сетевом уровне и далее, вплоть до приложений и доступа к самому по себе контенту в сети. «**Безопасность**» может открыть путь к перехвату, сканированию сетей, блокированию контента, управлению информацией и общему влиянию на контент в сети. Она поднимает вопросы о свободе слова. Можно сказать, что в связи с «вопросами безопасности», египетскую телекоммуникационную сеть можно было вполне законно отключить во время «арабской весны». Злоупотребления словом

«безопасность», имеющие целью полный контроль над информацией и репрессии широко распространены.

Безопасность сетей передачи данных может включать в себя клиентское оборудования, то есть компьютеры, защищаемые контролируемой правительством схемой идентификации (с помощью SIM-карт или RFID для доступа к сети). А это открывает путь к законодательству, требующему лицензии или паспорта для пользования любой сетью, включая Интернет.

Поэтому Великобритания предложила использовать слово «**надежность**», являющееся более техническим термином, означающим устойчивость, стабильность и доступность сети, находящейся под атакой или в условиях стресса. Это предложение было полностью и решительно **отвергнуто** сторонниками слова «**безопасность**».

Эта дискуссия также полностью игнорировала Резолюцию недавней Полномочный конференции ITU в Гвадалахаре. В самом деле, Решение 3 Резолюции 130 (Гвадалахара, 2010) устанавливает, что ITU не должен вовлекаться в разработку законов, и что вопросы, связанные с контентом, киберпреступностью, национальной обороной и безопасностью являются национальными вопросами, и не будут входить за рамки Регламентов.

Переговоры по этой теме были очень тяжелыми с самого начала. Сначала 35 минут обсуждения потребовалось, чтобы достичь точки, в которой не могло быть выбрано даже название, так как первоначально было 10 предложений только для самого названия раздела. Потом каждый пункт занял по 20 минут, чтобы зафиксировать **отсутствие консенсуса** и завершить обсуждение чем-то вроде попурри из слов (все в скобках), показывающих трансформации предложений. Некоторые страны буквально **настаивали на том, что контент должен быть включен в безопасность** – уже когда стало понятно, что в **Регламентах не будет ничего, касающегося контента**. Европа внесла несколько предложений, но все они были отклонены.

Определенно это было критической чертой для многих государств – в обоих направлениях. **Для RCC и их союзников критичным было упоминание «безопасности». Для других критичным было избежать упоминания «безопасности».**

Пока один блок говорил «черное», а второй – «белое», не было никакого способа сказать «серое» и все попытки найти что-нибудь «серое», к сожалению были торпедированы. Были сделаны попытки ограничить сферу применения «безопасности», но безрезультатно.

Консенсуса нет.

1.6.7 Статья 5B – Спам (нежелательные массовые электронные коммуникации).

Эта статья была предложена несколькими группами, в частности Африкой, арабскими странами и RCC.

Она тоже привела к одним из самых значительных разногласий в Регламентах, при том что сторонники новой статьи полностью игнорируют логику, отрицая очевидное. С самого начала было очевидно, что обе стороны дискуссии и не собирались достигать какого бы то ни было консенсуса.

С европейской точки зрения спам – это контент. Для того, чтобы классифицировать сообщение, будет ли оно в Интернете или в электронной почте, или же в SMS, как спам, необходимо его просканировать. Это подразумевает прочтение его, человеком или машиной. Вы не можете сказать об информации, что она – спам, не прочитав ее. Это так же очевидно как то, что вода – мокрая. В течение нескольких часов участники вращались вокруг этого вопроса, в конечном итоге сторонники переименовали его в «нежелательные массовые электронные коммуникации». Проблема тут двоякая: что означают «массовые электронные коммуникации», нигде не определено. Будет ли список рассылки «массовой коммуникацией»? Будет ли ретвтитнутый твит «массовой коммуникацией»? Будет ли RSS «массовой коммуникацией»? Если кто-нибудь напишет 100 получателям со своего аккаунта в Gmail – будет ли это «массовой коммуникацией»? Как насчет 20 получателей одновременно? А если он напишет каждому отдельно?

Вторая проблема состоит в том, что чтобы определить, является сообщение желательным или нежелательным, получателю придется **прочитать его контент**. На сетевом уровне определить желательность или нежелательность коммуникации невозможно. Или, возможно, **любое массовое распространение данных считается нежелательным**?

Это дает зеленый свет введению цензуры.

Аргумент в пользу включения такой статьи в Регламент был представлен весьма красноречиво развивающимися странами: их очень дорогая пропускная способность международных телекоммуникаций съедается спамом. Несколько представителей сделали сильные заявления о том, что от 80 до 90 процентов электронных писем были спамом, со ссылками на законные исследования западных компаний. Хотя эти цифры насчет процента электронной почты, являющейся спамом, не оспариваются, основной недостаток этого аргумента состоит в том, что электронная почта сама по себе составляет от 5 до 8% всего интернет-

трафика.

Этот вопросов рассматривается в нескольких отчетах:

[EN11] Envisional Technical report: an Estimate of Infringing Use of the Internet, January

2011

[SAND12] Sandvine Intelligent Broadband Networks: Global Internet Phenomena Report, 2H

2012

Cisco Visual Networking Index: Forecast and Methodology, 2011-2016

Источник:

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

Это подтверждает сведения из других источников о том, что наибольшими на сегодняшний день потребителями пропускной способности в Интернете являются четыре (4) вида услуг (не в каком-либо определенном порядке) - пиринговый файловый обмен, просмотр веб-страниц, развлечения в режиме реального времени, хранение и резервное копирование данных. Типичное письмо электронной почты небольшое по размеру, типичная веб-страница более чем в 20 раз больше него, а видео – в 20 000 раз больше. Интернет также является лишь подмножеством всего телекоммуникационного трафика в и из страны, и, если даже он составляет, допустим, 50% (что опять же завышено), то спам составляет 2,5% трафика.

Поэтому утверждение о том, что спам является основным источником телекоммуникационных перегрузок сети в целом, ложно.

По отдельности обе статьи 5A и 5B культивируют неоднозначность, давая возможность не относить их обе ни к контенту, ни к Интернету. Однако еще одно событие, состоявшееся неделей ранее на WTSA, повышает опасность подслушивания связи по умолчанию.

На WTSA ратифицирован стандарт ITU Y.2770.

Этот стандарт, подготовленный рабочей группой во главе с Китаем, обязывает использовать **глубокий анализ пакетов** (Deep Packet Inspection, DPI) в сетях следующего поколения. Это процесс, при котором информация, передаваемая через сеть, разбирается, расшифровывается и ее содержание анализируется. Этот стандарт явным образом связывает спам, сетевую безопасность и качество обслуживания. Особый интерес представляет раздел «Безопасность», цитируемый ниже:

– Начало цитаты –

1.2.3 Безопасность

Средства DPI могут быть развернуты для предоставления возможности выявления вредоносного трафика, могущего привести к снижению пользовательской производительности, истощению сетевых ресурсов, ухудшению инфраструктуры, и, в результате, сделать сеть недоступной для своих абонентов. Большая часть вредоносного трафика маскируется под обычный трафик и требует чрезвычайно большой полосы пропускания, например: исходящий спам (Примечание 1), сканирование IP адресов и портов, и т.п. Рисунок I.3 представляет типичный сценарий приложения, в котором когда злонамеренный трафик идентифицирован, он удаляется компонентами DPI из трафика, таким образом предотвращается его распространение в сеть.

Примечание 1 – так, функция DPI может быть составной частью интерактивной системы шлюзов для противодействия спаму в соответствии с [B-ITU-T X.1243]. Пункт 6 [B-ITU-T X.1243] демонстрирует возможные методы и условия политик для идентификации спама на основе DPI (то есть, «спам» представляет здесь «трафик приложений DPI»).

– Конец цитаты –

Таким образом, **DPI – это фильтрование контента**. Стандарт сам по себе – просто стандарт, использование которого необязательно. Он не стал обязательным, когда WTSA ратифицировала его – его просто сделали предпочтительным средством обеспечения «безопасности». С другой стороны, использование самих слов, содержащиеся в «безопасности» в статьях 5A и 5B в Регламентах – это еще один шаг к превращению этого стандарта в обязательный или по крайней мере делает DPI применяемым по умолчанию на практике в сетях.

В результате, обе статьи – 5A и 5B – оказались **критичной** проблемой для многих стран и **консенсус достигнут не был**. Вполне вероятно, что неудаленная статья 5B про спам и отказ использовать слова «устойчивость» или «надежность» вместо «безопасность» в статье 5A, приведет к тому, что некоторые страны, скорее всего, никогда не подпишут Регламент.

1.6.8 Статья 6: Тарификация и расчеты

В Регламенте редакции 1988 года, в частности в статье 6, было несколько устаревших концепций.

Например, концепция Администраций, на самом деле – государств-членов, устанавливающих модели ценообразования для телекоммуникаций, а также концепция того, что тарификация – внутренний вопрос, уже устарели. В 1988 году большинство международных телекоммуникационных услуг предоставлялись государственными монополиями. В 2012 году вся деятельность стала коммерческой, отсюда разгул рыночных цен. Западная Европа и Северная Америка хотели защитить свободу рынка. Это было отклонено некоторыми странами из развивающихся с объяснением, что полностью свободный рынок на самом деле убьет небольших местных игроков, и рынок телекоммуникационных услуг будет захвачен крупными транснациональными компаниями.

Консенсус был достигнут добавлением формулировки, чтобы концепция свободного рынка учитывала национальные вопросы:

– Начало цитаты –

42B 6.1 В соответствии с действующим национальным законодательством, условия для международных соглашений о телекоммуникационных услугах могут быть установлены путем коммерческих соглашений или по учетным принципам, установленным в соответствии с национальным законодательством.

– Конец цитаты –

Европа хотела исключить любые упоминания о налогово-бюджетных вопросах, поскольку считала их выходящими за рамки ITRs. Европа также хотела включить пункт о поощрении конкуренции в сфере предоставления международного роуминга. Конечно, у других регионов также были их запросы и точки зрения.

Напряженная работа, проведенная рабочей группой по выработке текста Статьи 6, привела к в конце концов к достижению. Она покрыла международные соглашения по телекоммуникациям, некоторые основные принципы тарификации, включая определение денежной единицы, которая будет использоваться в составе расчетных такс, сборов и платежей, и даже статья о налогообложении, а также две об услугах связи.

1.6.9 Другие спорные разделы

Было и несколько других предложений из всех регионов, дошедших

до дискуссионного стола конференции. Предложения о роуминге, например, были переданы вниз и включены в Регламент.

Например:

– Начало цитаты –

38A 4.4 Члены Союза должны способствовать мерам по обеспечению того, чтобы уполномоченные органы своевременно предоставляли бесплатную, прозрачную, актуальную и точную информацию по услугам международной связи конечным пользователям, в том числе о ценах международного роуминга и связанным с ним соответствующим условиям.

– Конец цитаты –

Это – европейская практика уже в течение некоторого времени. До сих пор предоставление таких подробностей было оставлено на усмотрение поставщика услуг. Другие пункты Статьи 4 упоминают также гарантию качества обслуживания для пользователей в роуминге, которое не должно отличаются качества от локальных пользователей, а также конкурентоспособные цены на роуминг.

Пакет предложений, инициированный Европейской организацией телекоммуникационных сетей (European Telecommunication Networks Organisation – ETNO) собрал много прессы до начала WCIT. Одно из таких предложений выглядело следующим образом:

– Начало цитаты –

3.2 Эксплуатационные организации должны стремиться обеспечить достаточные средства электросвязи для удовлетворения потребностей и спроса на международные услуги электросвязи. Для этой цели, а также для обеспечения адекватной отдачи от инвестиций в инфраструктуру высокой пропускной способности, эксплуатационные организации заключают коммерческие соглашения для достижения устойчивой системы справедливой оплаты услуг связи и, при необходимости, соблюдение принципа «платит сеть отправляющей стороны». Источник C 109 (ETNO).

– Конец цитаты –

Это вызвало **массовую реакцию в Интернете**: плоская модель ценообразования в Интернете оказалась под угрозой замены на «платит сеть отправляющей стороны». Интересно, что WCIT получила значительно

больше внимания СМИ отчасти из-за этого предложения, благодаря нескольким кампаниям, которые Google и другие организации провели для борьбы с предложением «платит отправляющая сторона». В то время как до WCIT поддержка этого предложения со стороны развивающихся стран была еще значительной, так как их подключение к Интернет было дороже, было ясно дано понять, что в соответствии с принципами свободного рынка, поставщик информации может, на самом деле, решить прекратить отправку информации вообще, поместив в черные списки диапазоны IP-адресов, обслуживаемые в режиме «платит отправитель». Короче говоря, серьезно раскрученное предложение было заброшено и закончилось тем, что не стало разрушителем договоренностей. В результате пункт гласит:

– Начало цитаты –

29 3.2 Члены Союза должны стремиться обеспечить предоставление достаточных средств связи для удовлетворения спроса на услуги международной связи.

– Конец цитаты –

Оставшаяся часть Статьи 3 вызвала серьезные разногласия в вопросах о маршрутизации. Некоторые страны настаивали на возможности определить, какие международные телекоммуникационные маршруты были использованы исходящим от них трафиком. Это вызвало массу обсуждений. С одной стороны, сторонники свободного рынка объясняли, что информация о маршрутизации зачастую конфиденциальна у операторов, и что провайдеры, предоставляющие канал для исходящего потока, не обязаны делиться своей маршрутной информацией. С другой стороны, группа стран, требующих информации о маршрутизации «от и до», настаивала на своих требованиях. Анализ этого разногласия дал тот факт, что у обоих лагерей есть свои законные интересы. Стало ясно, что технического способа для телекоммуникационной компании узнать точную маршрутизацию исходящего потока не существует, следовательно, это вопрос исключительно доброй воли провайдера верхнего уровня, затем следующего, и так далее и так далее. В сегодняшних телекоммуникационных сетях может быть много участвующих в процессе третьих сторон, и отслеживание, даже не говоря уже об управлении этим отслеживанием, технически и административно невозможно. Тем не менее, страны с законной озабоченностью по поводу конфиденциальности своего телекоммуникационного трафика решили, что они хотели бы, чтобы их трафик избегал отдельных стран из-за политической нестабильности.

В результате наконец был достигнут компромисс (в процессе множества дискуссий), сформулированный так: «Уполномоченная эксплуатационная организация, создающая трафик, может выбрать, чтобы ее исходящий телекоммуникационный трафик направлялся в определенном направлении,».

Это не удовлетворило все стороны, но это было лучшее, что могло быть достигнуто, чтобы выйти из тупика.

Было достигнуто соглашение о первой части Статьи 5, «Безопасность жизни и приоритеты коммуникаций», задающих приоритетность таких видов связи, как связь при бедствиях, а также публикацию номера экстренной службы, используемого на определенной телекоммуникационной территории. Конференция не достигла согласия о введении единого номера экстренной помощи для использования во всем мире из-за высоких затрат на внедрение в некоторых государствах, обладающих менее современной инфраструктурой.

Некоторые статьи не оспаривались, и после, не найдя возражений на пленарном заседании, были переданы в Редакционный комитет. Но проблема оказалась в том, что обсуждение некоторых других статей зашло в тупик.

1.7 В поисках консенсуса

По прошествии недели стало ясно, что по многим вопросам консенсус найден быть не может. В результате, Председатель конференции, г-н Аль-Ганим (Mr. Al-Ghanem), видя, что, путем отправки вопросов в небольшие рабочие группы результаты получены не были, решил сделать свою собственную небольшую рабочую группу, пригласив председателей всех регионов, плюс несколько отобранных представителей, избранных от каждого региона, а также глав делегаций, не входящих в регионы, на небольшое, закрытое вечернее заседание, продолжившееся в понедельник (10 декабрь 2012 года) ночью. Оно было названо «Узкое совещание председателя» и продолжалось до 1:30.

Результаты этого совещания были умеренными.

Положительная сторона:

- Рабочей группе удалось найти консенсус по ряду статей, которые были бесспорны или где зазор между точками зрения был небольшим;
- Тот факт, что работа проводилась лицом к лицу, сделал прогресс быстрее;
- Эта встреча дала Председателю конференции более четкую общую картину спорных и бесспорных статей;
- Обмен между делегатами был очень откровенный.

Отрицательная сторона:

- Встреча состоялась поздно ночью, за закрытыми дверями, в результате чего участники были отделены от своей делегации и, следовательно, было увеличено давление на них согласиться на консенсус тут же и сразу;
    - Полное отсутствие какой бы то ни было прозрачности при встрече
    - Неизвестно, существуют ли какие-либо записи этой встречи
    - Чрезмерное давление на делегатов, зависящих от своего региона, играло на пользу самостоятельных делегатов (это относится к тому, как делегаты работают)
        - В случае CEPT, 4 представителя от региона, состоящего из 48 членов, не могут гарантировать, что какая бы то ни было позиция окажется приемлемой для всех его членов
- Во время встречи было некоторое количество позерства, с психологическим давлением, оказанным из-за изоляции делегатов, сопротивляющихся переменам;
- Совещание, состоявшееся поздно ночью, использовало усталость делегатов, повышая тем самым возможность ошибочных решений под давлением. В коммерческом мире это может приравниваться к «действию под принуждением».

Привыкшие к переговорам по международным договорам участники сказали мне, что такой режим работы, **изоляция глав регионов вместе в комнате с тем, чтобы они договорились друг с другом – обычная практика**. Вместо того, чтобы рассматривать каждую статью по очереди, с учетом ее качеств, некоторые страны пытались заменить процесс на бартер, соглашаясь отказаться от некоторых требований, если другие будут оставлены в силе. Такой подход абсолютно порочен: вы не можете из двух неправильных законов сделать один правильный, принимая один и отвергая другой. Такой бартер может быть применим в международной дипломатии в отношении войн и территории, но просто не может применяться к Регламентам, влияющим на международные телекоммуникации.

Как бы его ни назвали – «пакетное соглашение», «бартер», «давать и брать» или «компромисс» – встрече не удалось достичь немедленного консенсуса по вышеуказанным пунктам. Руководители делегаций затем вернулись к своим делегациям во вторник утром, спрашивая, нет ли способа изменить позицию для достижения консенсуса. Это не стало достижением, заседания рабочих групп, **заседания COM 5 и пленарное заседание так и не продвинулись на следующий день**.

Отказ Евросоюза идти на бартер (хотя и открытость для некоторого рода пакетной сделки) был фактически использован против Европы: некоторые члены из арабского и африканского регионов, несколько раз в

течение остальной части заседания отметили в протоколе, что они пришли к столу и предложили много уступок и компромиссов в то время как Европа отказалась. Европу несправедливо объявили "плохишом" конференции.

На протяжении вторника 11 декабря делегации были разделены на более мелкие группы, так как больше времени было потрачено на более закрытые заседания для региональных лидеров. Хотя официальной информации с этих встреч проникло мало, некоторые делегации были четко проинформированы внутри. Некоторые рабочие группы также встретились и продолжили обсуждение менее спорных частей Договора хотя одна из сессий, о недискриминационном доступе к Интернету, шлифовка статьи 3.7 предложенной Кубой, оказались в патовой ситуации, и рабочая группа направила его обратно на пленарное заседание в таком виде:

[**Добавить**

31D 3.8 Члены Союза должны воздерживаться от принятия [односторонних и/или] дискриминационных действий, которые могут препятствовать доступу другого Члена Союза к публичным [международным телекоммуникационным сетям и услугам] / [Интернет-сайтам и использованию ресурсов].]

(Заметьте – все предложение кишит квадратными скобками)

Это и многие другие предложения были включены в согласованный текст Председателя, который затем поздней ночью опубликовал ITU. Большое количество текста в квадратных скобках по всему документу свидетельствует, что документу до консенсуса еще далеко.

Опять же, некоторые вопросы были обработаны один за другим, в рабочей группе Com 5, а затем на пленарном заседании в среду. Прогресс в сложных вопросах был медленным, так как рабочие группы вернули текст в том же виде, что и получили, иногда только с большим количеством квадратных скобок, чем в начале.

1.8 Карты на стол – часть 1

Можно сказать, что в главном конференц-зале к полудню в среду царила некоторая напряженность, когда стало известно о незначительности прогресса, достигнутого за последние 24 часа. К тому времени стало ясно, по каким статьи консенсус найти возможно, и какие станут разрушителями договоренностей. Некоторые наблюдатели полагали, что еще есть возможность заключить договор, если будет принят

статус-кво по остальным статьям, и будет подписан договор, обновляющий только те статьи, по которым найден компромисс или достигнут консенсус.

Напомним, что переговоры в Дубае предназначались для обновления Регламента 1988 года, поэтому по умолчанию подразумевалось, что если Договор подписан не будет, все вернется к Регламенту 1988 года. Для некоторых стран это было бы вполне приемлемым вариантом.

Тем не менее, хотя Председатель конференции г-н аль-Ханеми по согласованию с Генеральным секретарем ITU доктором Туре, мог предложить отложить действительно сложные вопросы на будущую работу ITU, тем самым проложив для нее путь, это не было явно озвучено в ходе сессий. Председатель в какой-то момент ссылался на такое решение, возможно, неофициально, но оказалось, что некоторые страны хотели покончить с вопросами здесь и сейчас, выдвигая обвинение, что за 24 года ожидания было время для подготовки решения **всех** вопросов немедленно – или договариваемся, или нет. Это было расценено как довольно жесткая тактика.

Во второй половине дня (или ранним вечером) в среду 12 декабря 2012 года начали обсуждать новую версия Регламента на основе прогресса или отсутствия прогресса в течение дня. Так как обсуждаемые вопросы – а именно все перечисленные выше «скользкие моменты» – уже обсуждались по несколько раз, то страсти разгорелись нешуточные. Несколько делегатов попросили микрофон и делали все более эмоциональные заявления, причем некоторые касались личных комментарии о поведении и способностях других делегатов. Председателю г-ну Аль-Ганиму было все труднее и труднее добиваться от делегатов соблюдения своих 3- или 2-минутных лимитов по времени выступления и обеспечить хоть какой-то прогресс из-за огромного списка стран, требующих слова и отвечающих друг другу в ключе «око за око». С ростом напряженности, Председатель попросил 15-минутный перерыв на кофе, созвав председателей регионов в место рядом со сценой, чтобы обсудить вещи лицом к лицу в надежде выпустить пар и ослабить напряженность в зале. Это было особенно важно, так как все пленарные заседания транслировались в прямом эфире и имидж ITU мог быть подпорчен тем, что дебаты теряют элемент вежливости.

Что происходило без микрофона и как бы за кадром (хотя широкоугольная камера показывала скопление людей неподалеку от сцены) – было ничем иным, как потасовкой, хотя и остающейся чисто словесной, но включающей бурные размахивания руками и связанные с ними телодвижения на близком расстоянии. Сформировались две группы, по два лагеря в каждой, с делегатом от Португалии (представляющим CEPT) и представителем Европейского союза, противостоящих главным образом Ирану и Бахрейну, с г-ном Аль-Ганимом, который пытался успокоить страсти, но одновременно принял одну из сторон, попросив европейцев сесть за стол переговоров и компромисса, а не продолжать цепляться за свои собственные позиции. В другой группа участвовал представитель Соединенных Штатов, не соглашаясь с Объединенными Арабскими Эмиратами, и д-р Туре, довольно расстроенный обвинениями, что ITU пытается подмять Интернет, но другие могли бы тоже сказать, что

Интернет пытался подмять телекоммуникации. В такой скандальной обстановке, при ежеминутно разгорающихся стычках, никому не удавалось по-настоящему понять все позиции, занимаемые участниками, так как люди говорили громко, перебивая друг друга. Когда вокруг столпились десятки людей, чтобы мельком услышать аргументы и устно выразить поддержку точки зрения «своему лагерю», зрелище получилось не очень красивым. Ряд участников попросил «встречу» перенести в более приватное помещение, ограничив круг участников только главами регионов, как для того, чтобы успокоить людей, так и для того, чтобы избежать нелицеприятных фотографий или видеозаписей перепалок. Официальный сюжет ITU для прессы гласил, что достигнут большой прогресс, и есть основания считать, что конференция будет успешной. На тот момент, в опубликованной в новостях информации сквозило доверие этому посылу, так как ITU проделал серьезную работу в популяризации этого мессиджа, а Генеральный секретарь ITU д-р Туре использовал возможность в течение некоторых сессий критиковать обман и клеветническую кампанию против ITU, которая велась прессой и в Интернете в попытках обречь эту конференцию на провал. По его мнению, ITU стал жертвой дезинформации.

Сотрудники вытеснили толпу за пределы зала пленарных заседаний в меньшую комнату, фильтруя тех, кому было разрешено присутствовать. Главам регионов провели в этом помещении немало времени, но по их поведению было понятно, что никакого прогресса не случилось.

Ночь обещала быть долгой.

1.9 Широкий консенсус, который не стал голосованием

(Резолюция: Способствовать созданию благоприятной среды для большего роста Интернета)

Среда 12 декабря перешла за полночь, и «утром в четверг» в 00:30 было объявлено о включении Резолюции об Интернете. Впервые текст появился в файловой системе каждого, без анонса и без рассмотрения государствами в ходе хоть какого-то ни было формального процесса.

Некоторые страны немедленно попросили слова, и экран Председателя заполнился запросами. Несколько стран высказались за или против резолюции. Пока не началась серьезная дискуссия и не появились альтернативные предложения по формулировке этой резолюции, Председатель объявил, что он хочет «замерить температуру в помещении», путем показывания карточек с кодами стран, сродни общему поднятию рук по этому вопросу. **Входила ли туда поддержка этой резолюции?**

Люди в комнате к тому времени очень устали. В самом деле, объяснение, чего же хотел председатель, было запутанным для многих не англоговорящих делегатов, и из-за путаницы многие страны не выразили

свое мнение вообще.

Так как **это было не голосование**, точного подсчета уровня поддержки для этого шага не было. Автор приблизительно оценивает, что около 50 стран высказались в пользу включения Резолюции в документ, в то время как половина от этого числа была против его включения. Большинства **примерно в две трети** оказалось для председателя достаточно, чтобы объявить, что **Резолюция ратифицирована и будет частью Регламента**. Представители Великобритании и Швеции запросили выступления по процедуре, и всякий раз Председателя просили объяснить свое решение – **было ли это голосованием**? Ответом стало, что это было не голосование, и что Председатель принял решение включить Резолюцию в Регламент основываясь на «температуре в помещении».

Так как Заседание было закрыто, многие страны все еще не знали, что произошло. Атмосфера недоумения заполнила помещение, а многие другие делегаты испытали сильное чувство недоверия.

Эта потеря доверия к процессу ITU и к Председателю была первым ясным признаком трещины в Регламенте, трещины, которая будет расширяться по мере того, как Регламент будет обсуждаться в ходе дальнейших сессий в четверг. Несколькими часами ранее в среду Генеральный секретарь ITU д-р Туре вновь подтвердил еще раз, что ни один из документов не будет иметь намеков на Интернет, и что никаких голосований не будет. С «температурой в комнате», использованной для включения Резолюции в текст Договора, когда время приближалось к часу ночи и делегаты возвращались обратно в свои гостиничные номера, обещания приобрели вид соломенных.

1.10 Позиция Европы

С самого начала Европейский союз (ЕС) поддерживал координацию на высоком уровне и его представители выступали под знаменем Кипра. Еще до Конференции, делегации стран-участниц получили сводный документ, включающий все вопросы, вызвавшие обеспокоенность в странах-участницах. Позиции по ним были четко определены, хотя уровень гибкости, продемонстрированной разными странами, мог отличаться. Для некоторых стран отдельные вопросы были критическими.

В частности, общим критическим вопросом было использование термина «Телекоммуникации» и «Информационные и коммуникационные технологии», которые, как уже упоминалось ранее, включили бы в себя не только телекоммуникационную инфраструктуру, но и все вычисления и услуги, тем или иным образом связанные с телекоммуникациями.

В ходе конференции общая позиция ЕС сохранялась при помощи ежеутренних брифингов и закрытых для не делегатов ЕС обсуждений. К началу второй недели переговоров некоторые участники от ЕС были

весьма удовлетворены тем, что наиболее решительно осуждаемые ими статьи оказались либо смягчены, либо нейтрализовались остальным содержанием Договора, либо вообще удалены из текста Договора. В результате некоторые страны, возможно, были более склонны подписать финальный Договор, чем другие. Существовала реальная обеспокоенность тем, что, будучи непримиримыми в стольких позициях, **участники от ЕС будут объявлены «плохишами» Конференции**. Несколько делегатов сообщили о резкой критике со стороны других регионов, смысл которой сводился к тому, что ЕС был единственным регионом, пришедшим к столу не для того, чтобы договариваться, а для того, чтобы **навязывать** свои позиции. **ЕС был обвинен в неготовности вести переговоры; высокомерии, колониализме; несправедливости и прибытии в Дубаи исключительно с целью срыва процесса Договора**. Это тоже создавало сильное психологическое давление на многих делегатов. В результате при изучении последней версии Регламента некоторые делегаты были более склонны видеть стакан наполовину полным, в то время как другие видели стакан наполовину пустым. Однако в целом сложилось понимание, что Европа пришла к конференции с полным стаканом и что она сделала много уступок, ни одна из которых не была принятой теми, кто их просил. Раздражающим моментом было то, что просящие об уступках страны просили все больше и больше каждый день, и это таки вернуло к ощущению реальности со стороны тех стран, которые были готовы подписать.

Важность европейского единства подтвердилась на последней встрече делегатов ЕС. ЕС, возможно, согласился бы с последней версией Регламента, предложенной Председателем, при условии, что будет включен ряд небольших правок (и некоторый свежий взгляд на определение спама), и при условии, что больше ничего уступать не придется. В результате европейские страны могли бы подписать Регламент, четко добавив оговорку под их подписью об отказе нескольким статьям – тем самым статьям, что были описаны ранее в этом документе. Положительным фактором было то, что несколько статей представляли собой результат отличного диалога и полностью поддерживались. Так что некоторые считали, что было бы жаль, если бы вся эта работа пропала впустую.

Поэтому было решено занять *выжидательную* позицию в следующем пленарном заседании. Было время для консенсуса и было признано, что Председатель Конференции проделал большую работу, чтобы этот консенсус был достигнут.

При этом было оговорено, что, если другие страны будут продолжать настаивать на дальнейших изменениях, идущих против позиции ЕС, страны ЕС вернутся обратно к позиции «не подписывать», что оставит в силе Регламент 1988 года, что рассматривалось как крайний приемлемый вариант.

Стоит отметить, что позиция ЕС преобладала в позиции СЕРТ, хотя в

CEPT входит больше стран, чем в сам ЕС. Так как от имени CEPT выступала Португалия, на плечи португальского делегата был возложен знасчительный груз.

1.11 Карты на стол – часть 2

По неофициальным каналам была получена информация, что арабский и, особенно, африканский регионы, остались недовольными компромиссным документом Председателя. Кроме того, оказалось, что некоторые участники из арабского региона будут очень активно отстаивать свои точки зрения в заключительном пленарном заседании. Оно началось в четверг вечером. Было ясно, что Председатель чувствовал, что «его» компромиссный документ мог пройти европейские страны, и обратная связь от этих стран к Председателю была положительной. Но, чтобы удержать хрупкий баланс, в этот документ нельзя было вносить больше абсолютно никаких изменений в другом направлении. Преамбула документа была минным полем, так как касалась непосредственно **прав человека**. Несколько стран из арабского региона и Африки выразили свое несогласие с текстом в предложенном виде. Они сразу же оседлали своего конька, при очень незначительном вмешательстве со стороны ЕС или Америк. Их тактика осталась прежней: забить заседание все той же риторикой против текста и вступить в поединок с Председателем г-ном Аль-Ганемом.

Как только предложенный кусок текста оказался слишком горячим, чтобы на нем настаивать, особенно в противовес позиции ЕС и США, для которых уже было ясно, что она критична, Председатель конференции отступил и решил исключить текст. Это взбесило делегатов из стран Ближнего Востока.

Опять всплыло предложение о включении имен, адресов и нумерации (Пункт 3.8 теперь был предложен как 3.5), которое сделало бы государства-участники ответственными за функции, в настоящее время принятые на себя ICANN и региональными Интернет-реестрами, даже после того, как это было неоднократно отклонено в предыдущих семинарах, на группе COM 5 и пленарных заседаниях. Предложившая его Танзания почувствовала жар и отозвала предложение. На минутку напряжение спало, и Председатель посмеялся: «*Если бы мы начали конференцию в таком духе, я думаю, мы бы закончили ее за три дня*.»

Это было затишьем перед бурей.

Несколькими минутами спустя, после подтверждения консенсуса, достигнутого по многочисленным статьям, Председатель вернулся к преамбуле и борьба за включение вопросов прав человека внезапно интенсифицировалась и трансформировалась во включение предложения Кубы, ранее уже отклоненного и на встрече специальной рабочей группы,

далее не нашедшего консенсуса на сессии Com 5 и теперь опять вернувшегося на пленарное заседание. В попытке найти компромисс Председатель предложил включить в текст преамбулы фразу «*и признать право доступа к услугам международной связи*».

Иран настаивал на правах **государств-участников**. Напряженность возросла еще больше, когда США и ряд европейских стран заявили о несогласии со смешиванием персональных прав человека с правом государств на недискриминационный доступ к телекоммуникациям, которое не имеет ничего общего с индивидуальными правами.

В результате список запросов на выступление резко вырос. «За» выступили Иран (от имени АРТ), Китай (подчеркивая свою поддержку обсуждавшимся ранее африканским предложениям), Куба, Россия, Алжир, Ботсвана (хотя они и пытались навести мосты), Объединенные Арабские Эмираты, Иордания. Противоположной точки зрения придерживались Швеция, США, Великобритания, Польша, Коста-Рика и еще длинный список стран. Некоторые делегаты, например, Ливан, тоже пытались навести мосты... но безрезультатно. Текст продолжали кромсать и тасовать, и стало ясно, что в глубине лежит скорее культурная проблема: с одной стороны, культура государства, ответственного за своих граждан, потому нуждающегося в «недискриминационных правах государств-участников» в целях обеспечения своих граждан «индивидуальным недискриминационным доступом», в то время как с другой стороны им противостояла культура «индивидуальных прав человека», включающая отсутствие дискриминации на индивидуальной основе.

Проблему достаточно четко объяснила Швейцария (из стенограммы):

«Мы хотели бы добавить кое-что, а именно: Означает ли это, что вы уравниваете индивидуальные права, которые, безусловно, являются правами человека, с правами государств-участниц. Это вряд ли может оказаться для нас приемлемым. На самом деле это шокирует нас и с точки зрения права, и с философской точки зрения. Это никак не может рассматриваться как одно и то же.

Права человека применяются к гражданам. Государства-участники – это нечто совершенно иное.

Мы понимаем проблемы, поднятые многими из присутствующих здесь государств в отношении недискриминационного доступа. И мы думаем, что... и мы не думаем, что можем идти в этом направлении. У нас сложилось впечатление, что это – попытка создать новое право человека. Так что нам придется очень постараться, чтобы найти другое решение стоящей перед нами проблемы, и проблемы, поднятой определенным количеством стран в отношении недискриминационного доступа.»

Эту позицию поддержала Дания, Чехия и Канада, но против выступили Бахрейн и Индонезия. Далее была попытка д-ра Туре, Генерального секретаря ITU, снизить напряженность, который попросил Председателя изъять текст из Регламентов вообще. Проблема была в том,

что его послание было неоднозначным. Председатель Конференции г-н Аль-Ганим считал, что сохранение оригинального текста, включая права человека, но исключая права государства было безопаснее. Он снова спросил насчет консенсуса по этому вопросу.

Это спровоцировало усиление давления со стороны Ливана, Ирана, Южной Африки (индивидуально, а затем представляющей Африканскую группу), Китай (с длинной лекцией о правах человека), Судана... пока **Иран внезапно не привлек правило ITU 100.03 сделав ход «закрытие дебатов» и «поставить африканское предложение на голосование».**

Напряжение достигло апогея: Генеральный секретарь ITU д-р Туре говорил несколько раз на протяжении конференции, что, если этой конференции придется прибегнуть к голосованию – это будет **провал**. Этот финальный демарш сломал тщательный баланс итогового документа, предложенного Председателем, тут же заморозил зал, а европейские страны твердо решили не подписывать Договор. Требование голосования выглядело как силовая игра, нарушившая вместе и консенсус и гармонию, и вызвавшая переход в защиту. **Вина за срыв Конференции лежит на тех, кто больше всего желал достичь результата**.

Далее последовало очень суматошное голосование, несколько стран выступали по порядку ведения заседания, не понимая чего от них хотели. Первое голосование было по закрытию дебатов. 93 – «За», 0 – «Против», 16 – «Воздержались».

Затем было голосование по включению следующего предложения в преамбулу:

«Эти Регламенты признают право доступа государств-участников к международным телекоммуникациям»

Необходимое большинство составляло 56 голосов. Результаты были 77 – «За», 33 – «Против» и 8 – «Воздержались». Текст был принят. Председатель немедленно объявил, что поскольку было проведено голосование о прекращении прений, они не могут быть вновь открыты для остальных Регламентов. Так, сделав все возможное для достижения консенсуса, это голосование сделало полный текст Регламентов DT/55, ***принятым в новой редакции***.

Этот драматический финал Конференции был логическим завершением двух недель возраставшей очевидности того, что закончилось разговором двух разных сторон не друг с другом, а друг мимо друга.

Соединенные Штаты, поддержанные Великобританией, Швецией и другими сразу же заявили, что их страны не станут подписывать Регламенты и попросили, чтобы их заявление было занесено в протокол. После нескольких заключительных ремарок

пленарное заседание закончилась в 22:30 перерывом. Следующее заседание было коротким и прошло без дебатов. Голосование было геймом, сетом и матчем – только не ясно, чья сторона победила и победил ли кто-либо вообще.

1.12 Эпилог по ITRs

В результате, из 144 стран, имеющих право подписи, 89 стран подписали ITRs, а 55 стран подписывать их не стали. Вполне может быть, что некоторые страны, не подписавшие Договор, сделают это до его вступления в силу в январе 2015 года. Это касается стран, делегациям которіх необходимо проконсультироваться со своим правительством или Национальным собранием.

Из подписавших стран, многие сопроводили подпись замечаниями и оговорками типа:

«При подписании Заключительных актов Всемирной конференции по международной электросвязи (WCIT-12), делегация [страны] оставляет за [страной] право не применять любые его положений, могущие противоречить его законам или международным соглашениям, в которые она входит.

Кроме того, [страна] оставляет за собой право не применять положения этих актов в отношении государств и организаций, которые не в состоянии соблюдать их или применять их.»

Календарь ITU полон последующими конференциями и встречами, более или менее связанными с результатами WCIT: Всемирный форум неофициальной группы экспертов по технологической политике (World Technology Policy Forum Informal Experts Group, WTPF13-МЭР) в феврале 2013 года; Всемирный саммит по информационному обществу (World Summit on Information Society, WSIS-13) открывает процесс консультаций в феврале 2013 года; заседания различных исследовательских групп по сетям следующего поколения, включая SG/WP13, а также координационное совещание по Интернету вещей; форум WSIS в мае 2013; WTPF13 в мае 2013; Полномочная конференция в октябре 2014 года и т.д.

Мультистейкхолдерный подход может настроить ITU на очень энергичную Полномочную конференцию, которая долдна состояться за несколько месяцев до вступления в силу новых Регламентов. Особый интерес представляет разрешение неловкой проблемы: как имплементировать Договор при том, что он не подписан более чем 50 странами? Создаст ли это два отдельных телекоммуникационных мира? Некоторые говорят о «расщеплении» Интернета на несколько отдельных частей, но вопрос гораздо глубже, так как Интернет – это всего лишь подмножество мировых телекоммуникационных сетей.

Нерешенными остаются вопросы: обязательны ли Регламенты? Если сейчас они не носят обязательного характера, могут ли они быть сделаны обязательными на Полномочной конференции? Если они станут обязательными для участников, подписавших Регламенты, как устанавливать взаимодействие с не подписавшими, помня, что для связи необходимы устройства на обоих концах линии связи? Имеет ли ITU возможность сделать Регламенты обязательными для всех, в том числе и для тех, кто их не подписывал? Помня, что Регламенты нужно еще и ратифицировать на местном уровне, не столкнемся ли мы со сценарием, когда в странах откажутся имплементировать Регламенты по соображениям суверенитета?

Ясно видно только то, что на горизонте просматривается много суматохи. Однако вместо того, чтобы ее игнорировать и позволить суматохе сбить мир с ног, вместо того, чтобы реагировать на нее пост-фактум, было бы целесообразно подготовиться к будущему. Многие правительства уже работают со своими командами по этому вопросу. WCIT – это уже прошлое и результат конференции изменить уже не получится, но она была важным событием, в первую очередь тем, что обнажила вопросы, вызывающие глубокие разногласия в зависимости от типа управления, предложенного на правительственном уровне. Понятно, что точки зрения государств фрагментированы. Хотя некоторые точки зрения основываются на геополитическом позиционировании, некоторые из них вызваны текущей недостаточностью разъяснений своей работы в рамках мультистейкхолдерной модели и в активности привлечения новых участников.

Второй раздел этого доклада будет посвящен предложениям о работе, которую необходимо проделать учреждениям, поддерживающим модель мультистейкхолдеризма, для заполнения пустот, на которые пеняли некоторые страны, легитимизируя ITU как основной, или, пожалуй, единственный «форум», на который стоит обращать свое внимание при рассмотрении будущего международной связи как в технических, так и в политических вопросах. Некоторые из этих предложений будут предназначены, в частности, для ICANN, и для сообщества At-Large ICANN, как примера управляемой интернециональной управленческой сети, начиная с самых низов и до всемирной политики присвоения имена и номеров.

2. Рекомендуемые дальнейшие действия

В этом разделе доклада речь пойдет о полученном опыте и рекомендациях автора касательно дальнейших действий, которые следует предпринять по итогам двухнедельной Всемирной конференции по международной электросвязи (WCIT).

2.1. *Внесение ясности*

- Будет неверным утверждать, что некоторые страны отказались от участия в знак протеста.
- Было бы неверным также утверждать, что некоторые страны умышленно пытались сорвать конференцию.
- Было бы неверным сказать, что конференция получила абсолютный успех. В сущности, во многих отношениях она потерпела крах.
    - Независимо от успешности этой конференции ITU будет и в дальнейшем организовывать мероприятия такого рода.
    - Существует еще много аспектов этой конференции, которые будут обсуждаться в других составах рабочих групп и деятельности ITU.
    - В огромном проигрыше оказались страны, которые действительно нуждались в отдельных регламентах международной электросвязи (ITRs) относительно сухопутных стран, роуминга, определения стоимости и других регуляторных вопросах. В результате подхода “все или ничего” многие страны не подписали ITRs, которые были бы полезны для них.
- Отсутствуют абсолютные победители как таковые.

Опыт, полученный в результате такой конференции, очень важен по нескольким причинам: это первая конференция такого рода за 24 года; она позволила всем странам обсудить будущее международной электросвязи и вынесла на всеобщее рассмотрение вопросы, которые ранее замалчивались. На сегодняшний день гораздо четче прояснился вопрос о роли каждой страны в сфере международной электросвязи, чем это было до начала Конференции.

Одним из основных уроков, полученных мною благодаря возможности присутствовать на всех формальных встречах в силу моей аккредитации в качестве полноправного представителя Соединенного Королевства, было

чувство непонимания действующей модели мультистейкхолдеризма, на которой построен Интернет. Существует также непонимание использования принципа “снизу-вверх”, процесса участия в этой многосторонней работе и отсутствие любых программ, способных предоставить государству информацию о направлениях развития Интернета, что приводит к глубокому недоверию к самой модели. В целом, большинство стран южного полушария убеждены в том, что Интернет фактически управляется и контролируется Соединенными Штатами и их союзниками. Они уверены, что сеть используется в качестве основного средства, направленного на ослабление их собственных экономик, тем самым приносит огромные социальные и политические изменения такими темпами, которые являются разрушительными, и не оставляет возможности таким странам для управления этими процессами. Существует мнение, что Интернет *регулируется* странами с сильнейшей экономикой и транснациональными компаниями в их собственных интересах. Этим в действительности обеспокоены не только представители государств, присутствовавшие на ВКМЭ, но также обычные граждане во многих из этих стран.

На самом деле, во многих странах мало известно об **изменениях в социальном и общественном развитии**, которые может принести Интернет в случае, если правительства, политики, частный сектор и гражданское общество (вместе с конечными пользователями Интернета) **на равных правах** примут участие в разработке модели Интернета в качестве заинтересованных сторон. Эти изменения уже оказывают положительное влияние в Северной Америке и Западной Европе (известных как Север и Запад), хотя отдельные представители в некоторых странах могут заметить, что модель представляет собой постоянную борьбу. Очевидно, для того, чтобы в итоге все страны оказались в выигрыше, потребуется немалое наращивание потенциала и повышение обучения модели мультистейкхолдеризма в рамках экосистемы в среде Интернет во всем мире.

2.2. *Общие рекомендации*

2.2.1. Принятие активных мер по поддержанию действующей мультистейкхолдерной среды управления Интернетом в целом

Действующая мультистейкхолдерная экосистема модели управления Интернетом включает в себя Оперативное техническое подразделение Интернет (IETF), Консорциум World Wide Web (W3C) и Международную корпорацию по присвоению имен и номеров (ICANN). Действуют также аналогичные организации для ПО с открытыми исходными кодами, антиспамовый консорциум, а также организации, которые занимаются многими другими аспектами Интернета - техническими, правовыми и т.д. Эти организации стремятся использовать открытую модель, поскольку новичкам предлагается принять участие и сформировать свою позицию, будучи вовлеченными в мультистейкхолдерный процесс.

В действительности, существует несколько барьеров на пути такой непрерывной интеграции:

- Отсутствие знаний у новичков:
    - Знание среды: что является конечной ключевой целью?
    - Исторические и институциональные знания: когда возможное решение/способ использовались в прошлом и принесли успех/поражение?
    - Политические знания: незнание мощи и потенциала каждого из участников дискуссии, что может привести к тому, что понадобится много времени для достижения компромисса.
    - Где находится центр управления знаниями?
- Закрытость сообществ / барьеры, связанные с вступлением в них:
    - Сама природа сообщества сводится к принадлежности к нему.

Каждый, кто не входит в сообщество, сталкивается с определенными трудностями при спонтанном желании принять участие в его деятельности;

- Скрытые преграды к полноправному участию в обсуждении: отсутствуют какие-либо “разрешения” или методы подтверждения законности или опыта участника, кроме их онлайн признания со стороны членов сообщества. Такой подход и является тем самым фактором, который часто приводит к плачевной практике, когда обсуждение оказывается закрытым для посторонних. К сожалению, среди членов сообщества существует обыкновенная тенденция подвергать сомнению *полезность* новичков, если их личность достоверно не известна.
- Неразбериха: очень сложно заинтересовать многоязычное сообщество без значительных инвестиций в устный и письменный перевод.

- Периодические поглощения коммерческими интересами некоторых управленческих процессов:
  - Время - деньги: участие в этих процессах занимает много времени. Корпорации, чей бизнес непосредственно связан с текущей работой, могут платить сотрудникам за то, чтобы они потратили полный рабочий день на решение задач. Другие же компании могут не иметь возможности командировать своих сотрудников в поездки с целью проведения личных встреч;
  - Большие фирмы используют лоббирование, а также другие средства в целях продвижения своих интересов. Таким образом, основанная на принципе «снизу-вверх» мультистейкхолдерная модель обвиняется в том, что она является всего-навсего пустыми словами, используемыми

транснациональными корпорациями.

- Неизвестная модель финансирования:
    - Регистрационный сбор; коммандировки; звонки - кто платит за все это?
    - Финансовая поддержка волонтеров: предоставляется или нет? Если предоставляется, то могут ли волонтеры все еще продолжать считаться таковыми?
- Неизвестная модель лицензирования:
    - Несмотря на то, что уже проделано много работы, становится все труднее определить интеллектуальную собственность в сфере функционирования модели мультистейкхолдеризма;
    - Различие юридических подходов в разных странах.

Очевидно, должны быть ответы на многие из этих вопросов. Не все многосторонние форумы открыты для всех. Не существует “инструкции” сродни вводному курсу по мультистейкхолдерному Интернету.

Для того, чтобы мультистейкхолдерная модель управления была успешной, и поскольку Интернет сам по себе является такой огромной средой, продвижение должно осуществляться на нескольких уровнях и в каждой организации, чья сфера деятельности охватывает сегмент деятельности модели. Кроме того, следует признать, что сценарий развития событий, который устраивал бы всех, невозможен. Существуют глубокие различия между развивающимися и развитыми странами, перед ними открываются разные социально-политические перспективы, что делает задачу продвижения мультистейкхолдерной модели более сложной, чем в случае с однородной аудиторией.

2.2.1.1. Продвижение действующей мультистейкхолдерной модели Интернета в развитых странах мира

- Привлечение населения (конечного Интернет пользователя)

Даже без детального изучения различных моделей знаний, которые подробно описаны в Интернете и которые могут быть подразделены на множество дополнительных уровней, начиная от незнания, и заканчивая квалифицированными знаниями, можно выделить три основных уровня знаний в данной сфере: незнание (невежество), приобретение знаний (обучение) и практика. К сожалению, в настоящее время большинство заинтересованных сторон в развитых странах мира все еще находятся на уровне “невежества” в отношении мультистейкхолдерной модели управления и развития Интернета. Эта пустота должна быть заполнена, потому что Интернет является сильным вектором перемен в развитых странах мира, к тому же все больше участников рассматривают этот вектор как некую угрозу, над которой они не имеют никакого контроля, чем и объясняется определенное противостояние изменениям.

Крайне важно привлечь население к изучению мультистейкхолдерной модели Интернета. Она должна преподаваться в школах, как и любой другой серьезный предмет, к примеру, математика, искусство или классические языки. Предмет также должен читаться в университетах: его сложность при широком толковании охватывает политику, право, а также технические науки. Компьютеры и другое электронное оборудование, которые до сих пор считались привилегией вундеркиндов, теперь являются частью жизни каждого человека, и участие в мультистейкхолдерных процессах, описанных в этом докладе, может быть реализовано только при определенном уровне компьютерной грамотности. Интернет является одновременно самим инструментом, который позволяет управлять мультистейкхолденрной моделью, и в то же время ее крупнейшим выгодоприобретателем.

- Привлечение политиков

Развитие модели Интернета напрямую зависит от государственной политики. Правительства являются ключевой составляющей мультистейкхолдерной

системы. Поэтому очень важно, чтобы политики, ответственные за принятие решений, понимали мультистейкхолдерную модель Интернета, а именно понимали саму роль правительств в модели, его связь с другими заинтересованными сторонами, а также использовали модель с целью предпринять совместные усилия, направленные на восстановление экономики. Кроме того, нужно понимать, что любой новый закон, вводящий ограничения на контент, следует рассматривать в свете того, будет ли он иметь негативное воздействие на права человека, а также учитывать его разрушительное действие в более широком экономическом смысле. Безусловно, для политиков должна быть разработана широкомасштабная программа действий.

- Привлечение средств массовой информации

Средства массовой информации являются способом информирования и просвещения широких масс населения. Таким образом, их следует привлекать как можно чаще в целях ознакомления населения с вышеперечисленными вопросами. В то время, как социальные Интернет сети могут быть использованы для активизации опытных Интернет пользователей, средства массовой информации обладают знаниями и возможностями для мобилизации масс.

- Привлечение частного сектора

Частный сектор, возможно, получает наибольшую выгоду от мультистейкхолдерной модели управления Интернетом благодаря конкурентоспособному и нерегулируемому открытому международному рынку, который предоставляет мгновенный доступ с глобальным охватом. Ряд корпораций, которые стали первопроходцами, получили огромные доходы и значительную валовую прибыль. В целях своего же развития частный сектор по всему миру должен быть заинтересован в создании здоровой конкурентной среды, свободной от излишнего регулирования и потенциальной коррупции. Сбалансированная мультистейкхолдерная модель управления Интернетом нуждается в поддержке - особенно те заинтересованные лица, которые

обладают гораздо более ограниченными ресурсами. Этот вопрос больше не является вопросом выбора. Это не только вопрос спонсорства. Скорее, это вопрос этики и готовности активно поддерживать мультистейкхолдерную модель Интернета.

2.2.1.2. Продвижение действующей мультистейкхолдерной модели Интернета в развивающихся странах мира

Многие страны, которые поддержали ITRs, касающиеся Интернета, на WCIT сделали это потому, что они не чувствовали своей принадлежности к действующей мультистейкхолдерной модели Интернета.

- Правительственное участие

Проблемы разъяснительной работы и вовлечения новых участников, характерные для развитых стран, еще более усугубляются в развивающихся странах за счет того, что зачастую основным потребностям инфраструктуры, таким как электричество, доступ к воде и канализации, отдается предпочтение перед телекоммуникационными технологиями. Несмотря на то, что развитие телекоммуникационной сети является менее приоритетным, сама потребность в установке физической инфраструктуры в жесткой среде оказала положительное влияние на мобильную связь, по существу положив начало ее внезапному росту. В результате такого наверстывания развивающиеся страны столкнулись практически с теми же проблемами, что и развитые страны. Однако развивающиеся страны являются скорее пользователями электросвязи, чем ее поставщиками, что усложняет ситуацию. Телекоммуникации и услуги, предоставляемые через использование электросвязи, в первую очередь рассматриваются как затраты, а не как средство дохода. Электросвязь во всем остальном мире дорогая из-за более ограниченной пропускной способности. Мобильные телекоммуникации также сильно ограничены пропускной способностью. Кроме того, государственные ресурсы, которые могут быть

направлены на участие в мультистейкхолдерной модели, еще более ограничены, чем в развитых странах. Таким образом, очень важно, чтобы их участие происходило в два этапа:

- Создание всех необходимых предпосылок на государственном уровне
- Финансирование командировок членов правительства с целью участия в международных мультистейкхолдерных встречах

Обе эти инициативы связаны друг с другом. Недостаточно просто обеспечить развивающимся странам открытый доступ к обсуждениям. Должна быть предпринята согласованная попытка активно привлечь развивающиеся страны за стол переговоров с возможностью покрытия их расходов в рамках программы развития, с целью содействия стране в оказании помощи самой себе. Только с помощью такого укрепления потенциала на государственном уровне правительства смогут разработать и реализовать планы развития, которые помогут местным общинам и предприятиям в полной мере воспользоваться теми возможностями, которые телекоммуникации принесут стране. Обучение государственных чиновников в мультистейкхолдерном формате является столь же важным, как и помощь правительствам в том, чтобы они чувствовали себя желанными и непринужденно принимали участие в самом процессе.

Тем не менее, следует также признать, что некоторые государства также активно препятствуют участию и привлечению своих граждан по политическим мотивам. Это заведомо проигрышная битва, учитывая минимизацию объема технологий и непрерывный технологический прогресс, направленный на то, чтобы сделать связь повсеместной и более доступной для новичков. Легкий доступ к кодированию является еще одним способом положить конец диктатуре... но этой дискуссии, скорее всего, стоит посвятить отдельную главу, если не целую (виртуальную) библиотеку.

- Участие бизнес кругов

Превращение себестоимости в чистую прибыль было бы невозможным без

эффективного создания местных информационно-коммуникационных технологий (ИКТ). Термин “ИКТ для развития” хорошо известен участникам Форума по управлению Интернетом (IGF), поскольку достаточно рано удалось понять, что информационные технологии и телекоммуникации способны ускорить развитие. В целях поддержания равновесия в равноправной мультистейкхолдерной модели очень важно, чтобы бизнес круги в развивающихся странах были одинаково заинтересованы в вопросах управления Интернетом и телекоммуникациями, особенно учитывая тот факт, что инновации часто являются предпосылкой к созданию богатства. Мы были свидетелями того, когда простые идеи превращались в приложение, работающее на мобильном устройстве, которое в свою очередь может превратиться в основной капитал для создания компании по разработке приложений.

- Участие пользователей сети Интернет

На сегодняшний день Интернет пользователь является основным конечным пользователем телекоммуникаций. Тенденции в использовании мобильного телефона меняются так быстро, что было бы бессмысленным не допускать такого важного участника к управлению Интернетом. Хотя, на первый взгляд, кажется, что существует большая разница между моделями телекоммуникационного бизнеса в развитых и развивающихся стран, факты свидетельствуют об обратном. Стремления к возможности установления связи и содержанию схожи, разнятся только финансовые возможности и технические детали. Кроме того, изменения, внесенные использованием телекоммуникаций в повседневной жизни, могут быть приравнены к землетрясению, как в развитых, так и в развивающихся странах. В то время как в развитых странах в законы должны быть внесены поправки в контексте телекоммуникационных услуг, в развивающихся странах, возможно, понадобится выстраивать новые политические рамки в целом. Поэтому крайне важно поддерживать отдельных лиц, достигших нужного уровня знаний, чтобы стать местными лидерами,

которые примут участие в мировой мультистейкхолдерной управленческой среде – и хотя бы предоставить им благоприятные условия и позволить объединяться с другими пользователями по всему миру, которые находятся на том же уровне, чтобы они могли защищать права Интернет пользователей в своей части мира.

Также важно, чтобы конечные Интернет пользователи были осведомлены о том, как функционирует модель мультистейкхолдерного управления Интернетом, построенная по принципу “снизу-вверх”, с тем, чтобы они могли обращаться к своим государственным чиновникам и промышленным кругам с просьбой принять практическое участие в этом процессе.

2.2.1.3. Продвижение действующей мультистейкхолдерной модели Интернета на форумах ITU

Действующая модель ITU не является мультистейкхолдерной. Вместо этого, она основывается на принципе многосторонних переговоров, который предоставляет национальным государствам исключительное право на принятие решений. Некоторые могут поставить под сомнение такую структуру, но в данном докладе отсутствуют комментарии по этому поводу.

Еще одним способом расширить мультистейкхолдерность является тот, который фактически открыто поддерживался руководством ITU в ходе WCIT: включение неправительственных участников в состав правительственных делегаций.

Несколько делегаций использовали эту модель. Она имела ряд преимуществ:

- Возможность сформировать более численную делегацию:
    - распределяя рабочую нагрузку между несколькими ее членами
    - возлагая на делегатов обязанность самостоятельно оплатить

свое участие, тем самым уменьшая расходы

- Более широкий спектр знаний, опыта среди своих собственных делегатов, которые могут быть применены в любой момент
- Возможность донести точку зрения многочисленных участников / гражданского общества, бизнес кругов и т.д.
- Более законная модель принятия решений, чем модель, построенная на концентрации власти

В ходе WCIT стало очевидным, что неправительственные члены правительственных делегаций часто использовали другие ресурсы для финансирования своего участия. В случае с бизнес структурами, плата за их участие могла предоставляться в качестве спонсорских средств, направленных на активизацию улучшения управленческой среды. В этом-то и состоит весь интерес для частного сектора, который и побуждает его участвовать в мультистейкхолдерных встречах. То же самое касается некоммерческих учреждений, которые профинансировали своих делегатов. Однако предстоит еще долгий путь до того, как удастся найти модель финансирования, которая будет в состоянии поддерживать самостоятельных участников или участников, представляющих организации гражданского общества, которые не могут полностью покрыть все расходы, и/или участников из развивающихся стран.

В результате, большинство мультистейкхолдерных делегаций на WCIT представляли развитые страны. Этот дисбаланс необходимо изучить, и найти соответствующее решение. Другие участники (государства и частный сектор) должны быть ответственными за поиск совместного решения с целью поддержания **равноправия среди заинтересованных сторон** за столом переговоров.

Безусловно, найдутся страны, которые будут **противостоять** мультистейкхолдеризму, рассматривая ее как вызов их суверенитету, не осознавая при этом, что эти два явления совершенно различны по своей

природе. Государство - суверенно. Помощь государству в принятии правильного решения не угрожает его суверенитету.

Таким образом, является ли жизнеспособной в долгосрочной перспективе действующая модель, что оставляет за государствами право выбора модели формирования их собственных делегаций, которые необязательно должны быть мультистейкхолдерными? Наверное, нет.

2.2.2. Улучшение мультистейкхолдерной модели с целью обеспечения максимального охвата

Каким образом мультистейкхолдерная модель может охватить всех и каждого, если иногда решения оказывают самое большое влияние на тех людей, которые имеют наименьшее отношение к предмету обсуждения?

С одной стороны, распространение информации в целях повышения осведомленности среди рядовых граждан является правильным шагом. Но если поток информации движется только в одном направлении – от правительственной верхушки к массам, и отсутствует обратная связь, то единственными, кто окажется в выигрыше от функционирования многосторонней системы, будут те, кто занимает наиболее влиятельную позицию.

Таким образом, все должны иметь право и возможность активного участия.

- Предоставление полномочий широким массам населения
  - Руководства к действию – основные документы
  - Обмен информацией/опытом между участниками
  - Документы, составленные с использованием передового опыта – повышение компетентности
  - Финансирование – основная составляющая развития

        - Сокращение ограничений на вступление
    - Усовершенствование двустороннего движения потока информации
    - Накопление потенциала и обучение

Все эти действия должны осуществляться одновременно. Ранее уже говорилось о том, что в некоторых случаях Интернет и социальные сети были использованы в качестве невероятно результативного способа распространения информации и обеспечения децентрализованного участия. Они вполне могут быть использованы в качестве одного из каналов связи для укрепления мультистейкхолдерной модели, но это далеко не единственный канал такого рода.

Все начинается с обучения пониманию истории: как мы дошли до точки, в которой находимся сейчас?

2.2.2.1. Институонализация действуйющей мультистейкхолдерной модели

- Всемирный саммит по информационному обществу (WSIS) (ICANN не должен способствовать этому, но, возможно, наши общественные структуры захотят сделать что-то из этого в своем собственном пространстве)

Всемирный саммит по информационному обществу (WSIS) – это конференция при поддержке ООН, которая проходила в два этапа. Первый этап проходил в Женеве в декабре 2003 года, второй – в Тунисе в ноябре 2005 года. Целью первого этапа была разработка и продвижение четкой концепции политической воли и принятие конкретных шагов по созданию основ информационного общества для всех с учетом различных интересов. Целью второго этапа была реализация Плана действий, принятого в Женеве, а также определение решений и достижение соглашений в сферах управления Интернетом, механизмов финансирования, исполнение и реализация документов, принятых в Женеве и

Тунисе.

WSIS +10 был проведен в 2013 году. На эту тему было много публикаций, но в то же время информация не афишируется должным образом, и, по нашим данным, история WSIS не всегда доступна на 6 официальных языках ООН. В компетенцию ICANN не входит помощь в составлении проекта, но многие общественные структуры могли бы быть заинтересованы в том, чтобы поделиться своим опытом и оказать посильную помощь. Несколько таких структур приняли участие в работе WSIS +10 и присутствовали в Женеве и Тунисе.

- IGF (ICANN не должен способствовать этому, но, возможно, наши общественные структуры захотят сделать что-то из этого в своем собственном пространстве)

Форум по управлению Интернетом (IGF), созванный по решению ООН, - это ежегодный международный мультистейкхолдерный форум для обсуждения вопросов управления Интернетом. Он влияет на формирование политики, но не занимается ее разработкой. IGF выпускает ежегодные публикации, но структурированная история IGF и объяснение особенностей его работы, его значение и дальнейшее развитие могут заинтересовать общественные структуры, тем более что многие из них принимали непосредственное участие в работе IGF, организации семинаров и пленарных заседаний и в распространении заявлений IGF среди соответствующих заинтересованных сторон во всем мире. Сотрудничество между самими общественными структурами может также установить некоторое базовое сотрудничество по восходящему принципу, например, создание совместными усилиями единого хранилища информации о деятельности IGF по всему миру, в том числе национальных и региональных IGF.

2.3. Рекомендуемые дальнейшие действия для ICANN

2.3.1. Для организаций поддержки и консультативных комитетов (SO / AC)

Внутренняя структура сообщества ICANN, которая охватывает все заинтересованные стороны, участвующие в процессах ICANN, свидетельствует о том, что ICANN является образцом открытости, предоставляя бесплатный и открытый доступ к участию во всех своих встречах, происходящих в режимах онлайн и офлайн. Организация подразделяется на **организации** поддержки (**SO**), в которых разрабатывается политика, и **консультативные комитеты** (**AC**), которые могут предоставить консультации по конкретным вопросам. Каждый новичок может подтвердить, что эту сложную организацию очень непросто понять.

Одной из основных сложностей в понимании ICANN является его организационная структура, базирующаяся на восходящей природе волонтерского состава **SO / AC**, нисходящей структуре штатного персонала и включающая в свой состав Совет, который исполняет гораздо больше функций, чем обычный корпоративный совет, и который избирается в другом порядке. Все это придает ICANN немалую долю своеобразности. Кроме того, если учесть серьезность вопросов, разрешаемых ICANN, его возможность влияния на более чем 2 миллиарда Интернет пользователей во всем мире, в конечном итоге придет понимание, что вы имеете дело с организацией, которая, как предполагается, благосклонна к новичкам, но все же требует уверенного уровня знаний для того, чтобы быть принятыми - знание истории, технологических процессов, словарного запаса, расстановки сил в мире, восходящих процессов, публичных консультаций, постоянных обзоров и т.д. Сообщество ICANN может быть требовательным и критичным, способным из-за любой допущенной ошибки превратить дружеский прием во враждебную среду.

Эта среда не для слабонервных: ICANN принимает очень серьезные решения, которые требуют разнообразных навыков многих участников в ходе

восходящего мультистейкхолдерного процесса.

Для того, чтобы мультистейкхолдерный процесс был равноправным, значительное количество усилий по наращиванию потенциала должно быть предпринято на нескольких уровнях:

- Формирование/обучение/ориентация на лидерство таким образом, чтобы следующая группа лидеров-волонтеров была полностью осведомлена о всех фактах, которые позволят им принимать обоснованные решения в будущем, особенно в условиях восходящей среды;
- Наращивание потенциала среди заинтересованных сторон – таким образом, чтобы многие заинтересованные стороны ICANN (Группы заинтересованных сторон как во **SO, AC**, так и в Организации поддержки общих имен (GNSO)) имели активных проинформированных участников, способных поддерживать рост организации. Это жизненно важно для организации, которая опирается на волонтеров, в условиях, когда необходимо избежать поредения в их рядах;
- Наращивание потенциала среди новичков, которое уже применяется на уровне стипендиальной поддержки (*Fellowship level*), но которое должно развиваться путем активного поиска достойных кандидатов по всему миру. В этом заключается разница между приемом заявок на стипендиальную поддержку, их пассивной обработкой и активным поиском лучших кандидатов в университетах и колледжах. Наращивание потенциала среди новичков следует также применять по отношению к лидерам и политикам в выбранной сфере производства.
- Локальная программа поддержки, которая включает, во-первых, поддержку новых потенциальных членов сообщества, а, во-вторых, наращивание потенциала среди конечных Интернет пользователей

во всем мире: какие права им принадлежат; что входит в их обязанности; как они влияют на решения, принимаемые ICANN, которые коснутся их в будущем? В конце концов, кто, если не конечные Интернет пользователи находится внизу пирамиды при восходящем процессе? Опять же, легко сказать “каждый может участвовать в обсуждении”, но как многие знают об этом праве, и как многие знают о том, как принять участие? Это ключевая задача, которая может быть решена на местном уровне с помощью обширной сети Консультативного комитета сообщества At-Large (ALAC) местных организаций At-Large

- Расширение границ наращивания потенциала на локальном уровне - на этот раз с бизнесом, прессой, правительствами. Очень важно, чтобы все заинтересованные стороны имели возможность участвовать в мультистейкхолдерном процессе ICANN. Опять таки, то, что уже было проделано, далеко от идеала. Все заинтересованные на данный момент стороны должны быть обеспечены средствами для передачи сообщений на локальном уровне или в глобальном масштабе.

Достаточно легко перечислить виды наращивания потенциала, необходимые для того, чтобы в рамках ICANN функционировал всеохватывающий мультистейкхолдерный восходящий процесс: мне понадобилась всего одна минута, чтобы составить приведенный выше перечень. Проблема состоит в том, что все усилия по наращиванию потенциала очень дорогостоящие в плане организации и эксплуатации. Многое может быть сделано путем использования современных инструментов дистанционного Интернет обучения и курсов с программой обучения, которая разрабатывается и курируется самими волонтерами, но любая серьезная учебная программа по-прежнему требует участия специалистов, а время - это деньги. Кроме того, телекоммуникации могут опираться на помощь, предоставляемую Интернетом, но в некоторых

странах во всем мире телекоммуникации по-прежнему находятся в очень плохом состоянии, и участники из этих стран сталкиваются с **реальной проблемой** невозможности участия в дистанционных курсах. Таким образом, неотъемлемым элементом наращивания потенциала на всех уровнях является способность участников регулярно **встречаться лично** на заседаниях ICANN или в любом другом месте. Одной попытки недостаточно, такие личные встречи не должны быть случайными, а вместо этого их следует проводить на постоянной основе. Следует установить разумный интервал между личными встречами, с тем, чтобы выбранные участники заседаний по наращиванию потенциала могли предоставить обратную связь по максимизации воздействия.

Основная проблема упирается в оплату командировок, гостиниц и суточных, которые формируют расходную статью. А в случае с ICANN, все эти расходы превращаются в доходную часть бюджета ICANN.

Кто-то может заметить, что ICANN не сталкивается с финансовыми проблемами благодаря фактическому “налогу” на миллионы доменных имен, которые продаются по всему миру, а также благодаря сбору, взимаемому за создание большого количества новых общих доменов верхнего уровня (gTLDs). ICANN накопил “немалые деньги” и сможет обеспечить *любой* объем наращивания потенциала, необходимый для продвижения восходящей равноправной многосторонней модели.

Полагать так было бы в самом деле крайне нерассудительным по нескольким причинам:

- Доменные имена - не дойные коровы. Уже завтра на смену доменным именам могут прийти другие технологии, и денежные поступления иссякнут;
- Нет никаких гарантий, что введение новых gTLDs не создаст единый рынок доменных имен, при этом себестоимость резко упадет, тем самым сократив доход от доменных имен;

- В долгосрочной перспективе будет ли справедливой просьба небольшой части всех Интернет пользователей, будь то корпоративные или индивидуальные пользователи, которые зарегистрировали доменные имена, поддержать совершенно новую систему управления?
- Бюджет ICANN не бесконечен. В сущности, в контексте более масштабной всемирной попытки продолжать разработку мультистейкхолдерной системы управления Интернетом, необходимость наращивания международного потенциала настолько велика, что ICANN **не сможет** предоставить финансирование в полном объеме.

Поэтому для заинтересованных сторон, включая правительства и частный сектор, который пользуется выгодами от системы мультистейкхолдерного управления, которая превратила Интернет в то, чем он является сегодня, очень важно рассмотреть возможность существенного увеличения финансирования этой мультистейкхолдерной системы управления на несколько порядков.

Альтернативная модель нисходящего управления, которая нам достаточно хорошо знакома, в том числе и на примере WCIT, перегружена устаревшими политическими установками XX столетия, что запросто может стать убийственным для Интернет инноваций, которые трансформируются в еще большие экономические торговые потери. Таким образом, существует острая потребность во внешней поддержке. Я умышленно не употребляю понятие “спонсор”, поскольку оно сходно с субсидией.

Финансирование мультистейкхолдерного процесса государствами и частным сектором должно рассматриваться как инвестиции, а не как благотворительная помощь.

Финансирование мультистейкхолдерной модели должно быть направленным на наращивание потенциала, при этом корпорация ICANN функционирует за счет своих собственных средств, а сама организация разрастается. Этот денежный

поток необходим для того, чтобы увеличивающиеся масштабы деятельности корпорации могли гарантировать самые безопасные и стабильные условия для функционирования Интернета, как в технической, так и в политической среде. Сюда входят инвестиции в незамедлительную интернационализацию корпорации ICANN и ее потенциальное превращение в будущем в международную структуру, понятную каждому человеку во всем мире.

2.3.2. Рекомендуемые действия для сообщества At-Large и Консультативного комитета сообщества At-Large (ALAC)

2.3.2.1. Наращивание потенциала

После того, как был составлен список дел в долгосрочной перспективе, стоит обратить внимание на использование уже имеющихся для этого возможностей сообщества пользователей и его Консультативного комитета сообщества At-Large (ALAC), который состоит из 15 членов и представляет интересы конечных Интернет пользователей в рамках сообщества ICANN, для создания потенциала. ALAC начал свою работу несколько лет назад. В настоящее время его программа поддержки и наращивания потенциала делится на несколько рабочих групп:

- Рабочая группа сообщества At-Large по разъяснительной работе
- Рабочая группа сообщества At-Large по наращиванию потенциала
- Рабочие группы региональных организаций сообществ At-Large (RALO) (наращивание потенциала общественной организации в Латино-Американском регионе (LACRALO), наращивание потенциала общественной организации в африканском регионе (AFRALO) ...)

Эти рабочие группы разрабатывают программы по наращиванию потенциала,

которые использует наше сообщество пользователей. Некоторые находятся на стадии оценки потребностей сообщества. Другие занимаются расширением программ, которые уже были запущены на личных встречах ICANN. Рабочие группы разрабатывают программы, которые могут быть использованы в режимах онлайн и офлайн (при непосредственном участии). Важно отметить, что на стадии проектирования эти группы, состоящие из волонтеров, не нуждаются в финансировании. Тем не менее, некоторые программы, которые они разработают, потребуют финансовых затрат. Например, для того, чтобы онлайн обучение было результативным, нужны соответствующие средства для "наращивания онлайн потенциала". Личное наращивание потенциала в ходе проведения различных мероприятий, таких как встречи ICANN, является дорогостоящим. В последнее время сообществу At-Large (ALAC) удавалось обеспечить участие одного представителя от каждой из своих более чем 150 общественных структур во встречах ICANN, обсуждениях на региональном уровне и разовых мероприятиях. Некоторые участники считают, что разовых личных встреч недостаточно. В самом деле, для того, чтобы понять сложную экосистему, в которой функционирует ICANN, понадобится не одна встреча. Новичок сталкивается с полным переворотом парадигмы – и остается еще так много всего, чему следует научиться!

Таким образом, очень важно позиционировать наращивание потенциала в качестве непрерывного процесса, а не разового мероприятия. В целях получения выгоды в долгосрочной перспективе статьи бюджета по наращиванию онлайн или офлайн потенциала должны быть постоянными.

2.3.2.2. Проактивные действия по достижению действительного членства

- Раскрутка своей способности найти общий язык с сообществами
- Обмен информацией/опытом
- Программа поддержки

Очень важно поддерживать общественные структуры наших членов (которых в настоящее время насчитывается более 150) в наращивании потенциала их сообществ, тем самым содействуя их участию в мультистейкхолдерном процессе. С этой целью ICANN и сообщества пользователей должны распространять среди конечных Интернет пользователей материалы по всем аспектам мультистейкхолдерной модели ICANN, стратегическим вопросам, рекламные материалы, информацию о текущих обсуждаемых вопросах, а также о том, насколько все это важно для сообщества. Это первый большой шаг на пути к ознакомлению сообществ с рДВУ, впрочем, еще не до конца известно, насколько значимой является стратегия системы идентификаторов Интернета для Интернет пользователей. Следует использовать четкий, простой язык. Серии Руководств для начинающих, которые возникли в рамках сообщества пользователей и были разработаны сотрудниками ICANN при участии сообщества, положили отличное начало. Должны быть предприняты действия по их распространению. Недостаточно предоставить открытый доступ к материалу: требуется проактивный подход.

Также очень важно поддерживать структуры At-Large в обмене информацией и накопленным опытом. Это можно сделать через использование онлайн методов, но в то же время члены сообществ пользователей должны иметь возможность для участия в мероприятии, организованном другим сообществом пользователей, если это мероприятие связано с ICANN. Настоящая кооперация может быть достигнута только за счет **систематического сотрудничества между сообществами At-Large**. Как сообщалось ранее, сюда относится также совместное участие сообществ At-Large во встречах ICANN, а также в других форумах, таких как IGF, WSIS и подобные им мероприятия. Они являются наилучшими представителями для ICANN, поскольку они и *есть* теми заинтересованными сторонами, которые формируют мультистейкхолдерный процесс. Многие уже имеют большое влияние, и получили большое уважение внутри общества. Многие уже владеют нужными связями, необходимыми для расширения связей самой организации.

Хотя в последнее время корпорация ICANN делает успехи в этом отношении, на сегодняшний день ее степень поддержки сообществ At-Large все еще не достигла нужного уровня. Опять таки, все упирается в финансирование.

Однако в этой сфере можно наблюдать позитивные изменения: предстоящие планы по созданию образовательной онлайн платформы для всей корпорации ICANN являются очень полезной инициативой. Сообщество At-Large уже приступило к предоставлению помощи в ее развитии, как на общем, так и на региональном уровне. И рабочая группа At-Large по наращиванию потенциала, и рабочая группа Академии ICANN будут тесно сотрудничать с сотрудниками и подрядчиками ICANN в вопросах разработки образовательной онлайн платформы ICANN.

2.3.2.3. **Раскрутка способности сообществ At-Large найти общий язык со своим правительством**

- Обмен информацией/опытом
- Региональное сотрудничество
- Использование локальных/региональных IGF и других форумов для установления контактов с правительством

Многие расширенные структуры оказали значительное влияние на свои правительства в ходе WCIT. Представители некоторых из них входили в состав государственных делегаций. Некоторые представители приняли участие в конференции, поскольку их организация является членом сектора ITU. Некоторые выступили в качестве непосредственных внутренних советников своих правительств, тем самым получив возможность дистанционно влиять на исход обсуждений, при этом не будучи членами делегации. Такое участие требует соответствующих затрат. Например, многие делегаты, которые вошли в состав государственных делегаций, самостоятельно покрывали свои расходы, в

частности проезд и проживание. Некоторые сообщества At-Large обладают достаточными финансовыми возможностями для покрытия таких расходов своих членов за собственный счет. Однако многие такой возможности не имеют, тем более, что защита Интернет модели может и не быть ключевым направлением их деятельности. Представлены местные структуры; развиваются знания, устанавливаются контакты, однако участие на международном уровне возлагает значительную финансовую нагрузку.

На ум приходит два варианта выхода из ситуации: сотрудничество в рамках ICANN может заложить основы сотрудничества между сообществами At-Large и их правительствами за счет привлечения других заинтересованных сторон в ICANN. Правительственный консультативный комитет (GAC), например, может послужить хорошей отправной точкой.

2.3.2.4. **Больше поддержки - в обоих направлениях**

Следует тщательно изучить потребности сообществ At-Large с целью их поддержки в работе с местными заинтересованными сторонами, особенно когда речь идет о консультировании и наращивании потенциала, которые в конечном счете принесут пользу их сообществам.

Первый цикл Расширенного Обзора был главным образом сосредоточен на сообществах At-Large. Следующий цикл Обзора может также сосредоточить внимание на более эффективной поддержке структур At-Large со стороны ICANN, принимая во внимание тот факт, что этот процесс будет двусторонним: региональные сообщества At-Large также продемонстрируют “Рентабельность инвестиций” в случае, если они получат поддержку в своей работе на местах. Безусловно, все будет зависеть от каждого конкретного случая, с учетом местного законодательства и готовности RALO действовать.

Предполагается, что одна из главных тем повестки дня Расширенного Саммита (ATLAS2) стимулирует сообщества At-Large, RALO и ALAC работать более

интенсивно над оптимизацией такой “Рентабельности инвестиций”. Личные встречи действительно обладают огромным потенциалом в качестве катализатора такой оптимизации на местном уровне.

2.3.3. Достижения сообществ At-Large/историческая перспектива

- Как происходило развитие сообщества *At-Large* вплоть до сегодняшнего дня?

Изначально планировалось, что ICANN будет подотчетна сообществу *At-Large*, при этом значительная часть Совета директоров будет избираться непосредственно международным электоратом Интернет пользователей. Эта идея потерпела неудачу по главной известной всем причине: размытость электората.

Версия 2.0, которая была разработана уже после официального представления сообщества *At-Large* 2.0, создания Rонсультативного комитета сообщества At-Large (ALAC), а также международной сети в составе 5 региональных организаций (RALOs) и участников их *At-Large* структур, местных организаций, деятельность которых направлена на привлечение местных Интернет пользователей к участию в процессах ICANN, преуспела и насчитывает более 150 структур *At-Large* по всему миру. Всего этого удалось достичь, преодолев многочисленные трудности, сумятицу, пережив взлеты и падения и проявив определенное упрямство. С учетом невероятного разнообразия волонтеров, инвестиции в сообщество *At-Large* порой приводили в удивление, как в положительном, так и в отрицательном смысле этого слова. Тем не менее, сообщество *At-Large* из нестабильного образования превратилось в стабильный орган, построенный по восходящему принципу, которому удалось достичь весьма впечатляющих результатов. Остается открытым вопрос, является ли это сообщество одновременно устойчивым и масштабным. По сути, если ICANN

это всего лишь эксперимент, тогда сообщество *At-Large* как составная часть ICANN вместе с ее Консультативным комитетом, имеющим возможность давать комментарии по поводу всего, что имеет хоть какое-то отношение к ICANN, представляет собой эксперимент внутри эксперимента, своего рода “эксперимент в квадрате”, который находится в самом центре мультистейкхолдерного восходящего процесса. Если сообщество *At-Large* окажется нежизнеспособным, будет ли это значить, что всю мультистейкхолдерную модель Интернета ждет та же участь, поскольку сообщество *At-Large* играет важную роль в мультистейкхолдерной системе?

- В чем заключалась изначальная функция сообщества *At-Large* в структуре ICANN?

Устав ICANN уполномочил сообщество *At-Large* представлять интересы Интернет пользователей в модели ICANN. Это достаточно сложная задача, с учетом того, что количество Интернет пользователей превысило 2 млрд человек и продолжает расти. Основная задача сообщества *At-Large* сводится к поиску наиболее эффективных способов сбора информации среди Интернет пользователей и обеспечению гарантий того, что их позиция найдет свое отражение в консультативных заявлениях в рамках деятельности ALAC. По всей видимости, сообщество *At-Large* никогда не сможет представлять эти интересы в полном объеме перед ICANN; вместо этого проводится репрезентативная выборка и текущая структура, взятая в какой-то определенный промежуток времени, превращается в масштабную модель. Будущее расширение возможно за счет создания новых слоев в мультистейкхолдерной модели сообщества *At-Large* или расширения возможностей региональных моделей в структуре RALO. Этот вопрос имеет решающее значение для развития не только сообщества *At-Large*, но и для мультистейкхолдерной модели управления, если она сумеет сохранить свою привлекательность.

- Где проходят рамки сообщества *At-Large*? Признается ли сфера

деятельности сообщества *At-Large*?

Сфера деятельности сообщества *At-Large* определяется уставом ICANN. Можно предположить, что она будет расширена таким образом, чтобы охватить управление Интернетом в целом, включая свободу слова, права человека и вопросы, несвязанные с системой идентификаторов Интернета. **Однако, в действительности это потребовало бы внесения изменений в устав ICANN или его стратегию.**

Если с такой инициативой выступят Интернет пользователи во всем мире, формально ALAC может обратиться в ICANN с просьбой рассмотреть приемлемость таких изменений, но ALAC не имеет полномочий вносить такие изменения самостоятельно. Кроме того, “обращение в ICANN с просьбой рассмотреть приемлемость таких изменений” это не просто запрос, поданный Совету директоров ICANN. Он повлечет за собой несколько раундов общественных обсуждений при участии всех заинтересованных сторон мультистейкхолдерной модели ICANN, а финальное решение должно быть принято путем консенсуса. Любой другой способ разворачивания событий подорвет саму мультистейкхолдерную систему, на которой основан ICANN и которая поддерживается ALAC.

Сфера деятельности сообщества *At-Large* была предметом толкования несколько раз. Например, ALAC была предоставлена возможность подать возражения против новых заявок на получение gTLD. Это стало еще одним шагом вперед на пути к признанию его оперативной роли по сравнению с чисто консультативными функциями. Приятно отметить, что сообщество подходит к такому погружению в “оперативную деятельность” с большой осторожностью благодаря разработке четких руководящих принципов, которыми руководствуется в своей деятельности Группа по рассмотрению заявок на новые gTLD. В некотором роде, мощь многонационального сообщества *At-Large* связана с его объединенным громадным опытом в сфере организации деятельности восходящей мультистейкхолдерной системы управления,

основанной на постоянном общении и регулярном поиске консенсуса благодаря объединению опытных председателей и участников, а также талантливых новичков, которые поддерживают свой уровень знаний благодаря помощи коллег.

При таком огромном количестве волонтеров, как опытных, так и новичков, всегда найдутся те, кто будет напоминать другим о необходимости адаптации миссии к новым условиям, в случае, если существует риск того, что сообщество *At-Large* выйдет за рамки своих полномочий.

- Использование активов сообщества *At-Large*

К сожалению, огромный потенциал сообщества *At-Large* до настоящего времени не используется в полной мере другими составляющими ICANN (вспомогательными организациями, консультативными комитетами, персоналом, Советом директоров). Это частично объясняется длительным периодом недоверия к сообществу *At-Large* из-за его нестабильной ранней истории, а частично из-за опасений по поводу масштабов, до которых может дорасти сообщество в случае, если продолжит развиваться такими же темпами. В конце концов, сообщество обладает самым большим человеческим потенциалом среди всех вспомогательных организаций и консультативных комитетов ICANN. Сообщество *At-Large* было бы поводом для беспокойства для многих, если бы оно стало слишком могущественным, поскольку оно является восходящей системой, основанной на консенсусе, его действия труднее контролировать, они непредсказуемы, возможно, для кого-то даже ненадежны. Однако в этом и состоит суть игры - если одни серьезно относятся к идее многонациональности, всегда есть “неизвестная” часть, которая должна быть принята. Следует разработать ключевые показатели эффективности (KPI), основанные как на результатах, так и на самом процессе – с той особенностью, что они относятся к волонтерам. К счастью, сообщество *At-Large* уже работает над этими вопросами. Тем не менее, трудности, связанные с привлечением участников (поддержание интереса волонтеров, обеспечение их активного

участия и предоставление им возможностей для личностного роста в структуре ICANN) и расширением потенциала (проактивное налаживание диалога с целью обеспечить максимальный охват, известное также как привлечение широких масс) требуют много внимания, и ограничиваться скудным бюджетом или непродуманными решениями здесь совершенно неуместно.

Сообщество *At-Large* совершенно не подходит на роль "центра затрат" - скорее наоборот: это невероятно экономически эффективный ресурс, что является преимуществом. Тем, кто не понимает всю "значимость" сообщества *At-Large*, следует с таким же успехом отказаться от мультистейкхолдерной системы, на которой построен Интернет, потому что без *конечных пользователей* мультистейкхолдерная модель нежизнеспособна, поскольку в итоге именно *конечные пользователи* финансируют всю экосистему в целом.

- Возможно ли воспроизвести модель сообщества *At-Large* в условиях, отличных от тех, что характерны для среды ICANN? Может ли мультистейкхолдерная модель ICANN быть воспроизведена в другой, отличной от ICANN среде?

Некоторые организации и участники считают, что модель сообщества *At-Large* можно воспроизвести в отличной от ICANN среде. Безусловно, структура глобального охвата с многоступенчатой системой безопасности, комитетами на нескольких уровнях и присущей ей рекурсивной процедурой обзора по-своему привлекательна. Но об этом еще слишком рано говорить. Сообщество *At-Large* существует с момента создания ICANN в 1998 году. Консультативному комитету *At-Large* (ALAC) всего 10 лет. Региональным организациям *At-Large* (RALOs) исполнилось только 5 лет. Все сообщество прошло долгий путь, чтобы достичь нынешних результатов. Долгий путь предстоит впереди, учитывая масштабы деятельности. В любом случае, стоит изучить модели *At-Large* и ALAC. Не испытав их в другом месте, мы так и не узнаем, пригодны ли они для функционирования в любой другой экосистеме.

Преждевременно также делать выводы о том, что касается

мультистейкхолдерной модели ICANN. До сих пор ICANN успел познать взлеты и падения. Система не совершенна, но сохраняет целостность и функционирует гораздо лучше, чем любая другая альтернативная модель. Она возглавляется собственной командой руководителей, чья компетенция значительно повысилась за последние годы. Организации выпало много шансов, чтобы извлечь уроки из своих прошлых ошибок - но ошибки были ожидаемыми как часть проекта, поскольку, в конце концов, это в огромной степени инновационный и новаторский эксперимент. Показательно, что сообщество ICANN становится все сильнее и привлекает по-настоящему талантливых людей (штатных сотрудников и волонтеров) уже на протяжении многих лет, тем самым интегрируя невероятно талантливый человеческий потенциал со всего мира в свою экосистему.

2.4. Заключение

Корпорация ICANN, по сути, превратилась в микрокосмическое отражение каждой сети, чьи идентификаторы (имена и номера) она должна была координировать.

Значимость Интернета не измеряется количеством всех компьютеров и телекоммуникационного оборудования;

также как не измеряется суммой затрат на все предоставленные онлайн услуги;

или показателями ВВП всех стран мира, полученными от прямого или непрямого бизнеса за пользование Интернетом;

ценность Интернета – в его пользователях.

Без этой критической массы пользователей, будь то потребители или поставщики, Интернет потеряет какую-либо привлекательность.

Благодаря уникальному сочетанию штатных сотрудников и волонтеров ICANN превращает эту критическую массу в восходящую мультистейкхолдерную

модель управления, которая владеет многообещающими возможностями в отношении экосистемы Интернета. Давайте объединим наши усилия на пути к улучшению этой модели. Это требует поддержки и сотрудничества.

Если Вы серьезно относитесь к мультистейкхолдерному управлению Интернетом, постарайтесь узнать о нем больше, принять участие в его разработке, а также оказать посильную помощь в предоставлении ресурсов, необходимых для улучшения и процветания этой модели.

4.1.2. Совет Европы. Комментарии, касающиеся свободы выражения мнений и свободы объединения в отношении новых общих доменов верхнего уровня

Генеральный Секретариат

Генеральный директорат
по правам человека и соблюдению законности

DG-I (2012) 4
12 октября 2012

Комментарии, касающиеся свободы выражения мнений и свободы объединения в отношении новых общих доменов верхнего уровня

Вольфганг Бенедек (Mr Wolfgang Benedek), профессор международного права и международных отношений в университете Граца, Австрия (при содействии Пола Грагла (Paul Gragl) и Маттиаса Кеттельманна (Matthias C.Kettemann))

Джой Лиддкот (Ms Joy Liddicoat), Ассоциация по прогрессивным коммуникациям, Новая Зеландия

Нико ван Эйка (Mr Nico van Eijk), директор Института информационного права в Университете Амстердама, Нидерланды

Содержание

Краткий обзор

Доменные имена являются не только техническими ресурсами Интернета. Люди могут использовать их в качестве средства получения и распространения информации, идей и мнений, либо указывать на ассоциации. Суды в различных юрисдикциях считают, что свобода слова и свобода объединения распространяется на доменные имена. Защита этих прав человека и основных свобод является важной в контексте программы новых общих доменов верхнего уровня (The new gTLDs programme).

Утверждение новых общих доменов верхнего уровня для делегирования и регистраций на втором уровне, ожидается, будет не механическим актом, а результатом процесса оценки, где решения будут приниматься на основании сочетания соображений как технических, так и связанных с контентом, и других. Эти процессы могут включать редакционные решения, аналогичные тем, что принимаются медийными организациями, что необходимо должно отразиться на медиа-свободах и обязанностях ICANN.

Введение новых общих доменов верхнего уровня (gTLD), содержащих слова и выражения, могущих оказаться чувствительными по национальным, культурным, религиозным или иным причинам, рассматривается как потенциальный фактор риска блокирования и фильтрации такого доменного имени с возможными последствиями для стабильности системы доменных имен (DNS). Запрет на делегирование новых gTLD на основании их чувствительности, рано как и блокирование и фильтрация TLD могут повлиять на возможность доступа к информации в Интернете по своему выбору для интернет-пользователей и их общения друг с другом.

Различия между национальными, культурными, религиозными или другими причинами повышенной чувствительности и вопросами политического характера бывают очень трудно различимыми. В случае если решения о введении новых чувствительных gTLD должны быть приняты, предпочтительнее отдавать приоритет обеспечения права на свободу выражения мнения и права на свободу объединений. Это можно сделать, управляя рисками DNS, вместо того, чтобы говорить, что заявка на новый gTLD не должна рассматриваться или должна быть необоснованно или несправедливо отвергнута. Подход с точки зрения прав человека позволил бы GAC исследовать широкий спектр возможностей, которые могли бы отразить нюансы и сложные соображения.

В конечном счете, согласно международному законодательству о правах человека государства обязаны защищать, уважать и поощрять права человека и основные свободы лиц, находящихся под их юрисдикцией. В государствах-членах Совета Европы любое вмешательство в эти права и свободы должно соответствовать условиям, изложенным в

Европейской конвенции по правам человека в интерпретации Европейского суда по правам человека. Эти обязательства сохраняют свою актуальность при участии государств в деятельности субъектов со специализированными техническими мандатами.

При том, что GAC не является ни органом, принимающим решения по новым gTLD, ни органом по правам человека, подход, основанный на правах человека, будучи принятым во внимание должным образом, поможет обосновать позицию GAC по новым gTLD и в то же время укрепит соответствие соблюдения общих прав человека международным стандартам. Государства, как носители обязанностей в публичной политике, имеют настоящие и законные причины избегать нарушений прав и свобод граждан в пределах их юрисдикции. Следовательно, Правлению ICANN следует уделять особое внимание рекомендациям GAC.

Введение

1. Компетенция ICANN, как правило, не распространяется на изучение контента, представленного в или размещаемого под TLD. Тем не менее, соображения, касающиеся интернет-контента, не выпадают полностью за пределы полномочий ICANN и обсуждение делегирования новых gTLD не ожидается, что будет чисто механическим процессом.

2. Роль GAC в ICANN заключается в предоставлении консультаций по деятельности ICANN, поскольку она касаются вопросов, касающихся правительств и деятельность ICANN может повлиять на вопросы государственной политики, в том числе касающиеся свободы слова, об этом, в частности, упомянуто в Принципах работы GAC.

3. Возможности GAC в разборе вопросов, связанных с контентом или выражениями, содержащимися в новых gTLD, ограничены, прежде всего, тем, что GAC не принимает решения в связи с заявками на новые gTLD. Тем не менее, рассмотрение может распространяться на связи между предложенными gTLD и возможным контентом, размещаемым под ними, основываясь на своих предположениях о них, понимании, фактическим или подразумеваемым смыслом или цели конкретного TLD.

Выступая в роли консультантов, члены GAC связаны особыми обязательствами по правам человека, которых у других заинтересованных сторон в сообществе ICANN нет.

4. Выступая в роли консультантов, члены GAC связаны особыми обязательствами по правам человека, которых у других заинтересованных сторон в сообществе ICANN нет. Члены GAC представляют правительства государств-членов ООН, их обязанности действуют независимо от текущего правительства в той или иной стране или отдельного чиновника, участвующего в GAC. Эти уникальные обязательства государств должны информировать о роли правительства в управлении Интернетом и

выработке государственной политики, упомянутой в Тунисской программе для информационного общества.

5. В контексте Совета Европы – особая ответственность государств-членов Совета Европы в управлении Интернетом была подтверждена в явном виде в Декларации Комитета Министров о принципах управления Интернетом.

6. Целью данного документа является предоставление справочной информации о стандартах прав человека, особенно о праве на свободу выражения мнения и праве на свободу объединения в соответствии с Декларации Комитета министров Совета Европы о защите свободы слова и информации и свободы собраний и ассоциаций в отношении имен доменов и текстовых строк. Он отражает международно-правовые обязательства по защите и поощрению этих прав и свобод и как эти обязательства могут быть учтены при взаимодействии GAC с Правлением ICANN.

7. В этом контексте роль GAC рассматривается с точки зрения его консенсусных консультаций как группы правительств, а не с точки зрения отдельных правительств на обязательства в области прав человека и как они могут быть подняты или рассматриваться в GAC. Причина этого – в существовании целого ряд процессов, при помощи которых отдельные правительства могут внести свой вклад в рассмотрение заявок на новые gTLD, а также в существовании отдельной процедуры разрешения споров, доступной для отдельных правительств, возражающих против каких-либо заявок на новые gTLD. В этом документе сделан сознательный выбор не комментировать какие-либо конкретные заявки на новые gTLD или заявленные для таких gTLD строки.

2. Обязательства государств по правам человека

8. Государства несут ответственность за и имеют обязательства по соблюдению, защите и поощрению прав человека и свобод своих граждан. У них есть эти обязательства, когда они действуют в связи со своими национальными вопросами и, в совокупности, разделяют международный консенсус в отношении основных стандартов прав человека. Это изложено и в не обязывающих документах, в том числе Всеобщей декларации о правах человека (Universal Declaration on Human Rights – UDHR) и в договорах, таких, как Международный пакт о гражданских и политических правах (International Covenant on Civil and Political Rights – ICCPR), а также в других документах. Государства могут также нести обязательства по правам человека, изложенные в соглашениях на региональном или многостороннем уровне, например, таких как предусмотрены в Европейской конвенции по правам человека (European Convention on Human Rights – ECHR) в отношении 47 государств-членов Совета Европы.

9. Недавно Совет ООН по правам человека принял Резолюцию

«Поощрение, защита и осуществление прав человека в Интернете», подтвердившую, что «те же права, что люди имеют в оффлайне, должны быть защищены также и в Интернете, в частности свобода выражения мнения, применимая независимо от государственных границ и осуществляемая через любые медиа по собственному выбору, в соответствии со статьей 19 Всеобщей декларации прав человека и Международным пактом о гражданских и политических правах».

10. GAC заявил в Принципах GAC о новых gTLD, что новые gTLD должны уважать «положения Всеобщей декларации прав человека, которая стремится утвердить фундаментальные права человека, в достоинстве и ценности каждого человека и в равноправии мужчин и женщин».

Когда государства участвуют в специализированных органах в основном с техническим мандатом, таких как работа GAC в ICANN – государства не слагают с себя свои обязательства в области прав человека.

11. Когда государства участвуют в специализированных органах в основном с техническим мандатом, таких как работа GAC в ICANN – государства не слагают с себя свои обязательства в области прав человека. В связи с этим следует отметить ряд соображений.

12. Во-первых, хотя GAC может предоставить рекомендации Правлению ICANN по вопросам государственной политики, которая может относиться к правам человека, GAC не является органом, разрабатывающим стандарты прав человека (например, в контексте Совета Европы, Европейский суд по правам человека (ЕСПЧ) может вынести решение, конфликтующее с GAC и создать прецедент, которому будут следовать государства-члены Совета Европы).

13. Во-вторых, при разработке рекомендации в контексте GAC, государства связаны согласованными на международном уровне стандартами прав человека, равно как и региональными и многосторонними соглашениями, которые они заключили.

14. В-третьих, в то время как существуют универсальные международные стандарты прав человека, которые правительства должны защищать, уважать и поощрять - в конкретном контексте данной статьи, такие, как право на свободу выражения мнения и право на свободу объединения – единого универсального, равно как и какого-либо единственно правильного пути для претворения в жизнь этих стандартов, не существует. Всеобщая декларация прав человека – наиболее общий согласованный государствами стандарт.

15. Ссылка на Всеобщую декларацию прав человека в Принципах GAC в отношении новых gTLD, таким образом, уместна, так как Всеобщая декларация прав человека является не обязывающим документом,

определяющим, для целей Устава Организации Объединенных Наций, значение слов «основные свободы» и «права человека». Устав Организации Объединенных Наций является обязательным для всех членов ООН.

16. Гарантии права на свободу выражения мнений, права на свободу ассоциаций и других основных прав и свобод доработаны в ICCPR, Международной конвенции о ликвидации всех форм расовой дискриминации, Конвенции о ликвидации всех форм дискриминации в отношении женщин и в других международных документах. Хотя они и не в полной мере обязательны для всех членов GAC, это оказывается хорошим подспорьем при интерпретации GAC-овских принципов уважения к Всеобщей декларации прав человека и могут стать основой при подготовке рекомендаций для Правления ICANN. Эти инструменты отдельно упоминаются в Справочном руководстве заявителя на новые gTLD (Справочном руководстве) в связи с процедурами возражения по ограничениям общественной политики.

3. Аспекты новых gTLD, связанные с контентом

3.1 Природа доменных имен

17. Для интернет-пользователей в целом доменные имена представляют собой важный механизм поиска и получения доступа к информации в Интернете. Доменные имена несут функции и адресации и описания. Соотношение между ними может варьироваться по масштабу и размеру. Слова или формы выражения, включенные в TLD, предлагают возможные ассоциации с характером деятельности и контентом, расположенным на сайтах зарегистрированных под этим конкретным TLD. Например, «.com» изначально ассоциируется с коммерческой деятельностью, хотя этот домен использует широкий спектр организаций. В отличие от него, «.org» и «.net», ассоциируются с некоммерческими организациями или деятельностью гражданского общества. Более узкие домены, такие как «.museum» и «.travel», еще сильнее связаны с тем, что представляется «музеями» и «путешествиями».

18. Национальные суды в различных юрисдикциях рассматривали (в основном – в контексте дел о торговых марках) вопросы, связанные с использованием доменных имен второго уровня в качестве средства выражения, некоторые из которых упомянуты ниже. По делу использования товарного знака в доменном имени второго уровня с целью критики, Парижский апелляционный суд посчитал, что это было сделано в осуществление права на свободу выражения мнения и оставил в силе такое выразительное использование товарного знака, постановив, что:

> «[...] Свобода выражения мнений, принцип конституционного уровня, как признано в договорах и

> конвенциях, напомненных [одним из заявителей], подразумевает, что [заявители] могут денонсировать, на Интернет-сайтах, связанных с этим случаем, в форме, которую они считают адекватной социальным последствиям [планов] осуществляемых подсудимыми; что, хотя эта свобода не является абсолютной, она может быть ограничена только в той мере, необходимость которой вызвана соблюдением прав других лиц»

19. Кроме того, Конституционный совет Франции подтвердил необходимость защиты свободы слова в контексте французского код страны TLD (ccTLD). По признакам, в частности, отсутствия гарантий конституционных свобод, особенно свободы слова, Совет признал неконституционной правовую норму Кодекса почтовой и электронной связи, на основании которой были назначены национальные регистры ccTLD и авторизованы для присвоения доменных имен.

20. В голландском дела, суд в Гааге в порядке упрощенного производства отказал протестному сайту (www.injeholland.nl) в праве использовать имя домена, напоминающее название организации, которая была объектом протеста (www.inholland.nl). Согласно решению суда – в поддержку выдвинутых аргументов защиты торговой марки – вредить торговой марке, включив ее в имя протестного сайта, не оправдано. Однако суд указал, что право протестующих на свободу выражения мнения осталось не нарушенным, так как было разрешено использовать название на самом сайте, в ходе дискуссии о репутации организации.

21. В других странах, соотношение между функциональностью и выразительностью доменов было рассмотрено более конкретно. Апелляционный Суд США второй инстанции, постановил в деле Name.Space, Inc против Network Solutions, Inc, что:

> «[...] Функциональность доменных имен не ставит их автоматически выше Первой поправки. Хотя имена доменов и имеют функциональное предназначение, сочетание функциональности и выразительности "существенно переплетенной с элементами коммуникации" зависит от рассматриваемого доменное имени, намерений регистранта, содержания веб-сайта, а также технических протоколов, управляющих DNS.»

22. Другие суды низших инстанций прецедентного права в Европе двигаются в том же направлении, и признают связь между выразительной функцией доменных имен и свободой выражения мнений.

Взаимоотношения между выражениями, включенными в верхний, второй и третий уровни доменов, могут повлечь за собой элементы и выразительные и коммуникационные, из чего следует, что TLD не должны

рассматриваться изолированно.

23. Ожидаемый ввод новых gTLD могут предоставить новые возможности для дальнейшего расширения выразительных возможностей доменных имен. Слова или формы выражения, содержащиеся в поданных новых gTLD, можно рассматривать как полезные для различных отдельных лиц или сообществ в целях выражения идей или взглядов, просто добавляя слова или выражения при регистрации доменов второго или третьего уровня. Взаимоотношения между выражениями, включенными в верхний, второй и третий уровни доменов, могут повлечь за собой элементы и выразительные и коммуникационные, из чего следует, что TLD не должны рассматриваться изолированно.

24. Доменные имена являются ключевыми элементами для Интернет-систем индексации информации и выборки, особенно работающих в поисковых системах. Запросы, сделанные в поисковых системах, состоящие из слов, сочетаний слов или целых предложений, являются важным средством как поиска доменных имен веб-сайтов, могущих содержать эти слова, так и доступа к контенту, размещенному на них. Вопрос, в какой степени индексация содержания сайта поисковыми системами может заменить роль доменных имен в доступе к информации, выходит за рамки данной статьи. Здесь достаточно сказать, что функциональность и выразительность доменных имен не могут быть строго отделены друг от друга или, что происходит постепенный переход из одного в другое.

3.2 Связанные с контентом выборы и решения

3.2.1. Рассмотрение заявленных для новых gTLD строк

25. Утверждение или отклонение заявки, поданной на делегирование нового gTLD для, которая включает слова, названия или формы выражения, не будет механическим процессом, а станет результатом оценки, согласно которой будет делаться выбор и приниматься решение. Руководство предусматривает три случая, когда такие выбор и решение могут быть непосредственно связанными с Интернет-контентом.

26. *Во-первых*, в Руководстве приведен список имен и слов, которые не могут быть делегированы. Он образовывает связанный с контентом выбор, уже априори сделанный ICANN, который, как ожидается, приведет к связанному с контентом решению всякий раз, когда возникнут вопросы, связанные с использованием любого из этих неприемлемых слов.

27. *Во-вторых*, проверка строки, являющаяся частью процедуры оценки, включает в себя оценку возможности заявленной новой строки gTLD оказать негативное влияние на стабильность и безопасность DNS. Это, похоже, включает учет рисков TLD-блокирования, которые можно

предвидеть как следствие различных чувствительностей, касающихся слов, названий или форм выражения, входящих в заявленную строку. Это имело место в ходе дискуссий по спорному заявленному домену .xxx, когда Правление ICANN решило, что риск блокировки не был достаточным, чтобы оправдать отклонение этой строки.

28. Как правило, оценка воздействия TLD-блокирования не может быть строго отделена от соображений относительно того, что именно может оказаться полезными или вредными для пользователей контентом, общин или органов государственной власти в одной или разных частях мира. В связи с этим, в Сан-Францисском коммюнике GAC была обозначена возможная роль ICANN в связанных с контентом оценках. Таким образом, рассмотрение поданных заявок может быть связано с суждениями о том, что контент, возможно, подходит или не подходит для включения в доменное имя и, косвенно, в веб-сайты (более подробный анализ этого вопроса можно найти в пятой части этой статьи).

29. *В-третьих*, Руководство описывает процедуры возражения в контексте которых могут возникнуть вопросы контента и потенциального конфликта между правом на свободу выражения мнения и правом на свободу объединения, с одной стороны, и других законных интересов и прав, с другой стороны.

30. Первые два основания для возбуждения процедуры возражения, а именно – возражение на основании конфликта строк и возражение по законным правам – четко направлены на защиту традиционных прав на товарный знак. На карту поставлен тонкий баланс, при котором свобода самовыражения должна быть сопоставлена с имущественными правами владельцев товарных знаков. Охрана товарного знака не должна быть использована в качестве средства, ограничивающего свободу выражения мнений и удушения общественного обсуждения.

31. Третье основание для возражения, а именно Возражение по ограниченным общественным интересам, касается случаев, когда заявленная строка для gTLD считается противоречащей общепринятым законодательным нормам морали и общественного порядка, признанным в соответствии с принципами международного права. В руководстве говорится, что «в соответствии с этими принципами [международного права], каждый человек имеет право на свободу выражения мнения, но осуществление этого права налагает особые обязанности и особую ответственность. Соответственно, могут применяться определенные ограничения».

32. По этой конкретной процедуре возражения заявленная строка проверяется на наличие в списке соображений морали и общественного порядка, относящихся к подстрекательству и пропаганде насилия и противозаконным действий, дискриминации, детской порнографии, а также проверяется, не противоречит ли заявленная строка определенным принципам международного права.

Применение правил и процедур из Справочного руководства может включать связанные с контентом выборы и решения.

33. Учитывая общий характер этих соображений и отсутствие единого международного их толкования, обсуждение может включать вынесение решения о том, возможно ли, чтобы пользователи Интернета или сообщества, нашли конкретную заявленную строку противоречащей нормам морали и общественного порядка и, следовательно, ограниченный общественный интерес. Эти решения могут иметь прямое влияние на доступность Интернет-контента. Кроме того, конкретные ссылки на право на свободу выражения, содержащиеся в Руководстве, являются признанием того факта, что обсуждения в этом контексте пересекаются с вопросами осуществления права на свободу выражения мнения.

34. Четвертое основание для отказа – возражения сообществ – относится к случаям, когда «есть существенная оппозиция к заявке со стороны значительной части сообщества, к которому эта строка может быть явно или неявно предназначена». Оно позволяет достаточную свободу действий, о чем свидетельствует утверждение спорного домена .xxx. Хотя было подано, множество возражений, они не оказались решающими при окончательном обсуждении на заседании Правления ICANN.

3.2.2 Домены второго и третьего уровней

35. Ожидается, что регистраторы и регистранты установят собственные политики в отношении регистрации доменных имен в доменах второго и третьего уровня. В зависимости от требований законов, существующих в их юрисдикциях и некоторых связанных с контентом спецификаций, утвержденных ICANN, ожидается, что политика регистрации на втором и третьем уровнях будет включать связанные с контентом выбор и решения, свободно принимаемые их операторами. Заявляя, что он не играет никакой роли в отношении интернет-контента ICANN утверждает, что вопросы, связанные с контентом, вероятно, будут рассматриваться регистрантами.

3.2.3 Решение, как у редактора

36. Описанные выше выбор и решения, касающиеся контента, в том смысле, что они могут привести к решениям о доступности информации в Интернете, похожи на редакционные решения, регулярно принимаемые СМИ в отношении того, какой контент соответствует общественному интересу и какой контент станет общественным достоянием.

37. Эта проблема является актуальной, так как с точки зрения права на свободу выражения мнений и доступа к информации, редакционная деятельность может потребовать особых гарантий и обязанностей. Они

относятся к свободе от вмешательства со стороны правительств или других действующих лиц и обязанностям по защите прав и свобод (редакционная ответственность, уважение достоинства и частной жизни, уважение к презумпции невиновности и справедливому судебному разбирательству, уважения к интеллектуальной собственности, средства для третьих сторон), а также к служению интересам общественности в получении доступа к разнообразной информации.

38. Понятие деятельности Интернет-посредников как редакторов в новой коммуникационной среде не ново. Рекомендации Совета Европы CM/Rec(2011)7, изданные Комитетом Министров для государств-членам о новом определении СМИ подтверждают, что редакционные функции могут быть свидетельством собственных политических решений действующих лиц по доступности или пропаганде контента, и по способу его представления или размещения. Редакционная политика может быть включена в программных заявлениях, в условиях использования или может быть выражена неофициально как приверженность определенным принципам. Отсутствие явного утверждения о редакционном управлении в средствах массовой информации не должно само по себе рассматриваться как признак на его отсутствия.

4. Допустимые ограничения на осуществление права на свободу выражения мнения и права на свободу собраний и ассоциаций – региональная перспектива

39. Все 47 государств-членов Совета Европы взяли на себя обязательство обеспечить гражданские и политические права и свободы, предусмотренные в Конвенции о защите прав человека и основных свобод (European Convention on Human Rights – ECHR). Изначальная и главная ответственность за защиту прав, изложенных в Конвенции, лежит на государствах-членах. Любой, называющий себя жертвой нарушения его/ее права и свободы любым из государств, подписавших Конвенцию, может обратиться в Европейский суд по правам человека (ЕСПЧ) после того, как будут исчерпаны внутренних возможности решения проблемы.

40. В отношении права на свободу выражения мнения, статья 10 Конвенции гласит:

> 1. Каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Настоящая статья не препятствует государствам осуществлять лицензирование радиовещательных, телевизионных или кинематографических

предприятий.

2. Осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков или преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

41. В отношении права на свободу собраний и свободу ассоциаций, статья 11 Конвенции гласит:

1. Каждый имеет право на свободу мирных собраний и на свободу объединения с другими, включая право создавать профессиональные союзы и вступать в таковые для защиты своих интересов.

2. Осуществление этих прав не подлежит никаким ограничениям, кроме тех, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности и общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности или защиты прав и свобод других лиц. Настоящая статья не препятствует введению законных ограничений на осуществление этих прав лицами, входящими в состав вооруженных сил, полиции или административных органов государства.

42. Любое вмешательство в осуществление этих прав и свобод должно: (1) быть предписано законом, (2) осуществляться по одной из законных целей, перечисленных исчерпывающим образом в Конвенции и (3) быть необходимыми в демократическом обществе (пропорционально преследуемой цели).

43. При определении того, были ли действия или бездействие государства-члена совместимы с условиями, изложенными в Конвенции, ЕСПЧ признает, что национальные власти пользуются определенной свободой действий в оценке остроты социальной потребности, делающей ограничение основных прав и свобод, необходимыми в соответствии с условиями, изложенными в Конвенции. В юриспруденции ЕСПЧ это называется свободой усмотрения доктрины. Дозволенная государствам-членам степень свободы варьируется в зависимости от обстоятельств, предмета разбирательства и других факторов.

44. Этот раздел документа посвящен построению ЕСПЧ некоторых понятий, таких как разжигание ненависти, защита нравственности, значение религии и общественного порядка в контексте случаев, касающихся статей 10 и 11 Конвенции. В нем также подчеркиваются некоторые из основных соображений в ЕСПЧ, где право на свободу выражения мнения и право на свободу объединения должны быть сбалансированы с другими правами. Эта информация имеет важное значение для информирования дискуссий, где при оценке поданных заявок на новые gTLD аналогичные понятия и упражнения в балансировании могут привести к опасности. Комментарии, включенные в эту часть статьи приведены не в ущерб для любых возможных будущих толкований ЕСПЧ и не должны рассматриваться как предложения о возможных применениях стандартов прав человека к какой-либо конкретной заявке на новую строку для gTLD.

4.1 Разжигание ненависти

45. Выражение взглядов, отрицающих основные ценности Конвенции, исключено из-под защиты Конвенцией как нарушение прав на основании статьи 17 Конвенции. При рассмотрении предполагаемого нарушения права на свободу выражения мнения на основании статьи 10 Конвенции, ЕСПЧ может обозначить определенные ограничения на выражение взглядов как необходимые в демократическом обществе в интересах национальной безопасности, общественного порядка, предотвращения беспорядков или преступлений, охраны здоровья или нравственности населения или защиты прав и свобод других лиц.

46. Выражение взглядов, представляющих собой подстрекательство к расовой ненависти и поддержку терроризма не защищены статьей 10. Сообщения о сторонниках ненависти, даже если это включает в себя передачу их мнения, однако, допустимы. Тексты, лишь полемические, фактически не утверждающие ненависти, входят в сферу защиты Конвенцией. Речи, пропагандирующие введение (или восстановление) недемократических, тоталитарных режимов, особенно включающие в себя призывы к насилию, не защищены статьями 10 и 11. Однако ожесточенная критика светского и демократического принципов охраняется как часть политического дискурса.

Свобода выражения мнения, гарантированная статьей 10 Конвенции, применима не только к информации или идеям, благосклонно принимаемым или считающимся безобидными или безразличными, но также и к оскорбляющим, шокирующим или внушающим беспокойство; таковы требования плюрализма, терпимости и широты взглядов, без которых нет демократического общества (Хэндисайд против Великобритании).

47. Отрицание Холокоста (негативизм) рассматривается как одна из «наиболее серьезных форм расовой диффамации евреев и

подстрекательства к ненависти к ним», и поэтому не защищено статьей 10. Статья 17 применяется скорее тогда, когда цели публикации взглядов явно несовместимы с основополагающими ценностями Конвенции. Антисемитизм и разжигание «ненависти к еврейскому народу», как особой этнической группе, также не защищены. Яростные атаки против религиозных групп в целом (например связь мусульман в целом с террористическими атаки 11 сентября 2001 года) также несовместимы с ценностями Конвенции.

48. Политические речи, особенно когда они способствуют расширению дискуссии по поднятым вопросам, находящиеся в согласии с целями Конвенции, находится под ее защитой, равно как и политические речи, ни призывающие к насилию, ни освобождающие от ответственности за него. Выражения взглядов, могущих «оскорблять, шокировать или внушать беспокойство» другим могут, по условиям статьи 10 Конвенции, быть защищены в соответствии с юриспруденцией ЕСПЧ.

4.2. Защита нравственности и общественного порядка

49. В разных случаях, касающихся осуществления права на свободу выражения мнений в контексте публикаций и выставок, Суд неоднократно устанавливал, что единую концепцию морали среди национальных законодательств государств, присоединившихся к Конвенции, найти не удается. Учитывая, что взгляды соответствующих законов, устанавливающих требования к нравственности, меняются в зависимости от времени и места, органы государственной власти «в принципе, находятся в более выгодном положении, чем международный судья, давая заключение о точном содержании этих требований а также о «необходимости» «ограничения» или «наказания», предназначенных для удовлетворения требований».

Суд неоднократно устанавливал, что концепцию морали или концепцию о значении религии в обществе, единые для национальных законодательств государств, присоединившихся к Конвенции, найти не удается.

50. Как и в случае с «моралью», ЕСПЧ заявил, что единую для всей Европы концепцию о значении религии в обществе создать невозможно. Следовательно «к всеобъемлющему определению, что является допустимым вмешательством в осуществление права на свободу выражения мнений, когда такое выражение направлено против религиозных чувств других, прийти невозможно. Поэтому следует оставить определенную свободу толкования в оценке наличия и степени необходимости такого вмешательства на усмотрение национальных органов власти». ЕСПЧ постановил, что «государствам, присоединившимся к Конвенции, предоставляется более широкая свобода при регулировании свободы выражения мнения в отношении вопросов, которые могли бы оскорбить интимные личные убеждения в сфере морали или, тем более,

религии».

51. Свобода действий национальных властей в этих областях широка, но не безгранична. ЕСПЧ строго рассматривает совместимы ли ограничения, применяемые национальными властями, с условиями статьи 10 Конвенции, в том числе, пропорциональны ли они преследуемой законной цели.

52. Цель предотвращения беспорядков или преступлений является одной из законных целей, предусмотренных статьями 10 и 11 Конвенции. ЕСПЧ постановил, что исключения из статьи 10 могут быть сделаны в интересах предотвращения беспорядков и защиты прав иммигрантов. В этом случае суд подчеркнул важность обстоятельств выражения взглядов (в данном случае во время предвыборной борьбы).

53. Хотя понятие общественного порядка в Статье 10 отдельно не упоминается, ЕСПЧ назвал его в своей практике. «Отрицание преступлений против человечности является одной из самых серьезных форм расовой диффамации евреев и подстрекательства к ненависти к ним. Отрицание или ревизия этого типа исторических фактов подрывает ценности, на которых основана борьба против расизма и антисемитизма и представляет собой серьезную *угрозу для общественного порядка*».

4.3. Коммерческие выражения

54. Коммерческие выражения в контексте рекламы могут быть защищены в рамках Конвенции и, следовательно, их запрет может представлять собой вмешательство в право на свободу выражения мнения. ЕСПЧ также постановил, что общие запреты уничижительных заявлений в сравнительной газетной рекламе могут представлять собой непропорциональное вмешательство в свободу коммерческой речи в секторе средств массовой информации.

55. Коммерческие выражения, однако, менее защищены, чем выражение политических или религиозных идей и государству предоставляется широкая свобода в отношении коммерческих выражений. Как правило, если не только (и даже не столько) коммерческие интересы находятся под угрозой, из-за вклада идей в более общую дискуссию по вопросам, представляющим общественный интерес, ЕСПЧ признает, что рамки свободы могут быть значительно сужены.

56. Чтобы различить коммерческие и некоммерческие элементы выражения, ЕСПЧ рассматривает цель выражения, а также является ли реклама целью первичной или вторичной. Для выражения не достаточно иметь форму рекламы, чтобы оно рассматривалось, как имеющее коммерческий характер. ЕСПЧ рассматривает содержание и цель взглядов, высказанные в рекламе.

57. Кроме того, при определении уровня защиты ЕСПЧ учитывает целевую аудиторию и роль прессы. Если выражение направлено на общество в целом (а не ограниченном кругу читателей), а не только предоставляет информацию коммерческого характера, оно с большей вероятностью будет засчитано как некоммерческая речь. Если обсуждаемые выражения являются только «коммерческими заявлениями», но и способствуют социальным дебатам, ЕСПЧ будет ограничивать свободу их рассмотрения. С этой точки зрения критика товара может рассматриваться как некоммерческая речь, если в ней нет рекламы альтернативных продуктов и тема представляет общественный интерес.

58. В случаях «гибридной речи» – когда коммерческие и некоммерческие элементы выражения нельзя отделить – они оцениваются вместе и рассматриваются как часть единого целого.

4.4. Защита торговых знаков

59. В вопросе жалоб о праве собственности (статья 1 Протокола №1 Конвенции) против национальных мер, запрещающих использование доменных имен на основе защиты товарного знака, ЕСПЧ установил, что исключительные права на использование доменов, о которых идет речь, имеют экономическую ценность и поэтому представляют собой «имущество». При рассмотрении вопроса об оправданности вмешательства в это право соответствии со статьей 1 Протокола №1, ЕСПЧ указал на необходимость защите товарных знаков и/или (бизнес)-имен соответствовать требованиям общего интереса, подтвердил широкую свободу государств в рассмотрении вопросов в этой области, и был удовлетворен тем, что национальные власти добиваются справедливого баланса между защитой имущества и требованиями общего интереса.

60. ЕСПЧ рассмотрел конфликт между товарными знаками и правом на свободу слова вне контекста доменных имен. В этой подборке случаев Суд систематически постановлял, что торговые марки составляют интеллектуальную собственность и, следовательно, являются «собственность» по смыслу статьи 1 Протокола №1 к Конвенции. Запрет для журналистов-расследователей представлять негативные высказывания в отношении определенного товарного знака не считался предварительной цензурой. Принимая во внимание ряд факторов, ЕСПЧ указал, что так будет только в том случае, если заявители будут обязаны представлять для утверждения в органы власти заявления, которые они хотели бы опубликовать, заранее.

61. Ложные коммерческие выражения, заключенные в рекламе, приняты ЕСПЧ как не защищенные статьей 10 гарантий права на свободу выражения мнения, так как реклама рассматривается как средство сообщения характеристик товаров и услуг, предоставляемых населению. В соответствии с этим рядом случаев, большинство форм использования товарных знаков подпадает под действие статьи 10, но на них могут быть

введены ограничения в целях защиты «прав других лиц», то есть права на товарный знак, в соответствии со статьей 10, пунктом 2.

4.5. Альтернативные способы выражения

62. Если когда случался конфликт между имущественными правами с одной стороны, и осуществлением права на свободу выражения мнения и права на свободу собраний с другой стороны, ЕСПЧ в таких случаях интересовался, были ли доступны заинтересованной стороне альтернативные способы выражения.

63. В случае, когда заявители были лишены возможности сбора подписей под петицией в торговом центре, принадлежащем частной компании, ЕСПЧ не нашел нарушений права на свободу выражения мнения заявителей. Изучая соответствие помех требованиям статьи 10, ЕСПЧ выразил мнение, что заявителям было запрещено представлять свое мнение только в определенных местах и они могли использовать альтернативные средства, в том числе кампании в центре города, агитацию «от двери к двери» или искать публичности в местной прессе, радио и телевидении.»

64. Кроме того, ЕСПЧ рассматривает, доступна ли была другая терминология, кроме фактически использованной, для выражения точек зрения, когда использование альтернативных терминов считается «необходимым в демократическом обществе» для защиты репутации и прав других лиц. По делу судебного запрета для политика использовать определенные слова – «нацистская журналистика» против клеветнической статьи во влиятельной газете – ЕСПЧ заключил, что судебное постановление запретило лишь повторение заявления или публикацию подобных ему заявлений, в то время как право заявителя высказывать свое мнение, было сохранено.

65. По делу о запрете для сотрудников вооруженных сил, полиции и служб безопасности присоединяться к любой политической партии и заниматься политической деятельностью, оправданном необходимостью обеспечения политической нейтральности государственных служащих, ЕСПЧ считает, что не было никакого вмешательства в право офицеров на свободу выражения и свободу собраний, тем более, что полиции предложили альтернативные способы выражения своих идей или создания ассоциации, кроме присоединения к политической партии.

66. Существование альтернативных средств выражения не препятствует, однако, тщательному и исчерпывающему анализу, уважаются ли гарантии свободы выражения мнения и свободы ассоциаций, как это предусмотрено в статьях 10 и 11. На самом деле, ЕСПЧ тщательно рассматривает, были ли соблюдены строгие требования этих положений Конвенции, а именно, было ли вмешательство предусмотрено законом, преследовало ли вмешательство законные цели, зафиксированные в

Конвенции и было ли такие вмешательство необходимо в демократическом обществе.

5. Чувствительные выражения и стабильность DNS

67. Потенциально вредное влияние заявленных новых gTLD на стабильность и устойчивость DNS имеет решающее значение для их оценки и принятия по ним решения. В GAC, похоже, придают особое значение вопросу о культурном нежелательных и/или чувствительные строках, отсутствие которых, как полагают, способствует обеспечению безопасности и стабильности DNS.

68. Размышления этом контексте происходят от озабоченности по поводу блокирования или фильтрования доменов, которые могли бы иметь место, при включении чувствительных выражений в новые gTLD. Так как такие риски существуют, то может прийтись выбирать между двумя вариантами: или не одобрять любые заявки, поданные на содержащую чувствительные выражения строку в целях сохранения стабильности и безопасности DNS, или же, утвердить такой домен, что в свою очередь может создать риски стабильности DNS.

69. Эта часть статьи рассматривает эти вопросы с точки зрения защиты права на свободу выражения мнения и права на свободу объединений. Она сосредоточена на вопросах блокирования TLD и последствий отказа в утверждении заявок на чувствительные строки с целью выявления соображений, могущих иметь отношение к рекомендациям GAK.

5.1 Чувствительные выражения

70. В данной статьи, термин «чувствительное выражение» понимается, в соответствии с Принципами GAC в отношении новых gTLD, как любые формы выражения к которым может применяться «чувствительность по терминам с национальным, культурным, географическим и религиозным значением".

... материалы еще не существуют на время заявки на новый gTLD и любой будущий контент не может быть точно известен или предсказан, пока gTLD не заработает.

71. При оценке проблемы чувствительности в этом контексте GAC может рассмотреть возможный контент, который будет размещаться в домене, такой как тематическое содержание или описание услуг. Широкий характер чувствительностей, упомянутых в Принципах GAC в отношении новых gTLD делает акцент на потенциальном контенте домена и суб-доменов как области риска для GAC с точки зрения обязательств по правам

человека. Риск состоит в том, что эти материалы еще не существуют на время заявки на новый gTLD и любой будущий контент не может быть точно известен или предсказан, пока gTLD не заработает. Прогнозировать конкретику будущего фактического контента в домене, а также на 2-м, 3-м или 4-м уровнях скорее всего невозможно. Рекомендация GAC в этом контексте, скорее всего, будет основана на предположениях и дедукции, и по этой причине будет проблематичной. Кроме того, конкретный gTLD может не быть адекватно говорящим о конкретном содержании, или может быть настолько общим, например *dotreligion*, что дать четкие рекомендации о последствиях для прав человека не представляется возможным.

72. В то же время, опасения по поводу чувствительных выражений могут быть реальными и в некоторых случаях значительными. Например, заявка может быть очень чувствительной, если она относится к конкретной географической области, где произошел вооруженный конфликт или война или где идет спор между странами или внутри страны о географических или национальных границах. Некоторая дополнительная информация может быть получена в ходе проверки заявителей и заявок о целях предлагаемого домена и других требований, предъявляемых в процессе подачи заявления. Например, в 2010 году было 320 религиозных организаций, имевших консультативный статус в ЭКОСОС при ООН. Чувствительность GAC по каким-либо конкретным заявкам типа dotreligion может широко варьироваться в зависимости от того, был ли заявитель государством-участником, другой частной компанией или организацией гражданского общества.

73. Государства хорошо осведомлены о своих обязательствах по правам человека и многие выражают серьезную озабоченность в связи с онлайн-контентом, нарушающий права человека, включая право на свободу выражения мнения. Опасения по поводу чувствительных выражений бывают весьма значительными, в частности связанные с ксенофобией и расизмом. Рассмотрение GAC новых gTLD должно учитывать обязательства по защите и поощрению прав человека и основных свобод. Угрозы насилия, например, или бурная реакция на заявку или против конкретного заявителя может заставить правительство реально и всерьез опасаться за безопасность своих граждан. В целом GAC и Правление ICANN, должны замечать такие чувствительности и подумать, как лучше принимать их во внимание в процессе ввода новых gTLD. Тем не менее, обеспечение безопасности и верховенства права в рамках своих национальных границ наилучшим образом – дело суверенных государств.

74. Эти вопросы актуальны при рассмотрении чувствительных выражений, когда они входят в поданную заявку на новый gTLD, так как gTLD – это глобальный общественный ресурс. Чувствительность может возникнуть только у отдельных, а не всех членов GAC или она может варьироваться в широких пределах и в различной степени среди членов GAC. Для определения характера и степени любого чувствительного выражения, такие выражения должны рассматриваться в контексте, в том числе в глобальном контексте.

5.2. Блокирование DNS и связанные с ним риски для устойчивости и стабильности DNS

75. Опасения по поводу чувствительных выражение в новых gTLD может подвигнуть некоторых или всех членов GAC постараться не допустить к новым gTLD граждан своих стран и/или граждан других стран с помощью блокирования и/или фильтрации DNS (это относится и к gTLD и к доменам второго уровня). Такие меры направлены на предотвращение доступа к Интернет-контенту.

76. Существуют серьезные опасения относительно уровня влияния блокирования и фильтрации на устойчивость и стабильность DNS. Предполагается, что с чисто технической точки зрения трудно провести грань между «хорошим блокированием DNS» и «плохим блокированием DNS». Кроме того, похоже, что существуют опасения по поводу нежелательных негативных последствий для более широких сообществ от блокирования целых доменов на уровне страны.

77. Тем не менее, фильтрации и блокирования DNS правительствами являются массовыми. Специальный докладчик ООН по вопросу о поощрении и защите права на свободу мнений и их выражения отметил, что многие меры фильтрации и блокирования являются нарушением международных стандартов прав человека, особенно права на свободу выражения мнения и право на свободу объединений, а также надлежащей правовой процедуры. Например, оправдание для блокирования определенного контента может быть необоснованным или может быть сделано «чрезмерно широким и расплывчатым образом», так что блокирования и фильтрации становятся произвольными и чрезмерными. Блокирования или фильтрации могут быть проделано для достижения целей, не являющихся законными или вообще не ясными, и, наконец, контент часто блокируется без возможности для независимой оценки.

78. Совет Европы принял руководящие принципы, адресованные его государствам-членам в отношении использования и управления интернет-фильтров для того, чтобы в полной мере осуществлять и пользоваться правом на свободу выражения мнений и информации. В случаях, когда блокирование или фильтрация доменного имени необходима как реакция на злоупотребления или другие виды незаконной деятельности и киберпреступности, в полной мере применимы положения Будапештской конвенции о киберпреступности.

79. Правительства в некоторых случаях предотвращают доступ к онлайн-контенту, включая чувствительные домены. Заявленные новые gTLD могут включать в себя выражения, чувствительные для некоторых или всех членов GAC до такой степени, что может возникнуть высокий риск многочисленных и разнообразных мер по фильтрации и блокированию TLD отдельными правительствами в рамках своих суверенных границ или

правительств, действующих сообща. Такие действия сопряжены с риском для устойчивости и стабильности DNS, у которой появляется все больше проблем и это вызывает вопросы в отношении международных стандартов в области свободы слова и доступа к информации, а также свободы ассоциаций.

5.3. Смысл рекомендаций GAC

80. Рекомендации GAC могут покрыть широкий круг вопросов, некоторые из которых содержатся в Принципах GAC по новым gTLD, в частности, важность «безопасности, надежности, совместимости и глобальной стабильности» DNS, поощрение потребительского выбора и географического разнообразия и обеспечения справедливости, прозрачности и недопущения дискриминации между заявителями в новом процессе gTLD. Проблемы, касающиеся особенно чувствительных выражений должны быть сбалансированы с этим и, возможно, с рядом других факторов. В свете подхода, основанного на правах человека, есть ряд конкретных соображений и факторов, которые приведены ниже.

81. Как отмечалось выше, конкретные чувствительности GAC будут зависеть от контекста каждой заявки и, скорее всего, широко варьироваться среди членов ПКК. Чувствительность может быть высказана в замечаниях о раннем предупреждении, которые не обязательно должны быть от всех членов GAC или иметь поддержку консенсуса GAC и формально не являются возражения против заявки, поданной на новый gTLD. Таким образом, акцент делается прежде всего на рекомендациях GAC, в частности, на рекомендации не обрабатывать заявку и на рекомендации не обрабатывать заявку, пока она не будет реабилитирована.

5.3.1. Рекомендация не обрабатывать заявку

82. Подход GAC к выражениям, могущим вызвать сильную чувствительность до такой степени, что GAC придется дать рекомендацию не обрабатывать заявку, как ожидается, будет новинкой для ICANN и GAC. Существующие методы борьбы с такими выражениями в национальном контексте могут оказаться непригодными в связи с глобальной публичной политикой в DNS.

83. С точки зрения прав человека важно вспомнить резолюцию Совета ООН по правам человека: Поощрение, защита и осуществление прав человека в Интернете, которая утверждает, что те же права, что люди имеют офлайн также должны быть защищены в Интернете, в частности свобода выражения мнений. Кроме того, Комитет ООН по правам человека недавно дал указания относительно действий правительства в отношении запрета на онлайн-контент и интернет-системы. Комитет отметил, что «допустимые ограничения в целом должно быть специфичными по

контенту; общие запреты работы отдельных сайтов и систем не совместимы с допустимыми пределами по Статье 19." Он пошел еще дальше, заявив, что "[также] несовместимо с [допустимыми пределами по Статье 19] запрещение сайту или системе распространения информации публикации материала исключительно на том основании, что он может содержать критику правительства или социально-политической системы, поддерживаемой правительством».

Декларация Совета Европы: «Выражения, содержащиеся в названиях интернет-сайтов, такие как доменные имена и строки, не должны, априори, быть исключены из сферы применения правовых стандартов в области свободы выражения мнений и права на получение и распространение информации и должны, таким образом, получать презумпцию в свою пользу.»

84. Различия в чувствительности национального, культурного или религиозного характера и политического характера могут быть трудно определимыми. Часто областями раздора становятся обвинения в коррупции и политическая сатира или комментарии. Декларация Совета Европы о защите свободы слова и доменных имен является полезным руководством по применению стандартов прав человека в этой области.

85. Очевидным является то, что принцип GAC об уважении чувствительности по терминам национального, культурного, географического и религиозного значения не мог, с точки зрения прав человека, являться основанием для рекомендации запрета политически чувствительных gTLD. Это особенно важно, поскольку это имеет отношение к вопросу о доступе к глобальным общественным ресурсам (новым gTLD), который коснется всех пользователей Интернета во всех странах, а не только в конкретных странах или регионах. В контексте Совета Европы, государства-члены Организации согласились с приверженностью делу защиты универсальности, целостности и открытости Интернета, в частности, «принимая все разумные меры для обеспечения того, чтобы разработка и применение стандартов, политик, процедур или практики управления критическими для функционирования Интернета ресурсами, включала защиту прав человека и основных свобод Интернет-пользователей в соответствии со стандартами прав человека, признанными в международном праве.»

86. Рекомендация GAC против чувствительного политического выражения, скорее всего, поднимет вопрос в отношении поддержания международных стандартов прав человека, запрещающих общий запрет на контент и информацию. Решения Правления ICANN могут оказаться открытыми для мощного правового разбирательства, если на рекомендации GAC такого рода будет основано решение об отказе либо ином поражении в правах заявки. Провести черту точнее в каждом конкретном случае может быть весьма трудно. У государств, тем не менее, есть позитивные обязательства по обеспечению гарантирования права на свободу выражения мнений даже в контексте деятельности, осуществляемой

частными лицами (например, ICANN), в частности, путем обеспечения того, что не будет накладываться необоснованных ограничений на свободу выражения мнения или цензура. По этим причинам Правление ICANN должно работать с GAC тщательно и конструктивно, чтобы полностью понять причины озабоченности GAC по поводу чувствительного выражения и чтобы иметь возможность обратиться к ним в полном соответствии с требованиями международных стандартов прав человека.

5.3.2. Рекомендация не обрабатывать заявку, пока она не будет реабилитирована

87. Подход утверждения прав человека предполагает, что, в случае принятия рекомендации не обрабатывать заявку, пока она не будет реабилитирована, шаги по ее реабилитации должны соответствовать международным стандартам прав человека. Например, меры по ее реабилитации должны быть согласованы с разумными ограничениями, разрешенными в Всеобщей декларации прав человека и других публичных стандартах политики, перечисленных в Руководстве. В случае сомнений, руководствоваться нужно другими стандартами, например такими, как статьи 19 и 20 Международного пакта о гражданских и политических правах.

88. Принципы GAC по новым gTLD требуют от заявителей обещания того, что они внедрят еще до запуска нового gTLD процедуры, позволяющие блокировать имена, имеющие национальное и географическое значение на втором уровне. В связи с этим необходимые обязательства со стороны заявителей не должны выходить за рамки условий международных стандартов прав человека.

89. Кроме того, для выявления убедительной причинно-следственной связи между чувствительностью, gTLD и фактическим вредом для людей, которых можно идентифицировать, рекомендуется использовать строгий основанный на фактах подход. Чем слабее прямая причинно-следственная связь, тем слабее и менее устойчиво оправдание любого вмешательства или ограничения широких рекомендаций по реабилитации. В связи с этим, некоторое представление можно получить в ходе проверки заявителей и заявления о целях предлагаемого домена и других требований, выполняемых в процессе подачи заявления.

90. Озабоченность GAC о заявителях и целях новых gTLD, однако, нуждается в привязке к стандартам прав человека. Вопросам, касающимся характера заявителя, его/ее расположения, цели gTLD и соотношения их с чувствительностями, должно быть уделено должное внимание в отношении свободы выражения мнений и свободы ассоциации, особенно в случаях, когда заявителем является сообщество.

91. Защита права на свободу ассоциации не ограничивается традиционным понятием общественных места (например, автомобильных

дорог общего пользования, дорог или других ощутимых пространств). Специальный докладчик ООН по вопросу о праве на свободу мирных собраний и ассоциаций пришел недавно к выводу, что право на свободу мирных собраний и ассоциаций применимо и к онлайн-пространству тоже, и призвал государства признать, что эти права и свободы могут быть реализованы с помощью новых технологий, включая Интернет.

92. Заявки на gTLD от сообществ могут поднять ряд конкретных вопросов, касающихся свободы ассоциации для групп. Это особенно касается случаев, когда gTLD относится к подтверждению прав сообществ по интересам или свободному выражению, не могущих быть в полной мере реализованных или принятых в конкретных государствах. Такие факторы будут иметь вес против рекомендации не обрабатывать заявку.

Утверждая подхода прав человека можно считать, что лучше принимать чувствительные выражения и иметь дело с последствиями, в том числе национальными внутреннеполитическими, при которых обладатели прав человека, простые граждане, имеют возможность обсудить их проблемы, участвовать в национальном диалоге по действиям для решения этих проблем и искать эффективные средства правовой защиты.

93. Таким образом, был бы предпочтительнее подход к рекомендациям GAC, совместимый с правами человека. Это позволило бы дать GAC возможность для изучения более широкого спектра вариантов рекомендаций, способного отражать более тонкие и сложные соображения. Например, необходим многоуровневый набор опций для восстановления, которые соответствуют международным стандартам в области прав человека на свободу выражения мнений и свободу ассоциаций, при консультациях по новым gTLD. Запросы на реабилитацию и рекомендуемые заявителям области должны исходить из самого разрешительного подхода, утверждающего большинство прав, сдвигаясь в сторону более ограничительного подхода, только когда это необходимо.

94. В общем, ожидается, что рекомендация не обрабатывать заявку, будет редким и исключительным случаем, возможным только тогда, когда выражение оказывается явно незаконным, просто потому, что полная предварительная цензура и ковровые запреты на выражение запрещены международным правом.

95. В итоге, для GAC было бы предпочтительнее предоставлять рекомендации в Совет ICANN, скорее поддерживающие право на свободу выражения мнения и право на свободу объединения, и принимающие управление любыми рисками, связанными с чувствительными строками, чем априорно ограничивающие права и свободы своих граждан (и глобальных Интернет-пользователей), порекомендовав не обрабатывать заявку на новый gTLD или необоснованно или несправедливо ее реабилитировать.

96. Как носители обязанностей, государства должны, в случае

сомнения, способствовать защите прав и свобод лиц, находящихся под их юрисдикцией, а не их собственной чувствительности. Декларация Совета Европы о свободе выражения мнения и доменных именах подчеркивает этот момент, отмечая, что окончательное решение о блокировании доменных имен должно приниматься компетентными органами, относиться к четко идентифицированному контенту и быть соразмерным.

6. Выводы.

97. В международном законодательстве по правам человека, государства несут ответственность и имеют обязательства по защите, уважении и поощрении прав человека и свобод лиц, находящихся под их юрисдикцией. У государств есть эти обязательства, и тогда, когда они участвуют в предприятиях со специализированными техническими мандатами. В свете этой роли государств, рекомендациям GAC должно быть уделено особое внимание Совета ICANN.

98. Так как новые gTLD могут быть использованы как средство выражения взглядов или как пространство для онлайн ассоциации, у них есть измерение прав человека и основных свобод, которое следует рассматривать вместе с другими техническими вопросами. Оценка заявки, поданной на новый gTLD, а также при регистрации на втором и третьем уровне доменов может включать связанные с контентом выбор и принятие решения. В то время как в решение ICANN не стоит вмешиваться неоправданно, ICANN должна выполнять свою роль с учетом основных прав и свобод и в полном соответствии с международными стандартами. В частности, любое вмешательство в осуществление права на свободу выражения мнения и права на свободу объединения должно быть проверено на соответствие требованиям международного законодательства о правах человека.

99. В контексте Совета Европы, такое вмешательство должно удовлетворять условиям Статей 10 и 11 Европейской конвенции по правам человека, в частности, быть установленным законом, преследовать одну из законных целей, специально описанных в Конвенции и быть необходимым в демократическом обществе. При осуществлении надзора за совместимостью мер, принятых государствами-членами Совета Европы, с этими условиями ЕСПЧ признает существование у национальных органов власти допустимого диапазона в первоначальной оценке остроты социальной потребности, делающей ограничения на эти права и свободы необходимыми в соответствии со Статьями 10 и 11 Конвенции. ЕСПЧ находит, что отсутствие единой концепции и интерпретации государствами-членами Совет Европы некоторых понятий, такие, как мораль и значение религии, приводит к расширению этого допустимого диапазона.

100. В отношении заявок, поданных на новые gTLD, вызывающие чувствительность, важно принимать во внимание их контекст, с учетом

глобального характера gTLD и DNS. Ковровые запреты на использование слова, названия или формы выражения в глобальном общественном ресурсе на основании политической чувствительности поднимали бы вопросы в отношении соблюдения международных стандартов по правам человека о праве на свободу выражения мнения и праве на свободу объединений. Рекомендации GAC, в которых предлагается не обрабатывать такие заявки на основании других чувствительностей, необходимо рассматривать в зависимости от конкретного случая. Различия между чувствительностями национального, культурного или религиозного характера и мерами политического характера часто может быть очень трудно найти. Подход к рекомендациям GAC, основанный на правах человека, создаст GAC возможности для изучения более широкого спектра вариантов рекомендаций, имеющего возможность отражать более тонкие и сложные соображения.

Глоссарий

ccTLD – country code Top Level Domain: домен верхнего уровня – код страны

DNS – Domain Name System: Система доменных имен

ECHR – European Convention on Human Rights: Европейская Конвенция по правам человека, Конвенция

ECtHR – European Court of Human Rights: Европейский суд по правам человека, ЕСПЧ

gTLD – generic Top Level Domain: общий домен верхнего уровня

ICCPR – International Covenant on Civil and Political Rights : Международный пакт гражданских и политических прав

IDN – Internationalised Domain Name: интернационализированное доменое имя

New gTLDs – new generic Top Level Domains: новые общие домены верхнего уровня

TLD – Top Level Domain: домен верхнего уровня

UDHR – Universal Declaration on Human Rights: Универсальная декларация прав человека

4.1.3. Отслеживание в Сети (трекинг) и неприкосновенность частной жизни: Приоритет уважения к контенту, прозрачность и контроль

Международная рабочая группа
по защите данных в телекоммуникациях

675.46.13

Рабочий документ

Отслеживание в Сети (трекинг) и неприкосновенность частной жизни:

Приоритет уважения к контенту, прозрачность и контроль

Заседание 53, 15-16 апреля 2013, Прага (Чешская Республика)

- **Введение**

1. Этот документ базируется на фундаменте уважения основных прав и свобод пользователей Сети. Хоть и не фокусируясь на конкретных технических средствах, документ предполагает, что технические действия веб-отслеживания должны быть законными, приемлемыми и что оно должно работать в строгих рамках прав пользователей Сети. Принципы выбора и контроля — по утверждению больший части индустрии — создают основу этой структуры, и эти принципы должны проводиться в жизнь с точностью на колоннах четкости, прозрачности и подотчетности. Обоснования для введения веб-отслеживания не самоочевидны и, таким образом промышленность и другие представители отслеживания должны постоянно стремиться искать решения, обеспечивающие эту деятельность не только непосредственно в рамках основных прав и неприкосновенности частной жизни, а также в соответствии с императивом «Конфиденциальность, заложенная в проекте».

2. В этом рабочем документе рабочая группа рассматривает вопрос веб-отслеживания и неприкосновенности частной жизни. Хотя четкого определения термина не существует, мы будем опираться на определение веб-отслеживания, как «сбор, анализ и применение данных по активности пользователей с компьютера или устройства при пользовании различными сервисами Информационного Общества (далее: Сеть) с целью ее комбинирования и анализа для различных целей, от благотворительных и филантропических до коммерческих». Мы считаем, что различные формы исследований рынка подпадают под это определение веб-отслеживания, например, измерение пропаганды (степень обслуживания пользователей рекламой в Сети), измерения вовлечения (степень взаимодействия

пользователей с сервисами в Сети) и измерения аудитории (степень возможности составления микропрофилей по взаимодействию пользователей с сервисами в Сети).

- **Сфера действия Рабочего документа**

3. Документ адресован всем провайдерам веб-сайтов, а также разработчикам программного обеспечения и провайдерам сервисов, предлагающих или использующих технологии отслеживания. В данной статье обсуждается развитие технологий отслеживания и их возможное влияние на неприкосновенность частной жизни граждан. Эта статья посвящена цифровым следам, оставленным при использовании различных сервисов Информационного Общества при помощи веб-броузера, в том числе уникальным идентификаторам, полученным методами, не использующими Cookies. В рассмотрение включены веб-броузеры и на других устройствах, например смартфонах и смарт-телевизорах.

4. Эта статья не рассматривает конкретные дополнительные риски, могущие быть обусловленными появлением приложений на мобильных устройствах. Тем не менее принципы, изложенные в этом документе, следует также применять для отслеживания механизмов, используемых в других сервисах.

5. Эта статья не рассматривает, как защитные меры могут быть реализованы (например, юридические требования для согласия). Заметим, что в то время как в некоторых странах, в зависимости от цели веб-отслеживания, требуется явное согласие (opt-in), в других юрисдикциях, отказ (opt-out) от веб-отслеживания считается достаточным для удовлетворения правовых требований, если выполняются определенные условия. Они включают в себя, среди прочего: адекватное уведомление об обработке, прозрачность в уведомлении; уведомление до или во время сбора, а также простой, эффективный и надежный способ отказаться от отслеживания. Может быть введен ряд дополнительных, в том числе ограничения на обработку конфиденциальной информации, такой как информация о здоровье, информация о политических или философских убеждениях и предотвращение отслеживания детей.

- **Предпосылки**

6. Технические возможности контроля за деятельностью пользователей на веб-сайтах за последнее десятилетие умножились и растущее «Информационное Общество» претерпело несколько кардинальных изменений с тех пор. Веб-отслеживания развилось с очень

скромного поначалу – когда отдельные провайдеры онлайн-сервисов начали следить за своими пользователями, чтобы определить, бывал ли этот конкретный пользователь у них прежде и что он делал – в почти всеобъемлющую картину, видимую маркетологам в наше время. В ней маркетолог, похоже, в состоянии контролировать каждый аспект поведения идентифицированного пользователя на веб-сайтах. Потенциально это может стать полной историей всего использования Интернета субъектом данных (буквально с колыбели до могилы), и может быть дополнено данными профиля из бывшего «оффлайнового мира» (включая любой аспект нашей жизни, доступный брокерам данных, в том числе финансовую информацию, а также информацию о, например, отдыхе, здоровье, политических и/или религиозных взглядах, информацию о местоположении).

7. Такое развитие событий – хотя и было встречено и поощряемо маркетологами и другими заинтересованными сторонами из более широкого бизнес-сообщества, и при содействии некоторых политиков на национальном и региональном уровнях – создает беспрецедентный риск для частной жизни всех граждан в информационном обществе. По сценарию «худшего случая» оно может превратить мир, который мы знаем, в глобальный паноптикум. Оффлайновым эквивалентом этого был бы кто-то нам неизвестный постоянно подглядывающий через плечо независимо от того, где мы находимся (на улице или в кажущемся конфиденциальности наших домов), или от того, что мы делаем (смотрим ли телевизор, делаем ли покупки онлайн, читаем газету, или занимаемся даже более интимной деятельностью), и не сообщающий нам когда он подсматривает, а когда нет.

8. Возможные последствия такого развития событий очевидны и их тяжесть не следует недооценивать. Это может покончить с некоторыми из основных принципов частной жизни (и аннулировать их) – в частности прозрачность и контроль ее человеком. Проще говоря, это может быть концом (частной жизни) мира, как мы его знаем.

9. Пропагандисты этого видения, с другой стороны, утверждают, что эти риски либо не существуют вообще, либо что они пытались их смягчить и преодолеть, по крайней мере частично. Со стороны некоторых заинтересованных лиц из индустрии имеется сильное сопротивление против признания, что уникальные идентификаторы в веб-данных являются персональной информацией. Одно из часто выдвигаемых заявлений состоит в том, что большая часть используемых данных является обезличенной (т.е. анонимной), и что, как только это было сделано, данные содержат сведения уже не о человеке, и потому не представляют опасности для конфиденциальности граждан. Также утверждается, что любые данные о поведении связаны исключительно с машинами и – это утверждение – в очень многих случаях не могут быть прослежены назад к индивидууму вообще.

10. Однако, эти утверждения вообще не имеют никаких научных доказательств, и игнорируют тот факт, что машины – и особенно смартфоны – становятся все более и более личными устройствами и позволяют легко добраться до любого отдельного пользователя. Следы также можно связывать друг с другом через различные устройства. Существуют также научные доказательства того, что многие, казалось бы анонимные данные (например, информацию о местоположении мобильных телефонов) можно отследить (т.е. де-анонимизировать), для любого пользователя при достаточной базе данных и сроках. Хуже того, современные академические исследования говорят о том застраховать «анонимные» данные от де-анонимизирования в принципе невозможно, если длительность накопления данных, описывающих поведение, достаточно велико (то есть, гарантировать, что «анонимные» данные не могут быть прослежены обратно к индивидууму с течением времени, концептуально невозможно). Если это окажется правдой, это изменит правила игры и сделает бесполезными несколько основных предположений о том, как использование различных типов данных может или не может повлиять на частную жизнь.

11. Кроме того, и в несколько ином ключе, практические ежедневные происшествия также добавляет сомнений к заявлениям индустрии. В то время как реклама вполне может быть адресованы машинам на техническом уровне, в конце концов пресловутую красивую пару красных туфелек покупает не машина – а индивидуум. Таким образом, утверждение, что обработка данных для поведенческого маркетинга направлена «всего лишь» на машины в первую очередь, вполне может рассматриваться как попытка размыть наше видение общественной серьезности проблемы, когда на самом деле пользователь, а не машина является единственной целью, обеспечивающей «успех» такого рода операциям слежения для его сторонников (т.е. когда красные туфли, наконец, покупают).

- **Короткая история технологий мониторинга**

12. В попытке проследить развитие описанного выше до его скромного начала, в качестве одной из вех мы видим разработку «технологии Cookies» почти 20 лет назад. HTTP-Cookies были введены в 1994 году, в первую очередь, чтобы решить «мелкую» проблему надежной реализации виртуальной корзины. Благодаря главным образом не хранящей состояние природы Hypertext Transfer Protocol (HTTP), пользовательские агенты не смогли до тех пор сохранять информацию о состоянии. Хранение информации о состоянии имеет решающее значение для виртуальной корзины, чтобы помнить выбранные предметы во время шопинга. Прозрачность уже тогда была проблема частной жизни, так как использование Cookies не доводилось др рядового пользователя. В то

время, Cookies были включены по умолчанию в настройках браузера и пользователь не был уведомлен об их использовании.

13. Для смягчения риска конфиденциальности и безопасности из-за утечки информации из Cookies на другие сайты была имплементирована политика того же происхождения. Эта политика означала, что Cookies могут быть прочитаны только тем же доменом, что их установил. Тем не менее, важно обратить внимание на рекомендации нового стандарта, предложенного Консорциумом World Wide Web (W3C), на Совместное использование ресурсов разного происхождения (Cross Origin Resource Sharing – CORS), позволяющего обмен информацией между определенными доменами. Хотя CORS является добровольным стандартом, он не совместим с политикой того же происхождения.

14. В 1998 году эта группа рассмотрела различные вопросы конфиденциальности связанные с систематическим сбором или использованием персональных данных в Сети. В своем рабочем документе, она обратилась к P3P (Проект платформы для предпочтений конфиденциальности, Platform for Privacy Preferences Project), протоколу, разработанному W3C и предназначенному для блокирования Cookies третьим сторонам до тех пор, пока посещенный пользователем вебсайт, не предложит принимаемую пользователем политику P3P. Однако, только один крупный производитель браузера реализовал стандарт. В результате не используется P3P широко в Сети.

15. Cookies третьих сторон стали кровью жизни комплекса индустрии цифровой рекламы. В 2008 году маркетологи компаний веб-отслеживания обсудили будущее аналитики и статистики сайтов. На пятилетнее будущее была предусмотрена интеграция традиционной статистики посещения сайтов (далее: аналитика первой и третьей сторон) и аналитики данных от других сервисов в Сети, включая, например, видео, виджеты, социальные сети, игры и поисковые движки (далее: веб-аналитика).

16. Сегодня данные веб-аналитики представляет собой новую форму экономической ценности. В то время как эта группа не ставит под сомнение преимущества, которые измерение потребительского поведения может принести для онлайн поведенческой рекламы (в реальном времени) (online behavioural advertising – OBA), она твердо верит, что такая практика не должна осуществляться за счет прав граждан на защиту частной жизни и данных.

- Веб-отслеживание

17. Веб-отслеживание включает в себя сбор и последующее

хранение, использование или обмен данными по индивидуальному поведению онлайн на нескольких сайтах путем использования Cookies, JavaScript или любого типа меток устройств. Технология веб-отслеживания обеспечивает в режиме реального времени постоянный поток информации о пользователях, например, регистрационных данных поисковых запросов, поведенческих данные, статистики посещения, а также преобразование сведений о том, как пользователь ответил на индивидуальные предложения. Эти данные можно использованы для оценки интересов пользователей, их политических убеждений или медицинского состояния. Эти данные можно обработать, чтобы оценить, выработать отношение или повлиять на состояние или поведение индивида. Данные об индивидуальном поведении приводят к бизнес-решениям на основе профилей клиентов. По предполагаемой цифровой идентификации человека могут быть вычислены намерения о покупке. Ценность потенциального клиента связана с вероятностью убедить его купить товар.

18. Технология веб-отслеживания присутствует на мобильных устройствах. Смартфоны и другие мобильные устройства редко используются совместно разными пользователями, вследствие чего связь между устройством и индивидуумом сильнее, чем, например, у настольных компьютеров. Мобильные устройства содержат массу уникальных идентификаторов, таких как специфичные рнкламные идентификаторы, уникальный идентификатор устройства (Unique Device ID –UDID), адрес физического сетевого контроллера (Media Access Control – MAC), MAC-адрес контроллера Bluetooth, MAC-адрес контроллера коммуникаций ближнего поля (Near Field Communications – NFC), Международный идентификатор мобильного абонента (International Mobile Subscriber Identifier – IMSI, уникальный номер SIM-карты) и Международный идентификатор мобильного оборудования (International Mobile Equipment Identifier – IMEI). Эти идентификаторы не доступны к изменению обычными пользователями. В дополнение к уникальным идентификаторам, смартфоны могут нести богатый набор личных данных пользователя, таких как его имя, пароль, возраст, пол, адресная книга... Мобильных устройств могут предоставить точные поведенческие данные, связанные с местонахождением пользователя. Точные геолокационные данные легко доступны для броузеров в мобильных устройствах.

19. Технологии веб-отслеживания развернуты по-разному. Цифровые следы данных могут возникнуть в результате непреднамеренного или нежелательного разглашения сведений, и может привести к ненужным раскрытиям (персональных) данных. Есть несколько способов для создания цифрового следа данных. Например, менеджер кампании сетевой рекламы может назначить уникальный идентификатор для пользователя, броузера или устройства. Другой способ заключается в персонализации ссылочной информации, когда к ней добавляются сведения о принадлежности к тому или иному сегменту аудитории (микропрофили) во время серфинга в Сети, так чтобы другие сайты, участвующие в кампании

могли отслеживать пользователя, броузер или устройство. Третьим примером может быть установление связи между уникальными идентификаторами и данными, собранными во время прошлых посещений определенного сайта. Четвертым примером может послужить, способ веб-отслеживания для кампании, объединяющий новые данные отслеживания (данные о пользователе, броузере или устройстве) с ранее собранными данными на конкретном сайте, либо данными, полученными от другой (третьей) стороны. Последний пример предполагает использование сервиса сопоставления Cookies, могущего консолидировать цифровые следы, оставленные одним и тем же пользователем, броузером или устройством в различных частях Сети.

20. Веб-отслеживание состоит из нескольких автоматизированных шагов, начиная со сбора данных в Сети, сохранение этих данных, и их использование. При помощи рекомбинации, корреляции и деконтекстуализации, эти данные могут быть использованы для построения очень подробного интеллектуального профиля индивидуального поведения. Наконец, веб-отслеживание приводит к фактическому применению построенного профиля к человеку.

21. Данные могут храниться в виде графов в базах данных различных сервисов в Сети. Структура графов позволяет выявление поведенческих шаблонов, которые могли бы остаться незамеченными. Данные веб-отслеживания в графе могут показать актуальные шаблоны в поведении пользователей как сами по себе, так и в сочетании с другими данными из различных источников. Например, в то время как отдельные уникальные идентификаторы, привязанные прямо или косвенно к пользователю или компьютеру, могут выдать относительно немного информации о случайном серфере, то массив связанных с ним уникальных идентификаторов демонстрирует его привычки и интересы в Сети. Такой массив уникальных идентификаторов уже вполне может быть использован для конструирования цифровой «личности».

Веб-отслеживание и право на неприкосновенность частной жизни и защиту личных данных

22. Ключевой принцип широкого круга актов международного законодательства состоит в праве на частную жизнь, которое пользователь Сети имеет независимо от технологии. Ключевыми элементами являются прозрачность, контроль и уважение к контексту. Тот факт, что пользователи не знают, что их отслеживают является риском для конфиденциальности. Веб-отслеживание как процесс использует ряд технических средств, ограничивающих возможности уведомления о них для пользователей. Например, пикселы (например, веб-маяки) и мини-веб-страницы (например, iFrame) невидимы для пользователя и их включение в веб-страницу инициирует автоматический HTTP запрос, давая

возможность устанавливать и использовать Cookies, содержащие уникальные идентификаторы.

23. Многие технологии веб-отслеживания были разработаны и внедрены в бизнесе без предоставления информации пользователям, чьи данные собираются и не давая им никакого выбора. Сигналы пользователя, которые могли бы быть поняты как выражение возражения против отслеживания не принимались во внимание и активно создавались технические средства для обхода таких аозражений, например, путем повторной установки удаленных Cookies, (пассивного) сбора «отпечатков», и обхода настроек броузера. Заинтересованные стороны принимали обязательства уважать свободную волю пользователей только тогда, когда эти действия были обнаружены и публично раскритикованы. В таких случаях иногда добавлялись схемы отказа пост-фактум, часто приводящие к неуклюжим механизмам ограничения полезности сайта для пользователя. Эти случаи причинили большой ущерб доверию пользователей к надежности и честности всех провайдеров веб-услуг и подорвали здоровое развитие инновационных веб-сервисов.

24. Веб-отслеживание считается обработкой персональных данных во многих странах в связи с тем, что технология позволяет индивидуализацию или идентификацию пользователей и/или выработку автоматизированных решений о них. Примером такой практики можно назвать автоматические движки с алгоритмами принятия решений в реальном времени у платформ электронных торгов для выдачи персонализированной поведенческой рекламы.

25. Со стороны некоторых заинтересованных сторон существует сильное сопротивление в отношении классификации уникальных идентификаторов в веб-данных как личной информации. Часто выдвигается претензия, что как только данные были обезличены, они становятся уже не о человеке. Однако, ясно видно, что «целевой» элемент также может быть ответственным за тот факт, что информация «относится» к определенному лицу или содержит сведения о нем.

Потенциальное воздействие (или отсутствие воздействия) стандарта «Не следить» (Do Not Track – DNT) – изучение вопроса

26. В сентябре 2011 года W3C создала Рабочей группы по защите от слежения (Tracking Protection Working Group). Группа работает над стандартом «Не следить» (Do Not Track – DNT). Все основные броузеры взяли на себя обязательства по реализации стандарта (и большинство из них уже реализовано такой заголовок HTTP), однако среди тех участников обсуждения, что поддерживают запрос DNT:1, сохраняется открытая дискуссия по частям этого добровольного стандарта. Некоторые

заинтересованные стороны указали, что они не будут поддерживать флаг DNT по различным причинам. Общий успех DNT зависит от фактической поддержки флага DNT у принимающих запросы организаций и фактическим принятием стандарта DNT по всей Сети всеми заинтересованными сторонами.

27. Еще важны установки DNT по умолчанию и действия веб-отслеживающей организации по умолчанию. Чтобы стать эффективным инструментом управления для пользователя, для DNT очень важно, чтобы исполнитель веб-отслеживания был уверен, что получаемый им DNT сигнал является подлинным свидетельством желания пользователя. При отсутствии полной информации о выборе пользователя, организации веб-отслеживания должны считать, что пользователь не знает о веб-отслеживании и, следовательно, действовать по умолчанию, как если бы они получили сигнал DNT:1, указывающий на желание пользователя, чтобы его не отслеживали.

28. Любая технология, используемая для целей веб-отслеживания должна быть соразмерной. Используемые во всем мире принципы защиты данных базируются на том, что данные должны собираться для определенных, явных и законных целей и не подвергаться дополнительной обработке способами, несовместимыми с этими целями. Обработка данных должна быть адекватна и не чрезмерна по отношению к целям, для которых они собираются и/или дальнейшей обработке.

29. Наконец, любая технология должна быть «устойчивой к судам», если она предназначена служить защитой частной жизни. DNT находится в опасности остаться инструментом, с помощью которого пользователь может просто выразить пожелания к провайдерам сервисов в информационном обществе, так и не став эффективным инструментом диалога. Это оставляет пользователя самого по себе или любое публичное (или частное) лицо, требующее соблюдения этих правил или пожеланий (в том числе и через соответствующие юридические обязательства соблюдать любой такие выбор, сделанные индивидуально) с пустыми руками один на один с этими провайдерами. Некоторые заинтересованные стороны в отрасли пытаются отстаивать свою позицию, что DNT не представляет собой обязательство исполнять такое желание. Хотя это понимание более чем сомнительно, факт остается фактом: было ли пожелание пользователя исполнено или нарушено – доказать очень трудно. Другими словами, с точки зрения органов правоприменения, DNT может остаться сахарной пилюлей вместо настоящего лекарства и останется бесполезным как таковой.

- Рекомендации

30. Неограниченное веб-отслеживание может изменить баланс между провайдерами сервисов и пользователями, в том числе в отношении защиты частной жизни. Рабочая группа подчеркивает, что контекст, прозрачность и контроль остаются важными элементами в контексте веб-отслеживания.

31. Для того, чтобы внести свой вклад в выявление рисков конфиденциальности частной жизни человека, Рабочая группа выносит следующие рекомендации для различных заинтересованных сторон, играющих свои роли в экосистеме веб-отслеживания.

Вновь ввести учет контекста и цели ограничения в качестве основных принципов для любого использования личных данных:

- ввести принципы предосторожности в любые практики (автоматизированного) сбора данных, их обработки и обмена, так чтобы данные, собранные в одном контексте не могли быть использованы в другом контексте; и:
- сообщать о цели сбора данных заранее и не менять цели без нового сообщения и принятия решения пользователем.

Вернуть прозрачность:

- Воздерживаться от использования невидимых элементов слежения;
- Как минимум, уведомлять пользователя понятным для человека способом, когда пользовательский агент собирается отправить/получить идентификатор веб-отслеживания от/на сервер происхождения/назначения;
- Отображать индикатор достаточно заметным для пользователя всякий раз, когда ведется веб-отслеживание; и
- Сделать индикацию активности веб-отслеживания также доступной для групп пользователей со специальными требованиями, в том числе инвалидов по зрению.

Вернуть пользователю контроль:

- Внедрить механизмы, позволяющие пользователям осуществлять свое право на защиту частной жизни и данных в Сети и не разворачивать никакие (новые) механизмы контроля, не снабженные механизмом управления

пользователем; предложить пользователям явных выбор в отношении отслеживания – если нужно установить, активировать или обновить броузер или иное программное обеспечение нужно дать выбор пользователю;

- если броузер или иной пользовательский агент не снабжен пользовательским интерфейсом, по умолчанию настройка должна запрещать отслеживание пользователя;
- дать пользователям возможность пересмотреть свой выбор и изменить параметры после первоначального решения в любое время; позволить пользователю без приложения больших усилий изучить (автоматизированные) выборы, сделанные по отношению к веб-отслеживанию; и напоминать пользователю, что его выбор в отношении (автоматизированных) настроек веб-отслеживания может быть отозван в любое время и убедиться, что пересмотр любого такого выбора технически возможен без приложения больших усилий человека;
- выполнять запросы пользовательского агента, запрещающие отслеживание;
- воздерживаться от (пассивного) сбора информации о пользователе, например, сбора пользовательских данных (например, конфигурации сервисов, или строк пользовательского агента), дающей уникальный идентификатор пользователя (метку устройства), если пользователь выразил нежелание быть отслеженным; и
- удостовериться, что применение любой технологии, позволяющей пользователю сделать выбор, является проверяемым и может быть приведено в исполнение компетентными частными или государственными органами, следящими за соблюдением правил, особенно закрепленных в различных существующих правовых системах, создающих фундамент для защиты частной жизни человека во многих юрисдикциях по всему миру.

4.1.4. Винт Серф, Патрик Райан, Макс Сенджес Управление Интернетом – наша общая ответственность

Управление Интернетом – наша общая ответственность

Авторы: Винт Серф, Патрик Райан, Макс Сенджес *

Публикация выйдет в
Политико-правовом журнале информационного общества
10 ISJLP ___ (2014) (www.is-journal.org)

Предварительная версия
(перевод окончательной версии будет доступен на сайте euromediaplatform.org)

Вступление

Интернет – это универсальное пространство, которое, как ожидают многие, останется открытым, свободным и безграничным.[1] Однако, в течение последних нескольких лет, органы власти пытаются все больше контролировать поток информации в Интернете. Одним из способов установления контроля стало заявление, что два сходных понятия – Интернет и облачная обработка данных – каким-то образом стали различными сферами, и что Интернетом и «облачной технологией» возможно управлять раздельно.[2] То, как лучше всего разделить Интернет на различные секции и управлять ими, являлось одним из ключевых вопросов Интернет политики. Данная тема обсуждалась в прошлом году в рамках Всемирной конференции по международной электросвязи (ВКМЭ-12), которая, как отметили многие, привела бы к увеличению разделения мирового Интернет пространства.[3]

В отличие от многих других изобретений человечества, Интернет является одновременно и технологией, и социально-экономическим пространством. Интернет не является традиционным правом на общественное пользование с ограниченными ресурсами, поскольку его объем может увеличиваться в зависимости от желания тех, кто им пользуется, и организаций, которые инвестируют в его расширение. Однако, даже не являясь традиционным правом на общественное пользование, Интернет, тем не менее, представляет собой совместное пространство. Пропускная

1

[*]Авторы работы – Винт Серф, доктор наук, Вице-президент Google и главный «отец» Интернета, является одним из разработчиков протокола TCP/IP; Патрик Райан, доктор наук, является Старшим советником политики Google и Старшим ассоциированным исследователем в Левенском католическом университете; Макс Сенджес, доктор наук, является администратором политик в Google в Берлине. Хотя все три автора работают в компании Google, данная работа написана полностью на основе их личных и научных возможностей, и не отображает мнение их работодателя. Авторы перечислены в алфавитном порядке согласно правилам Харди-Литлфилд.

2

Бертран Ла-Шапель, Мультистейкхолдерное управление – Принципы и задачи инновационной политической парадигмы, #2: Формирование Интернет политики, Вольфган Кляйнвехтер (изд.), Берлин, 2011 год, *Доступно на:* http://www.collaboratory.de/w/MIND_2_-_Internet_Policy_Making [далее: «Ла-Шапель, Мультистейкхолдерное управление»].

3

Заключительные акты Всемирной конференции по международной электросвязи, Дубай, 2012 год, *доступно на:* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf [далее: «ВКМЭ-12 Заключительные акты»]

способность и мощность сервера не ограничены, и их использование подразумевает выбор оптимального соотношения; это сравнимо с рыбаками, которые разделяют богатства моря, или фермерами, которые совместно пользуются одной прерией для разведения домашнего скота.[4] Тем не менее, Интернет не является таким пространством, как территория государства – другими словами, неограниченную территорию Интернет не следует считать пространством, которое подчиняется верховной власти государства, а сам по себе Интернет не является суверенной единицей.[5] Понятие суверенитета, инновационное понятие, введенное в Вестфальском мирном соглашении в 1648 году, предоставило странам возможность провести границы в государствах, и установить правящую власть в определенных границах.[6]

•*Управление в совместном пространстве*

Интернет – это совместное пространство; сами по себе решения, которые принимаются на основе суверенитета на одной территории, могут повлиять на Интернет пользователей других территорий – пользователей Интернет экосистемы в других частях мира.[7] Пользуясь еще одной метафорой об окружающей среде, загрязнение реки, которая течет через всю страну, может попасть в другие страны по течению. Таким образом, решение правительства какой-либо территории загрязнить реку может повлиять на соседей данной территории[8]. Парадоксальная ситуация, с которой мы сталкиваемся сегодня, заключается в том, что мы все настолько связаны, что у нас существует совместная ответственность по отношению друг к другу в таких аспектах, которые мы даже не могли себе представить. Онлайн-пространства объединены настолько сильно, что у нас существуют совместные виртуальные права, и мы не можем избежать ответственности за свои действия, даже те из них, которые считаются или подразумеваются суверенными.

При использовании Интернет необходимо учитывать перспективы всех участников независимо от того, принадлежат ли они к части географической территории,

---

4 Гаррет Хардин, Трагедия прав на общественное пользование, с.162, НАУКА 1243, 1968 год. *Также:* Гаррет Хардин, Трагедия неурегулированных прав на общественное пользование: Население и изменение внешнего вида г. Провиденс, ПРАВА НА ОБЩЕСТВЕННОЕ ПОЛЬЗОВАНИЕ БЕЗ ТРАГЕДИИ: ЗАЩИТА ОКРУЖАЮЩЕЙ СРЕДЫ ОТ ПЕРЕНАСЕЛЕНИЯ — НОВЫЙ ПОДХОД 162, 168, Роберт В. Андерсон (изд.), 1991. *Также:* Элинор Остром, УПРАВЛЕНИЕ ПРАВАМИ НА ОБЩЕСТВЕННОЕ ПОЛЬЗОВАНИЕ: ЭВОЛЮЦИЯ УЧРЕЖДЕНИЙ ДЛЯ КОЛЛЕКТИВНОГО ДЕЙСТВИЯ, издательство Кембриджского университета, 1990 год.

5 Лоуренс Лессиг, Кодекс 2.0: Кодекс и другие законы виртуального пространства, *доступно на* http://codev2.cc/download+remix/Lessig-Codev2.pdf (как доказательство того, что Интернет сам по себе является не суверенной системой).

6 *См.* Ден Филпотт, «Суверенность», СТЭНФОРДСКАЯ ЭНЦИКЛОПЕДИЯ ФИЛОСОФИИ (Издание 2010 г., Эдвард Н. Залта (изд..)), *доступно на* http://plato.stanford.edu/archives/sum2010/entries/sovereignty/ (изложение событий, которые привели к подписанию договора).

7 *См.* Ла-Шапель, Мультистейкхолдерное управление, цитировано *выше* на ссылке 2.

8 *См.* Патрик С. Райан, Применение доктрины публичного доверительного фонда и принципов рационального использования природных ресурсов в электромагнитном спектре, с.10, ОБЗОР ЗАКОНА О ТЕЛЕКОММУНИКАЦИЯХ И ТЕХНОЛОГИЯХ В МИЧИГАНЕ 2 (2004), *доступен на* http://ssrn.com/abstract=556673 (описание того, как принципы закона о защите окружающей среды и принципов водного законодательства относятся к сектору технологии).

находящейся в юрисдикции исполнительных органов. В то время как Интернет является материальным продуктом разработки с различными составляющими во многих странах, виртуальное пространство, созданное этим продуктом, определяется скорее логическими, а не геофизическими границами. Эти границы выражаются разными способами: возможностью подключения автономных систем (например, сети) Интернет, разделениями, отображенными в пространстве Системы Доменных Имен (DNS), а также такими приложениями, как Facebook, Evernote, Twitter и iTunes.

В ходе таких размышлений становится понятно, что могут возникнуть некоторые трудности, когда суверенные государства решат ограничивать поток информации, или блокировать информационное содержание в Интернет. Также становится очевидным, почему множество организаций пользуются так называемой «мультистейкхолдерной моделью управления» Интернетом – моделью, которая требует участия в принятии решений органов власти, частного сектора, гражданского общества и технической общественности. Рабочая Группа ООН в 2005 году сформулировала это определение следующим образом: мультистейкхолдерное Интернет управление – это «разработка и применение органами власти, частным сектором и гражданским обществом их соответственных функций, совместных принципов, норм, правил, процедур по принятию решений, и программ, которые обуславливают эволюцию и использование Интернет».[9] Поскольку границы являются менее значимыми для виртуального мира, подход мультистейкхолдеров открывает путь к выходу за пределы географических границ физического пространства и вместо этого сосредотачивается на пользователях виртуального Интернет пространства. Справедливости ради необходимо отметить, что подход мультистейкхолдеризма может быть запутанным и неудобным, как и любой демократический процесс, однако он предоставляет самый лучший механизм управления Интернет пространством благодаря своей всеобъемлемости.

Б. Новый подход к управлению Интернетом

Не существует единого универсального подхода к управлению Интернетом; наоборот, правила Интернета быстро развились в различных организациях, таких как Рабочая группа проектирования Интернет (IETF), которая способствовала развитию открытых стандартов; Интернет-корпорация по присвоенным именам и номерам, учрежденная для создания доменных имен и адресов (ICANN); гражданское общество пытается предоставить независимую перспективу от имени пользователей; и частный сектор, который инвестирует в развитие инфраструктуры. Конечно же, органы власти активно задействованы в регулировании Интернет путем установления правил для таких понятий, как личное пространство, правомерное использование, клевета, антимонополизм, различные формы лицензирования, и тому подобное. Деятельность технологического сообщества распространяется на многие сектора, и создает скрытые, а иногда и видимые границы в поведении.[10] Это всего лишь несколько примеров, и удивительно то, что все эти группы соревнуются между собой за установление коллективных правил для развития Интернет экосистемы.

---

9 Программа действий для информационного общества в Тунисе, §35, WSIS-05/TUNIS/DOC/6(Rev. 1)-E (2005), *доступна на* http://www.itu.int/wsis/docs2/tunis/off/6rev1.html [далее: “Программа действий в Тунисе”].

10 ЛАРРИ ЛЕССИГ, КОДЕКС: ДРУГИЕ ЗАКОНЫ ВИРТУАЛЬНОГО ПРОСТРАНСТВА, ОСНОВНЫЕ РАБОТЫ, 1999 год.

Определяющей задачей для руководящего управления в Интернет является скорость инновации в этой комплексной сети, которая настолько высока, что традиционные практики регулирования не поспевают за ней. В результате, другие стейкхолдеры оказывают давление, чтобы прийти к согласию среди бесчисленного количества предлагаемых технических, правовых, политических и деловых аргументов. При более детальном рассмотрении, это глобальное пространство в реальном времени вызвало изменение системы мировоззрения в вышеупомянутых профессиональных сферах. В отличие от органов регулирования в телекоммуникационных компаниях, к примеру, больше не существует единого универсального подхода, которым можно было бы воспользоваться в случае обращения к относительно простому набору вопросов, с которыми столкнулась телефонная компания.

Вполне очевидно, что Интернет является основой или операционной системой на глобальных рынках, представляя увеличивающееся количество внутреннего валового продукта в наиболее развитых странах.[11] Одна за другой специализированные организации, такие как Совет ООН по правам человека, начали вовлекать участников в дискурс Интернет управления – не путем присоединения к развивающимся форумам по Интернет политике, а с помощью публикаций отчетов и политики, охватывающей Интернет практики с точки зрения их специфических перспектив.[12] Такая вовлеченность добавляет еще одну масштабную задачу к развитию Интернет управления. Чем больше стейкхолдеров присоединится к дискурсу, тем сложнее для большего круга участников будет понять цели каждого отдельного стейкхолдера.

Интернет способствует взаимодействию традиционно независимых средств массовой информации. Сегодня все больше и больше средств кинематографа, телевидения, радио, телефонной связи и печати появляются или изначально в цифровом режиме, или оцифровываются, и впоследствии используют гибкую инфраструктуру Интернета. Каждое из этих средств массовой информации имеет четко установленные и уполномоченные управленческие учреждения, и создало основу национальной и международной политики для своей специфической технологии. Как так называемый «новый подход», управление Интернетом находится в стадии развития, однако, ему необходимо будет решать вопросы, связанные с наложением полномочий учреждений политики средств массовой информации и развивающимися учреждениями управления Интернетом. Еще более важным является то, что много принципов, которыми управляются традиционные методы массовой информации, не обязательно имеют способность переноситься на Интернет экосистему, или даже быть целесообразными к Интернет-версии услуги. Фактически, взаимодействие технологии с доступом к сети может привести к необходимости изменений в специально-технических практиках управления, или наоборот исключить их.

---

11 Собрание различных экономических работ, которые показывают ценность Интернета в мировых экономиках, доступно на www.valueoftheweb.com.

12 Генеральная Ассамблея ООН, Совет по правам человека, *Постановление относительно содействия, защиты и использования прав человека в Интернете,* A/HRC/20/L.13, 29 июня, 2013; *Также см.* Джиллиан С. Йорк, Постановление Совета по правам человека ООН *относительно Интернета и Прав человека – шага в новом направлении*, EFF DEEPLINKS, 26 июля, 2012, доступно на https://www.eff.org/deeplinks/2012/07/un-human-rights-councilresolution-Internet-and-human-rights-step-right-direction.

В данной научной работе мы будем рассматривать следующие вопросы: как лучше всего определить соответствующие роли стейкхолдеров, чтобы отреагировать на быстро меняющиеся проблемы, связанные с управлением Интернетом, и как мы можем заниматься построением процесса «углубленного сотрудничества» для того, чтобы обеспечить отображение международной политикой совместного характера глобального социально-экономического онлайн пространства? Учитывая острую необходимость системных проблем, которые мы указали выше, мы предложим открытую, продуктивную и мультистейкхолдерную модель управления как ответ на указанные выше вопросы.

•ОБЩЕЕ ОПИСАНИЕ СФЕРЫ ПОЛНОМОЧИЙ

Интернет – это сложная система, которая разными способами отражает социальные, политические и деловые связи в мире, в котором мы живем. Дэвид Кларк, совместно с другими авторам, однажды красиво подвел итог заданий управления. Данный автор утверждает, что, «как только Интернет становится основной тенденцией, он неизбежно движется от первоначальной разработки, которая удовлетворяет инженерное любопытство, к отображению сообществ, в которых он функционирует».[13] Действительно, Интернет управление всегда было тем, что Кларк называл «спорным моментом» между различными группами стейкхолдеров (напр., телекоммуникационные компании, провайдеры услуг онлайн, пользователи, правоохранительные органы и регулирующие органы) – не учитывая споры между членами одной и той же группы стейкхолдеров. Однако с учетом того, что сложность и комплексность Интернет быстро растет в связи с вызовами глобализации (и не имеющими отношения к делу доводами относительно сохранения суверенитета), следующее утверждение Кларка совместно с другими авторами, высказанное в 2002 году, попадает в самую точку:

> Разрабатывайте проекты для внесения изменений в их результат таким образом, чтобы результат мог быть различным в различных местах. Спорные моменты имеют место существовать внутри проекта, но при этом не искажая или нарушая его. Не создавайте проект таким образом, чтобы была возможность предсказать результат. Проекты с жесткими рамками терпят крах; те же проекты, которые предоставляют возможность для вариаций, изменят свои рамки под давлением и выживут.[14]

Если перефразировать данную цитату, мы должны находить пути, чтобы экспериментировать с политикой управления и предоставлять возможности для естественного регулирования на всех уровнях (локальный, национальный, и региональный), а не иметь один централизованный международный договор по Интернет управлению. Рик Уитт также приводит убедительные аргументы в пользу адаптивного проведения политики.[15] Это один из способов, которым можно

---

13 Д. Д. Кларк, Й. Врославски, К. Соллинс, и Р. Бранден, «Спорные места в виртуальном пространстве: Определение Интернета будущего», внутри процесса ACM SIGCOMM, август 2002, *доступно на:* http://groups.csail.mit.edu/ana/Publications/PubPDFs/Tussle2002.pdf [далее: “Спорные места в виртуальном пространстве”].

14 *там же.*

15 *См.* Ричард С. Витт, *Адаптивный процесс формирования политики: Развивающиеся и применяющиеся новейшие решения для информационной политики США*, 61 FED. COMM. L.J. 483 (2009) (автор развивает предложение для «адаптивного процесса формирования политики»

попытаться разрешить «спорные моменты» (напр., неизбежные разногласия), которые всегда существовали между различными Интернет стейкхолдерами. Хотя теоретически возможно, что подход к управлению Интернетом «сверху вниз» будет работать, невозможно предсказать будущее, и мы твердо убеждены, что подход управления «сверху вниз», скорее всего, будет препятствовать инновации (это, фактически, часто повторяющееся выражение Винта по поводу «инновации без разрешения»). В отличие от групп мультистейкхолдеров, которые поддерживают развитие Интернета, подход управления «сверху вниз» редко находит согласие между различными группами, поэтому он не только препятствует инновации, но и эффективность от него краткосрочная.

Мы не можем проводить опрос среди всех мультистейкхолдеров в данной работе, однако одна из сфер, в которой мы предлагаем продолжать укрепление позиций, – это роль Форума по управлению использованием Интернета (IGF). IGF был основан в 2005 году главами государств как место транслирования различных взглядов на Интернет политику без проведения переговоров, которые имеют место тогда, когда проводится конференция для заключения договора или отчета о какой-либо ситуации. Действительно, IGF позиционировался как совещательный орган (но не орган, который принимает решения) для всех стейкхолдеров, для того, чтобы: 1) продвигать возникающие вызовы перед Интернет управлением и сообщать об успехах и решениях по поводу существующих вопросов управления, 2) обсуждать самый лучший подход к разрешению вопросов по управлению, которыми будут заниматься соответствующие партии, и 3) создавать добровольные совместные группы, сформировавшиеся из организаций с должной сферой полномочий по решению установленных проблем.[16] Мы будем использовать IGF как пример во всей работе, и снова вернемся к нему далее, в Разделе III.

Возвращаясь к дискуссии о том, как экспериментировать с политикой – подход с участием всех заинтересованных сторон (мультистейкхолдеров) является одним из способов, на которые были ориентированы другие наблюдения Кларка: «Функции, которые находятся внутри пространства, в котором существуют спорные моменты, должны быть логически отделены от функций вне этого пространства, даже если для этого не существует веской технической причины. При таком образе действий спорный момент заканчивается с минимальным искажением других аспектов функционирования системы».[17] Другими словами, мы должны пытаться отделять политические вопросы от анализа, поскольку мы будем проводить любые эксперименты в техническом и научном смысле. Именно поэтому всем

правительствами, чтобы внести адаптивные изменения с технологией, основанной на предпосылках «предоставление возможностей без навязывания правил». Много идей в данной работе построены на вдохновлении от этой книги.)

16 Здесь мы перефразировали Программу действий в Тунисе, цитированную выше в ссылке 9. (Обратите внимание, что пункт (iii) покрывается сферой полномочий, как в ней указано: «Помогайте находить решения на вопросы, возникающие при использовании и чрезмерном использовании Интернет, особенного интереса каждодневных пользователей; содействовать дискурсу между органами, которые взаимодействуют с различными междисциплинарными международными государственными политиками относительно Интернета и обсуждать вопросы, которые входят в рамки какого-либо существующего органа; интерфейс с надлежащими межгосударственными организациями и другими учреждениями в вопросах их сферы компетенции; усилять и углублять вовлеченность стейкхолдеров в существующих и \ или будущих механизмах Интернет управления, особенно касающихся развивающихся стран; - важно, чтобы стейкхолдеры сформировали углубленное сотрудничество, а затем были задействованы в процессе формирования политики, но не IGF».)

17 Спорные моменты в виртуальном пространстве, цитируется выше в ссылке 13.

заинтересованным сторонам (стейкхолдерам) важно иметь равное количество голосов, поскольку все эти стейкхолдеры представляют собой уникальные перспективы относительно таких важных тем, как личная информация и безопасность, контроль, авторское право, и схожие понятия. Даже если мнения стейкхолдеров внутренне не объединены, мы можем делать различные предположения относительно точки зрения правительства о контроле (общепринятая: органы власти одобряют увеличение контроля, поскольку он помогает им поймать «злоумышленников»); или точки зрения гражданского общества (общепринятая: мнение, что весь контроль нужно проверять при помощи процедуры одобрения и выпуска общепринятых стандартов); и даже технического сообщества (общепринятая: сходна с точкой зрения гражданского сообщества, но разрабатывает шифрование и другие инструменты для предоставления выбора всем стейкхолдерам). Как только мы выделим эти вопросы как отдельные и изолированные проблемы, а также группы, которые больше всего заинтересованы в их разрешении – мы сможем представить и интегрировать их с остальной экосистемой. Это дает возможность группам, которые действительно являются экспертами в своей сфере, высказывать мнение убедительным способом.

Соответственно, мы предлагаем добавить новый Социальный уровень в утвержденную многоуровневую модель всеобщего управления Интернетом. Этот Социальный уровень обеспечивает нам дополнительную призму, чтобы обнаружить и создать иерархию соответствующих учреждений, в сфере компетенции которых лежит взаимодействие с постоянным руководством практик и постоянной оценкой и управлением увеличивающимися в количестве вопросами политики. Как можно увидеть на Иллюстрации 1, этот новый уровень будет взаимодействовать с практиками, которые определяют важнейшие права и принципы, связанные с «общественным поведением» онлайн.[18]

18

См. Йохай Бенклер, «От покупателей к пользователям: Переход от более глубоких структур регулирования к постоянным правам на общественное пользование и доступу пользователей», 52 *FED. COMM. L.J.* 561, (2000).

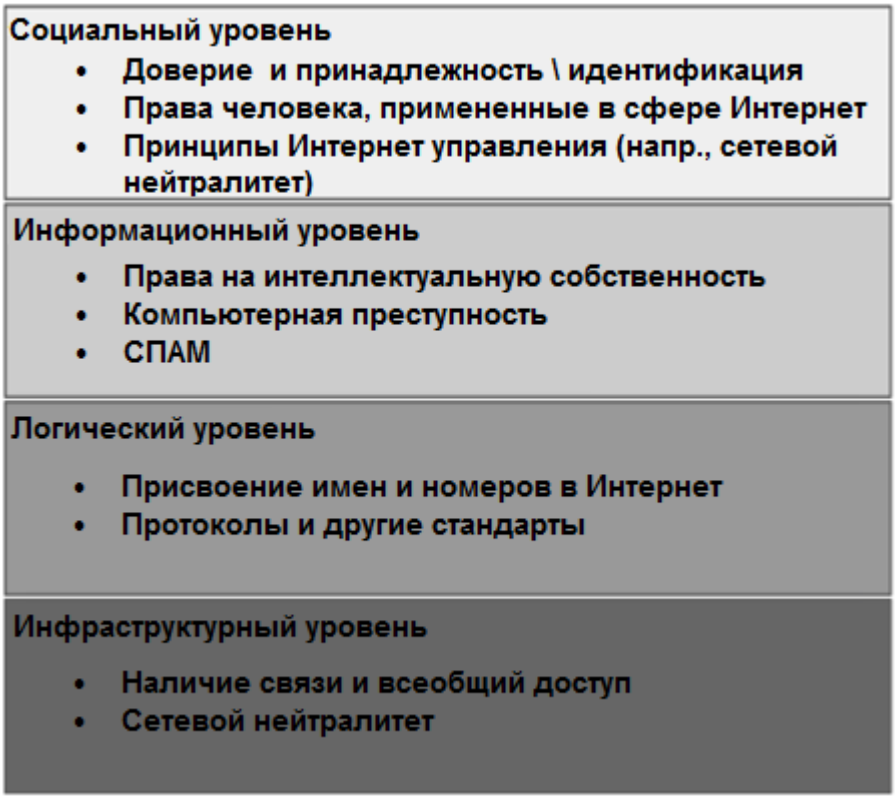


Иллюстрация 1 – Социальный уровень, добавленный к утвержденной модели управления Интернетом

Мы предоставляем эту разработку концептуальной модели для того, чтобы начать дискуссию о том, какие учреждения и группы стейкхолдеров должны быть законно вовлечены в вопросы Интернет политики. Рассматривая этот вопрос с другой стороны, мы считаем, что будет целесообразнее для функционирования всей онлайн экосистемы, если сфера полномочий учреждений будет составлена и обозначена с учетом их соответствия практикам и определениям политики руководящим управлением Интернетом. Следовательно, Иллюстрация 2 показывает схематический пример нанесения на схематический рисунок учреждений с соответствующей сферой полномочий, наложенными на уровни управления Интернетом.[19] В данной иллюстрации мы показываем, что IGF расположен в центре, поскольку он не имеет функции принятия решений, однако при этом он расположен так, чтобы способствовать и сдерживать упомянутое принятие решений в других организациях. Согласно терминологии Кларка, в IGF мы разделяем «спорные моменты» на форуме, где их могут проанализировать на воркшопах и сессиях для обсуждений, а затем взобновить на других различных форумах для принятия решений.

19 Данная иллюстрация не охватывает всех относящихся к ней учреждений. Ее целью является предоставление визуальной перспективы подхода в общем.

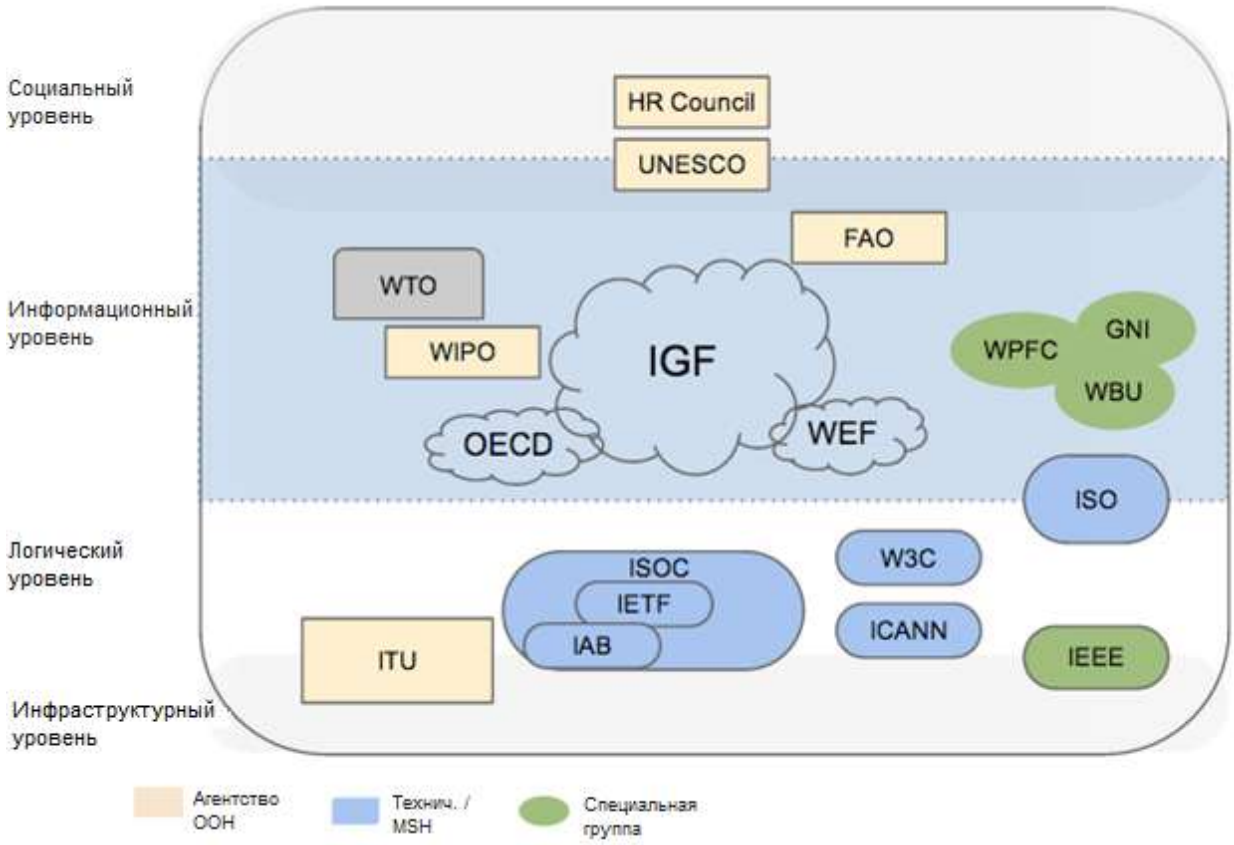


Иллюстрация 2 – Экосистема управления Интернетом [20]

В существующей мультистейкхолдерной экосистеме Интернет управления органы власти не играют доминирующей роли в управлении, однако участвуют на равных правах в качестве представителей своих соответствующих избирателей благодаря местным правилам, или же участию в организациях при государственных учреждениях, таких как Международный телекоммуникационный союз (ITU), который более детально описан в следующем разделе. Конечно же, правительства стран устанавливают уникально важную роль в Интернет управлении, поскольку они прежде всего издают правила в публичных интересах и разрабатывают сферы полномочий для обеспечения правопорядка, конкуренции, агентств защиты потребителей, органов, ответственных за защиту данных, и других государственных и межгосударственных организаций. Однако, учитывая то, что каждое правительство само по себе является группой стейкхолдеров, мы воздержались от подробных описаний, включающих отдельные правительства в иллюстрацию. Поскольку задачи, поставленные перед Интернет политикой, являются, как мы указали, глобальными задачами права на общее пользование, а не задачами для независимых государств, мы определяем сферу международного управления как самую важную.

20 Полные названия аббревиатур учреждений, а также их основную сферу полномочий можно найти в Приложении.

•ОТОБРАЖЕНИЕ СУЩЕСТВУЮЩЕЙ ЭКОСИСТЕМЫ

•*Опыт ВКМЭ в Дубае*

Мультистейкхолдерная экосистема управления Интернетом может показаться чуждой тем людям, которые не вовлечены в нее должным образом. Мы считаем, что недостаточное ознакомление с данной системой является одним из ключевых факторов, которые привели к конфликту на ВКМЭ-12, проведенной в Дубае, столице Объединенных Арабских Эмиратов. На данной конференции ООН, при помощи Международного телекоммуникационного союза (ITU), убедила страны мира якобы доработать Международный регламент связи (ITR), который был принят вот уже десятки лет. Вместо этого продолжились проверки этого договора, что могло бы оказать отрицательное воздействие на доступность и открытость содержания в Интернете. В данном разделе мы будем рассматривать некоторые аспекты предложенного соглашения и опишем некоторые вопросы, которые возникли в сфере учреждений, которые управляют Интернетом.

Переговоры по поводу Регламента ярко отобразили, что мир разделился на два больших блока. С одной стороны – Европа, Канада и США – фактически, страны, в большей части ответственные за развитие Интернета и многих приложений. С другой стороны – Россия, Китай, и группа стран, определяемых ITU как «Арабские государства» – страны, которые хотят иметь намного больше контроля над потоком информации в Интернете. Правительство Латинской Америки еще не определилось (4 члена правления проголосовало против соглашения), а страны Африки (за исключением Кении) присоединились к Арабским государствам, России, Китаю, и другим странам в данном блоке. Такое разделение является тем, что в предыдущей работе мы назвали «Сверхважным Моментом», виртуальным столкновением между перспективами новых технологий, разработанных Западным миром, и желанием применить новые правовые нормы к этим технологиям другими странами, которые чувствуют себя выбывшими из процесса управления Интернетом, или, в случае с авторитарными режимами, рассматривают Интернет как угрозу их власти. [21]

Возникший в результате проведения ВКМЭ-12 договор отобразил противостояние между двумя идеологиями. В общей сложности, 89 стран утвердило данный договор, включая Россию, Китай, Арабские Эмираты, и много других стран из Азии, Африки и Латинской Америки (далее в данной работе используется термин «Дубай-89»). 55 стран, которые не подписали соглашение, включают в себя все страны Европейского Союза, Соединенных Штатов, Канады, и несколько других стран (далее – «Дубай-55»). Многие страны вносили «оговорки», которые определили и ограничили более конкретно те положения, которые в конечном итоге страны утвердили.[22] В последнем разделе мы рассмотрим некоторые примеры того, как две указанные выше группы рассматривают так называемые «спорные моменты». Как мы увидим далее, некоторые из самых сильных концептуальных направлений, отделяющих «Дубай-89» от «Дубай-55», могут рассматриваться этими объединенными группами на

---

21 *См.* Патрик С. Райан, «ITU и важнейший момент Интернета», Обзор закона о технологии Стенфордского университета, том 2012, No. 8, 13 июля, 2012, *доступен на* http://ssrn.com/abstract=2110509.

22 *См.* Патрик С. Райан, «ITU и важнейший момент Интернета», Обзор закона о технологии Стенфордского университета, том 2012, No. 8, 13 июля, 2012, *доступен на* http://ssrn.com/abstract=2110509.

инфраструктурном и логическом уровне совместно с информационным, а также социальным уровнями.

Б. Инфраструктурный уровень

Интернет система по присвоению имен и номеров формирует основу ее инфраструктуры. Интернет-корпорация по присвоенным именам и номерам (ICANN) является мультистейкхолдерной группой, ответственной за предоставлении мировому Интернет сообществу нисходящей (здесь подразумевается наличие одной единой системы), и распределяющей системы (путем возложения ответственности на региональные базы конфигурации системы). Это обычная система для администрирования доменов высшего уровня, таких как .net, .com, .edu, .xxx, .fr, .de,.br, и числовых IP-адресов.[23] Один слаженный механизм для присвоения имен и номеров предотвращает непоследовательность и бессистемность. Например, представьте, если бы Вы ввели в поисковой системе «www.pepsi.com» в одной стране, результаты запроса указали бы вебсайт компании «Pepsi», но при введении того же адреса в другой точке мира, вы могли бы оказаться на другом адресе. ICANN помогает устанавливать правила движения сотен тысяч еще более соединенных между собой серверов – Системы доменных имен, или DNS – действовать совместно, чтобы убедиться, что к вебсайтам по всему миру можно получить доступ при помощи только одной именной и цифровой схемы.

Любой человек, которому довелось работать с ICANN, может подтвердить, что эта организация является сложной, использующей на каждом шагу аббревиатуры, трудной для исследования. В то время как процесс принятия решений в ICANN совершенно не является простой моделью, ее скрытые процессы разработаны для обеспечения того, чтобы донести мнения различных стейкхолдеров в Интернете. Одновременно с этим специальные группы специфических аудиторий должны обеспечить четкое понимание всех перспектив различных групп. Как следствие, это также означает, что органы управления должны иметь равное количество голосов наравне с другими органами в таких кругах, как деловая и научная среда, гражданское общество.[24] Например, это требование являлось затянувшейся причиной недовольства Бразилии, и этим частично объясняется, почему такая демократическая страна должна объединиться в данном вопросе с Россией, Китаем и другими странами образовавшегося союза. После того, как в мае 2013 года ITU провел Форум по политике мировой телекоммуникации в Женеве, представитель бразильского правительства объяснил разочарование по поводу ограниченной роли для органов правления:

> Факт заключается в том, что правительства сейчас имеют только ограниченную консультативную роль в международном управлении Интернетом, и никакой фактической вовлеченности в процесс принятия

23

См. Джей П. Кесан и Раджив Шах С., «Обманете нас один раз – позор вам, обманете нас дважды – позор нам: Чему мы можем научиться от приватизации базовой (магистральной) сети и системы доменных имен Интернет», 79 Ежеквартальное юридическое обозрение, Вашингтонский университет, 89, 2001 на 171, *доступно на:* http://ssrn.com/abstract=260834 (предоставляется исторический обзор создания корпорации ICANN и других учреждений).

24

Программа действий в Тунисе, цитированная выше в ссылке 9. (Признание того, что Интернет управление требует сотрудничества всех сторон: «Более того, мы берем на себя обязательства за стабильность и безопасность Интернета как глобального устройства, и обеспечиваем необходимую правомерность его управления, основанного на полноценном участии всех стейкхолдеров, как от развитых так и развивающихся стран, с учетом их соответствующих ролей и обязанностей».)

> решений. Последние события показали, что даже ранние рекомендации, предоставленные правительствами стран в определенных вопросах, имели незначительное влияние на фактические решения, относящиеся к вопросам, в которых они были прямо заинтересованы. К сожалению, попытки разрешить этот факт провалились из-за низкого уровня участия большинства правительств на существующей арене международного управления Интернетом.[25]

Несмотря на приведенное выше утверждение, мы считаем, что не совсем честно утверждать, что правительства не были вовлечны в процесс принятия решений. Упомянутое выше исключение относится к работе ICANN, которая, фактически, требует в своем регламенте принимать во внимание точку зрения органов правления и других стейкхолдеров.[26] Однако, именно здесь находится камень преткновения: ни одна из сторон – включая органы правления – не имеет право ветировать, и именно это право так важно для Бразилии, вот о чем она просит в своем заявлении. Следует вспомнить, что деятельность ICANN является фундаментальной в части установления универсальной системы присвоения имен и цифр, включая расширения .NET и .COM с приложениями, которые разрабатываются в настоящее время для новых доменов, таких как .GAY, .AMAZON и .PATAGONIA.[27] То, что хотят получить органы власти, не является «фактической вовлеченностью» в процесс принятия решений; то, чего они хотят – это право на вето. По сути, правительства хотят иметь возможность отклонять решения, которые может принять ICANN, в том случае, если они противоречат интересам отдельного региона.[28] Многие страны Латинской Америки, например, регионы Амазония или Патагония, требуют защищенной Интернет доменной системы, однако такая практика защиты не совсем понятна ICANN. Соответственно, при нынешнем положении дел, если ICANN и группа соискателей не смогут выработать компромисс между этими правительствами, то они будут настроены еще агрессивнее, чем когда-либо, одно по отношению к другому, и будут требовать право на вето, которого они так желают.

Это напряжение, связанное с желанием увеличить власть разными правительствами, может никогда полностью не разрешиться, и противостояние, само по себе, наверное, является приемлемым компромиссом. Однако Интернет сообществу потребуется оставаться бдительным, чтобы обеспечить внедрение инноваций в экосистеме, не забывая при этом тщательно следить за преднамеренными

---

25 Даниэль Каваланти, *Задействование роли правительств в Интернет управлении*, блог ITU, 5 июня, 2013, доступно на: http://itu4u.wordpress.com/2013/06/05/operationalizing-the-role-of-governments-in-Internetgovernance/

26 *См., напр.,* Статья XI, Раздел 2.1 Постановлений об Интернет-корпорации по присвоению имен и номеров, согласно поправке от 11 апреля, 2013 года, доступно на http://www.icann.org/en/about/governance/bylaws#XI (разрешение Государственного консультативного комитета, чтобы «непосредственно рассмотреть вопросы в правлении, путем предоставления комментария или предварительного совета, или путем особой рекомендации к действию или развитию новой политики, или же пересмотру существующей политики».)

27 Эли Шугармен, *Кому должна достаться «Патагония?»,* THE ATLANTIC, 23 апреля, 2013, *доступно на:* http://www.theatlantic.com/international/archive/2013/04/who-should-own-patagonia/275214/.

28 *Perú y Brasil se enfrentan a Amazon en defensa de la Amazonía*, EL COMERCIO, 4 мая, 2013, *доступно на:* http://elcomercio.pe/actualidad/1572165/noticia-peru-brasil-se-enfrentan-amazon-defensa-amazonia

действиями некоторых стран, целью которых является кардинальная смена правил. Именно это и случилось во время ВКМЭ-12, где можно было увидеть, что страны и регионы хотят использовать Международный регламент электросвязи в качестве материальной возможности лишения ICANN ее полномочий и приведения администрации по присвоению доменных имен в рамки исключительно такого государственного агентства, как ITU. В частности, одно из предложений в Дубае выдвинули Россия, ОАЭ, Китай, Саудовская Аравия, Алжир, Судан и Египет, потребовав следующее:

> Страны-участники должны иметь равные права для управления Интернетом, включая рассмотрение распределения управления, подписание и использование Интернет ресурсов по присвоению цифр, имен, адресов и идентификационных номеров для поддержки функционирования и разработки базовой Интернет инфраструктуры.[29]

Идея о том, что «Государства-участники должны иметь равные права для управления Интернетом» является ключевой, поскольку она подтверждает желание правительств («стран») стать ключевыми игроками, и здесь нет и упоминания о других стейкхолерах – гражданском обществе, техническом обществе, или частном секторе, которые сейчас участвуют в управлении Интернетом. Указанное выше предложение было полностью односторонним, однако оно сопровождалось поверхностной декларативной частью, которая взывает о необходимости развития мультистейкхолдерами «совместных принципов, норм, правил, процедур по принятию решений и программ».[30] Однако, декларативная часть документа в данном предложении является «пустым сосудом», и было бы невозможно согласовать с ее очевидным утверждением: «Государства должны…управлять Интернетом».

Соответственно, если переходить от функциональности ICANN к управляемому исключительно государством механизму, что было бы необходимым хотя бы для некоторых членов «Дубай-89», почему это не предложение не приняли в финальной версии договора? Единого ответа не существует, однако, к удивлению многих, ITU сам по себе сыграл в данном случае роль посредника. Генеральный секретарь ITU Хамадун Туре пригласил Фади Шехаде, нового Исполнительного директора ICANN, предоставить комментарии по поводу дня открытия ВКМЭ-12.[31] Появление Шехаде было немного противоречивым в рамках сообщества ICANN, свидетельством чему была серия множественных, публичных случаев противостояния между ICANN и ITU. В одной из таких конфронтаций ITU публично осадил просьбу предыдущего Исполнительного директора ICANN Рода Бекстрома посетить одно из собраний их

---

29 Текстовый документ, Предложение России, ОАЭ, Китая, Саудовской Аравии, Алжира, Судана и Египта, 5 декабря, 2012, пункт §3A.2, *доступно на:*http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf. Это положение также входит в документ 47-E, предложение Алжира, Саудовской Аравии, Бахрейна, Китая, ОАЭ, России, Ирака и Судана, пункт §3A.2, 11 декабря, 2012, *доступно на* http://files.wcitleaks.org/public/S12-WCIT12-C-0047!!MSW-E.pdf [далее: «Документ 47-E»].

30 *См.* Документ 47-E, §3A.1, цитата приведена в ссылке выше («Интернет управление должно осуществляться путем развития и задействования правительствами, частным сектором и гражданским обществом совместных норм, правил, процедур по принятию решений и программ, которые влияют на развитие и использование Интернета»).

31 *См.* Кирен Маккарти, Ключевые моменты и самые проблематичные места на ВКМЭ, dot-nxt.com, 15 декабря, 2012, *доступно на:* http://news.dot-nxt.com/2012/12/14/highlights-and-low-points-wcit.

Совета.[32] В связи с этим событием, основной тон Шехаде на открытии ВКМЭ-12 донес очевидное сообщение миру, что ICANN желает объединить в усилия с ITU и оставить прения в прошлом.[33]

В настоящий момент в этом вопросе дела обстоят хорошо. Точно не установленное сотрудничество с ITU было объявлено частью «нового периода в ICANN» Шехаде, фразой, которая была подхвачена и упомянута теперь в тысячах статей и веб записях.[34] В конце концов, с тех пор как заседания ВКМЭ происходят только частично открыто, мы можем точно никогда не узнать, почему или как активные предложения взять на себя работу ICANN исчезли, несмотря на предложения России, ОАЭ, Китая, Саудовской Аравии, Алжира, Судана и Египта. Но теперь мы знаем, что эти предложения существовали и горячо обсуждались перед проведением ВКМЭ-12, а затем они тихо растворились в тумане переговоров ВКМЭ без каких-либо публичных дебатов. В связи с этим, допустимо сделать вывод, – даже без прямого доказательства – что проактивная вовлеченность ICANN содействовала этому процессу. Это отдельное противостояние будет продолжаться, но «битва» будет отложена на другой день.

Важные неразрешенные вопросы относительно системы присвоения имен и цифр будут, скорее всего, продолжать оставаться неопределенными. На наш взгляд, одним из самых важных действий, направленных на уменьшение необходимости дальнейших противостояний в вопросе присвоения имен и номеров в будущем, будет определяться развитием ICANN. ICANN необходимо продолжать устанавливать контакты со странами и регионами, которые в данный момент считают, что не имеют право голоса в управлении Интернетом. Для ICANN также будет важно продолжать предпринимать меры, чтобы правительства ощущали более сильное чувство вовлеченности в процессы ICANN, и были уверены, что их мнение услышано, а также показать, что такие конфликты, как .AMAZON и .PATAGONIA[35] могут решаться внутри системы. Новое руководство в ICANN уже достигает этой цели, в том числе, заявив о своем намерении переместить и создать ответственные группы за пределами Объединенных Штатов, объявив об открытии своих филиалов в Стамбуле, Сингапуре и Пекине.[36] Это шаг в правильном направлении.

---

32 Кэвин Мерфи, главные негативные моменты (снобы) *ITU, Бекстром корпорации ICANN*, сфера деятельности доменов, 24 августа, 2010, *доступно на:*http://domainincite.com/1857-itu-chief-snubs-icanns-beckstrom.

33 Кирен Маккарти, Исполнительный директор *ICANN и Председатель собрания при открытии ВКМЭ,* DOT-NXT, 30 ноября, 2012 года, *доступно на:* http://news.dot-nxt.com/2012/11/29/icann-ceo-and-chair-attend-wci.

34 Исследование, проведенное 11 июня, 2013 года, в рамках «нового сезона» в icann, 6,200 результатов. См. http://goo.gl/wxqLU.

35 Подразумевается запрет стран Латинской Америки на присвоение доменных имен таким географическим названиям, как Амазония и Патагония (прим. перев.). источник: http://www.internetnews.me/2013/04/07/latin-american-countries-reject-amazon-patagonia/

36 Райан Хуан, *ICANN выбирает Пекин для открытия первого исполнительного \ задействованного центра*, ZDNET, April 8, 2013, *доступно на:* http://www.zdnet.com/cn/icann-picks-beijing-to-open-first-engagement-center-7000013656/. *Также см.* Микаэль Рикнас, *ICANN объявляет об открытии офиса в Стамбуле как часть попытки глобализации*, PC WORLD, 25 апреля, 2013 года, *доступно на:* http://www.pcworld.com/article/2036366/icann-announces-opening-of-istanbul-office-as-part-ofglobalization-effort.html

B. Широкополосные соединения: Доступ в Интернет для всех

По приблизительным подсчетам, на сегодняшний день количество Интернет пользователей достигает 3 миллиардов, и еще 4 миллиарда жителей не имеют доступ к Интернету – хотя они могут подвергаться его воздействию. Большая часть органов власти хочет расширить для своих граждан широкополосную сеть и способность подключения к Интернету, но, в то же время, органы власти борются за определение самой лучшей экономической модели, чтобы оплачивать такую возможность подключения. Следует ли воспринимать широкополосные соединения как общественное благо, к которому отсносятся дороги или канализационные системы, или правительствам следует воздержаться от вовлеченности в данном вопросе, чтобы способствовать развитию конкуренции?[37] Именно эти политические вопросы рассматриваются в инфраструктурном уровне.

Сейчас проводится грандиозный эксперимент, чтобы рассмотреть данные вопросы, и будет интересно наблюдать за его развитием в последующие годы. Например, Австралия и Уругвай переходят на использование версии с относительно национализированной моделью, рассматривая Интернет как финансируемое из государственного бюджета общественное право – как дороги или канализационные системы – в то время как такие страны, как Соединенные Штаты и Болгария применяют подход, более ориентированный на рынок.[38] Эти различные модели являются высокоуровневыми проявлениями двух совершенно разных общественных концептуальных подходов. Пользователи фактически однопровайдерной Интернет системы в Уругвае, кажется, наслаждаются самыми низкими ценами на широкополосные соединения для всех своих партнеров в Латинской Америке.[39] Далее, в 2010 году в Уругвае было самое большое широкополосное прохождение в Латинской Америке.[40] Для сравнения, Болгария также делает большой вклад в развитие свободного рынка, где, как шутят наши коллеги, существует более 800 (некоторые говорят, что не менее 2,000) поставщиков услуг, и покупателям предоставляется большой выбор.[41] Слишком рано судить о том,

---

37 *См.* Сьюзан П. Кроуфорд, Слушатели поневоле: Телекоммуникационная промышленность и власть монополии в новом «позолоченном веке» (1870-1898 гг. в США), типография Йельского университета (2013) (приводится пример, в котором широкополосной доступ в Интернет становится монополистическим процессом, и требуется больше вмешательства правительства).

38 *См.* Хендрик Руд, «Угрожающе высокий уровень «кабельной» монополии», 29 YALE L. & POLICY REV. INTER ALIA 34 (2010), *доступно на:*http://yalelawandpolicy.org/sites/default/files/YLPRIA29_Crawford.pdf (в данной работе автор утверждает, что недостаток регулирования процессов в США ведет к консолидации и беспрепятственной монополии на рынке услуг широкополосного доступа, уменьшению конкуренции). *См. также* «Скоросное широкополосное покрытие в Европе: Сравнение Нидерландов и Болгарии»,TPRC 2010, *доступно на:* http://ssrn.com/abstract=1989172 (показывает, как усилена конкуренция в Болгарии, где на 670 официальных ISPs приходится 2,000 незарегистрированных ISPs). *См. также* Сьюзан П. Кроуфорд, «Угрожающая «кабельная» монополия», 29 YALE L. & POL'Y REV. INTER ALIA 34 (2010), *доступно на:t* http://yalelawandpolicy.org/sites/default/files/YLPRIA29_Crawford.pdf (в данной работе автор утверждает, что недостаток регулирования процессов в США ведет к консолидации и беспрепятственной монополии на рынке услуг широкополосного доступа, уменьшению конкуренции).

39 *Banda ancha uruguaya es la más barata de América latina*, EL PAIS, 16 июня, 2012 года, *доступно на:* http://genteynegocios.elpais.com.uy/banda-ancha-uruguaya-es-la-mas-barata-de-america-latina

40 *См.* «Широкополосной индикатор Cisco. Уругвай лидирует в проникновении широкополосной сети в Латинской Америке», 16 ноября, 2011 года, *доступно на:* http://newsroom.cisco.com/uk/press-release-content?articleId=554136&type=webcontent.

41

какая модель является самой лучшей, – модели все еще пересматриваются – и в конечном счете покупатели выиграют в долгосрочной перспективе. В то время как, наверно, не существует одной правильной модели, мы считаем, что в одном вопросе точно существует определенность: передавать полномочия одному типу экономической модели путем подписания международного соглашения было бы ошибкой.

Возвращаясь к теме ВКМЭ, уполномоченная экономическая модель – это именно то, чего многие участники пытались достичь в Дубае. Дебаты были инициированы Европейской Ассоциацией операторов сетевых телекоммуникаций (ETNO), группой провайдеров европейской телекоммуникации, под руководством телекоммуникационных компаний «Telecom Italia», «Telefonica», «France Telecom», и «Deutsche Telekom».[42] Предложение данной Ассоциации призывало к принятию системы «платит сторона-отправитель», которая была бы уполномочена законом через подписание договора.[43] В сущности, это означало бы, что любому провайдеру содержимого в Интернете нужно было бы платить за то, что его информация доставлена получателю – и это была бы дополнительная оплата к налогам, которые уже оплачивает провайдер содержимого, чтобы подключиться к Интернету, и в дополнение к тем налогам, которые платит пользователь за доступ к сети. Следует вспомнить, однако, что процесс подписания договора ITU требует вынесения на рассмотрение и принятия предложений странами, а не отдельными лицами или группами. Однако, Европейской Ассоциации операторов сетевых телекоммуникаций удалось найти страну, чтобы сделать предложение от ее имени – Камерун – и его приняло большинство африканских стран в качестве совместного предложения.[44] В частности, данное предложение запрашивало следующее условие в Международном регламенте электросвязи (ITR):

> Исполнительные органы должны пытаться предоставить надлежащие средства телекоммуникаций, чтобы соответствовать требованиям и потребностям международных телекоммуникационных услуг. Для выполнения этой цели, а также для обеспечения адекватной прибыли на инвестиции в высших широкополосных инфраструктурах, исполнительные

Таня Тодорва, *Доступ к широкополосному Интернету в Болгарии,* STROITELSTVO, 21 января, 2013 г., *доступно на:* http://stroitelstvo.info/show.php?storyid=1987738

42

См. Марк Пейдж, Лука Росси и Колин Ранд «Реалистичная модель будущего Интернет», A.T. 41 Отчет Керни (2010), доступен на: http://www.atkearney.com/index.php/Publications/a-viablefuturemodel-for-the-Internet.html (при поддержке телекоммуникационных компаний «Deutsche Telekom», «France Telecom», «Telefonica» и «Telecom Italia»). *См. также* Дж. Скотт Маркус и Алессандро Монти, «Операторы сетей и поставщики информационного содержимого: кто несет расходы?» WIK Consult, 13 сентября, 2011 г., *доступно на:* SSRN: http://ssrn.com/abstract=1926768 (в данной работе приводится контраргумент к отчету Керни).

43

См. Синтия Вонг, *с соавторами,* «Предложение ETNO грозит уменьшить доступ к открытому, глобальному Интернету», CDT White Paper, June 21, 2012, *доступно на:* https://www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf.

44

Всемирная конференция по международной электросвязи, документ 19-E, Общие предложения от правительств Африки по работе конференции, документ 19-E, 2 ноября, 2012 г., *доступно на:* http://files.wcitleaks.org/public/Статья 6 содержит положения предложения ETNO.) *См. также* Всемирная конференция по международной электросвязи, документ 15-E, Заявление от Республики Камерун, 2 октября, 2012 г., *доступно на:* http://files.wcitleaks.org/public/S12-WCIT12-C-0015!!MSW-E.pdf. (В дополнение к изменениям в Статье 6 о совместном предложении от стран Африки, предложение от Республики Камерун включает в себя определение «концентрации информации», которая требует Эполной оплаты в связи с «концентрацией \ централизованностью» *в том же месте.,* пункт §2.15.)

> органы будут составлять коммерческие соглашения, чтобы достигнуть устойчивой системы справедливой компенсации за телекоммуникационные услуги, где соответствующая, уважающая принцип стороны-отправителя сеть будет платить.[45]

Предложение Европейской Ассоциации операторов сетевых телекоммуникаций привлекло чрезмерно много внимания в подведении итогов конференции в Дубае. Если бы это предложение было принято, оно бы полностью подорвало экономическую модель Интернета (в которой пользователи платят за свой доступ в Интернет) путем введения дополнительной оплаты за информацию «отправителей». Такая модель могла бы разрушить открытость Интернета, поскольку провайдеры бесплатного содержания вынуждены были бы платить дополнительные налоги, тем самым увеличивая цифровой барьер путем принудительных экономических выборов, которые могли бы принести прибыль только провайдерам телекоммуникационных услуг.[46] (Хотелось бы привести пример, каким образом это бы работало: обучающие программы онлайн в свободном доступе на сайте MIT (Массачуссетского технологического института), Стенфордской, или Академии Хана, не могли бы более предлагаться этими некоммерческими организациями, если бы они должны были бы платить дополнительный налог за предоставление информационного содержания развивающемуся миру.[47])

После месяцев дебатов на данную тему, перед проведением конференции в Дубае, Председатель конференции убрал эти условия из основного текста, и присоединил их к Международному регламенту электросвязи в виде относительно безобидного решения, предписывая ITU создать «рабочую группу» для рекомендации следующих шагов.[48] С одной стороны, решение Председателя перейти от дебатов к рекомендательной рабочей группе могло быть хорошим политическим компромиссом. Однако, ITU разделена на три секции: одна из них посвящена разработке стандартов (сектор «ITU-T»), другая отвечает за частотный ресурс (сектор «ITU-R»), и третья – за развитие (сектор «ITU-D»). Рабочая группа была сформирована из секции «ITU-T», и это вызывает у нас беспокойство, поскольку «ITU-T» – отделение ITU, группа, разрабатывающая телекоммуникационные стандарты – не является надлежащим местом для проведения оценки экономических бизнес моделей для Интернета. Если же такую политику необходимо проанализировать, ОЭСР было бы более подходящим для этого местом, поскольку в ее компетенции лежит экономический анализ – фактически, ОЭСР высказала свое мнение именно по этому делу и сделала заключение о благоприятной ситуации на

---

45 Статья Совета Рабочей группы 109, CWT WCIT12/C-109, 6 июня, 2012 г., *доступно на:* http://files.wcitleaks.org/public/ETNO%20C109.pdf.

46 Рохан Самараджива, «Гигантский шаг назад, или путь вперед», LIRNEasia, сентябрь, 2012 г., *доступно на:* http://lirneasia.net/wp-content/uploads/2012/09/Samarajiva-WCIT-Final_9.12.pdf [далее: " Самараджива, «Гигантский шаг назад»]. (Описание следующей проблемы: «Даже если поставщики информационного содержимого \ интернет-контента не решаться на всеобщее отключение, будут вынуждены передать дополнительные расходы в связи с положением «платит сторона-отправитель». Для школьницы в Гане это может означать, что видео уроки Ханской академии больше не являются для нее бесплатными.")

47 *В том же месте.* (пояснение о том, что модель «платит сторона-отправитель» демотивирует создателей бесплатного информационного содержимого, используемого для развивающегося мира).

48 Заключительные акты ВКМЭ-12, постановление PLEN/5.

рынке.[49]

Прежде чем мы перейдем к следующему пункту, давайте рассмотрим этот вопрос немного подробнее, и свяжем его с процедурой определения полномочий, которую мы описывали ранее. Необходимо вспомнить, что мы описывали модель изолированных проблем Кларка для анализа внутри групп, которые являются экспертами в данных темах и более всего заботятся только о них. Поэтому, при поверхностном рассмотрении можно сделать вывод, что система работает правильно, вынося на рассмотрение проблему «платит сторона-отправитель», и ее результат в рабочей группе для ее анализа. Однако, относить эту экономическую дискуссию к процессу, которым руководит только правительство, или же с ярко выраженным доминированием правительства, совершенно не верно. По аналогии, это было бы равнозначно передаче чьих-либо вопросов налогообложения архитектору, а не дипломированному бухгалтеру или налоговому эксперту. Несомненно, архитектор образован, имеет квалификационное удостоверение, и даже может иметь личное мнение по поводу налогов и денег – и даже того, как определенные строительные технологии могут оказаться дешевле, или привести к получению налоговой льготы. Однако, необходимо констатировать факт: архитекторы занимаются построением и разработкой объектов, в то время как бухгалтеры имеют дело с налогами и деньгами. Рассматривать вопрос налогообложения и пытаться изолировать его внутри группы, которая занимается архитектурой – это ошибка, при которой существует риск создать результат, который может ввести в заблуждение разработчиков стратегии. Именно такой случай происходит с рассмотрением секцией «ITU-T» экономического Интернет моделирования. Члены этой группы выскажут экспертное мнение, и, может быть, даже наймут экономистов, которые будут помогать им в данном вопросе, но экономическое моделирование не является их основной компетенцией. Нельзя сказать, что ITU в некотором роде не должна быть вовлеченной в другие сферы интересов, однако, она должна делать это очень осмотрительно и почтительно, и проводить четкую линию во время осуществления законодательной деятельности (например, при помощи Международного регламента электросвязи) в сферах, которые находятся вне ее компетенции.

Г. Информационный и социальный уровни

Существует много информации, имеющей значение для людей в Интернете, такая как электронная почта, блоги, видео и обмен информацией через информационный и социальный уровни Интернета, и это еще один главный источник напряжения в управлении. Это становится особенно проблематичным при объединении информационного уровня с инфраструктурным, или логическим уровнем. Два отдельных примера показывают, как несвоевременное регулирование в инфраструктурном или логическом уровнях может реально повлиять на вопросы свободы слова: спам и информационная безопасность. Безусловно, эти примеры нелегко отнести к любому из данных двух уровней. Однако, анализ спама и информационной безопасности через призму многоуровневой модели может быть полезным для разработчиков стратегии.

---

49 *См.* Рудольф Ван дер Берг, *Трафик межсетевого обмена данными: 2 миллиарда пользователей – и подтверждается установление связи,* OECD INSIGHTS, Oct. 22, 2012, *доступно на:* http://oecdinsights.org/2012/10/22/Internet-traffic-exchange-2-billion-usersand-its-done-on-a-handshake/.

•Спам

Нежелательные массовые электронные сообщения, несомненно, являются вопросом, который относится к информационному уровню: данное сообщение определяется одновременно как «нежелательное» и как «средство коммуникации» в связи с некоторым исследованием его содержимого. Нежелательные массовые электронные сообщения также встречаются на социальном уровне, где речь, и тот, кто говорит, должны в данном случае рассматриваться одинаково, что, в свою очередь, сигнализирует читателям о личностях отправителей и убеждает, что данное свойство присуще этим личностям. Интуитивно мы понимаем, что электронное письмо, которое мы получаем от известной компании (например, pepsi.com, united.com или deloitte.com) скорее всего, окажется более надежным, чем это же самое электронное письмо, полученное от пользовательского адреса (например, hotmail.com, gmail.com или gmx.net.). Тем не менее, невозможно определить, является ли сообщение «нежелательным» или нет без проведения определенного анализа или чтения содержимого сообщения. Учитывается контекст, и «нежелательное» в сообщении основывается исключительно на его содержании, или же полностью на его источнике. Если рассматривать более сложные случаи, в большинстве стран некоторые виды речи защищаются даже тогда, когда они не являются «не нежелательными» сами по себе.

Доступно множество технических решений, чтобы распознавать спам. Например, автоматизированная система обнаружения подозрительной деятельности (например, распознавание «массовости» в «массовых сообщениях») может встречаться на логическом уровне. Таким образом, если бот-сеть «захватывает» сеть компьютеров в регионе, и начинает отсылать сообщения приблизительно одного размера и от одного и того же отправителя, можно заключить, что происходит кибернетическая атака.[50] Автоматизированные системы имеют возможность распознавать определенные структуры, и компьютерные системы могут предположительно определять массовые сообщения одного размера и объема как бот-сеть, кибернетическую атаку, или просто как спам. Вот в чем заключается трудность: даже если массовые сообщения могли бы предположительно распознаваться на логическом уровне, невозможно постоянно отделять массовые сообщения от остального стека без применения действий и к остальному содержимому. Автоматизированные папки для спама более или менее сносно работают, но в большинстве случаев спам идет в отдельную папку, все еще доступную для просмотра пользователями.

Процесс отправки любого сообщения – одного или множества – является делом индивидуального выбора и определяет гражданские права, и не является сферой, подконтрольной органам власти. Например, политическая пропаганда является так называемой «защищенной» речью в Соединенных Штатах, и во многих странах экстренная связь «продвигается» через различные системы (по электронной почте, в текстовых сообщениях и по телефону). Если же они не востребованы, сами по себе, такие сообщения подразумеваются ценными для публики и считаются защищенной речью.[51] Сторонники условий Международного регламента электросвязи,

---

50 *См.* Дэвид Декари-Хету и Бенуа Дюпон, «Социальная сеть хакеров», GLOBAL CRIME, 28 июля, 2012 г., *доступно на:* http://ssrn.com/abstract=2119235 (описание бот-сетей (ботнетов) и осложнений при идентификации их источника и отслеживания злоумышленников).

51 Марк Свит, «Политическая электронная почта: Защищенная речь, или

направленного на защиту от спама, часто указывают на первый раздел в Международном регламенте электросвязи, в котором утверждается, что регламент «не выступает против тех аспектов телекоммуникаций, которые относятся к содержанию».[52] Однако, для того, чтобы это утверждение имело ценность, необходимо было бы поверить, что спам может контролироваться только на логическом уровне, не учитывая содержания. Как указано выше, мы не считаем, что это возможно.

Россия выдвинула предложение относительно спама на ВКМЭ-12, что иллюстрирует одну влиятельную – но опасную – точку зрения по поводу спама. В данном предложении Россия определила спам, как

> информацию, которая массово передается по телекоммуникационным сетям, такую как текст, аудиозапись, изображение; при этом реальные данные используются в интерфейсе реальных людей, нося беспорядочный рекламный характер, или не имея какого-либо значимого сообщения, передаются одновременно, или за короткий промежуток времени, большому количеству определенных электронных адресов без первоначального согласия адресата (получателя) получить данную информацию или информацию такого рода (выделено ударением). [53]

Выбор слов здесь очень важен, поскольку данное предложение определило спам как «информацию», которая не несет «значимого сообщения». Если бы такие определения принимались только правительством (как сделало бы это предложение России), они стали бы ярко выраженным проявлением цензуры.

В конечном итоге, условие правительства России не было включено в договор. Возможно, предложение по поводу «нежелательных массовых электронных сообщений» не вступает в силу, поскольку в нем нет прямых указаний для стран к действию – данное условие всего лишь утверждает, что «Страны-участники должны предпринять попытки к введению необходимых мер, чтобы препятствовать распространению нежелательных массовых электронных сообщений».[54] Даже если это действительно так, как мы утверждали в начале данного раздела, не принятые условия, такие, как приведенные выше, конечно же являются показателями того, к чему идет будущее Интернет политики. Пока Россия не смогла убедить остальную часть мира, что ее определение спама должно стать предметом международного законодательства, очень возможно, что авторитарные страны будут продолжать настаивать на принятии этой точки зрения на национальном уровне.

И важным вопросом является даже не фактическая возможность приведения в исполнение (или его отсутствия) условия о спаме. На самом деле очень мало – почти

нежелательный спам?» 1 DUKE LAW & TECHNOLOGY REVIEW 1-9 (2003), *доступно на:* http://scholarship.law.duke.edu/dltr/vol1/iss1/71 (анализ различных форм политического спама и их защиты согласно Первой поправке к Конституции США (гарантирует свободу слова и печати)).

52 Заключительные акты ВКМЭ-12, пункт §1.1.. *См. также автора Эрика Пфаннера*, «Сообщение, если оно тайное, от США остальному миру», THE NEW YORK TIMES, 14 декабря, 2012 г., *доступно на:* http://www.nytimes.com/2012/12/15/technology/in-a-huff-a-telling-us-walkout.html?pagewanted=all&_r=0 (описание, насколько эти положения могут быть невразумительными).

53 Документ 47-E, §2.13, цитируется на ссылке 29.

54 Заключительные акты ВКМЭ-12, пункт §5B, цитируется выше.

даже ничего – в этом положении прямо приводится в исполнение. Однако, включение положения о спаме в Международный регламент электросвязи сигнализирует миру о том, что национальным правительствам разрешено принимать такие меры по защите от спама, относящимся к информационному содержанию, какие они считают нужным выбирать сами.

Многие утверждали, что такие опасения не обоснованы, поскольку страны могут ссылаться на «оговорки» любого отдельного положения, фактически отказываясь принять его внедрение в свою национальную систему. Такая точка зрения опасна. Следует вспомнить, что положение о спаме (в таком виде, в каком оно было принято) является относительно безвредным, поэтому высказывание огоровок по поводу него, скорее всего, вряд ли будет иметь значительное правовое различие. Этот вопрос на самом деле относится к принципам и подходам: мир или соглашается, или возражает, что контроль правительства над сообщенями является для него приемлемым. То, как мы сейчас это видим, представляется двояким вопросом.

2.Информационная безопасность

Делегаты в Дубае обсуждали информационную безопасность так же активно, как они обсуждали положение о спаме. Много предложений, которые находятся в обширном диапазоне применения безопасности, не закончились подписанием договоров, но много дней и ночей было потрачено на обсуждение запросов от множества стран по поводу увеличения безопасности, а также и контроля, в Интернете. Например, Россия и Арабские страны настояли на том, что регулирующие органы должны знать направление всего Интернет трафика.[55] Теоретически, знание схемы соединений может привести к усилению контроля над компьютерными преступлениями и мерам по информационной безопасности.[56] Однако, если рассматривать процесс направления трафика более подробно, то это окажется несовместимым с проектированием самого Интернета, поскольку пласты информации в Интернете функционируют путем выбора динамического маршрута, который может меняться за долю миллисекунды в зависимости от таких факторов, как перегруженная сеть.[57]

Даже если какое-либо из предложенных положений об информационной безопасности в Международном регламенте электросвязи обязало бы ITU предпринять какие-либо меры (обязательства касались бы скорее стран-участников, чем на ITU как учреждения), было бы много дискуссий о том, является ли сам по себе ITU соответствующим форумом для обсуждения вопросов информационной безопасности.[58] Хамадун Туре, например, опубликовал свою независимую статью в

---

55 Документ 47-E, пункт §3.3, цитируется выше, ссылка 29. (В данном документе предлагается: «Операционные агентства должны определять по взаимному согласию, какие международные маршруты должны быть использованы. Страна-участник имеет право знать международный маршрут своего трафика, где это является технически возможным».)

56 *См.* Алекс Фитцпатрик, «Почему защитники Интернета ненавидят предложение России поменять сеть», MASHABLE, 5 декабря, 2012 г., *доступно на* http://mashable.com/2012/12/05/russia-Internet-proposal.

57 *См.* Корпорация Ранд., Пол Бэран и происхождение Интернет, доступно на: http://www.rand.org/about/history/baran.html.

58 *См.* Майк Мэсник, «Вы действительно хотите, чтобы ООН заведовала

журнале, в которой кратко объявил, что предложенные нормы Международного регламента электросвязи не повлияли бы на свободу слова.[59] В любом случае, так же, как и в положении о спаме, заявление России и ее союзников касательно положения об информационной безопасности было очевидным: правительства этих стран не ощущают, что существующие группы мультистейкхолдеров рассматривают волнующие их вопросы.

В данном случае, «Дубай-89» может иметь правильную точку зрения. Ключевые мультистейкхолдерские группы, которые управляют информационной безопасностью и вопросами спама, в основном отсутствуют во многих регионах, включая регионы развивающихся стран. Такие группы, как Рабочая группа по борьбе со злонамеренной передачей сообщений (MAAWG), Рабочая группа по борьбе с банковским мошенничеством – фишингом[60] (APG), и Союз по защите от нежелательной электронной почты, содержащей рекламу (CAUCE), работают более активно в Соединенных Штатах и Европе, но не известны в Африке, Латинской Америке и Юго-восточной Азии. Благодаря этому становится известным о решениях мультистейкхолдеров относительно вредоносного программного обеспечения в Европе и в других странах, однако этот случай не подходит для любого другого места.[61] В дополнение к этому, частный сектор еще не показал эффективных результатов по вовлечению высших должностных лиц, регуляторных органов, предпринимателей и гражданского общества в данных регионах касательно лучших практик по защите от спама и обеспечения информационной безопасности. То же самое касается проведения какой-либо дискуссии о последствиях применения распоряжения по «поднятию стека» на информационный и социальный уровни. В заключение, мы считаем, что если «Дубай-55» хочет убедить «Дубай-89», что существующая система мультистейкхолдеров рассматривает эти проблемы, то предназначенные для этого организации по информационной безопасности, например, такие, как вышеупомянутые, должны проводить более активную информационно-разъяснительную деятельность, обучение, и принимать мобилизирующие меры.

- ОБЪЕДИНЕНИЕ ТЕОРИИ И ПРАКТИКИ

В этом последнем разделе мы предлагаем подход, который способствует управлению этого чрезвычайно высокоорганизованного пространства. Мы считаем, что разделяемое всеми понимание лучших практик для усиленного сотрудничества будет содействовать эффективности управления Интернетом. Кляйнвехтер, совместно с другими авторами, предложил три уровня кооперативной групповой

стандартами информационной безопасности?» TECHDIRT, 12 сентября, 2012 г., *доступно на:* http://www.techdirt.com/articles/20120910/02004020322/do-we-really-wantun-charge-cybersecurity-standards.shtml.

59 Хамадун Туре, «Собрание ITU не несет угрозы для свободы слова», CNN OpEd, 5 декабря, 2012 г., *доступно на:*http://edition.cnn.com/2012/12/05/business/toure-itu-wcit-Internet-connectivity.

60 Фишинг – новый вид банковского мошенничества. Путем отправления спам-сообщений такой вид мошенничества получает секретные данные о личных счетах адресантов (прим. перев.).

61 *См. Марк Боуден*, «Враг находится внутри», THE ATLANTIC, июнь 2010 г., *доступно на:* http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/308098/ (описывается история о компьютерном черве Conficker, и попытках его контролировать).

вовлеченности и участия.[62] Первым уровнем является углубленная коммуникация, которая предлагает, чтобы «все стейкхолдеры имели возможность дискутировать с другими стейкхолдерами». Открытость в коммуникации в рамках списка адресатов и публично доступных встреч удовлетворяет данное условие. Второй уровень, или углубленная координация, должна сильнее вовлекать партнеров для создания «конгломерата решений», означающего, что «стейкхолдеры стараются разделить задачи на «тематические комплексы работ», которые касаются соответствующего учреждения. Каждое учреждение тогда следует своим принципам, чтобы обсуждать взаимосогласованные компромиссы». Третий уровень кооперации, или углубленное сотрудничество, вовлекал бы группу стейкхолдеров, разрабатывающих совместное решение, необходимым условием которого является установление новой практики (и, возможно, нового учреждения) при поддержке установленной кооперативной группы.

А. Укрепление позиции Форума по Интернет управлению

Задачи, стоящие перед управлением Интернетом, обсуждаются на нескольких форумах. Мы считаем, что в существующей институционной экосистеме IGF является самым подходящим местом проведения для главных обсуждений относительно того, какие участники должны добровольно участвовать в углубленной кооперации. IGF также хорошо подходит для определения того, какие учреждения на установленных уровнях Интернета могут рассматривать вопросы, относящиеся к данным уровням. Только сфера полномочий IGF достаточно обширна и характерна для управления Интернетом. Как было указано ранее, IGF не является органом, который принимает решения, и тот факт, что он сам по себе не наделен властью, делает его лучшим учреждением, в рамках которого собираются все соответственные стейкхолдеры. Группы стейкхолдеров со всех концов мира (члены правительства, представители промышленности, пользователи, негосударственные организации и научные круги) посещают воркшопы, двухсторонние переговоры, собрания по формированию коалиции и другие события, и играют активную роль в IGF. Это среда, в которой противоречивые вопросы могут решаться конструктивным образом всеми присутствующими сторонами без политических манипуляций и ведения переговоров, которые могут проводиться в том случае, когда на повестке дня стоит принятие решения, такое как регулятивное производство.

Важным является тот факт, что открытые дискуссии между различными экспертами проходят в процессе заслушивания различных точек зрения и обучения. IGF разработан для всех участников, которые заинтересованы в функционированиии Интернета; на форуме не существует ограничения по поводу участников, которые могут присоединиться или высказывать при всех свое мнение. Список участников включает руководителей ведущих компаний, активистов по гражданским правам, и даже молодежь, которая пользуется Интернетом для обучения и развлечения. Возможно, самым сильным местом IGF является то, что он позволяет всем стейкхолдерам (включая и жителей развивающихся стран) вести переговоры и строить отношения с коллегами в других странах, а также активно принимать участие в деятельности рабочих групп и проектах, которые распространяются и выходят за рамки самого IGF.

62

Вольфган Кляйнвехтер, Интернет управление мультистейкхолдеров: Роль правительств у Бенедека, Бауэра, Кеттеманна; Интернет управление и информационное общество: глобальные перспективы и направления деятельности Европы, одиннадцатое международное издание (2008).

Мы не пытаемся навязать IGF, однако это бессомненно единственный истинный форум мультистейкхолдеров, который созывает такое множество различных влиятельных лиц на регулярной основе. Многие стейкхолдеры не хотят, чтобы IGF стал органом, который принимает решения. Изменение миссии IGF путем трансформации его в организацию, которая принимает решения, противоречило бы сфере полномочий форума, сформулированной на Всемирном саммите по информационному обществу (WSIS). Однако, формат IGF не останется неизменным. Одним из способов улучшить IGF могло бы стать установление других форумов и учреждений для решения различных вопросов, поднятых на IGF. Это может восприниматься как вид «интеллектуальной передачи технологии» или «политической передачи технологии». Можно также разрабатывать воркшопы для развития неофициальных рекомендаций по рассмотрению некоторых вопросов управления Интернетом. Например, вопросы безопасности технического характера могут стать рекомендацией к действию от IETF, или даже таких организаций как FIRST или IEEE. В результате проведения каждого воркшопа члены дискуссии и участники записывают свои рекомендации для следующих шагов по рассмотрению каждого отдельного вопроса в своей стране или регионе.

В дополнение к вышесказанному, IGF нуждается в финансовых ресурсах для более эффективной работы в качестве платформы для других групп. IGF функционирует в рамках очень ограниченного бюджета, который составляет менше 1 миллиона долларов в год. В штате IGF находится один сотрудник, работающий полный рабочий день.[63] При сравнении с бюджетом ITU, который составляет более 150 миллионов долларов за год, становится очевидным, что участники имеют возможность увеличить свои финансовые взносы в IGF, чтобы создавать для форума более независимое будущее.[64]

Появление многих так называемых «региональных» IGF также является очень положительным фактом, где много вопросов политики обсуждаются перед проведением самого IGF. Например, будущая разработка вебсайта IGF могла бы проводиться с учетом региональных IGF, и, если возможно, предоставлять центральное место хранения для отчетов, видео, и другой информации. Эта база данных совместного пользования послужила бы для региональных IGF, и также могла бы служить источником материалов для центрального IGF каждый год. Это не означает, что региональные IGF должны соблюдать ту же тематику обсуждений, которая существует на центральном IGF. Однако, вебсайт IGF можно использовать для улучшения возможностей совместного использования информации в рамках IGF для более широкой глобальной аудитории. Мы надеемся, что в рамках IGF будет утверждена рабочая группа для развития таких идей, как вышеприведенная, а также их воплощения.

Б. Более подробно о финансировании IGF

Как мы определили в предыдущем разделе, IGF является одним из самых лучших форумов для обсуждения Интернет управления. Соответственно, укрепление позиций данного форума при помощи предложенных выше способов только

---

63 Финансирование *IGF, вебсайт* IGF, *доступно на:* http://www.intgovforum.org/cms/funding

64 *Финансовый план на 2012-2015 годы, новости* ITU, No. 9, 2010, *доступно на:* https://itunews.itu.int/En/985-Financial-Plan-for-the-years-20122015-.note.aspx.

увеличит его способность функционирования как организации, которая действительно признает и выносит на рассмотрение потребности всех групп стейкхолдеров. Система мультистейкхолдеров предоставляет собой свободный поток информации, и способствует открытой дискуссии среди стейкхолдеров, но эта деятельность не является бесплатной. По этой причине обществу необходимо найти пути финансирования IGF и сходной с ним деятельности такими способами, чтобы форум смог сотрудничать на равных условиях с такими организациями с солидной научной базой, как ITU. Хотя мы не защищаем какую-либо агитацию по «уменьшению финансирования» ITU, следует отметить, что два главных спонсора ITU – это Соединенные Штаты и Япония, каждый из которых вкладывает в него около 11 миллионов долларов ежегодно.[65] Для сравнения, на дату написания данной работы, эти две страны не предлагали когда-либо какого-либо финансирования для IGF.[66] Это необходимо изменить – и это касается не только таких стран, как Соединенные Штаты и Япония, но и многих других стран – в особенности, если страны, входящие в «Дубай-55» действительно надеятся отстаивать преимущества системы мультистейкхолдеров.

B. Следующие шаги развития IGF

Управление Интернетом должно стать совместным усилием, приложенным государствами и мультистейкхолдерами. Мы оцениваем и продвигаем IGF как форум для обсуждений, более всего подходящий для того, чтобы предоставить возможность всем стейкхолдерам добавлять темы к программе действий, проводить обсуждения по этим темам, и определять самый лучший способ решения возникших проблем. Интернет предоставил возможность продолжения развития инновации очень быстрыми темпами, и все стейкхолдеры и учреждения должны одновременно быть готовыми адаптироваться к ним и быть готовыми к участию в данных процессах для поиска баланса между различными интересами.

Вопрос участия правительств в управлении Интернетом вполне очевиден: правительства всегда имели регуляторные функции в границах своих стран на протяжении столетий. Намного тяжелее убедить частный сектор и гражданское общество, что очень важно активно и постоянно участвовать в делах управления. Если Интернет пользователи по всему миру желают полагаться исключительно на свое правительство, которое будет устанавливать правила, мы, скорее всего, будем наблюдать увеличение попыток установления контроля над Интернетом с помощью таких «топорных инструментов», как попытка подписания международного договора в Дубае.

И, наконец, правительству, при помощи любого учреждения, и особенно IGF, необходимо иметь четко обозначенные процессы. Эти процессы не должны быть статичными и негибкими, но они должны быть предсказуемыми. В то время как основа миссии IGF характеризуется отсутствием принятия решений, она может дополнить свою роль основной платформы для обсуждений путем установления прочных методов для документации и архивации развития тем Интернет политики и

---

65 «Линия фронта», проведенная *к следующей конференции ITU*, INFO SECURITY, 17 января, 2013 г., доступно на: http://www.infosecurity-magazine.com/view/30283/battle-lines-being-drawn-for-the-next-itu-conference/

66 *См. вебсайт* IGF, ссылка выше.

управления, а также с помощью разрешения на добровольное углубленное сотрудничество формировать и бороться с установленными вызовами. Во многих отношениях, IGF имеет потенциал развития в учреждение, которое может сделать намного больше, чем делает сегодня.

ВЫВОДЫ

Интернет является глобальным ресурсом, и принципы, которые внедряются для того, чтобы руководить Интернетом на глобальной основе, влияют на его совместное пользование. Правительства различных стран постоянно пытаются установить контроль над Интернетом путем внедрения своей национальной политики на глобальном ресурсе. Эта тенденция продолжает теорию банкротства, согласно которой Вестфальская система в материальном мире может также применяться к глобальной сети Интернет. Однако, в сегодняшней глобальной среде с высоким количеством соединений становится все более и более невозможным введение локальных или региональных правил в Интернете. В связи с этим совершенно необходимо постоянно искать соглашение на уровне международных принципов управления, даже если постоянные решения никогда не будут достигнуты. Поскольку процесс инновации происходит очень быстро, существует относительная ценность в обсуждении и рассмотрении «спорных моментов» таким образом, чтобы стейкхолдеры могли понять перспективы друг друга, и работать в направлении поиска компромиссов. В некоторых случаях именно спорные моменты имеют наибольшее значение, а также желание стейкхолдеров находить общий язык друг с другом, и пытаться выработать политику, соответствующую «использованию кодекса поведения и достижению относительного консенсуса». Данный процесс сам по себе, а также разнообразие участников внутри него, может быть важнее достигнутых результатов, коммюнике, точек зрения и других усилий решить разногласия.

Поскольку целый мир рассматривает возможность установления системы управления Интернетом, мы должны избегать искушения закрепить скрытые правила в международных договорах. Хотя договоры, которые относятся к управлению Интернетом, могут устанавливать нормы, пересекающие международные границы, в процессе установления таких норм существует риск узаконивания правил для повышения цензуры и предоставления возможностей для централизированного контроля Интернета. В таком случае существует большой риск замедления инновации и тех благ, которые Интернет уже предоставил.

Вместо того, чтобы пытаться установить «контроль» над Интернетом путем подписания договоров, предложенный в данной работе анализ показывает, что страны должны сосредоточиться на улучшении работы существующих учреждений, которые способствовали развитию Интернет политики, и помогать этим организациям развивать и совершенствовать свои компетенции в соответствующих сферах. Улучшение работы существующих учреждений и организаций – это действительно непростое задание, и могут появиться мысли бросить его, а затем начать заново, однако совершенно не обязательно, что новые, непроверенные подходы могут принести такое же колоссальное значение, которое на сегодняшний момент уже принесли существующие организации. Более того, поскольку форма новых учреждений будет обсуждаться все теми же участниками, результаты могут быть похожими на предыдущие.

Существует длинный список тех вопросов, которые необходимо улучшить. Он включает в себя сотрудничество с IETF в таких сферах, как технические Интернет

стандарты, с ICANN – в сфере присвоения имен, и, при помощи региональных Интернет-регистраторов, рассмотрения Интернет политики, а также увеличения принятия решений на глобальном уровне. Предусматривается сотрудничество и с ITU как местом инфраструктуры доступа, что является очень важной задачей, особенно на рынках, которые развиваются, и в которых этого еще нет. При неизбежных спорных моментах, которые всегда существовали между регионами, стейкхолдерами и интересами сторон, IGF является «круглым столом», который может объединить стейкхолдеров из различных сообществ, чтобы обсуждить будущую политику. Всем этим организациям необходимо быстро реагировать на изменения, а также требуется провести непрерывную реформу по мере развития Интернет. Однако мы должны обратиться к этим организациям и повлиять на улучшение эффективности их соответствующих обязанностей, а не создавать новые договора, охватывающие все сферы деятельности или полномочий.

Опыт на ВКМЭ в Дубае продемонстрировал в подписанном договоре недальновидность Интернет регулирования. В Дубае представители со всего мира пытались установить правила в течение двухнедельного периода, что стало результатом подписания на самом деле неблагоприятных союзов: кто мог предположить, что Арабские Эмираты, Россия, Африка и Латинская Америка («Дубай-89») объединятся, чтобы подписать договор с Соединенными Штатами, Канадой и Европой, отказывающимимся подписать договор («Дубай-55»). Существуют некоторые «отступники» в каждой из этих групп (например, Коста-Рика, Перу, Чили, Эквадор и Кения вступили в «Дубай-55», в то время как близкие союзники этих стран, такие, как Мексика, Аргентина, Бразилия и Южная Африка вошли в «Дубай-89»). Только в течение длительного периода времени можно будет понять мотивацию стран в этих союзах. Однако, фактом остается то, что делегаты в Дубае не знали до самой последней минуты конференции, кто из них будет подписывать договор, а кто нет, что является доказательством того, что переговоры такого рода могут привести к непредсказуемым результатам, что, в свою очередь, не является хорошим результатом в случае закрепления правил в международном праве. В сущности, мы рассмотрели некоторые из примеров противоречий между «Дубаем-55» и «Дубаем-89», и предполагаем, что в будущем появятся пять следующих тем, поэтому важно принять по ним соответствующие меры уже в следующие месяцы:

1. Доменная политика должна оставаться исключительно сферой компетенции ICANN. Многие страны не считают, что имеют достаточно полномочий в сегодняшней системе присвоения доменных имен, и пытаются сделать это функцией правительства. И все же, самое лучшее решение при подходе мультистейкхолдеров – озвучить эти вопросы в рамках ICANN и рассмотреть их здесь: бороться за их решение, обсуждать их, оспаривать и добиваться принятия необходимых мер. Можно было бы больше задействовать Государственный консультативный комитет для достижения такого результата. Для того, чтобы лучше показать возможность решать эти вопросы, ICANN необходимо продолжить расширение своей корпорации за пределами Соединенных Штатов, и стать более глобальной организацией.

2. Сильное место ITU – это Интернет инфраструктура, а не его стандарты. В годы телеграфной связи, телефона и факса ITU был инструментом, который предоставлял возможность взаимосвязанности и способности к взаимодействию. Однако, в случае с Интернет, IETF доказал, что он

эффективно развивает открытые стандарты взаимосвязанности и способности к взаимодействию. Функции ITU сегодня больше ориентируются на инфраструктуру, и меньше – на стандарты, иначе группа внутри ITU – ITU-T, которая устанавливает стандарты – будет продолжать считать своей компетенцией то, что на самом деле выходит за рамки ее полномочий и экспертизы. Так, к примеру, случилось на ВКМЭ, когда группа ITU-T взяла на себя ответственность разработки следующей стадии ответного действия на предложение «платит сторона-отправитель», которое фундаментально изменило бы экономическую модель Интернет. Ответственность за решение таких вопросов лучше всего предоставлять таким экономическим организациям, как ОЭСР.

3. Информационный и социальный уровни ни в коем случае не должны фигурировать в новых договорах; мы должны работать над улучшением уже существующих договоров, оставляя обсуждения и «передачу политичекой технологии» для IGF. Одной из самых дискуссионных сфер Интернет политики является то, как руководить информацией, которая циркулирует в Интернет пространстве. Такие международные организации, как ЮНЕСКО, Совет ООН по правам человека и Совет Европы позиционируют себя как защитники свободы слова в документах договора, и проведение реформы в этом направлении должно продолжаться. Много стран по различным причинам пытается получить влияние относительно доступности информации. Спорные моменты и дискуссии могут происходить на уже существующей арене, обсуждаясь на IGF, который является уникально подходящим местом для проведения дискуссий, поскольку IGF не устанавливает новых правил самостоятельно, однако может информировать участников на других форумах. В Дубае мы увидели конфликт интересов свободы слова и предложений об информационной безопасности и спаме. Хотя окончательные пункты договора исключили большую часть двояких положений, попытка контролировать информационное содержание, скорее всего, будет продолжаться, поскольку снова возникнут побуждения создавать новые договора и правила, которые приведут к еще большей неуверенности из-за международного конфликта законодательств, которую будет намного проблематичнее решить. И снова хотелось бы отметить, что форумам, которые не принимают решения, как, например, IGF, очень важно развиваться. На таких форумах разработчики стратегии могут встретиться с другими стейкхолдерами для обсуждения политики, которая будет устраивать интересы всех заинтересованных лиц без риска, что каждое из них установит новые правила, в которых необходимо будет разбираться адвокатам для воплощения их в жизнь.

4. IGF необходимо продолжать развиваться. У IGF существует много возможностей для развития. Как для начинающей организации, о чем мы писали неоднократно, IGF необходимо не становиться организацией, которая принимает решения, поскольку исследовательская дискуссия, совместно с честным и конструктивным обсуждением, будет нивелирована в определениях и переговорах. Однако, формат IGF не останется неизменным. На основании этих положений IGF может рассматриваться как основанный на политике «инструмент передачи технологии», или, образно выражаясь, как «политическая лаборатория» всех видов решений. Например, к этому относятся рекоммендации по подведению итогов

определенных ключевых воркшопов, на основании которых можно будет рассматривать вопросы, находящиеся в сферах компетенции системы мультистейкхолдерного управления. Последующие собрания IGF могли бы отследить выполнение вынесенных на рассмотрение вопросов.

5. Стейкхолдерам необходимо понимать, что управление Интернетом не предоставляется бесплатно. Такие организации, как IGF, остро ощущают недостаточное финансирование, поэтому органам власти и стейкхолдерам всего мира необходимо предпринять меры, и оплатить свою часть расходов. Мультистейкхолдерное управление уже способствовало инновации Интернета, однако в восприятии того, как должна развиваться политика финансирования, существует серьезный дисбаланс. Например, существует много стран, которые вкладывают много денежных средств в ITU, но совершенно не предоставляют финансирования для IGF (такими примерами, которые уже обсуждались выше, являются США и Япония). Мы считаем, что стейкхолдеры в национальных и частных секторах, которые являются участниками IGF и извлекают пользу из обсуждений на данном форуме, должны предоставлять финансовую поддержку, чтобы обеспечить его продолжительное функционирование.

В заключение хотелось бы отметить, что мы можем никогда не решить отдельные вопросы полностью, и различные стейкхолдеры могут никогда не прийти к одному мнению в «спорных» сферах. Однако, постоянное напряжение существует в любой функционирующей системе, и совершенно приемлемо и правильно, если существуют некоторые такие разногласия, даже если это продолжается до бесконечности. Однако, в системе Интернет политики необходимо способствовать отображению динамического и быстро меняющегося характера самого Интернета. Как установил Кларк, технический дизайн Интернета позволяет логическое разделение функций внутри технического пространства, и вопросы его разумного разделения могли бы стать самым большим вызовом для международного определения политики. Мы не высказываем предположение, что что-либо должно быть статичным, но каждой организации важно понимать свое место в «стеке» Интернета и плодотворно работать, чтобы решать глобальные проблемы в рамках ее стека и основных сфер компетенции. Если все будет проведено правильно, этот процесс будет избегать дальнейших шагов в направлении всеобщего контроля отдельными международными агентствами всего стека.

Комплексные проблемы управления Интернетом, а также стремления максимально увеличить общественную полезность Интернета для всего человечества позволяют сделать только один вывод: Интернет – это наша совместная ответственность.

Приложение – Учреждения и сферы полномочий экосистемы управления Интернетом

Данная таблица предоставляет перечень необходимых учреждений в экосистеме управления Интернетом, приведенных на Иллюстрации 2. Список не является обязательным, но мы надеемся, что смогли включить самые значимые учреждения, а также подходящие примеры для всех трех категорий.

Агенства ООН являются традиционной ареной для всей международной дипломатической деятельности, включая ведение переговоров по подписанию договоров и принятия определенной политики. Большая часть данных учреждений основывается на межгосударственных практиках, и взаимодействует с гражданским обществом и частным сектором только в случае второстепенных консультаций. За последние десятилетия началось множество процессов, которые находятся в стадии разработки в других сферах Интернет управления: например, политический дискурс и совместная деятельность, направленная против глобального потепления, развивают успешные подходы по мультистейкхолдерному управлению.

«Исконные» учреждения управления Интернетом были основаны естественным образом на протяжении последних 25 лет и сформировались в научной или инженерной сфере. В связи с успешным распространением сети и скоростью развития и инноваций, учреждения следовали открытому (мультистейкхолдерному) подходу в участии (участвуют все, кто в этом заинтересован), а также коллективной общественной поддержке практик по принятию решений (выполнение кодекса поведения или твердое согласие).

Как описано в разделе 1, многие профессии и мультимедийные технологии объединяются в Интернете. Профессиональные ассоциации этих традиционных участников (например, журналистов), а также «исконные» онлайн профессии (например, провайдеры услуг в Инициативе по глобальной сети) являются также важными голосами в дискурсе и источниках саморегуляции и моральных практик (например, профессиональные кодексы поведения).

Название	Сфера полномочий или миссия
ISOC – Интернет сообщество	Способствовать открытому развитию, эволюции и использованию Интернета на благо всех людей по всему миру. http://www.Internetsociety.org/who-we-are/mission
IETF – Рабочая группа инженеров Интернет	«Улучшение работы Интернет путем выпуска высококачественных, значимых технических документов, которые влияют на способ, при помощи которого люди разрабатывают, используют и обращаются с Интернетом». http://www.ietf.org/about/mission.html
IAB – Архитектурный совет Интернет	«Структурный контроль деятельности IETF, контролирование и влияние на процесс принятия Интернет стандартов, и назначение редактора документов RFC». http://www.iab.org/about/
ICANN – Интернет-корпорация по присвоенным именам и	«Координировать, на общем уровне, уникальные имена (идентификаторы) глобальной системы Интернет, и в частности обеспечивать стабильное и

номерам	безопасное функционирование уникальных систем идентификации Интернет». http://www.icann.org/en/about/governance/bylaws#I
W3C – Консорциум всемирной паутины (www-консорциум)	«Вести всемирную компьютерную сеть («всемирную паутину») к раскрытию ее полного потенциала путем разработки протоколов и принципов, которые обеспечат долгосрочный рост сети». http://www.w3.org/Consortium/mission
ITU – Международный телекоммуникационный союз	«Размещать глобальный диапазон радиочастот \ радиочастотный спектр и спутниковые орбиты, разрабатывать технические стандарты для обеспечения легкого \ беспрепятственного межсетевого взаимодействия сетей и технологий, и прилагать усилия для улучшения доступа к информационно-коммуникационным технологиям для сообществ, которые в них нуждаются, по всему миру». http://www.itu.int/en/about/Pages/default.aspx
IEEE – Институт инженеров по электронике и радиоэлектронике	«Содействовать технологической инновации и превосходству на благо человечества». http://www.ieee.org/about/vision_mission.html
ISO – Международная организация по стандартизации	«Разработка международных стандартов». http://www.iso.org/iso/home/about.htm
WPFC – Всемирный комитет по свободе печати	Защита и содействие свободе печати во всех средствах массовой информации. http://www.wpfc.org/?q=node/2
GNI – Инициатива по глобальной сети	Помогает компаниям по информационно-коммуникационным технологиям «столкнувшись с давлением правительств, справляться с давлением, действуя такими способами, которые могут повлиять на основные права человека на охрану личной жизни и свободу слова». http://www.globalnetworkinitiative.org/about/index.php
WBU – Всемирный союз радио- и телевизионного вещания	«Координационный орган для союзов по радио- и телевизионному вещанию, которые представляют сети телевещания по всему миру». http://www.worldbroadcastingunions.org/wbuarea/about/about.asp
WEF – Всемирный экономический форум	«способствовать политике, которая будет улучшать экономическое и социальное благосостояние сетей по всему миру». http://www.oecd.org/about/
OECD – Организация экономического сотрудничества и развития	«способствовать политике, которая будет улучшать экономическое и социальное благосостояние сетей по всему миру». http://www.oecd.org/about/
IGF – Форум по управлению использованием Интернета	«созыв нового форума для диалога политики мультистейкхолдеров» http://www.intgovforum.org/cms/aboutigf
WIPO – Всемирная организация по защите	«способствовать инновации и творческому потенциалу \ инициативности для экономического,

интеллектуальной собственности	социального и культурного развития все стран с помощью сбалансированной и эффективной международной системы интеллектуальной собственности». http://www.wipo.int/about-wipo/en/
WTO – Всемирная торговая организация	«предоставляет форум по обсуждению условий договоров, целью которых является уменьшение препятствий для международной торговли и обеспечение равных условий конкуренции для всех участников, что таким образом вносит вклад в экономический рост и развитие». http://wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm
ЮНЕСКО – Организация Объединенных Наций по вопросам образования, науки и культуры	«создавать условия для диалога между цивилизациями, культурами и народами, основанного на уважении разделяемых всеми ценностей». http://www.unesco.org/new/en/unesco/about-us/who-weare/ introducing-unesco/
UNHRC – Совет ООН по правам человека	«усиление содействия и защиты прав человека по всему миру, и вынесение на рассмотрение дел, в которых нарушаются права человека, а также внесение рекомендаций относительно их решения». http://www.ohchr.org/EN/HRBodies/HRC/Pages/About Council.aspx
FAO – Продовольственная и сельскохозяйственная организация ООН	«улучшать питание, повышать сельскохозяйственную продуктивность, повышать стандарты жизни сельского населения и участвовать в глобальном экономическом росте». http://www.fao.org/about/en/

4.1.5. Форма отчетности для национальных и региональных Форумов по управлению Интернетом

Сессии межрегионального диалога IGF

Информация, собранная при помощи этой формы, будет использована для определения тем для обсуждения на сессиях межрегионального диалога, запланированных на IGF в Балиі.Пожалуйста, поделитесь информацией с точки зрения вашего национального или регионального IGF.

* Обязательно

Имя и электронная почта лица, заполняющего эту форму *

Для связи в случае проблем с собранными данными

Полное название события *

Как были обозначены общие вопросы встречи, какие темы обсуждались?

Как были обозначены подтемы встречи? Пожалуйста, перечислите их и приведите определения, если необходимо.

Как разрабатывалась программа встречи, какие темы сессий или рабочих групп были основными?

Результаты встречи, приоритетные вопросы, определенные на встрече: Какие именно? Почему они важны? Каковы будут следующие шаги?

Как событие было воспринято другими заинтересованными сторонами (уровень участия и заинтересованности, влияние IGF на другие национальные и региональные процессы)

Как событие связано с «питающими» событиями? Например, в случае AfIGF, LACIGF, EURODIG, ArabIGF это будет ради понимания, как они связаны с индивидуальными и субрегиональными инициативами по управлению Интернетом в их географической области.

Как региональные мероприятия позиционируют глобальный IGF в своих собственных процессах?

4.1.6. Региональные и национальные инициативы IGF - предложение для предваряющего круглого стола

Региональные и национальные инициативы IGF - предложение для предваряющего круглого стола

Информация, собранная в этой анкете, будет использована в качестве исходных данных при подготовке региональных и национальных круглых столов и рассматривается как часть предварительных работ по подготовке IGF в Бали. Пожалуйста, предоставьте как можно больше информации о вашем региональном или национальном событии.

* Обязательно

Имя и электронная почта лица, заполняющего эту форму *

Для связи в случае проблем с собранными данными

Полное название события *

Веб-сайт и контакты в социальных сетях *

Сокращение, используемое для обозначения события

Например,Asia Pacific regional Internet Governance Forum известен как APrIGF

Основной контакт оргкомитета события: *

Пожалуйста сообщите полное имя, организацию, электронную почту и телефон

Использовались ли в процессе организации логистики/общего менеджмента какая-либо методология управления проектами? Который (которые) из стейкхолдеров играли координирующую роль в организации вашего регионального/национального мероприятия? *

Пожалуйста, предоставьте информацию о том, как и кем координировалось мероприятие.

Описание организационного процесса

Пожалуйста, сформулируйте принципы, которыми руководствовался в своей работе организационный комитет, а также опишите его структуру.

Как модель мультистейкхолдеризма отстаивалась в Оргкомитете?

Краткий анализ ролей и ответственностей.

- Наука и образование
- Гражданское общество
- Госструктуры
- Техническое сообщество
- Частный сектор
- Другое:

Как модель мультистейкхолдеризма защищалалась в Программном комитете?

Краткий анализ ролей и ответственностей.

- Наука и образование
- Гражданское общество
- Госструктуры
- Техническое сообщество
- Частный сектор
- Другое:

Как модель мультистейкхолдеризма проявлялась в поддержке волонтерами?

Краткий анализ ролей и ответственностей.

- Наука и образование
- Гражданское общество
- Госструктуры
- Техническое сообщество
- Частный сектор

- ☐ Другое:

Как модель мультистейкхолдеризма поддерживалась докладчиками и выступающими?

Краткий анализ ролей и ответственностей.

- ☐ Наука и образование
- ☐ Гражданское общество
- ☐ Госструктуры
- ☐ Техническое сообщество
- ☐ Частный сектор
- ☐ Другое:

Как модель мультистейкхолдеризма осуществлялась в модерировании и обслуживании?

Краткий анализ ролей и ответственностей.

- ☐ Наука и образование
- ☐ Гражданское общество
- ☐ Госструктуры
- ☐ Техническое сообщество
- ☐ Частный сектор
- ☐ Другое:

Как модель мультистейкхолдеризма обеспечивалась присутствием участников?

Краткий анализ ролей и ответственностей.

- ☐ Наука и образование
- ☐ Гражданское общество
- ☐ Госструктуры
- ☐ Техническое сообщество
- ☐ Другое:

Как модель мультистейкхолдеризма реализовалась финансовой и иной спонсорской поддержой?

Краткий анализ ролей и ответственностей.

- ☐ Наука и образование
- ☐ Гражданское общество
- ☐ Госструктуры
- ☐ Техническое сообщество
- ☐ Частный сектор
- ☐ Другое:

Каким образом можно было принять участие в организационном/программном комитете?

Сообщите нам, пожалуйста, каким образом осуществлялось вступление в члены комитета (комитетов), которые занимались организацией мероприятия

	отметить
Ситуативно	☐
Путем избрания	☐

отметить

Другое

Коммуникационные стратегии

Разъясните нам, пожалуйста, как организационный комитет популяризировал мероприятие и распространял информацию о его результатах информацию о его результатах

Использованные инструменты коммуникации/координации совместной работы

Расскажите, как мероприятие освещалось в массах до, во время и после проведения

- веб-сайт/URL
- электронные рассылки
- Фейсбук
- Аккаунт в Твиттере/хештег
- Google+
- Другое:

Описание подготовительного процесса

Опишите вкратце , пожалуйста, временные рамки и методологию подготовительного процесса

Общий бюджет мероприятия

Предоставьте, пожалуйста, информацию о денежных инвестициях и оказании помощи товарами и услугами, которые обеспечили успешное проведение вашего мероприятия

Источники финансирования

Список организаций/частных лиц, оказавших поддержку мероприятию

Механизмы финансирования, которые были использованы

Расскажите нам, пожалуйста, как организационый комитет осуществлял сбор средств для успешного проведения мероприятия

- ☐ Благотворительные взносы
- ☐ Спонсорство
- ☐ Помощь товарами или услугами
- ☐ Платное участие
- ☐ Краудфандинг (народное финансирование, сбор средств, попрошайничание)
- ☐ Другое:

Как регистрировались участники?

- ☐ На сайте
- ☐ На месте
- ☐ По электронной почте
- ☐ Другое:

За сколько начала до мероприятия была открыта регистрация?

- ☐ Более, чем за 3 месяца до мероприятия
- ☐ Менее, чем за 2 месяца
- ☐ За 1 месяц
- ☐ Другое:
- ☐ Другое:

Должны ли были регистрироваться также и дистанционные участники?

- ☐ Да
- ☐ Нет

Какие программные или он-лайновые инструменты использовались для управления регистрацией?

Пожалуйста, дайте ссылку на окончательный вариант программы

Методики, которые использовались для проведения секций/панелей, в том числе стимулирование аудитории к участию в обсуждении

Описание культурной составляющей

Шаги, предпринятые для поддержания гендерного баланса

Общее количество участников

Классификация участников

Пожалуйста, предоставьте имеющуюся у вас статистику по представительству различных групп стейкхолдеров, различных имущественных слоев, пола, возрастных групп, образовательного уровня, людей с ограниченными возможностями.

Обеспечение дистанционного участия

Пожалуйста, предоставьте информацию о технологиях, которые использовались, об их стоимости, о качественном составе и количестве дистанционных участников

Полученные результаты (распечатанные, размещенные онлайн, и т. д.) и как их распространение вписывается в коммуникационную стратегию

Никогда не используйте формы Google для передачи паролей.

Готово!

4.1.7. Себастьен Башоле. Управление Интернетом: пора браться за работу!

Управление Интернетом: пора браться за работу!

Себастьен Башоле (Sébastien Bachollet), член Совета Директоров ICANN, подводит итоги 8-го Форума по управлению Интернетом, который состоялся на Бали (Индонезия).

В ходе 8-го Форума по управлению Интернетом (Internet Governance Forum - IGF), который недавно завершился на Бали (Индонезия), вопросу распределения ролей различных сторон, вовлеченных в управление Интернетом многочисленными стейкхолдерами, был посвящен целый ряд встреч, как включенных в программу, так и неформальных.

Т ри основных события придали еще больше остроты форуму, целью которого является развитие управления Интернетом:

разоблачения Эдвардом Сноуденом роли Агенства национальной безопасности (National Security Agency - NSA)

- реакция на эти разоблачения президента Бразилии, и, наконец,
- обнародование заявления Монтевидео, призывающего к созданию мультистейкхолдерной колации в целях управления Интернетом.

Первое из вышеперечисленных событий ставит на повестку дня более острый, но при этом фундаментальный вопрос о том месте, которое американское правительство занимает в системе администрирования и управления Интернетом. Оно также актуализирует проблему поиска одной (или нескольких) альтернатив.

10 организаций (так называемые I* организации, а именно 5 Региональных Интернет Регистратур (РИРов) - AFRINIC, ARIN, APNIC, LACNIC, RIPE NCC — а также Совет по ахитектуре Интернета (Internet Architecture Board), Интернет корпорация по присвоению имен и адресов (ICANN), Инженерный Совет Интернета (IETF), Всемирное Общество Интернета (Internet Society Worldwide), Консорциум World Wide Web (W3C)), которые повседневно занимаются решением технических вопросов функционирования Интернета, приняли совместное заявление по результатам встречи лидеров этих организаций, состоявшейся в Монтевидео в начале октября 2013 года. Один из пунктов этого заявления гласит: «Они идентифицировали необходимость постоянно прилагать усилия для того, чтобы отвечать на вызовы, возникающие в процессе управления Интернетом, и договорились катализировать усилия всего сообщества по развитию глобальной мультистейкхолдерной Интернет-

кооперации».

Президент Бразилии обратилась к Генеральной Ассамблее ООН с призывом найти многостороннее решение (то есть на уровне только правительств и/или международных межправительственных организаций).

Вслед за заявлением Монтевидео Фади Чехаде, исполнительный директор ICANN, встретился с Дилмой Руссеф, президентом Бразилии, в результате чего возникла Бразильская инициатива по проведению в Бразилии «саммита» в начале мая 2014 года для обсуждения проблем управления Интернетом и с участием представителей всех стейкхолдеров максимально возможного количества стран.

Целью этого «саммита» станет не нахождение решений каждой из проблем, стоящих на пути развития Интернета, а создание открытой мультистейкхолдерной конструкции, которая создаст условия для нахождения подобных решений.

Таким образом, в центре обсуждений на Бали оказались роль США в управлении Интернетом, заявление Монтевидео и проект саммита в Бразилии.

В ходе IGF на Бали группа I* провела ряд различных информационных и дискуссионных мероприятий, ккоторыми постаралась охватить всех остальных Интернет-стейкхолдеров.

Целью было создание «коалиции» основных лидеров и стейкхолдеров Интернета для ответа на вопрос, каким образом действительно мультистейкхолдерные решения каждой и всех проблем управления Интернетом могут быть имплементированы. Эта «коалиция» должна будет также быть задействована при подготовке встречи в Бразилии, к организации которой подключатся некоторые другие страны, в организации информационной кампании, а также в вовлечении и поощрении участия всех стейкхолдеров со всего мира...

В ходе этих встреч различные стейкхолдеры высказали различные точки зрения, которые я попытаюсь суммировать следующим образом.

После ВКМЭ (Всемирной конференции по международной электросвязи — WCIT) и событий последних недель, «коалиция доброй воли», чьей официальной целью была защита мультистейкхолдерной модели управления Интернетом, и в которой правительство США выступало основным игроком, значительно ослабила свои позиции и не смогла выдвинуть никакой

альтернативы.

Этот процесс зашел так далеко, что сегодня существует реальный риск того, что управление Интернетом подпадет под контроль единственной межправительственной организации, без участия общества и частного сектора.

Не существует единой конструкции (по крайней мере, общепризнанной), которая позволяет находить решения различных проблем, возникающих в процессе управления Интернетом. К таким проблемам относятся, среди многих прочих, проблема спама, защиты детей и подростков от он-лайн порнографии, использования собираемой информации.

Поэтому пришло время разработать альтернативу и существующей форме мультистейкхолдерного управления Интернетом, в которой чрезмерно завышена роль одного государства (США), и чисто ООН-овскому решению, из которого исключаются негосударственные стейкхолдеры, непосредственно обеспечивающие функционирование Интернета.

Предстоящие 18-24 месяца станут решающими в защите истинно мультистейкхолдерной модели, и положат конец битве за влияние и контроль над критическими ресурсами Интернета, которую развязали государства (и между собой, и не только).

Предлагаемые решения (сценарии) должны быть поданы до 1 марта 2014 года. Для анализа этих предложений и/или подготовки проекта решения «коалицией» может быть сформирован независимый руководящий комитет.

На Бали я смог наблюдать, как быстро поменялись позиции различных стейкхолдеров, вовлеченных в управление Интернетом, по сравнению с периодом виртуальной «холодной войны», которая отбросила нас во времена последнего Всемирного Саммита по информационному обществу под эгидой ООН. Комбинация нынешних событий и международного календаря (Полномочная конференция МСЭ, обсуждение в ООН подготовки нового Всемирного саммита и т. д.) создает острую необходимость глубокого анализа и достижения максимально широкого консенсуса в отношении закладки новой формы управления Интернетом, в которою все могут быть вовлечены и которая будет открыта для всех стейкхолдеров. Если мы не сможем достичь такого консенсуса, мы будем отданы на откуп безрезультативной конфронтации между отдельными государствами, корпоративному лоббированию, бюрократическому подходу международных организаций. Если мы немедленно и твердо не возьмемся за принятие решений по управлению Интернетом сами, за нас это сделают другие. Пользователи Интернета и стейкхолдеры управления

Интернетом заслуживают лучшего. За работу!

4.2. Переводы студентов кафедры «Кибермир»

4.2.1. Кодекс сумлінної практики з управління Інтернетом

Кодекс сумлінної практики з управління Інтернетом

Версія 1.1, червень 2010[67]

Вступ

Інтернет стає все більш важливим у всіх аспектах людського життя. Він знаходиться у постійному розвитку – розвиваються технології, покращуються умови доступу до нього, збільшується кількість користувачів. Його вплив на соціальне, культурне та політичне життя швидко зростає. Використання мережі Інтернет та її сервісів наразі впливає на кожну людину так само, як і електронний уряд – незалежно від того, наскільки часто ми користуємося мережею.

Розвиток Інтернету та управління ним були значною мірою побудовані на принципах відкритості (гласності), обміну інформацією, участі зацікавлених людей і відкритого обговорення та прийняття рішень. Ці принципи сприяли динамізму та всеосяжності мережі.

Цей кодекс сумлінної практики ґрунтується на досвіді багатьох організацій, пов'язаних з управлінням Інтернетом, і створений для підвищення відкритості, збільшення кількості інформації та користувачів. Він задуманий як перелік принципів і рекомендацій, які допоможуть цим організаціям підтримувати та розвивати відкритість та всеосяжність, оскільки кількість користувачів, контенту та загальна значущість Інтернету продовжує зростати. Способи, в рамках яких ці принципи й установки будуть реалізовані, варіюватимуться в залежності від обставин та обов'язків різних зацікавлених організацій.

Визначення

У цьому Кодексі практики термін **"Управління Інтернетом"** означає вдосконалення та застосування урядами, приватним сектором і громадянським суспільством в цілому, в рамках їхніх зобов’язань, загальних принципів, норм, правил, процедур прийняття рішень і програм, які формують умови для розвитку і використання Інтернету, як це було визначено в Туніській програмі з питань інформаційного суспільства, узгодженої на Всесвітньому самміті з питань інформаційного суспільства в 2005 році.

---

[67] Кодекс сумлінної практики з управління Інтернетом є ініціативою Асоціації прогресивних комунікацій, Ради Європи та Європейської економічної Комісії ООН. Цей перший варіант тексту містить зворотню реакцію, отриману від різних зацікавлених сторін та організацій, пов'язаних з управлінням Інтернетом на Форумі з управління Інтернетом у Шарм-ель-Шейху у грудні 2009 року.

У цьому Кодексі практики під терміном **"прийняття рішень"** маються на увазі всі процеси, що включають в себе систему обговорень та рішень, стандартів, координацію та управління Інтернетом, а також ті процеси, що пов'язані із взаємодією Інтернету з іншими суспільно-політичними сферами. Тобто прийняття рішень включає в себе всі процеси, починаючи з дня впорядкування програми і закінчуючи імплементацією, що впливає на управління Інтернетом, як визначено вище.

Принципи управління Інтернетом

Є багато різних організацій, що займаються питаннями управління Інтернетом. Хоча вони відрізняються одна від одної за статусом та обов'язками, усі вони притримуються принципів відкритості та обміну інформацією, участі зацікавлених сторін та відкритого обговорення і прийняття рішень, які були сформульовані на основі характерних для розвитку Інтернету рис. Їх зобов'язання притримуватися даних принципів прописано в "Принципах Всесвітнього саміту з питань інформаційного суспільства", включено до підсумкового документу Туніської програми з питань інформаційного суспільства, що постановляє, що "Міжнародне управління мережею Інтернет має бути багатостороннім, прозорим і демократичним та реалізовуватись за участю урядів, приватного сектора, громадянського суспільства і міжнародних організацій. Воно повинно забезпечувати справедливий розподіл ресурсів, сприяти загальнодоступності мережі, гарантувати стабільне і безпечне функціонування Інтернету, враховуючи при цьому багатомовність".

Наступні принципи базуються на цій концепції для забезпечення відкритості та прозорості управління Інтернетом:

1. Розвиток Інтернету урівноважив участь та запити різних зацікавлених груп - зокрема, уряду, бізнес-сегменту, громадянського суспільства та Інтернет-спільноти. Участь всіх зацікавлених груп стала і повинна залишатися загальноприйнятою нормою для управління Інтернетом.
2. Розвиток Інтернету є дуже важливим для будь-якого суспільства. Тому необхідним є залучення зацікавлених сторін з усіх організацій та об'єднань, що мають різний соціальний, економічний і культурний досвід.
3. Розвиток Інтернету вимагає залучення всіх видів Інтернет-користувачів і повинен відображати їхні різноманітні цінності, інтереси та потреби. Але він має охоплювати не лише Інтернет-фахівців та досвідчених користувачів, а й майбутніх користувачів Інтернету й тих, хто не може або не користується Інтернетом самостійно.
4. Розвиток Інтернету вимагає обговорення ряду питань, розробки стратегії та імплементації рішень на різних рівнях, від глобального до регіонального, національного та місцевого, що має бути зроблено за участі різних зацікавлених сторін на всіх цих рівнях.
5. Інтернет все більше і більше взаємодіє з багатьма іншими

управлінськими сферами. Це важливо як для мережі, так і для суспільства в цілому, що ті, хто в першу чергу пов'язані з відмінними від Інтернету стратегічними галузями - такими як телекомунікації та засоби масової інформації, соціальний та економічний розвиток, навколишнє середовище і права людини - також можуть зробити свій внесок у розробку стратегії та прийняття рішень.

6. Для того щоб полегшити вищезгадану взаємодію, мають бути розроблені технічно складні інтерфейси.

7. Особи та організації, що володіють достатньою інформацією, є запорукою існування відкритої і всеосяжної глобальної мережі Інтернет. Доступ до інформації та можливість брати участь в прийнятті рішень, що стосуються Інтернету і його взаємозв'язку з іншими аспектами життя суспільства є обов'язковими, якщо принципи зобов'язання мають бути успішно виконаними.

Принципи, що стосуються інформації

Визначення

У цьому кодексі сумлінної практики термін **"Інформація"** включає в себе як:

а) довідкову інформацію, яка уможливлює процес прийняття рішень та матеріали, з якими мають ознайомитись учасники процесу прийняття рішень (як наявні, так і потенційні), інші зацікавлені сторони і широка громадськість;

так і

б) матеріали (програми, довідкова документація, інформація про процеси прийняття рішень, протоколи, резолюції і т.д.), які, власне, є частиною процесу прийняття рішень.

1. Процеси прийняття рішень та рішення, пов'язані з управлінням Інтернетом, повинні бути – і їх мають бачити лише такими – відкритими, прозорими та всеосяжними.

2. Уся інформація, яка стосується прийняття рішень та управління Інтернетом, або яка стосується роботи організацій, пов'язаних з управлінням Інтернетом, повинна бути доступною усім потенційним учасникам у такий спосіб та у такому форматі, який є зручним для них. Винятки з цього принципу повинні бути публічно обговорені та пояснені.

3.Організації, пов'язані з управлінням Інтернетом, повинні активно сприяти поширенню інформації за допомогою Інтернету або використовуючи інші способи і підвищувати обізнаність суспільства щодо своєї роботи в цілому, щодо питань, якими вони займаються, тих рішень, які приймаються та процесів, за яких рішення будуть прийняті.

4. Щоб домогтися цього, вони повинні підготувати та розповсюдити – серед Інтернет-спільноти, засобів масової інформації та широкої громадськості – інформаційні ресурси, які підсумовують їхню роботу, конкретні питання і процеси прийняття рішень.

5. Ці інформаційні ресурси повинні полегшити розуміння та усвідомлення процесу прийняття рішень користувачами. Ресурси мають містити матеріали,

які написані таким чином, щоб їх легко могла зрозуміти не дуже компетентна у цьому питанні людина.

6. Організації, пов'язані з управлінням Інтернетом, повинні намагатись надавати інформацію різними мовами та у різних форматах аби сприяти залученню всіх потенційних груп користувачів.

7. Організації, пов'язані з управлінням Інтернетом, повинні забезпечити зв'язок з користувачами, в тому числі й в офф-лайн режимі, для отримання ними подальшої інформації про роботу організацій, процеси прийняття рішень, а також про процеси, за допомогою яких ці рішення приймаються.

8. Організації, пов'язані з управлінням Інтернетом, повинні поширювати дані принципи і практики аби розпочати діалог та спільну роботу з іншими органами управління, у тому числі з тими, чиї завдання, в основному, знаходяться поза межами Інтернету.

Принципи щодо участі

Визначення

У цьому кодексі сумлінної практики термін **"Участь"** означає можливість, яка надається тим, хто цього бажає, зробити свій внесок у процес прийняття рішень, який, на їх думку, впливає на них (або такий, де, як вони вважають, їхня думка має бути почута), а також механізми, які дозволяють їм зробити свій внесок.

1. Організації, пов'язані з управлінням Інтернетом, та процеси управління повинні закликати та надавати можливість усім, хто бажає взяти участь у процесах прийняття рішень стосовно мережі Інтернет зробити свій внесок, сподіваючись на те, що їхні пропозиції будуть враховані.

2. Організації, пов'язані з управлінням Інтернетом, повинні активно сприяти участі у своїй роботі всіх тих, на кого впливає або може вплинути, або тих, хто вважає, що на нього вплинули рішення організацій, в тому числі, участі приватних осіб і спільнот з усіх регіонів світу.

3. Організації, пов'язані з управлінням Інтернетом, повинні прагнути залучення до їхніх обговорень країн та осіб, які недостатньо представлені та охоплені, які знаходяться у меншості, в тому числі як тих, хто користується Інтернетом, так і тих, хто поки що ні, і повинні враховувати потреби своїх майбутніх користувачів.

4. Будь-яка особа або організація повинна мати можливість винести на обговорення питання щодо програми розвитку Інтернету, розробки стандартів, координації або управління, а також щодо менеджменту та структури організацій, пов'язаних з управлінням Інтернетом. Вони також повинні мати можливість брати участь у таких дебатах.

5. Інформація щодо можливості взяти участь у роботі організацій, пов'язаних з управлінням Інтернетом, має набути широкого розголосу задля того, щоб всі, хто бажає взяти участь, були ознайомлені з нею. Організації, пов'язані з управлінням Інтернетом, мають усвідомити, що недостатнє

поширення інформації може вплинути на здатність потенційних учасників співпрацювати з ними, а тому повинні сприяти участі тих, у кого існують проблеми зі зв'язком.

6. Для полегшення участі і взаємодії організації, пов'язані з управлінням Інтернетом, повинні підготувати і поширити чітку й зрозумілу інформацію про приклади участі в процесах формування програми розвитку Інтернету, розробки стандартів, координації або управління. Вони повинні усвідомити, що некомпетентність та недостатня обізнаність учасника може стати бар'єром для співпраці, і тому повинні надати новим учасникам можливість ознайомитись з роботою організацій у форматі реальних та онлайн-зустрічей.

7. Організації, пов'язані з управлінням Інтернетом, повинні намагатись унеможливити залежність участі у процесі прийняття рішень від місцезнаходження, особистої мобільності та фінансових ресурсів учасників. Зусилля, спрямовані на досягнення цієї мети, мають включати як офф-лайнові й інші механізми, що відповідають потребам відповідних спільнот, так і дистанційну онлайн-участь.

8. Організації, пов'язані з управлінням Інтернетом, повинні поширювати дані принципи і практики аби розпочати діалог та спільну роботу з іншими органами управління, у тому числі з тими, чиї завдання, в основному, знаходяться поза межами Інтернету.

Моніторинг та огляд

Організації, пов'язані з управлінням Інтернетом, повинні регулярно переглядати свої погодження щодо поширення інформації, участі користувачів та механізмів управління, у світлі даного Кодексу практики, з метою використання результатів таких оглядів для підвищення відкритості, якості, прозорості, своєчасності та відповідальності за прийняття рішень, пов'язаних з розвитком Інтернету. Бажаною є участь усіх зацікавлених сторін. Для досягнення цього будуть використані методи експертних оцінок та інші схожі або сторонні методи оцінки. Організації, пов'язані з управлінням Інтернетом, повинні оприлюднити результати такого аналізу.

4.2.2. Роберт Аткінсон. Хто є хто в проведенні Інтернет політики: Систематика Політики Інформаційних Технологій

Хто є хто в проведенні Інтернет політики: Систематика Політики Інформаційних Технологій

Автор: Роберт Аткінсон, 1 жовтня 2010 року

Десятиліття тому, до того, як різко припинився технологічний бум та сталася криза економіки цифрових технологій, деяким здавалося, що питання, пов'язані з інформаційними технологіями (IT), можуть стати ключовими в обговореннях у XXI ст. Проте після 11 вересня 2001 року наші думки були спрямовані на зовсім інше, а «цифрова політика» стала здаватися нудним телешоу. Технократи, любителі та комп'ютерні інженери сперечалися з таких питань, як тонкощі переваг відкритих вихідних текстів та запатентованого програмного забезпечення, у той час як решта з нас використовували Інтернет у мирних цілях. Проте останнім часом цифрова політика почала повертатися «на круги своя», піднімаючи проблемні питання у засобах масової інформації та перед Конгресом практично щотижня.

Питання IT дійсно важливі нині, а в багатьох відношеннях мають ще більше значення, аніж мали у 1990 р. Питання IT та пов’язані з ними сприяють розвитку політичного дискурсу, оскільки торкаються кожної сфери нашого життя та економіки і все більше ускладнюють певні соціально-політичні питання, які вже довго перебувають на порядку денному. Дискусії виникли навколо безлічі питань IT, таких як захист авторських прав, недоторканність приватного життя, відкриті закупівлі програмного забезпечення, кібербезпека, оподаткування, володіння засобами управління використання Інтернету (наприклад, Інтернет корпорація із присвоєння імен та номерів - ICANN), електронне голосування, широкомасштабність розміщення та утвердження, спектр антитрастових реформ, мережевий нейтралітет, цензура в мережі, рівність доступу. Ці проблеми піднімають аналогічні правові та політичні питання у певних неспоріднених контекстах. Вони також спричинили важливий та жвавий, проте надзвичайно гострий та політичний дискурс щодо цифрової політики. Насправді, питання IT настільки схвилювали всіх, що під час президентської кампанії 2008 р. усі кандидати стверджували, що вони є Інтернет підкованими. Сьогодні групи інтересів різного роду, включаючи цілий ряд організацій із захисту інтересів, зазвичай виступають проти питань щодо Інтернет та цифрової економіки.

Особи, які приймають рішення, повинні бути практичними та поважати унікальність Інтернету, а також не заважати розвитку цифрових інновацій та прогресу. Однак, із суспільної точки зору, спираючись на яку ми ведемо дискурс, політика в галузі IT стає все більш насиченою жорсткими заходами, і в багатьох випадках – ідеологічно скерованими рішеннями, тому стає все важче вирішувати проблеми і виробляти правильні рішення.

Неприємні політичні дилеми виникають постійно, з появою кожної нової бізнес-моделі та інновації у сфері Інтернету, створюючи все нові і нові наріжні камені у дискусіях.

Соціологи мають побоювання, що розширення кола прав та можливостей Інтернету буде перебрано транснаціональними корпораціями та статичними урядами, які змінять його у власних вузьких інтересах (або можуть вкрасти нашу приватність, обмежити нашу свободу в Інтернеті, слідкувати за нами, або все це разом).

Те, як ми вирішуємо ці нові проблеми, матиме важливе значення для темпів та масштабів наших цифрових перетворень та збільшення економічного росту та якості життя у кілька наступних десятиліть. Особи, які приймають рішення, повинні бути практичними та поважати унікальність Інтернету, а також не заважати розвитку цифрових інновацій та прогресу. Однак, із суспільної точки зору, спираючись на яку ми ведемо дискурс, політика в області IT стає все більш насиченою жорсткими заходами, і в багатьох випадках – ідеологічно скерованими рішеннями, тому стає все важче вирішувати проблеми і виробляти правильні рішення.

Дебати із питань політики IT не ведуться у закритому форматі або лише в коридорах Конгресу. Від «мізкових центрів» до торгових асоціацій, до рухів підтримки якогось питання, низка організацій веде боротьбу заради створення цифрових політичних дебатів. Нижче наведено приклад для кращого розуміння читачем політики IT.[1] Він описує головні групи гравців у дебатах та дискурсах щодо політики IT, як вони розходяться у думках щодо двох ключових аспектів формування політики – індивідуальні можливості проти соціальних вигод та принцип невтручання проти урядового регулювання. Потім він використовує чотири доречні та важливі політичні справи (недоторканність приватного життя, оподаткування, захист авторських прав, а також мережевий нейтралітет) для того, аби відповісти, як ці теорії нині розігруються у Сполучених Штатах. Хоча дана робота і зосереджена у першу чергу на американській цифровій політиці, вона не є потенційно унікальною для випадку Сполучених Штатів.

ГОЛОВНІ АКТОРИ

Основні гравці у суперечці щодо політики IT поділяються на вісім основних груп:

Борці за свободу кібер простору

Ці «постійні жильці Інтернет мережі» вважають, що розпочали Інтернет революцію. «Фонд безкоштовного програмного забезпечення» та «Фонд боротьби із порушеннями конфіденційності та громадянських свобод за допомогою електронних технологій», а також віддані читачі журналу “Wired” вірять у те, що «інформація прагне вільного доступу», а також те, що будь-яке програмне забезпечення має бути у вільному доступі. Вони притримуються тої думки, що технології можуть самостійно вирішити багато проблем, які самі ж і створюють (якщо тільки користувачі достатньо розумні для того, аби створити програмне забезпечення, для свого захисту), і що кібер простір має регулюватися не офіційними вимушеними соціальними правилами (наприклад, «мережевий етикет»), які поширилися серед молодих користувачів. За прикладом Перрі Барлоу у його Декларації про незалежність кібер простору від 1996 року[2] вони піддають осуду як урядову участь у мережах, так і її широку комерціалізацію. На їх думку, будь-хто, хто робить припущення, що суспільство, за допомогою законно обраних урядових керівників, можливо має певну роль у формуванні Інтернету, включаючи захист авторських прав, «просто чогось ще не зрозуміло». Борці за свободу кібер простору вірять у те, що Інтернет має регулюватися користувачами. Ви боїтесь того, що порушується ваше приватне життя? Технологічно уповноважені користувачі є найкращим виходом, оскільки вони встановлюють власні веб-браузери для відхилення «cookies», використовують програми збереження анонімності та кодують власний веб трафік. Ви хвилюєтесь за те, що індустрія звукозапису втрачає доходи від Інтернет піратства? Заохочуйте авторів шукати нові бізнес моделі, як наприклад, продаж футболок та організація більшої кількості концертів. Занепокоєні слабкою конкурентоспроможністю IT індустрії у Сполучених Штатах? Не панікуйте; урядове втручання зазвичай все погіршує. Врешті решт, Силіконова долина не потребувала допомоги Вашингтону, аби досягнути того рівня, на якому вона знаходиться нині.

Соціальні інженери

Ці ліберали вважають, що Інтернет розширюється, але вони побоюються, що його зростання ненавмисно, проте інколи все таки має серйозні негативні наслідки для суспільства. Вони посилаються на так званий «цифровий розрив», передбачувану втрату конфіденційності, мережевий нейтралітет, та стурбованість тим, що корпорації контролюють використання цифрового контенту. Вони не довіряють як уряду, так і корпораціям, особливо великим телекомунікаційним компаніям та Інтернет компаніям, які роблять гроші на використанні особистих даних споживачів (Як не дивно, використання цих даних дозволяє їм надавати безкоштовні послуги).Велика кількість груп та окремих осіб можуть бути у цьому обвинувачені, у тому числі Фонд Бентона, Центр демократії і технологій, Центр цифрової демократії, Громадянський форум з прав на комунікаційну політику, Проект споживачів із технологій, Інформаційний центр з електронної приватності, Вільна преса, Проект із доступу до ЗМІ, а також стипендії, такі як Тім Ву із Колумбії, Девід Рід від «MediaLaboratory», більшість з яких є випускниками Гарвардського Центру Беркмана (серед яких Ларрі Лессиг та Йохан Бенклер).Соціальні інженери схильні вірити, що Інтернет повинен виконувати головним чином послуги із освіти та зв'язку. Вони побоюються, що розширення прав і можливостей буде скасовано потужними транснаціональними корпораціями та урядами, які зроблять перетворення в ньому у своїх власних вузьких цілях (або втрутяться у наше приватне життя, обмежать нашу свободу в Інтернеті, будуть шпигувати за нами, або все разом). Таким чином, вони зменшують його роль в якості економічного двигуна, а приділяють більше уваги впливу інформаційних технологій на соціальні питання, такі як недоторканність приватного життя, спільноти, доступу до інформації та контенту, та громадянських свобод.

Вільні маркетологи

Ця група розглядає цифрову революцію як велику третю хвилю економічних інновацій в людській історії (після сільськогосподарської та промислової революції). ІТ зменшують транзакційні витрати і полегшують застосування ринків для багатьох інших галузей людської діяльності. Вільні маркетологи вбачають різке послаблення ролі уряду, спричинене тим, що Інтернет відкриває можливості для людей, полегшує роботу підприємцям і дає поштовх ринкам. Під впливом таких груп, як Інститут Катона, Центру Меркатуса, Тихоокеанський науково-дослідний інститут, Центр Феніксу, Фонд Свободи та Прогресу, Інститут технологічної політики, які вважають, що поява Інтернету в якості засобу для торгівлі (наприклад, обмін товарів, послуг та інформації на ринку), а також способу звільнення і прогресу. Вони скептично ставляться до необхідності державної участі, навіть до урядових партнерських зв'язків з промисловістю з метою більш швидкого введення цифрової економіки.

Модератори

Ця група твердо розглядає ІТ як рушійну силу цієї епохи для економічного зростання та соціального прогресу. У той час, як вони розглядають Інтернет як унікальний феномен, до якого не можуть застосовуватися старі правила і закони, вони вважають, що повинні бути розроблені відповідні керівні принципи, якщо є мета повністю реалізувати свій потенціал. Крім того, вони стверджують, що у той час як норми і правила не повинні сприяти компаніям, які обслуговують своїх клієнтів (див. нижче) через Інтернет, і не віддавати переваги Інтернет компаніям. Більше того, вони стверджують, що у той час, як уряд повинен «не нашкодити» в обмеженні ІТ інновацій, слід також «активно приносити користь», прийнявши політику заохочення цифрового перетворення в таких сферах, як багато мережевий зв'язок, здорові ІТ, інтелектуальні транспортні системи , мобільні платежі, цифрові підписи та інше. Приклади модераторів включають

Центр перспективних досліджень в галузі науки і технічної політики, Центр стратегічних і міжнародних досліджень, Фонд інформаційних технологій та інновацій і Центр Stilwell.

Моральні консерватори

Ця група розглядає Інтернет як небезпечний простір, віртуальне лігво беззаконня, населений порнографією, гравцями, педофілами, терористами та іншими виродками. На відміну від вільних модераторів, моральні консерватори не відчувають докорів сумління за залучення уряду до регулювання Інтернету. Вони були рушійною силою Закону про благопристойності комунікацій та присутність дітей в Інтернеті, Закону про охорону Інтернету в бібліотеках, і працювали над тим, щоб підштовхнути ухвалення Закону про заборону азартних ігор онлайн. Вони також об'єднали зусилля із ліберальними соціальними інженерами в прагненні до правил «мережевого нейтралітету», побоюючись, що Інтернет провайдери (ISP) якимось чином дискримінують християн онлайн. Ця група стверджує, що, тому що Інтернет є публічним простором, необхідні деякі правила і закони для управління поведінкою. Вони не вважають, що технологія може вирішити всі соціальні проблеми, а, навпаки, вважають, що Інтернет, як правило, в подальшому гнобить культуру. Тим не менш, у деяких випадках вони сприймають Інтернет у якості інструменту, про що свідчить колишній секретар К-12 з освіти Вільям Беннетт з Інтернет проекту по домашньому навчанню. Загалом, моральні консерватори не визнають осіб, уповноважених антигромадською поведінкою, вони не визнають корпорацій, що сприяють такій поведінці. Прикладами є такі групи, як Християнська коаліція і Фокус на сім'ю з усього світу, зокрема, такі країни, як Індонезія, Таїланд, Саудівська Аравія та інші релігійно-консервативні країни, спрямовані на обмеження діяльності в Інтернеті.

Управлінці старої економіки

Ця група вважає, що, по суті, немає нічого унікального в Інтернеті, і що він повинен регулюватися таким же чином, як держава регулює все інше, у тому числі старі технології. Існує певне почуття терміновості серед деяких виборних посадових осіб, державних чиновників, і «суспільно заінтересованих» адвокатів, які вважають, що кіберпростір знаходиться в стані, близькому до анархії – є притулком для злочинців, шахраїв, і хижих корпорацій. Приклади цієї групи включають в себе співробітників правоохоронних органів, які прагнуть обмежити використання шифрування та інших інноваційних технологій, ветеранів регламентарної війни, які передували розпаду «Ma Bell», правових аналітиків, що працюють над соціальною інженерією аналітичних центрів, а також чиновників, які прагнуть встановлення обмежувальної нормативної бази в галузі широкосмугового доступу. Оскільки мова йде про старих регуляторів економіки, то Закон про зв'язок 1934 р. (або, можливо, його оновлення 1996) відповіли на всі питання, які можуть виникати у зв'язку з Інтернетом. Більше того, європейські, китайські та інші старі регулятори економіки зарубіжних країн побоюються, що за відсутності більшого регулювання, їхні країни будуть осторонь від левіафанського американського Інтернету.

Технологічні компанії та торгові асоціації

Ця група включає в себе ряд організацій від політично зорієнтованого програмного забезпечення, гігантів з виготовлення програмного забезпечення та комунікацій до Інтернет стартапів. Ці підприємства, від досвідчених IBM, AT&T та HewlettPackard до ще молодих CiscoSystems та Microsoft, а також більш менш досвідчених Google та Facebook, так само, як і торгові асоціації такі як Асоціація з конкурентоспроможної технології, усвідомлюють, що торгівля, податки, нормативні та інші питання державної політики

все більше впливають на їх позиції загалом та на позиції у конкуренції. У той час, як гравці цієї групи (як і в сфері обслуговування клієнтів в офісах) не мають такого ж рівня

ідеологічної згуртованості як у вищевказаних групах, вони мають певний набір інтересів, який виправдовує їх угруповання. Вони розуміють, що погодження на чийсь напрям в політиці є більш ніж правильним. Це вимагає переконливої гри у ті самі правила. Час від часу деякі технологічні компанії можуть зайняти кібер лібертаріанську позицію, тобто стверджувати, що Інтернет повинен бути вільним. Як правило, вони роблять це тільки для того, щоб уникнути регулювання, яке могло б поставити їх у невигідне конкурентне становище. У цілому, технологічні компанії, як правило, вважають, що регулювання може бути як вигідним, так і шкодити; вони не проти всіх правил, а виступають за ті, що вигідні для них (а іноді і «невигідні» для конкурентів)[3]. Вони також іноді захищають ту політику, яка сприяє технологічній галузі чи економіці у цілому. У той час як телекомунікаційні компанії вже давно визнали важливість уряду, більшість IT компаній ігнорують уряд і політичні питання, і дуже зайняті створенням технологій, які ведуть до цифрового світу. Але з ростом та досвідом ці компанії усвідомлюють, часто через болючий досвід, те, як вирішені у Вашингтоні питання можуть вплинути на їх практику, а багато які з них перетворилися на політично проникливі. І в той час, як окремі технологічні компанії можуть займати різні позиції із різних питань, ці відмінності у значній мірі виходять із інтересів бізнес-моделей, а не ідеологічних поглядів про ринок або уряд.

Сфера обслуговування клієнтів в офісах

У цю групу входять компанії, професійні групи та спілки, які живуть із дотримання принципів класичної економіки. Вони включають в себе як виробників, так і дистриб'юторів з посередниками (наприклад, роздрібна торгівля, автодилери, оптові продавці вина, аптеки, оптика, агенти з нерухомості, профспілки, що представляють інтереси працівників у цих галузях). Багато хто побоюється, і часто небезпідставно, що Інтернет затримує їх розвиток, поки інші працюють над тим, щоб комерціалізувати власні справи. В останні роки спостерігається розширення прірви між сферою обслуговування клієнтів в офісах та дистриб'юторами і посередниками (а також спілками, які представляють їх працівників). Виробники почали усвідомлювати, що вони можуть використовувати Інтернет для безпосереднього спілкування зі своїми споживачами, оминаючи (або хоча б мінімізуючи) роль обслуговування клієнтів в офісах. Посередники і союзи активно працюють над тим, щоб цього не сталося або, принаймні, щоб якомога більше відстрочити, не соромляться заручатися підтримкою уряду з метою «зрівняння умов гри». Звичайно, протистояння, яке триває вже досить давно за оподаткування продажів через Інтернет, представляє собою боротьбу між сферою обслуговування клієнтів в офісах і технологічними компаніями. Крім того, профспілка робітників продуктового магазину у Каліфорнії нещодавно вимагала прийняття закону щодо ускладнення системи самообслуговування на виїзді з магазинів[4].

РОЗМЕЖОВУВАЛЬНА ЛІНІЯ

Відношення вищезгаданих груп до політики щодо Інтернету можна розмістити у двох векторах:

Індивідуальні можливості vs. Соціальні Вигоди

У цьому розділі розмежовуються групи на основі уявлень про головну мету Інтернету. У певному сенсі це класична напруженість між свободою та рівністю. Тим не менш, вона виходить за рамки представлення напруженості між індивідуалізмом та общинністю, причому перша теорія виступає за індивідуальні права, а друга – кидає виклик соціальним вигодам, таким як економічне зростання, безпека і покращення якості життя.

Ті, хто входить у категорію за індивідуальні можливості,вірять, що головною функцією IT є звільнення особи від контролю або від залежності з боку великих організацій. Для них

Інтернет є величезним, відкритим і глобальним комунікаційним середовищем, призначеним головним чином для того, щоб люди могли вільно спілкуватися і мати вільний доступ до інформації. Обговорюючи будь-яке питання, вони розглядають його, головним чином, через призму того, як воно впливає на індивідуумів, а не на суспільство у цілому. Таким чином, питання про мережевий нейтралітет висвітлюється з точки зору його впливу на індивідуальну свободу діяти за бажанням. Такі групи бажають зрівняти як малих гравців, так і досвічених, що означає підтримку малих провайдерів, невеликих ЗМІ, або окремих відкритих кодерів джерела.

Ті, що належать до табору тих, хто вірить у соціальні вигоди, притримуються думки, що основною роботою Інтернету є збільшення продуктивності в економіці, заохочення уваги і ефективності роботи уряду, а також сприяння розвитку нових і більш якісних послуг для споживачів в цілому. Вони, як правило, досліджують окремі питання IT політики через призму того, як вони впливають на общинні інтереси, і готові прийняти компроміси за особисту свободу, якщо вони сприяють підвищенню загального економічного чи соціального благополуччя.

Ті, хто входить у категорію за індивідуальні можливості, вірять, що головною функцією IT є звільнення особи від контролю або від залежності з боку великих організацій. Для них Інтернет є величезним, відкритим і глобальним комунікаційним середовищем, призначеним головним чином для того, щоб люди могли вільно спілкуватися і мати вільний доступ до інформації.

Кібер лібертаріанці і соціальні інженери в цілому вважають, що Інтернет має зосереджуватися тільки на індивідуальних можливостях. Вони обурюються його комерціалізації та вважають неминучим розширення прав і можливостей. Індивідуалісти, як уже говорилося раніше, вважають, що Інтернет повинен виконувати, головним чином, освітні послуги та слугувати соціальним інструментом. Вони бояться, що можливості розширення прав будуть відібрані потужними транснаціональними корпораціями та урядами, які змінять Інтернет у своїх власних вузьких цілях (прибуток у першому випадку, контроль – у другому). Обидві групи вважають, що хакери і пірати виступають єдиними борцями свого роду у боротьбі проти жадібних та корпоративних левіафанських урядів.

Сфера обслуговування клієнтів в офісах та також старі економічні регулятори вбачають IT в інструментальному сенсі, як призначений для торгівлі, а розширення – на користь суспільства. Їм просто не подобається у що перетворився Інтернет, чи то у конкуренцію з боку доткомів чи розповсюдження шифрування, яке є об'єктом пильного стеження урядом, цензура та ін. Технологічні компанії також вбачають у ньому більше інструментарію, стверджуючи, що його робота має сприяти ефективній комерції. Моральні консерватори не бажають надання можливостей для індивідуалістів, оскільки це призведе до ще більшої антисоціальної поведінки, а також вони не бажають, аби корпорації сприяли такій поведінці.

Модератори та вільні маркетологи займають проміжне положення. Вони вважають, що цифрова економіка відкриває великі перспективи для підвищення продуктивності і поліпшення життя суспільства. У той же час, вони вбачають у Інтернеті можливість створення спільнот, підвищення рівня освіти, більшого контролю за власним життям. Вільні маркетологи не вірять у те, що індивідуальні

інтереси обов'язково повинні враховувати корпоративні інтереси компанії, оскільки вбачають в них юридичних осіб, хоча індивідуальні права для них (на відміну від інтересів) є найголовнішими.

Невтручання vs. Урядове регулювання

Групи у цій категорії розділяються за ступенем, в якому уряд накладає формальні правила на IT та Інтернет.

Кібер лібертаріанці і меншою мірою вільні маркетологи вважають, що Інтернет має

управлятися користувачами. Ці групи притримуються позиції невтручання. Вони вважають, що Інтернет є унікальним і може вести себе неочікувано, модель того, як має бути організоване суспільство. Вільні маркетологи вважають, що суть Інтернету полягає у тому, що існує суспільство з низькими операційними витратами і ринками. (Економіст Рональд Коуз припустив, що високі транзакційні витрати породили великі організації.)

З іншого боку – групи на боці державного регулювання, які бачать Інтернет як новий «Дикий Захід», який кличе шерифа для захисту вразливих громадян від нав'язливого уряду і прибутків жадібних корпорацій. Моральні консерватори, соціальні інженери, а також прихильники класичної теорії економіки, як правило, дотримуються цієї точки зору, стверджуючи, що уряд може обмежити діяльність компаній. Так що сфери з обслуговування клієнтів в офісах, хоч і в меншій кількості, але в принципі не можуть виступати у ролі способу постійного ослаблення економічного становища.

Модератори та технічні компанії займають «золоту середину». Вони вбачають в Інтернеті унікальність і вважають, що загалом він потребує невеликого регулювання, якщо IT прагнуть зростати. Проте у деяких ключових галузях, як наприклад, кібер безпека та захист авторських прав, вони вважають, що Інтернет потрібно жорстко регулювати, особливо уповноважити правоохоронні органи карати злочинців. З інших питань, таких як конфіденційність несекретних даних, мережевий нейтралітет, вони притримуються думки, що саморегулювання для спільних урядових та ділових партнерств є не найкращим рішенням для захисту споживачів, оскільки так компанії набувають гнучкості.

ITIF був створений для просування прагматичних рішень у коло все більшої кількості політик щодо технологічних проблем. Ми вважаємо, що зростання цифрової економіки та суспільства залежить від синтезу цих поглядів: правильна позиція лежить на перетині двох осей. Дихотомія між індивідуальними можливостями та інституційною ефективністю не є грою з нульовою сумою. Індивідууми приносять користь – як соціальну, так і економічну, у випадках, коли уряди і корпорації працюють більш ефективно і результативно, коли особи інформовані і здатні робити вибір. Неглибоке регулювання важливе для підтримки гнучкості, необхідної для роботи у швидкозростаючій економіці, але дії уряду також необхідні, щоб вселити підприємствам і споживачам впевненість, що Інтернет не є вертепом розбійництва або протистояння добросовісній конкуренції, а допомагає прискоренню цифрового перетворення (наприклад, повсюдне використання IT в економіці і суспільстві).

ТРИВАЮЧІ ДЕБАТИ

Звичайно, вищезазначена типологія недосконала, при чому багато осіб та організацій входять до більш ніж однієї групи, або навпаки не входять в жодну. Але коли людина спостерігає за головними політичними баталіями, які стосуються майбутніх інформаційних технологій, стає очевидною конкуренція між фракціями. У якості прикладів розглянемо останні дебати по чотирьох ключових питаннях: конфіденційність, оподаткування, захист авторських прав і мережевий нейтралітет.

Конфіденційність

У той час, як позови цього року проти Facebook і Google Street View, що є найбільш наочними прикладами, збір і використання корпораціями і урядом особистої інформації про користувачів є джерелом багатьох емоційних дискусій. Регулятори за класичною теорією та соціальні інженери хочуть нав'язати широкомасштабні правила, які б дали людям контроль над «своїми» особистими даними. І поки вони знаходяться в стані очікування, рекламуючись як справжня, істинна Інтернет модель для контенту, вони бажають обмежити ефективність Інтернет реклами, і рівень доходу від неї, пояснюючи це прихованим страхом.

Багато технологічних компаній прагнуть повної свободи для збору особистих даних, за умови, що вони відповідають політиці конфіденційності. І хоча деякі технологічні компанії підтримують помірні «повідомлення і вибір» законодавства, більшість компаній, як і раніше, побоюються будь-якого федерального регулювання приватного життя, навіть якщо вони визнають необхідність федеральних законів, щоб упередити усі більш неспокійні законодавчі збори штату від утвердження різних законопроектів Інтернет конфіденційності .

Регулятори старого типу економіки та соціологи прагнуть нав’язати широкомасштабні правила гри, які б надали людям контроль над «власними» особистими даними. І поки вони знаходяться в стані очікування, рекламуючись як справжня, істинна Інтернет модель для контенту, вони бажають обмежити ефективність Інтернет реклами, і рівень доходу від неї, пояснюючи це прихованим страхом.

Кібер лібертаріанці очікують, що технології вирішать ці проблеми. Наскільки їм відомо, користувачі повинні нести відповідальність за своє власне особисте життя та застосовувати інструментарій для захисту своїх персональних даних.

Вільні маркетологи відкидають потребу в єдинстві законодавства, стверджуючи, що шкода від регулювання буде переважати переваги і що державне регулювання, ймовірно, буде заважати індивідуальній свободі і вибору, у тому числі, основних прав на свободу слова. У той час, як помірковані турбуються, що занадто суворі закони про конфіденційність придушать інновації і збільшення витрат на споживачів, вони також вважають, що за відсутності будь-яких правил користувач не розвиватиме довіру, необхідну для цифрової економіки та суспільства заради процвітання.

Ситуація із Facebook є прекрасним прикладом того, як ці питання розігруються. Ця соціальна мережа оголосила про введення двох нових функцій у цьому році: миттєва персоналізація, яка дозволяє користувачам обмінюватися даними з їх Facebook профілю з дружніми сайтами, і соціальні плагіни для сторонніх веб-сайтів, які дозволяють користувачам легко обмінюватися веб-сторінками із своєї соціальної мережі за межами Facebook[5].

Соціальні інженери виступили на знак протесту, вимагаючи, щоб обмежувальні постанови уряду заборонили подібну практику. Деякі, як Дана Бойд, науковий співробітник Центру Беркман Гарварду, зайшла так далеко, що стверджувала, що Facebook функціонує як комунальне підприємство і повинно регулюватися як таке[6].

Facebook не поспішав реагувати, спочатку орієнтуючись на просування своїх інноваційних інструментів. Тим не менше, пізніше він достойно відповів, пропонуючи своїм користувачам зручнішу та прозорішу систему контролю за конфіденційністю.

ITIF та інші модератори, а також вільні маркетологи стверджують, що державний контроль над політикою конфіденційності соціальних мереж не є необхідною для захисту споживачів і, крім того, шкодить майбутнім інноваціям. У період палких політичних дискусій державне втручання, ймовірно, може стати нормативним перебором. У той же час, стверджують, що стурбованість конфіденційністю особистих даних і конфіденційних даних (фінансової або медичної інформації, наприклад) мають бути вирішені за допомогою комплексних галузевих кодів саморегулювання, запроваджених урядом (наприклад, FTC заходи проти компаній, які не сприймають саморегулювання, а згодні на недобросовісну практику із торгівлі).

Коли справа доходить до збору і використання даних урядом, коаліції змінюють свій порядок. Кібер лібертаріанці, соціальні інженери і маркетологи співпрацюють усі разом. Якщо мова йде про уряд, який збирає додаткову інформацію або використовує існуючу інформацію за новим призначенням, проти нього зазвичай виступають. Протестуючи проти зростаючої практики міст введення червоного світла, колишній республіканський лідер більшості в Палаті Дік Армі зауважив: «Це повномасштабна система спостереження. Чи справді ми хочемо створити суспільство, де ніхто не може ходити по вулиці, не будучи поміченим?»[7]

Високотехнологічні компанії були втягнуті у дискусію з приводу використання державою та доступу до даних, що у значній мірі засновано на ділових інтересах. Технологічні компанії, безпосередньо зацікавлені у наданні державі технологій для збору інформації (наприклад, смарт-карти і біометричні дані) виступили сильними прихильниками конкретних ініціатив. Інші технологічні компанії, турбуючись, що доступ уряду до даних може обмежити торгівлю або скоротити споживчу довіру до Інтернету (наприклад, у сфері заповнення анкет та заяв, де споживчі дані зберігаються віддалено), закликали уряд ввести обмеження на доступ до даних.

Чи можна знайти «золоту середину» у дискусії з приводу урядової конфіденційності, залишається відкритим питанням. Модератори підтримують впровадження нових технологій урядом, якщо буде чітко доведено, що вони виконують важливу суспільну місію, і якщо потенційні проблеми конфіденційності будуть ефективно вирішуватися, особливо щодо проектування захисту конфіденційності в мережах. У той же час, вони підтримують введення адекватних правил і захисту доступу до цих даних з боку уряду.

Податки на Інтернет продажі

Податкова політика є спірним питанням у будь-яких умовах, але, можливо, ще більш спірним, коли мова йде про Інтернет. Збір державних і місцевих податків з продажів в Інтернеті є настільки нез’ясованим питанням, що п’ятнадцять років після того, як вперше було його піднято, воно все ще продовжує обговорюватися. Прихильники старої економіки виступають за те, щоб податки з продажів збиралися і були введені високі податки на послуги зв'язку для підтримки їх доходів. Штат Колорадо навіть зобов’язав продавців в Інтернеті надавати інформацію про імена та власне покупки

жителів Колорадо (таким чином, щоб штат між збирати «споживчу» інформацію з Інтернет-магазинів). Компанії з обслуговування клієнтів через офіси прагнуть, аби податки були введені аби зберегти свої конкурентні позиції по відношенню до Інтернет продавців. Деякі соціальні інженери виступають не тільки за збір податків із продажів, а й за спеціальні податки на використання широкомасштабного доступу на субсидування малозабезпечених і сільських домогосподарств.

На відміну від вищезгаданого, технологічні компанії, які займаються Інтернет торгівлею, не бажають отримати на себе тягар збору податків і вони не хочуть втрачати свої цінові переваги. Крім того, вони не хочуть аби широко розповсюджений телефонний зв'язок несправедливо обкладався за вищими ставками. Інші, як наприклад, представники вільного ринку і кібер лібертаріанці, виступають проти Інтернет податку на реалізацію з принципу. Вони вважають, що «чим менше податків, тим краще», особливо, коли мова йде про просування нової цифрової економіки.

Кібер лібертаріанці, технологічні компанії і представники вільного ринку, швидше за все, продовжуватимуть виступати проти надання державам права на введення податку з продажів в Інтернеті за межами своїх кордонів. Уряди штатів будуть тиснути, виступаючи за таке право, посилаючись на їх великий бюджетний дефіцит. І, швидше за все, модератори виступлять на користь державних податків з продажу, особливо якщо вони будуть пов'язані угодою, що змусить держави скасувати закони та нормативні акти, які дискримінують електронну комерцію, і якщо оподаткування буде запроваджено таким чином, щоб мінімізувати адміністративне навантаження. Зараз, однак, дискусія все ще триває, а держави юридично не в змозі збирати податки з продажів, і більшість держав встановлює високі, дискримінаційні податки на послуги зв'язку.

Кібер лібертаріанці стверджують, що вік Інтернету знаменує припинення прав інтелектуальної власності, тому що стає складно забезпечувати захист авторських прав на цифрових носіях (звідси і походить відома назва «інформація прагне свободи»).

Охорона авторського права

Оскільки практично всі ЗМІ стали дублюватися в електронному форматі, захист авторських прав став нагальною проблемою. Майже десять років тому тільки почалися спори про копіювання музики системою Napster. Розповсюджені файлообмінні технології, у поєднанні з комп'ютерними, можуть копіювати цифрові файли з CD-дисків або DVD-дисків, а високошвидкісні широкомасштабні мережі, які можуть швидко передавати великі файли, означають, що «цифрове піратство» вийшло на глобальний рівень. Кібер лібертаріанці стверджують, що вік Інтернету знаменує припинення прав інтелектуальної власності тому, що стає складно забезпечувати захист авторських прав на цифрових носіях (звідси і походить відома назва «інформація прагне свободи»). Ці прихильники стверджують, що некомерційні файлообміни, захищені авторським правом засобів масової інформації, є однією з форм добросовісного використання, як вони стверджують, і є законними, відповідно до закону про авторське право. Наприклад, кампанія Електронного форуму свободи «Нехай грає музика» протестує проти копіювання музики і файлів кіноіндустрії. В ідеальному світі деякі багаті компанії «дот-коми» створять окрему країну на безлюдному острові, пов'язану з рештою світу за допомогою високошвидкісного волоконно-оптичного кабелю та хостингу масивних комп'ютерів з рогом достатку піратського цифрового контенту, і все це – за межами національних законів про авторське право.

Багато соціальних інженерів займає позицію кібер-лібертаріанців, хоча і з абсолютно різних причин. Вони побоюються, що технологія надасть можливість власникам авторських прав контролювати зміст, що традиційні поняття добросовісного використання стають неактуальними. І вони бояться, що управління правами (DRM) на цифрові технології стане настільки суворим, що діяльність споживачів (як здатність відтворювати музичні файли на більш ніж одному пристрої) буде заборонена. Обидва активно виступають проти будь-яких зусиль з поліпшення управління крадіжками авторських прав, які можуть зазіхати на свободу особи або окремих прав, як свобода слова (наприклад, дозвіл

ISP фільтрувати незаконний контент, блокувати сайти, які незаконно порушують авторські права і розробку міжнародних договорів, таких як АСТА (Торговельна угода по боротьбі з контрафакцією) для зміцнення та гармонізації боротьби з піратством).

Через їх акцент на права власності, найбільші прихильники вільних модераторів, як правило, рішуче підтримують зусилля з обмеження крадіжки цифрового авторського права. Але, з акцентом на свободу, лише деякі стверджують, що свобода перевершує власність, надання прав інтелектуальної власності уряду зводиться до надання санкціонованої державою монополії[8]. На їх думку, люди повинні вільно використовувати цифровий контент так, як вони хочуть, і саме власники контенту, а не інші особи, такі як цифрові посередники, повинні нести відповідальність за охорону використання їх змісту.

Модератори також підтримують зусилля з обмеження крадіжки цифрових авторських прав, вважаючи, що це не правильно, і що надійна цифрова екосистема вимагає стимулів до виробництва часто дорогого цифрового контенту. У той же час, однак, вони не є абсолютними, і, зокрема, прагнуть збалансувати витрати і вигоди захисту копірайта, особливо в рамках сумлінного використання.

Соціальні інженери є прихильниками мережевого нейтралітету, але вони співпрацюють з прихильниками традиційної економіки і кібер лібертаріанцями.

Компанії з обслуговування клієнтів в офісах, у тому числі Асоціація звукозаписної індустрії Америки – спочатку працювали у напрямку блокування розвитку нових технологій, полегшення правил гри і, можливо, завантаження піратської музики. Але більше десятиліття потому такі галузі борються із технологіями не настільки сильно, як вони працюють над розвитком і використанням технологій, які можуть протидіяти крадіжкам авторських прав, та переслідують організації, які дозволяють крадіжки широко поширеного цифрового контенту (наприклад, як і шведський сайт Pirate Bay). І незважаючи на те, як вони з усіх сил намагалися впоратися з піратством музики і кіно, виробники контенту в значній мірі змирилися з реаліями цифрової ери. Вони розпочали надання юридичних, доступних і вигідних для споживача засобів купівлі або перегляду цифрового контенту захищеного авторським правом з магазину iTunes Apple і Hulu, що є найбільш яскравими прикладами.

Хоча в цілому вони схильні до позиції контент-провайдерів авторських прав, багато високо технологічних компаній (наприклад, Інтернет провайдери, пошукові системи, соціальні мережі) бояться, що федеральний уряд буде вимагати від них скорегувати свій бізнес так, щоб стати наглядачами за копіюванням контенту, або через необхідність вжити заходи проти їхніх клієнтів, або шляхом створення захисту контенту за допомогою дорогих технологій. Знову ж таки, постає питання, чи може бути знайдений компроміс, гарантуючи, що власники контенту будуть мати правовий захист і економічні стимули, вони повинні продовжувати виробництво захищених авторським правом матеріалів без накладення надмірно великого навантаження на технологічні компанії, і розширення своїх клієнтів.

Мережевий нейтралітет

Надзвичайно спірним питанням стало те, що мережевий нейтралітет відноситься до ідеї про те, що окремі мережі колективного формування Інтернету контролюються користувачами, а не їх власниками і операторами. У той час, як мережеві оператори знаходяться в унікальному становищі, тобто, щоб керувати своїми ресурсами, прихильники мережевого нейтралітету вважають, що не може існувати довіри до того, щоб використовувати свої знання на благо спільноти користувачів Інтернету.

Соціальні інженери є прихильниками мережевого нейтралітету, але вони співпрацюють з прихильниками традиційної економіки і кібер лібертаріанцями. Дійсно, соціальний інженер Тім Ву придумав загадковий термін «мережевий нейтралітет». Ці групи побоюються, що унікальна природа Інтернету знаходиться під загрозою з боку сил чинних телекомунікаційних і кабельних компаній, що надають послуги широкомасштабного доступу. Якщо такі компанії доб'ються свого, нейтралісти бояться, що Інтернет буде йти шляхом кабельного телебачення, «величезної пустелі», де елітарні програми, такі як «The Wire» конкурують з популістськими програмами, такими як American Idol, які підтримуються рекламними агентствами.

Вільні провайдери вбачають у мережевому нейтралітеті ще один напад уряду на Інтернет, останній оплот свободи. Вони стверджують, що ринкові сили і споживчий вибір завжди будуть дисциплінувати будь-які анти-споживчі порушення мережевого нейтралітету, у той час, як цивільне правопорушення законів буде слугувати зручним інструментом для усунення будь-яких порушень.

Питання державної політики, яка оточує IT революцію, більше не є інтермедією або просто політичною дискусією між невеликим колом професіоналів, а також не є королівських шляхом до утопії незліченного багатства і нескінченного прояву волі.

Технологічні компанії розділилися з цих питань, в основному, навколо яких вони і працюють. Ті технологічні компанії, що надають послуги в мережі (наприклад, Інтернет провайдери і великі виробники обладнання), як правило, виступають проти правил на підтримку мережевого нейтралітету (принаймні, щодо самої мережі), а компанії, чиї бізнес-моделі залежать від використання мережі для отримання доступу до клієнтів (наприклад, контент і сервіс-провайдери, як Google) є або нейтральними, або виступають на стороні більш сильного регулювання (принаймні щодо інфраструктури, на відміну від інших частин Інтернету «стеку», наприклад, додатків). Проте, ці відмінності почали дещо стиратися, про що свідчить недавня спільна заява про мережеву нейтральність оголошена Google і Verizon.

Модератори взагалі вбачають в Інтернеті проект, який розробляється по ходу. Модератори вважають за позитивне, що виробники мережевого устаткування поліпшують Інтернет, і що оператори одноособово володіють вузькоспеціальними знаннями, необхідними для забезпечення справедливого доступу до Інтернет ресурсів. Але вони також усвідомлюють, що помірна конкуренція не працює таким чином і так само ефективно, як у деяких мережевих ринках, як це відбувається на ринках загального призначення споживчих товарів і послуг. Іншими словами, деякі мережеві ринки перебувають поза конкуренцією (через мережеві ефекти ринкового впливу), так що ринки самі по собі не є достатніми для забезпечення відкритого Інтернету для кожного[9]. Роль держави в регулюванні Інтернету має полягати у забезпеченні всіх споживачів користуванням плодами інвестицій та інновацій, але тільки таким чином, щоб не обмежувати постійні інвестиції та інновації.

Оскільки ці та інші питання, як і раніше, виносяться на обговорення в законодавчих органах і громадах по всій країні, урядові чиновники повинні шукати рішення, які збалансують потреби людей з інтересами суспільства, і які запропонують убезпечення кодифікованих законів, якщо це необхідно і забезпечать гнучкість, коли будуть діяти неформальні правила. Дебати щодо технологічної політики тривають, і різні фракції наполягають на рішеннях, які відповідають їх ідеології та інтересам, політиці, які стимулюють ріст і життєздатність цифрової економіки і не буде заведена в крайність, а замість цього – в життєвий цикл.

МАЙБУТНЄ ЦИФРОВОЇ ПОЛІТИКИ

Дехто може посперечатися, що ці проблеми є тимчасовими і відхилити думку про те, що цифрова економіка є важливою і досі розвивається. Але є всі підстави вірити у протилежне. Дебати, які настроюють онлайн споживачів проти постійних посередників, ймовірно, продовжаться, з розвитком нових форм поширення Інтернету. Поява набагато швидших і всюдисущих провідних і бездротових широкомасштабних мереж означатиме більшу кількість американців-користувачів цих мереж і більшу кількість моделей розвитку бізнесу, щоб скористатися ними. Дані, отримані за допомогою нових технологій, таких як бездротові локаційні системи, цифровий підпис, інтелектуальні транспортні системи, електричні мережі, IT для охорони здоров'я та радіочастотні ідентифікаційні пристрої – деякі використовувані урядом, інші приватним сектором будуть стимулювати нові питання конфіденційності серед соціальних інженерів і їх прибічників. У певному сенсі, цифрова революція була настільки успішною, що набагато більш ранні аналогові політичні питання стали цифровою історією, а з іншого боку, політичні питання майбутнього залишаються несформованими, саме тому, що технології змінюються так швидко.

Питання державної політики, яка оточує IT революцію, більше не є інтермедією або просто політичною дискусією між невеликим колом професіоналів, а також не є королівським шляхом до утопії незліченного багатства і нескінченного прояву волі. Стратегії боротьби уже розроблені, а питання цифрової політики є серйозним і складним. Цифрова політика буде відігравати надзвичайно важливу роль у нашому майбутньому, якщо навіть не найважливішу.

ЗАУВАЖЕННЯ

- Для більшої інформації щодо створення Інтернет політики зверніться до "Cyber-Libertarianism: The Case for Real Internet Freedom" http://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet- freedom/; та "Are You an Internet Optimist or Pessimist? The Great Debate over Technologys Impact on Society" http://techliberation.com/ 2010/01/31/ are-you-an-internet-optimist-or-pessimist-the-great-debate- over-technology%E2%80%99s-impact-on-society.
- "Declaration of the Independence of Cyberspace", https://projects.eff.org/~barlow/Declaration-Final.html
- Погляд технологічних фірм на суспільну політику: ACT's "Understanding the IT Lobby: An Insider's Guide", (Washington, DC: ACT), 2008, http://actonline.org/publications/2008/08/0 5/understanding-the-it-lobby-an-insiders-guide/.
- Robert D. Atkinson, "Innovation and Its Army of Opponents," *Businessweek.*, September 23, 2010, http://search.businessweek.com/Search?searchTerm=innovation+and+its+army+of+opponents&resultsPerPa.
- Для більш детальної інформації зверніться до: Daniel Castro, "The Right to Privacy is Not a Right to Facebook," (Washington, D.C.: Information Technology and Innovation Foundation, April 2010), http://itif.org/publications/facebook-not- right; та Daniel Castro, "Facebook is Not the Enemy," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http://itif.org/publications/facebook-not-enemy.
- Danah Boyd, "Facebook is a utility; utilities get regulated," *Apophenia*, May 15, 2010, http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.
- Thomas C. Greene, "Cops using high-tech surveillance in Florida," *The Register,* July 2, 2001, http://www.theregister.co.uk/2001/07/02/cops_using_hightech_surveillance/.
- "Against Intellectual Monopoly," (Washington, D.C.: Cato Institute, 2008), http://www.cato.org/event.php?eventid=5362.

Richard Bennett, "ITIF Comments on FCC Broadband Reclassifying," Information Technology and Innovation Foundation (August 10, 2010), http://www.itif.org/publications/itif-comments-fcc-broadband- reclassifying.

ПОДЯКА
Автор висловлює подяку тим, хто зробив внесок у написання даного звіту: Річарду Беннетту, ITIF; Даніелю Кастро, ITIF; Моргану Ріду, ACT; БерініСзоці, Фонд прогресу і свободи; АдамуСієру, Фонд прогресу і свободи; Сью Уандер, Стіву Нортону і Кетрін Ангтадт, ITIF. Будь-які помилки та упущення належать лише автору.

ПРО АВТОРА
Д-р Роберт Аткінсон є президентом Фонду інформаційних технологій та інновацій. Він також є автором книги «Минуле і майбутнє американської економіки: Довгі хвилі інновацій, які живлять цикли росту» (Едвард Елгар, 2005). Доктор Аткінсон отримав ступінь доктора філософії з міського та регіонального планування в Університеті Північної Кароліни в Чапел-Хілл в 1989 році.

ПРО ITIF
Фонд інформаційних технологій та інновацій (ITIF) знаходиться у Вашингтоні, округ Колумбія, і є мозковим центром у розробках інноваційної політики та вивченні того, як досягнення в галузі інформаційних технологій створюють нові економічні можливості для поліпшення якості життя. Організація є некомерційною та політично незалежною, пропонує прагматичні ідеї, які суперечать вільні економічної теорії, народжені задовго до першого комп'ютера і задовго до виникнення сучасного Китаю. ITIF, заснований в 2006 році, присвячений розвитку і заохоченню нових способів мислення щодо технологій керованої продуктивності, конкурентоспроможності та глобалізації, що э вимогами 21-го століття.
ITIF публікує доповіді з питань політики, проводить форуми та обговорення, консультує виборних посадових осіб та їх співробітників, і є активним ресурсом для засобів масової інформації. Він розвиває нові творчі пропозиції політиків, аналізує існуючі політичні питання через призму зміцнення інновацій та продуктивності, і виступає проти політики, яка перешкоджає цифровим перетворенням і нововведенням.

Фонд інформаційних технологій та інновацій є 501(C)3 некомерційною організацією.

ДЛЯ ДОДАТКОВОЇ ІНФОРМАЦІЇ ЗВЕРТАЙТЕСЯ ЗА ТЕЛЕФОНОМ 202.449.1351, ЕЛЕКТРОННОЮ ПОШТОЮ**MAIL@ITIF.ORG**, АБО ВІДВІДАЙТЕ НАШ САЙТ**WWW.ITIF.ORG**.

4.2.3. Мілтон Мюллер. Чи знаходимося ми в стані цифрової Холодної війни?

Чи знаходимося ми в стані цифрової Холодної війни?

Мілтон Мюллер (Milton Mueller)

Представлено на семінарі глобального управління в Інтернеті GigaNet ,17 травня 2013 Женева, Швейцарія.

Про концепцію цифрової Холодної війни щодо цифрової мережі Інтернет я вперше почув після конференції з міжнародних телекомунікацій, що проходила в Дубаї (Dubai World Conference on International Telecommunications (WCIT). Там країни світу, здавалося, розділили свої погляди з приводу майбутнього управління Інтернетом навпіл. Один письменник навіть дав назву цьому явищу - "Ялта Інтернету" (Klimburg 2013).

Концепція набрала своєї сили з публікацією доповіді у лютому 2013 року, приписуючи систематичне кібер-шпигунство підрозділу китайської Народно-визвольної армії. (Mandiant 2013). Раптом стало відомо, що американські фірми із гарантування кібербезпеки мали прямі зв'язки з американськими військовими, що відкрито говорили про довгострокові, систематичні загрози з боку іноземної держави і це нагадувало застереження ери 1960-их щодо комуністичного плану світового панування. Журналісти та ЗМІ підхопили цю тему. Колишній глава ЦРУ фактично порівняв використання Stuxnet (комп'ютерного хробака) з Хіросімою.

Моя перша реакція на цю метафору була інтуїтивно негативною. Я вважав, що сам акт обрамлення проблеми таким чином сприяв мілітаризації Інтернету і віщував похмуре майбутнє: перспективу Інтернет – політики, де домінують інтереси національної безпеки та конфлікти між великими державами. Проте я не міг не почати думати про подібне. Що ж саме було невірним в характеристиці конфліктів кібер-простору як "Холодної війни"? Які ж будуть політичні наслідки, якщо ми й далі продовжимо це робити? Для того, щоб відповісти на ці питання, необхідно дослідити метафору, а не відкидати її рішуче, без будь-яких роздумів.

Через це я змінив своє ставлення до цього питання. Хоча я, як і раніше, відкидаю цінності й політичні уподобання нових прихильників Холодної війни, все ж простежується насправді зростаючий зв'язок між кібер-політикою та національною безпекою. Правдою є також і те, що політичні конфлікти між захисниками Інтернет-свободи і захисниками державного регулювання вплутали кіберпростір в міждержавні конфлікти.

Крім того, з обох сторін є зацікавлені групи та ідеологи, які хочуть активно сприяти цифровій Холодній війні. Ці проблеми не зникнуть, якщо ми відмовляємося визнати або обговорити концепцію «кібер Холодної війни». І дійсно, ігнорування або байдуже ставлення до цієї паралелі з Холодною війною, ймовірно є так само небезпечним фактом, як абсолютне її сприйняття.

Кращою відповіддю на виклик був би історично обгрунтований розгляд характеру та природи Холодної війни, в поєднанні з неупередженим аналізом його подібності та відмінності з нинішньою кібер-ситуацією. Що ж ми можемо дізнатися з цього порівняння?

Тривала війна

Перша здогадка приходить від пізнання та більш глибокого осмислення того, чим же була Холодна війна насправді. У своїй книзі «Щит Ахілла» Філіп Боббіт переконливо доводить, що те, що ми зараз називаємо Холодною війною, було в дійсності останнім епізодом епохальної війни за національну державу (з притаманною їй природою) XX-го століття. (Bobbitt 2002). З цієї точки зору цілий ряд конфліктів - Перша світова війна, більшовицька революція, громадянська війна в Іспанії, Друга світова війна, американо-радянське протистояння та Корейська і В'єтнамська війни – є епізодами однієї тривалої війни. Всі ці конфлікти точилися з приводу одного набору конституційних питань, які були стратегічно невирішеними, доки Паризький договір 1990 року не поклав офіційний кінець Холодній війні. Якими ж саме були так звані "конституційні питання?" Тривала війна точилася аби визначити, яка з трьох нових, конкуруючих форм національної держави замінить імперські держави Європи XIX-го століття : ринково-орієнтована парламентська демократія, комунізм чи фашизм. Борючись ніби за ідею створення "безпечного світу для демократії", Перша світова війна фактично не вирішила питання, якого роду система має превалювати. Навпаки, вона виплекала комунізм (російська революція), і фашизм (у першу чергу, в німецькій реакції на Версальський договір). Не вирішивши суперечки серед конституційних систем, Перша світова війна «тільки узагальнила це питання практично для всіх держав». (Bobbitt 2002 p. 27) Велика депресія посилила конкуренцію між цими суперечливими соціальними укладами (Berman 2006). В 1930-х роках вже не було країни в розвиненому світі, і лише декілька в колоніальному світі, у якої не було б місцевих фашистських, комуністичних та ліберально-демократичних чи соціал-демократичних партій.

Друга світова війна усунула фашизм в якості “життєздатного” варіанту соціального ладу для великих держав. Однак поразка Німеччини, Італії та Японії лише спровокувала утвердження біполярного світового ладу. Дві великі наддержави, що вбачали два різні шляхи побудови та становлення держави, все ще напружено та конкуруючи між собою стояли один проти одного в завойованій Німеччині 1945-го року, розділивши Європу на дві частини. Вони відображали різні системи політичної економії, які були визначені як несумісні і взаємовиключні: капіталізм та демократія з одного боку та соціалізм, комунізм, Марксизм-Ленінізм, анти-імперіалізм та інші з іншого. Це “змагання” визначило міжнародні відносини на наступні 45 років, втягуючи в нього більшість держав та міжнародних процесів, прямо чи опосередковано.

Холодна війна

У змаганні між США та СРСР не військова міць Радянського Союзу або навіть не його недемократична система викликали американську та британську ініціативи Холодної війни.

Скоріше, це був страх, що радянська система могла заробляти на післявоєнних політичних потрясіннях, щоб схилити чашу терезів влади на свою користь. *Як писав Пол Кеннеді про цей період (1987, 380), "[Друга світова війна] викликала величезну соціальну і політичну турбулентність ... навіть у країнах, безпосередньо не захоплених вторгненням армій (наприклад, в Індії чи Єгипті). Традиційні соціальні устрої нігілювалися (були знігільовані), колоніальні режими були дискредитовані, націоналістичні партії процвітали і кількість рухів опору виросла, що призвело не лише до військової перемоги, але й до певних політичних перетворень. "*

Зростаюча популярність комуністичних партій в післявоєнній Європі та хвиля революційних і націоналістичних рухів в результаті відступу європейського колоніалізму все частіше розглядалися з боку США як загроза. США побоювалися, що країни третього світу і ключові частини (центральні частини Європи) Європи будуть приєднуватися до комуністичної системи в глобальній конкуренції.

Таким чином, вже в березні 1946 Уїнстон Черчилль закликав до дипломатичного наступу проти Радянського Союзу. Американські дипломати Джордж Кеннан і Кларк Кліффорд вимагали заходів щодо стримування зростаючої могутності СРСР й наголошували та радили відповідно, щоб Америка

надавала"підтримку і допомогу всім демократичним країнам, яким так чи інакше погрожував Радянський Союз". 12 березня 1947 року Президент США Гаррі С. Трумен рішуче ввів США в Холодну війну, заявивши, що "майже всі країни повинні вибирати між альтернативними способами життя." Нова «Доктрина Трумена» проголосила американську зовнішню політику, яка «спрямована підтримувати вільні народи, які чинять опір спробам підпорядкування збройним меншинам або зовнішньому тиску ". Американець Генрі Уоллес, член лівої партії, заперечив, що" Немає режиму занадто реакційного для нас, що впровадив би стандарти в експансіоністську Росію, та не існує країни настільки віддаленої, що слугувала би певною ареною для суперечок…. ”

Хоча економічні та ідеологічні аспекти конкуренції були визначальними, не слід забувати про технологічні досягнення в озброєнні, що також відігравали важливу роль. Розвиток ядерного озброєння США в якості домінуючої сили зміцнив статус держави. Стратегічні переваги, які могли бути отримані за допомогою ядерної зброї, викликали гонку озброєнь між США і Росією, що стало причиною незліченних втрат в процесі виробництва стратегічних запасів. Взаємно гарантоване знищення в кінцевому рахунку (і, можливо, тільки на щастя) стримало прямий збройний конфлікт між двома великими державами, але це не завадило розвитку конфлікту в інших областях. Це сприяло розвитку запеклих війн та значних конфліктів в спірних, конфліктних регіонах світу, включаючи руйнівні конфлікти в Кореї, В’єтнамі, Лаосі та Камбоджі. Це була міжнародна система постійних напружень, високих ризиків та численних воєн. В кінцевому рахунку війну виграла

ліберальна капіталістична демократія, але не через свій високий військовий потенціал.

Причиною перемоги ліберальної капіталістичної демократії була неспроможність соціалістичної планової економіки до інновацій і виробництва так званих багатств для своїх громадян, що підривала їх легітимність зсередини і призупиняла їх розвиток і військову потужність (Kennedy 1989, McMahon 2003). З кінця 1970-х контраст між матеріальним благополуччям Південної Кореї і Північної Кореї, між Тайванем і материковим Китаєм, між Східною та Західною Європою ставав все більш очевидним. Було також очевидно, що технологічна перевага Заходу, особливо в галузі інформаційних технологій і телекомунікацій, мала вплив як на військову справу, так і на економіку. Спроба Горбачова з реформування та активізації радянської економіки,

відома всім як Перебудова, була спробою подолати цей розрив. Оскільки він мав подолати опір корисливих інтересів для досягнення перебудови, він спробував створити умови для розвитку політичної системи в цілому, коли ситуація вийшла з-під контролю і радянська система почала давати збій. Так, ще до 1990 року друга з трьох альтернативних конституційних форм сучасної національної держави була фактично ліквідована. Це врегулювало 80-літню боротьбу за домінуючу форму сучасної конституційної держави. З цієї точки зору, Холодна війна була лише передостаннім епізодом тривалої війни.

Війна та трансформації в державі

Ширше бачення Холодної війни важливе для студентів,що вивчають управління Інтернетом. Увага приділяється трьом важливим фактам, що стосуються поточної ситуації.

По-перше, форма прийнята державою з часом змінюється, і змінюється швидше, ніж ми зазвичай розуміємо та усвідомлюємо. Поширена думка, що ми перебуваємо у "Вестфальській" системі з 1648 року, не є вдалою. Bobbitt (2002, 17) оскаржує дане ортодоксальне твердження (загальновизнане твердження), стверджуючи, що:

... Національна держава є відносно новим явищем – маючи трохи більше, ніж столітню історію – і їй передували інші форми держави, у тому числі й форми, які передували довгій Тридцятилітній війні. Дана форма держави вмирає, але це означає лише те, що, як і в минулому, нова форма держави - народжується.

Форми держави, що існували до Першої світової війни, значно відрізнялися від сучасної національної держави, що виникла в минулому столітті. Ідеали Вестфальської системи мало схожі на передуючі Першій світовій війні імперії Великобританії та Австро-Угорщини, Османської імперії, царської Росії та бажаючих розширення Японію та Німеччину. Вчені, що займаються управлінням Інтернету, наприклад я, які підкреслюють чому проблеми управління Інтернетом ведуть до інноваційних відхилень від національного державного управління (2002 Мюллер, Мюллер 2010), можуть знайти підтримку в цьому погляді на історію. Ті, хто наполягають, з іншого боку, що проблеми управління Інтернетом можуть бути вирішені лише вдаючись до вірної ієрархії класичної національної держави повинні подумати ще раз. Те, що вони уявляють та пропонують як відновлення "нормального" способу ведення справ, фактично буде винятковим ступенем застою, дивною паузою в процесі політичної еволюції. Це є нормою для нових технологій, що впливають на військову, економічну і політичну сили задля зміни форми держави.

По-друге, серйозні зміни в конституційній формі держави, як правило, супроводжуються насильницькими конфліктами (війни, революції тощо), а також корелюють з технологічними інноваціями у військовому потенціалі. Це природно, оскільки сама держава задумана як монополія з використання законної сили. За наявності конкуруючих уявлень про законність або способи існування держав, найбільші несумісності між ними виллються у внутрішні і міжнародні конфлікти, швидше за все, це будуть насильницькі конфлікти, якщо такі уявлення співіснують всередині одного й того самого суспільства. Це означає, що ми всерйоз подумати про відносини між кібер-простором і військовим конфліктом (принаймні, аналітично) оскільки, якщо Інтернет і кіберпростір внесуть певні зміни у війну і політику, то неминучими будуть також трансформації самої природи держави, і, внаслідок цього, відбудуться також зміни і в міжнародній системі. Хто насправді буде потрібен у такій ситуації, так це, як каже старе прислів'я, генерали, які готуватимуться до останньої війни, а не тієї, хто, з якою ми можемо зіткнутися у майбутньому».

По-третє, такий підхід потребує більш пильної уваги в дебатах з Інтернет управління.

Молодші національні держави – ті, які лише з'явилися в період після Другої світової війни - здається, найбільш твердо схильні дивитися назад, використовуючи заснований на принципах суверенітету нео-Вестфальський підхід до управління Інтернетом. Здебільшого, боротьба за бачення управління Інтернетом не може бути охарактеризована абсолютно точно як боротьба між авторитарними, недемократичними державами з одного боку та ліберальними, волелюбними державами з іншого, але її можна охарактеризувати як конфлікт між давніми, космополітичними державами і новими державами, які все ще побоюються за свій суверенітет. У певному сенсі це зрозуміло. Домігшись незалежності від імперських та колоніальних структур Заходу лише декілька поколінь тому, і, нарешті, дочекавшись "своєї черги", щоб запустити “державний механізм”, такі країни як Бразилія, Росія, Індія, Китай і Південна Африка стурбовані, до якою міри такий важливий сектор постмодерністської економіки, зв'язку та інформатизації раптом звільняється від класичної моделі національного контролю. Однак, це спостереження не повинно тлумачитися як виправдання для застосування підходу, заснованого на захисті суверенітету. Знадобилося кілька десятиліть, щоб нові незалежні держави зрозуміли, що соціалістичні й комуністичні ідеології, які були ефективними для мобілізації боротьби за незалежність і повалення колоніалізму, були катастрофічно контрпродуктивними в якості керівництва економічної політики коли вони були при владі. Можливо знадобиться ще близько десятиліття, щоб зрозуміти, що територіальне управління національної держави є безповоротньо контрпродуктивним в галузях комунікацій та інформаційної політики XXI-го століття.

Доцільне порівняння

З урахуванням цих двох чинників, що можна порівняти і що є принципово відмінним в нинішній (поточній) ситуації ? Спершу ми поглянемо на Китай, потім на ідеологічну та конституційну поляризації і, нарешті, відповімо на запитання чи ведуть кібер можливості до трансформації війни.

Випадок Китаю

При розгляді питання про Китай, можна стверджувати, що тривала війна ніколи насправді не закінчувалася, і, таким чином, Холодна війна все ще триває. Це все тому, що Китай, на відміну від Росії, досягнув успіху в реформуванні своєї соціалістичної економіки - відкривши її достатньо для ринкових сил, щоб вивести свій народ з бідності - при успішному збереженні монополії комуністичної партії на політичну владу. З марксистсько-ленініської точки зору, Ден Сяопін досяг успіху там, де Горбачову не вдалося. Тому Китай може розглядатися як розвинена форма комуністичної держави, яка краще підготовлена до боротьби за панування з США у військовому та економічному сенсі. Він також пропагує альтернативну ідеологію стосовно ролі інформації в суспільстві, підкреслюючи агресивне управління публічним вираженням, деструктивність і небажаність інакомислення і незгоди, що є метою 'гармонійного' Інтернету. Китай приєднує велику кількість країн «Групи 77» до ідеї міжурядового, суверенного підходу до інтернет-політики на засіданнях Міжнародного союзу електрозв'язку. Китай також є новою, великою державою, яка розбудовує як економічні можливості, які в кінцевому рахунку просто перевершать, захлеснуть економічні можливості США, так і свою військову міць. Чи посів Китай місце СРСР в продовженні тривалої війни? Це приблизно так само імовірно, як і вірогідність настання Холодної кібер війни. Але існують деякі очевидні проблеми такого сценарію (розвитку подій).

По-перше, рівень економічної інтеграції та взаємозалежності між США і Китаєм значно підриває порівняння з Холодною війною. Сполучені Штати є найбільшим торговим партнером Китаю. Якби економіка США була знищена або «захоплена» Китаєм так чи інакше, або навпаки, то економіки обох держав погіршилися б до такої міри, що це поставило б під загрозу життєздатність їх обох. Оскільки легітимність комуністичної партії Китаю майже повністю залежить від продовження підвищення рівня життя, то нанесення серйозної шкоди США буде представляти реальну загрозу. Войовничі американські розмови про кібератаки Китаю припускають, що Китай рішуче налаштований на наше руйнування і поглинання, а потім (не) інтерпретуватиме шпигунство і крадіжки інтелектуальної власності в якості військових дій. Насправді, незаконне привласнення інтелектуальної власності з більш розвинених країн є перевіреною часом стратегією економічного розвитку, яку колись застосовували і США.

Реалісти-теоретики міжнародних відносин не вірять в тезу, що економічна взаємозалежність буде запобігати війні. Але навіть вони вважають, що дві великі держави, розділені великими океанами, і озброєні ядерною зброєю, будуть представляти невелику пряму військову загрозу одна одній. (Mearsheimer 2001).

Інша проблема цього сценарію полягає в тому, що йому не вистачає біполярності і винятковості конкуренції Холодної війни. Ні держава Китай, ні її Інтернет не розглядається як маяк або модель, яка оживить та надихне решту світу. Решта світу не знаходиться в стані так званого порогу, як це було після Другої світової війни, коли формувалися десятки нових постколоніальних урядів. Немає комуністичних партій в Японії, Південній Кореї, Таїланді, Єгипті, Туреччині, Греції, Італії чи Індії, пов'язаних та маючих підтримку китайської компартії, які були б цілком спроможні захопити владу і перетворити ці держави в сателітів Китаю. Дійсно, Китай має мало реальних військових союзників. Європейський союз, Росія, Індія та інші сформулювали незалежні політичні, військові та економічні відповіді на підйом (ріст) Китаю, - тобто, вони не будуть просто тулитися під американську парасольку безпеки.

Вибір між «альтернативними способами життя»?

Чи існує ідеологічний поділ у світі, в порівнянні з дихотомією капіталізму / демократії проти соціалізму / комунізму ? В Інтернет-сфері – так, частково. Але життєво важливою історичною відмінністю є те, що цей розподіл не визначається та не здійснюється державами.

Існує ідеологічна розбіжність навколо двох різних питань. По-перше, це відповідні інституційні форми Інтернет управління, по-друге - основні аспекти інформаційної політики. Щодо форми управління, молодші держави і авторитарні держави виступають за вирішальну роль суверенітету в інформаційній політиці, на що і покладаються на переговорах з укладання міжурядових угод з глобального управління. Інша сторона, актори приватного сектору в технічному співтоваристві, бізнесі, і в деякій мірі громадянському суспільстві, підтримують органічно розвинені Інтернет установи (Мюллер, 2010), які представляють собою транснаціональне управління і більш відкриті інституційні механізми взаємодії.

Щодо основних особливостей інформаційної політики, то в транснаціональному громадянському суспільстві в розвинених країнах світу і в багатьох країнах з середнім доходом або країнах, що розвиваються, є партія Інтернет-свободи, яка виступає проти цензури, спостереження, монополії і пропагує високий рівень захисту інтелектуальної власності за підтримки інновацій, свободи слова та приватного життя; з іншого ж боку є держави з авторитарними тенденціями, які хочуть відновити суверенну владу над цифровим зв'язком (комунікаціями) з метою захисту своєї місцевої політичної рівноваги проти космополітичних порушень. Коротше кажучи, існує конфлікт між прихильниками індивідуальної свободи і державно-орієнтованого регулювання. Зазвичай (але не завжди) прихильники multistakeholderism(багатосторонності) групуються із захисниками Інтернет-свободи, а прихильники міжурядового управління прагнуть сприяти більшому регулюванню та контролю над Інтернетом. Але на відміну від Холодної війни, конкуренція між цими різними баченнями Інтернету насправді не закріплена і поляризована навколо двох великих держав, які прагнуть залучити інші країни у взаємовиключні системи політичної економії. Завжди сумнівна спроба уряду США позиціонувати себе в якості прапороносця Інтернет-свободи, нещодавно завершилася з викриттям щодо спостереження Національним агентством з безпеки (NSA). Держави-актори, які виступають за Інтернет-свободу і “багатосторонню модель” по суті лицемірять. Навіть тоді, коли вони безпосередньо не суперечать самі собі, їх підтримка інституціям управління Інтернетом здається опортуністичною, непослідовно і частковою – особливо, коли це стосується питань національних інтересів і національної безпеки.

Що є разюче новим в поточній ситуації, так це те, що TCP / IP дійсно об’єднує всіх. Держави, бізнес та громадянське суспільство є частиною Інтернету. Справжня Інтернет-Холодна війна означатиме, що обидві сторони об'єдналися навколо альтернативних протоколів передачі даних. Тим не менше, ніхто не пропонує конкуруючий, несумісний протокол передачі даних, що дозволив би одній частині світу вимкнути їх TCP / IP. Так є брандмауери і фільтри, але немає альтернативної кореневої DNS, немає іншого системного реєстру Інтернет-адрес. Справді, це не просто Інтернет як такий, що об'єднує наш світ інформації та комунікації: так роблять стандарти 802.11 для операційних систем Wi-Fi, Windows, Apple і Android; пристрій виробляють в Кореї, Китаї, Європі та США. В деякій мірі це роблять Twitter, Google і Facebook, всі з яких відомі і за якими сумують, коли доступ до них заблокований.

Навряд чи можна переоцінити цей аспект відмінності між історичними епохами. Під час Холодної війни відбувся розрив дипломатичних, економічних, технологічних зв'язків з одного боку і соціальних зв'язків з іншого. Очолювана американцями Intelsat система, наприклад, була спрямована на Захід. СРСР не приєдналися до неї і поскаржилася на її панування в США. Вони не намагалися посприятим, щоб Міжнародний союз електрозв’язку "взяв керівництво на себе." Натомість, вони створили Інтерсупутник, альтернативну систему супутника, яка зв’язувала разом Східний блок. Аналогічно, торгівля, імміграції та подорожі між Сходом і Заходом були вкрай обмеженими. Економіки Сходу і Заходу були різними. Фізичні стіни були побудовані, щоб розділити їх, і людей розстрілювали, якщо вони намагалися перетнути їх. Сьогодні цього не відбувається.

Кіберзброя

Посилаючись на Stuxnet, колишній директор ЦРУ генерал Майкл Хейден сказав: "Це був подув серпня 1945 р. ... Хтось, ймовірно національна держава, просто використовувала кіберзброю в мирний час ... щоб знищити те, що інший народ міг описати як їхню критично важливу інфраструктуру». Чи трансформують кібервійни і кіберзброя військовий потенціал, який, як зазначалося раніше, може бути шляхом до цифрової Холодної війни?

Ні. Хейден або має щось на порядку денному, якусь інформацію, або він знаходиться поза реальністю. Кіберзброя не є революційним фактором, здатним змінити військове суперництво між державами в глобальному масштабі. Я згоден з Томасом Рідом, що військові кібер аспекти були надзвичайно завищені (Rid 2013). Простіше кажучи, досі не було жодної кібервійни. Те, що ми називаємо кіберзброєю, не спровокувало утворення нового типу конфлікту, який змінив би стратегічний баланс між державами, які беруть участь у військових конфліктах. (Великі інтернет-спостереження, можливо, займаються цим, але це вже інша історія, яка виходить за рамки цієї статті.) Сьогодні не відбувається нічого, що можна було б порівняти з з французькою інновацією – запровадженням мобільної артилерії у 1494 році, яке призвело, на думку Боббіта, до кінця епохи князівств та початку ери королівств і територіальних держав. Також сьогодні ніщо у галузі кіберзброї не може бути порівняно з ядерною зброєю.

Давайте порівняємо кіберзброю та ядерну зброю. У невеликому проміжку 6-ти років (1939-1945 рр.) зобов'язання зі створення ядерної зброї були зроблені і зброя була розроблена, випробувана та використана. Її використання не тільки сприяло кінцю Другої світової війни, але й рішуче змінило умови подальших стратегічних відносин між великими державами на подальші п’ять десятиліть. Володіння ядерною зброєю і здатністю доставити її донині є основним чинником, що визначає міждержавні владні відносини, як це демонструють нам суперечки з приводу Ірану.

На противагу цьому, ми говорили і писали про кібервійни протягом більш ніж п’ятнадцяти років (Arquilla і Ronfeldt 2001) ; за цей час жодна держава не було повалена, жодна реорганізація територіальних кордонів ніколи не мала місця, грунтуючись виключно або в першу чергу на кібер-атаках і кіберзброї. Graham (2012), посилаючись на інциденти 2008 , в яких Росія нібито напала на Грузію за допомогою використання кіберметодів узгоджених з військовими нападами, стверджує категорично, що "немає жодних доказів того, що кібер-атаки проводилися урядом Росії, або, що вони були чимось більшим ніж застосування хакерства з політичними цілями. "Посилені, стійкі" китайські загрози, про які ми читали в лютому були спрямовані на шпигунство і крадіжку інтелектуальної власності; навіть якщо вони були спонсоровані державою, вони в жодному разі не були військовими діями чи чимось подібним. Вони нічого не знищили. Терористи продовжують реалізувати свої цілі, прищеплюючи бомби, а не нападаючи на DNS або на критично важливі об’єкти інфраструктури при допомозі кіберзасобів.

Кращим прикладом кіберзброї, який ми тільки можемо придумати, є Stuxnet, який, незважаючи на свою неймовірну вишуканість кібер-експлойта, був не більше, ніж актом саботажу проти кількох високоспеціалізованих одиниць техніки. Черв'як був всього лише однією маленькою частиною загальної програми економічних санкцій, кінетичних військових загроз і дипломатичної ізоляції. І, до речі, іранська ядерна програма досі триває. Порівняння з "Серпнем 1945», здаються повним абсурдом.

Можуть виникати бунти і громадянські заворушення в кіберпросторі (Естонія); можуть статися акти вандалізму і соціальні протести (Anonymous); може статися тимчасовий зрив або припинення (DDoS атаки державних або недержавних структур); можуть мати місце випадки електронного шпигунства і крадіжки даних (APTs from China); можливі навіть варіанти саботажу (Stuxnet). Всі вони можуть бути впливовими в тій чи іншій формі. Але досі немає жодних доказів того, що це може призвести до масової загибелі людей і руйнувань або, що існує можливість зміни стратегічного балансу сил між державами у світі.

Повторення

Тим не менш, структурні відмінності між Холодною війною і сьогоденням не перешкоджають політичним та психологічним пожвавленням, створюючи небажану політичну динаміку. Всередині наддержав Холодна війна винагородила політичних акторів, які стверджували, що їх уряд був вразливим або відставав у гонці озброєнь. Хоча на той час США користувалися величезними перевагами в ядерно-ракетному потенціалі, ліберал-демократ Джон Кеннеді провів успішний політичний напад на вихідну адміністрацію Ейзенхауера, стверджуючи, що існував "ракетний розрив" між США і Радянським Союзом.

Перспектива стійкої, глобальної конкуренції з іншою наддержавою дала прихильникам жорсткої політики дивні риторичні переваги в публічних дебатах. З справді екзистенційними ставками та притаманною нездатністю знати з абсолютною впевненістю, чи дійсно питання важливе до того часу, поки боротьба не розпочнеться, багато виборців і законодавців були готові помилятися в бік «більшої» безпеки. Ця фракція також була підкріплена зацікавленими економічними групами, які отримали прибуток від військових витрат. Ця динаміка здається дуже схожою на ту, що ми можемо прослідковувати сьогодні. Навіть не потрібно єдиної глобальної конкуренції наддержав; подібні ефекти наприклад, були досягнуті у «війні з тероризмом». З боку США Холодна війна як правило, була направлена на об'єднання ліберальних ідеалів з антикомунізмом, тобто вона підпорядковувалася досягненням ліберальних свобод задля запобігання розповсюдженню радянського комунізму. Це надало підтримку диктаторам у світі, що розвивався, доки вони привселюдно були на боці антикомунізму, повалювали або ж підривали авторитет демократично обраного, але лівого політичного лідера, побоюючись, що саме він приведе країни до так званого комуністичного табору (Іран, Греція). Вдома ж пожертвували свободою та демократією.

Холодна війна призвела до масового поширення, в масштабах американської держави, підвищення рівня державного втручання в ключові галузі економіки, обмеження громадянської свободи і свободи преси, а подовжила військові призови – все те, що конституційно та ідеологічно мав забезпечити ліберальний порядок. Все це логічно випливає з постійного стану війни або воєнної готовності, спровокованих Холодною війною. Американські праві - консерватори, які так чи інакше пов'язували національну безпеку держави з риторикою «менше уряду» та «свобода» - опинилися в пастці цієї дилеми на десятиліття.

І в цьому випадку перспектива повторення є цілком реальною. Загроза чуток про небезпеки для кібербезпеки фактично перешкоджає порядку денному ліберальних демократичних держав. Це призводить до концентрації і централізації влади (як політичної, так і економічної), не до її децентралізації і дифузії. Визначаються пріоритети національної безпеки над особистими правами і безпекою людини; це призводить до більш детальних урядових спостережень і скорочень належної правової процедури, а також це призводить до обмежень на інновації в Інтернет-бізнесі. Було цікаво спостерігати за урядом США, який нібито підтримує ідеї вільної торгівлі, а в цей же час демонізував виробника телекомунікайного обладнання Huawei, маючи на це мало підстав. У цьому випадку завдання національної безпеки були так чудово поєднані з протекціоністською економікою, що ті, хто захищає вільний ринок обладнання так чи інакше вибачається перед китайцями.

Висновок

Ретельно дослідивши поставлене питання, можна зазначити, що метафора Холодної війни не забезпечує достатньо хорошого і вагомого обгрунтування для відновлення традиційних форм національної державної влади в ім'я кібербезпеки. Навпаки, пряме порівняння підкреслює глибокі відмінності в типі конфлікту, з яким ми зіткнулися в минулому, і тим, який ми спостерігаємо зараз. Це привертає нашу увагу до великих держав та трансцендентності традиційних суперечок з приводу контролю та розширення їх територій

(багато в чому завдяки ядерній зброї) та їх економічної і технологічної взаємозалежності.

Якими б не були політичні загрози відродження менталітету Холодної війни, її використання в якості порівняння може бути повчальним і корисним. Ми повинні розмістити геополітичний конфлікт в історичному контексті, який підкреслює триваючі трансформації держави, викликані новими формами взаємозалежності, озброєнь і конфліктів, що тривають донині. Ми не повинні повторювати помилку Холодної війни, а замість того розглянути основоположне питання - за що ми насправді воюємо і проти чого.

Посилання :

Arquilla, J. and D. Ronfelt, Eds. (2001). Networks and Netwars: The future of terror, crime and militancy. Santa Monica, CA, RAND Corporation.

Berman, S. (2006). The Primacy of Politics: Social Democracy and the Making of Europe's Twentieth Century. Cambridge, Cambridge University Press.

Bobbitt, P. (2002). The shield of Achilles : war, peace, and the course of history. New York, Knopf.

Kennedy, P. M. (1989). The rise and fall of the great powers : economic change and military conflict from 1500 to 2000. New York, Vintage Books.

Klimburg, A. (2013) The Internet Yalta. Center for a New American Security http://www.cnas.org/theinternetyalta,

Mandiant (2013). APT1: Exposing One of China's Cyber Espionage Units. Washington, DC, Mandiant, Inc.

McMahon, R. (2003). The Cold War: A Very Short History, Oxford University Press.

Mearsheimer, J. J. (2001). The tragedy of Great Power politics. New York, Norton.

Mueller, M. L. (2002). Ruling the Root: Internet governance and the taming of cyberspace. Cambridge, MA, MIT Press.

Mueller, M. L. (2010). Networks and States: The global politics of Internet governance. Cambridge, MA, MIT Press.

Rid, T. (2013). Cyber war will not take place. Oxford, Oxford University Press.

4.2.4. Франческа Мусіані. Децентралізована система доменних адрес? Контрольована користувачем інфраструктура як альтернатива управління Інтернетом

Децентралізована система доменних адрес? Контрольована користувачем інфраструктура як альтернатива управління Інтернетом

Франческа Мусіані, співробітник Yahoo! Джорджтаунського університету

Переможець 2013 року у номінації "Краща стаття" в сфері комунікаційної політики і технологічній секції, IAMCR , Дублін , 25-29 червня 2013

Вступ

«Серце проблеми DNS не знаходиться в самій ICANN . Воно знаходиться в урядах та компаніях, які можуть контролювати ICANN. Система є централізованою». Пітер Санде, грудень 2010.

Кінець 2010 року. WikiLeaks розкриває тисячі американських дипломатичних таємниць, а через кілька днів по тому втрачає свій веб –хостинг та домен wikileaks.org. Дискусії про "новий конкуруючий кореневий сервер", який здатний конкурувати з корпоративним присвоєнням імен та номерів (ICANN), незабаром почне заповнювати веб-простір, чому сприяє відомий Інтернет "анархіст " Пітер Санде. Альтернативний реєстр доменних імен передбачається як децентралізована пінгова (P2P) система, в якій всі користувачі будуть володіти частиною системи доменних імен (DNS) на своїх комп'ютерах, так що будь-який домен, який буде тимчасово недоступний через блокування, все ще зможе функціонувати на альтернативному реєстрі. Замість того , щоб просто додати більше варіантів DNS адрес до вже прийнятих і які управляються ICANN, цей проект має на меті усунення централізованого контролю на користь розподіленої інфраструктури для користувачів.

Технічні та політичні дебати щодо децентралізованої, альтернативної системи DNS адрес є наслідком вилучення доменних імен з метою утримання посередництва, що є хорошою ілюстрацією того, що Лора Денардіс нещодавно описала як «поворот у бік

інфраструктури» в управлінні Інтернетом. Ці дебати показують, що інфраструктурне управління Інтернетом, яке все частіше використовується у політичних цілях, не має жодного відношення до його основної функції - управління Інтернетом" [Денардіс, 2012], і, в свою чергу, що розробники прагнуть обійти цей контроль шляхом створення нових механізмів управління мережею.

Ця стаття заснована на дослідженнях науки і технологіях (зокрема дослідження програмного забезпечення та критичного дослідження коду), а також на інтерв'ю з технічними та політичними суб'єктами, які беруть участь в управлінні DNS, задля внеску у вивчення «альтернативного Інтернету» [Аттон , 2005] .

1. Схожість P2P з водопроводом «P2P - це водопровід , і більшості людей не має відношення до водопроводу», відзначив декілька років тому Ден Бріклін, «батько» електронних таблиць, у своїй програмній книзі про потенціал P2P, як підривної технології [Бріклін, 2001: 59]. Ця оцінка перших файлообмінних програм, напевно, правильна: ймовірно, їх успіх викликаний більше зручністю таких інструментів, що дають змогу швидко знайти та закачати конкретний контент. Декілька спеціалістів, натрапляючи в Інтернеті на науково-технологічні дослідження (STS), намагалися в останні роки вивчити соціальні та політичні якості інформаційної інфраструктури та знайти "матеріал" у віртуальному програмному забезпеченні та коді [Стар & Боукер , 2002; Монберг 2005 ; Манович, 2001; Фуллер , 2008; Марино , 2006; Райбс & Лі , 2010 ; Кіршенбаум , 2003; Денардіс , 2009, 2010] .

Паралельно із СТС-орієнтованми підходами і концептуалізацією мережевих архітектур на політичному, соціальному та правовому рівнях – деякі закони та економічні вчення зосередились на відносинах між архітектурою Інтернету та інноваціями. Стверджується, що еволюція Інтернету, ймовірно, в середньо та довгостроковій перспективі, залежить від топології та технічних моделей Інтернет програм, а також від інфраструктури, що лежить в їх основі [Аігрейн, 2011]: таким чином, акцент робиться на тому, як «нижчі рівні» мережевих програм інформують об’єктів, що де факто має вирішальне значення для користувачів, про обробку та зберігання даних, обчислювання ресурсів, вилучення інформації та агрегацію; а також на матеріальності мережевих систем, що є джерелом «технологічних» наслідків, як для прав користувачів так і для регулювання [Елькін – Корен, 2006]. Архітектура Інтернету, так само як і його послуги, були предметом

суперечок в минулому, в даний час також є складним питанням. Після визнання його важливості, як регулятивного механізму, Інтернет стали все більше аналізувати як важіль для розвитку, а також точку відліку для ринкових можливостей (так само як і обмежень) [Ван Швейк, 2010], визнаючи його придатність до змін та модифікацій [Барман, 2011].

- P2P: пошук альтернатив, побудованих на наріжному камені історії Інтернету, з'єднання рівноправних вузлів P2P (комп'ютерна мережа, що структурована у децентралізованому порядку, так що зв'язок чи обмін відбувається між рівноправними вузлами системи). Учасники мережі роблять доступними системі їх обладнання те ресурси; доступні безпосередньо з боку рівноправних вузлів, ці загальні ресурси необхідні для нормального функціонування сервісу, який пропонується мережею.

Дихотомія між сервером, постачальником ресурсів та клієнтами, що шукають ці ресурси, що є характеристикою моделі клієнт-сервер, замінена на ситуацію, коли кожний учасник надає частину своїх ресурсів і всі мають до них доступ [Шолімер, 2001].

Для більшості користувачів Інтернету з самого моменту ознайомлення із P2P за допомогою Napster у 1999 році технологію де факто ототожнюють із (нелегальним) завантаженням контенту; для інших він представляє собою унікальну утопію техно-егалітаризму, або просто представляє більш стійку організаційну модель суспільства завтрашнього дня. У будь-якому аналізі P2P не можна повністю ігнорувати будь-яку із цих точок зору. Однак, не нехтуючи цими поглядами, ця стаття не прагне зробити додатковий внесок у вже існуючу дискусію з приводу обміну/крадіжки діалектики, з якою система P2P природно пов'язана. Скоріше, цю статтю слід приймати в якості відправної точки «чеснот» децентралізації – ефективності, стабільності та стійкості, які роблять вирішальний внесок у політичне та технічне значення системи P2P [Елькін – Корен, 2006].

Розвиток послуг на основі децентралізованої, розподіленої P2P мережевої архітектури визнається протягом декількох років – навіть, і особливо, сьогодні, у часи «Хмарних» технологій та великого об'єму даних – як одна із цікавих осей трансформації наших умов зв'язку і управління цифровим контентом. Концепція децентралізації вкладається в якійсь мірі в самому ядрі Інтернету, особливо в організації та передачі пакетних даних. Проте, сьогоднішній Інтернет інтегрує цей принцип лише частково: у той час, як кожний користувач мережі Інтернет став, принаймні потенційно, не лише

споживачем, але і розповсюджувачем та виробником цифрового контенту, концентрація значної кількості даних відбувається в певних регіонах Інтернету [Мінар і Хедлунд, 2001; Бернерс – Ли, 2010]. Повертаючись до децентралізованої архітектури мереж та розподілених організаційних форм для Інтернет послуг, передбачається ряд проектів, компаній та послуг, що у перспективі підвищать ефективність, подолають певні труднощі в управлінні а також сприятимуть цифровому «сталому розвитку».

Так само як і ряд децентралізованих альтернатив Інтернет послугам, які ми досліджували [Мусіні, 2013], проект P2P DNS описується в цій статті як специфічний вибір: передача відповідальності та контролю над даними «краям», полям, або просто периферії інфраструктури мережевих систем. Необхідні операції для належного функціонування цих систем, а також їх здатність коректно надавати послуги, для чого вони і призначені, технічно залежить від користувачів: їх терміналів, їх цифрових ресурсів, мобілізованих таким чином, щоб служити спільній меті. Ми зосередимо нашу увагу на «зустрічі» між рішенням про розробку технічної архітектури P2P та складним і суперечливим компонентом інфраструктури Інтернету – системою доменних імен (DNS) – що у сучасній формі чітко визначається я дихотомія між постачальниками Інтернет-ресурсів – Інтернет реєстрами і реєстраторами, що підконтрольні ICANN, та клієнтами, які потребують цих послуг. Намагаючись усунути «Балет програмістів, програмного забезпечення та користувачів» [Аббате, 2012], будується проект децентралізації для DNS. Ця стаття вносить свій внесок у вивчення соціально-політичних наслідків розподіленого та децентралізованого підходу до технічної архітектури Інтернету.

•Управління Інтернетом. Сфера управління Інтернетом (IG) на сьогоднішній день є перспективною, дослідження цієї сфери також знаходяться «у процесі становлення» [Латоур, 1987]. Робоче визначення IG було надано раніше, після Всесвітнього саміту з питань інформаційного суспільства (ВСІС) Організації Об’єднаних Націй, робочою групою з управління Інтернетом, визначення, що досягло консенсусу через його загальну прийнятність, але, мабуть, воно є занадто широким у розумінні, а тому навряд чи може бути корисним в розробці більш точного значення [Малкольм, 2008]: управління Інтернетом являє собою розробку та застосування урядами, приватним сектором та громадянським суспільством, загальних принципів, норм, правил, процедур прийняття рішень та програм,

які формують умови розвитку та використання Інтернету [WGIG, 2005].

Таке широке визначення передбачає участь багатьох сторін, а також можливість розгорнути безліч механізмів управління для них. Управління Інтернетом було описано як суміш технічної координації, стандартів та політики [Малкольм, 2008 та Мюллер, 2010]. Технічна координація здійснюється через норми, ринок та інститути, що управляють технічною архітектурою Інтернету та його ресурсами. Розробка стандартів – це набір безлічі процесів, через які, за допомогою норм та архітектури працюють технічні стандарти, розроблені для роботи в Інтернеті. Публічна політика управління пов'язана із розвитком міжнародної громадської політики Інтернету, а також адрес, зокрема регулювання таких питань, як конфіденційність в Інтернеті. Інтернет політика здійснюється на національному та наднаціональному рівнях, а також обговорюється на глобальному рівні в таких місцях, як запроваджений Організацією Об'єднаних Націй Форум з управління Інтернетом. Саме в контексті цього форуму концепція «мульти-акціонерного» управління була вперше застосована до управління Інтернетом, будучи втіленням ідеї, що кожен «тримач акцій» в Інтернеті повинен мати голос, який почують у проектуванні мережі мереж [Левінсон, 2010].

2.1 Спірне визначення

Незважаючи на відкритість приведеного вище визначення IG, воно невблаганно оскаржується різними групами з політичних та ідеологічних причин. Одна із основних суперечностей полягає у питанні повноважень та участі конкретних суб'єктів, таких, як національні уряди, юридичні особи та суспільство. У контексті Інтернету, основними учасниками в процесі управління є не тільки уряди. Дійсно, у сфері компетенції свого суверенітету, уряди виконують певні функції, такі як регулювання зловживань, антимонопольний контроль, а також використовують фільтрацію контенту та блокувальні методи для спостереження за цензурою. Роль урядів в управлінні Інтернетом залишається центральною та часто неоднозначною. Тим не менш, інші сфери IG, такі як розробки Інтернет протоколів та координація Інтернет ресурсів, які історично належали до сфери повноважень як транснаціональних організаційних структур, так і приватних осіб [ДеНардіс, 2013].

Крім того, слід бути обережним, підписуючись під двома протилежними ідеологічними позиціями [Мюллер, 2010], одна з них повна ентузіазму але наївна, що веде до «цифрової революції», інша – просте відтворення традиційних форм державного управління стосовно Інтернету, стверджуючи, що «Інтернет не несе у собі нічого нового». Слід також утриматись від палкого підтримання однієї із сторін. Поширена помилка, що стосується IG, наприклад, це ототожнення із процесами ООН, що призвели до створення Форуму з управління Інтернетом, багатостороннього діалогу, що хоча і є цікавим у своєму роді, але не є місцем, де відбувається «управління Інтернетом» [ДеНардіс, 2013]. Крім того, Інтернет-корпорація з присвоєння імен та номерів (ICANN), в той же час являється одним із важливих інститутів управлінням Інтернетом, що керує делікатною частиною Інтернет інфраструктури, але представлена таким чином, що люди можуть повірити, що саме вона керує Інтернетом, що не є так.

2.2. Система доменних імен: У центрі уваги Інтернет - інфраструктури…

Сценарій, викладений вище, часто призводить до нехтування або ігнорування того, що насправді є важливим, хоча і непомітним аспектом управління Інтернетом: існує цілий ряд компонентів інфраструктури Інтернету та технічної архітектури, в конструкції яких закладені, в деякій мірі, механізми управління.

Серед випадків, коли було виявлено «політичну матеріальність» Інтернету, важливим є наявність системи Інтернет протоколу (IP). Усі пристрої, що обмінюються інформацією через Інтернет, ідентифікуються унікальним двійковим номером, що дає змогу визначити його віртуальне положення, тимчасове чи постійне. Інтернет маршрутизатори використовують ці адреси, щоб визначити, куди спрямовувати пакети даних через Інтернет. В даний час стандартом для Інтернет адрес є протокол IPv4, але він майже вичерпав усі незайняті адреси. Тим не менш, з цілого ряду політичних та технічних причин, оновлення на IPv6 все ще перебуває в зародковому стані, в той час як остаточне виснаження адрес все ближче, з усіма витікаючими наслідками.

Іншим прикладом критичності Інтернет інфраструктури є точки обміну трафіком (IXPs). Це фізичні точки, де різні сервери обмінюються пакетами даних та відправляють їх у потрібному напрямі. Наслідком управління та регулювання точок обміну трафіком є

формування конкурентних механізмів спостереження та фільтрації. Є ще багато чого сказати, але давайте сфокусуємо увагу на центральному питані цієї статті, системі доменних імен. У двох словах, DNS – це широка система управління базами даних, що розташовані ієрархічно, але поширюються по всьому світі; DNS переводить буквено-цифрові імена доменів у відповідні їм IP адреси, необхідні для маршрутизації пакетів через Інтернет. Через це Інтернет часто називають «Телефонною книгою». Станом на сьогодні кількість запитів, що направляються через DNS, складає кілька мільярдів на добу, тож DNS є важливим компонентом функціонування Інтернету. Кореневі сервери Інтернету містять так званий майстер файл, відомий як файл кореневої зони, із значенням IP адреси і відповідними іменами офіційних серверів DNS для всіх доменів вищого рівня: загального характеру, таких як .com, .edu, .gov, тощо, і коди країн, таких як .us, .uk, .fr.. Право на використання доменного імені делегується реєстратором доменних імен, акредитованим ICANN, організацією, якій доручено стежити за іменами та номерами системи Інтернету, а також контролювати кореневий сервер системи та кореневий файл системи.

Цей аспект просто наповнений суперечками за участю міжнародних інституціональних організацій, що прагнуть здобути владу над DNS, а також питаннями законності, демократії та юрисдикції. Нещодавно була організована конференція на цю тему в Інституті вивчення дипломатії Джорджтаунського університету, http://internetphonebook.eventbrite.com/ , де Каліфорнійська організація приватного права, а також де-факто ексклюзивний менеджер однієї із найделікатніших інфраструктур управління Інтернетом, заявила, що ICANN знаходиться під постійним міжнародним контролем с тих пір, як Інтернет став глобальним, суспільним феноменом, у зв’язку із його тісними зв’язками із урядом США, що передбачає відсутність прозорості.

Існують і інші політичні наслідки від використання DNS: спочатку він був обмежений символами ASCII, що виключають доменні імена з використанням скриптів багатьох мов, таких як арабська, китайська чи російська. На сьогодні вже ввели багатомовні доменні імена (IDN). Крім того, в 2011 році, правління ICANN ухвалило рішення про припинення дії більшості обмежень на ім’я загального домену вищого рівня (gTLD), яких раніше було доступно лише 22. Компанії та організації тепер зможуть обирати по суті довільні домени вищого рівня в Інтернеті, тим самим полегшуючи споживачам пошук брендів та інформації в Інтернеті. Інші спірні питання навколо DNS стосуються відносин між доменними іменами

та свободою вираження думок, безпекою товарних знаків та іншим.

2.3. … та її зміни

Хоча ці суперечки і відіграють важливу роль у формуванні сучасного Інтернету, крім того вони вже неодноразово були докладно розглянуті у літературі, дана стаття присвячена дещо іншій, хоча і пов'язаній темі, –інфраструктурі Інтернету. В останні роки ми є свідками ряду (більш-менш успішних) спроб об'єднання інфраструктур управління Інтернетом в інших цілях, ніж ті, які були визначені спочатку. Йдеться не лише про управління інфраструктурою як зазначалось до цього моменту, але і про управління через «творче» використання інфраструктури. Особливо це стосується контенту: конфлікти з приводу того, яким чином інформація передається та циркулює Інтернетом все частіше мають місце на нижчих рівнях. Сили глобалізації та технологічних змін зменшили можливості суверенних національних держав та виробників медіа контенту на контроль інформаційних потоків через закони та політику, тому ці учасники визнають інфраструктуру в якості механізму відновлення цього елементу керування. Те що Лаура ДеНардіс [2012] називає «поворотом інфраструктури для управління Інтернетом» тягне за собою не лише питання економічної свободи, але і проблему інформаційно-комунікаційних свобод.

Прикладом того, як суперечки з приводу посередництва контенту перейшли в сферу інфраструктури управління Інтернетом, можна знайти, наприклад, у санкціонованих урядами навмисних відключеннях основних телекомунікацій та Інтернет інфраструктур через приватних суб'єктів, чи то за допомогою протоколів, блокування програм або заборону в доступі. Уряд ініціював відключення Інтернету в умовах революції та повстання в Єгипті та Лівії, що підтверджує попереднє твердження. Проте, DNS, мабуть, на сьогодні є найкращою ілюстрацією цього «управління інфраструктурою». DNS використовує систему доменних імен для перенаправлення запитів від усього веб-сайту, а не для порушення контенту, тому, останнім часом розглядається як відповідний засіб дотримання прав інтелектуальної власності. DNS був у центрі суперечок з приводу законодавчих проектів «Захистіть IP» (PIPA) та «Зупиніть Онлайн Приватність» (SOPA).

•На шляху до децентралізованої альтернативи DNS? Дебати, баланси, побоювання

Наприкінці 2010 року організація під назвою WikiLeaks розкриває тисячі секретних даних США і вже через кілька днів втрачає свою веб-хостинг компанію та домен wikileaks.org. Дискусії з приводу «нового конкуруючого кореневого серверу», який буде здатний конкурувати із ICANN, підняли нову хвилю інтересу в Інтернеті, яку очолив відомий «анархіст» Пітер Санде. Альтернативний реєстр доменних імен передбачається як децентралізована пінгова (P2P) система, в якій всі користувачі будуть володіти частиною системи доменних імен (DNS) на своїх комп'ютерах, так що будь-який домен, який буде тимчасово недоступний через блокування, все ще зможе функціонувати на альтернативному реєстрі. Замість того, щоб просто додати більше варіантів DNS адрес до вже прийнятих і які управляються ICANN, цей проект буде на меті усунення централізованого контролю на користь розподіленої інфраструктури для користувачів. Далі у цьому розділі будуть розглядатись суперечки з приводу децентралізованої, контрольованої користувачем інфраструктури у відповідь на DNS кооптацію.

- Історія незадоволеності, історія спроб

Незадоволеність з приводу того, у який спосіб керується DNS, навряд чи просто так згасне. У зв’язку із ієрархічністю, а також з тим, що система була побудована без урахування питань безпеки, невпевнені люди робили його центром уваги раніше, ще до згаданих спорів та суперечок, і, зокрема, питання контролю над кореневою системою, що, як стверджувалось, де-факто керувалась урядом США через ICANN викликало чимало міжнародних та міжурядових нарад.

В останні роки проект Закону про боротьбу з онлайн порушеннями (COICA) 2010 року, а також його переписана, але не менш суперечлива версія 2011 року (Запобігання справжній онлайн загрозі та крадіжці інтелектуальної власності, чи скорочено PIPA), привернули увагу громадськості до ризику контролю над Інтернетом за допомогою DNS. Не чекаючи можливого прийняття COICA, уряд Сполучених Штатів в листопаді 2010 року

приступив до скасування певних доменних імен. Відповідно до слів члена мозкового центру ІКТ, це було зроблено цілком і повністю від імені «індустрії розваг». Основний матеріал для цієї секції брався із інтерв'ю з технічними розробниками, науковцями чи приватними особами, а також з спеціалістами Інтернет управління, більшість з яких побажали залишитись невідомими. Інтерв'ю були проведені в Вашингтоні, Нью-Йорку та Бостоні, а також віддалено в Італії та Франції, з вересня 2012 по квітень 2013 року.

Випадок із WikiLeaks також чудово демонструє тиск, який спричиняється через сервіс DNS проти свободи вираження думки, а також ризик концентрації: wikileaks.org був неробочим протягом багатьох днів, оскільки був лише один DNS-хостинг для цього домену. Хоча ця ситуація ілюструється багатьма епізодами щодо того, що відбувається із американськими установами та компаніями, проте ця проблема характерна не тільки для Сполучених Штатів. У Франції Закон щодо орієнтації та програмування задля гарантування внутрішньої безпеки (the Loi d'orientation et de programmation pour la performance de la securite interieure (LOPPSI) передбачає обов'язкову фільтрацію доменних імен, які уряд розцінює як загрозливі, через сервіс DNS. Розчарування з приводу управління DNS, сьогоднішнє та майбутнє, є великим та закономірним. «Заклик до зброї» Пітера Санде є тією роботою, яка вже призвела до створення ряду альтернативних DNS-проектів, спрямованих на створення альтернативних кореневих серверів таким чином, щоб обійти ICANN або інші існуючі реєстратори, або ж зорієнтованих на розвиток систем, що не використовують ієрархію DNS, наприклад, системи на основі розподіленої хеш-таблиці (DHTs). До таких проектів можна віднести систему Cornell, проект CoDoNS5, або італійську децентралізовану кореневу систему Netsukuku6 на основі ANDNA. Здається розробники нових систем, альтернативних DNS проектів дійшли консенсусу, але слід задуматись, чому деякі з цих проектів (такі як CoDoNS, або ORSN припинили існування у 2008) здаються інноваційними, але при цьому ніколи не зазнають значного розвитку. В іншому випадку, всіх їх, рано чи пізно, спіткає спільна доля.

3.2 Що потрібно замінити?

З технічної точки зору, розробники роблять кілька зауважень з приводу доцільності децентралізованої системи чи P2P DNS. DNS виконує 2 основні операції: реєстрація імен

(управління резервуванням доменних імен в Інтернеті для різних осіб) та дозвіл імен (закулісне завдання перетворення доменних імен у відповідні їх IP-адреси). Історично склалося, що термін «Система Доменних Імен» відноситься до обох цих операцій, ніби вони обов'язково пов'язані між собою. Але це далеко не так, навіть якщо служба реєстрації імен та дозволу взаємодіє, обидва мають деревоподібну структуру. Механізм реєстрації забезпечує унікальність імен, одну із найважливіших функцій DNS, а механізм дозволу дозволяє терміналу отримувати інформацію, наприклад IP-адреси в обмін на доменне ім'я. Таким чином, можна замінити лише одну із них. Саме це і робив проект CoDoNS – заміняв функцію дозволу DHT, в той час як реєстрація імен мала колишній вигляд. Заміна механізму дозволу хоча і не є простою задачею (вона повинна модифікувати тисячі терміналів), проте, є можливою: сьогодні існують альтернативні механізми. Заміна ж системи імен та реєстрації виглядає менш реалістичною для систем, що надають сервіс пошуку, в якому відповідальність за збереження інформації розподіляється між вузлами таким чином, що зміна в наборі учасників системи викликає мінімальні порушення.

Стандартизовані у двох запитах про коментарі Цільової групи проектування Інтернету (IETF) меморандуми опубліковані IETF описують методи, моделі поведінки, дослідження, або прийнятні інновації роботи Інтернету та пов'язаних з Інтернетом систем: RFC 1034 та RFC 1035. Один із розробників описує користувачів, як «Те, що набагато складніше оновити, ніж програмне забезпечення», посилаючись на кумулятивний ефект «сніжного кома». Вирішальним та спірним питанням є те, як пояснити ту функцію, яку буде виконувати проект P2P DNS.

У своєму першому заклику Пітер Санде згадує створення альтернативної кореневої папки, крок, який потягне за собою фундаментальні еволюції в механізмі реєстрації доменних імен. В минулому інші казали про створення нового доменного імені вищого рівня, а ще хтось прагне замінити DNS механізмом BitTorrent. Декілька різних проектів співіснували поміж розробниками, кожний з різними специфікаціями, що розділяли лише загальну соціальну на політичну невдоволеність існуючою системою. Іншим питанням, що обговорюється в контексті альтернативних проектів DNS є ступінь, до якого нинішній механізм DNS може бути зміненим, або ж він може бути знищений повністю. Кілька розробників, що беруть участь у проектах P2P DNS, відмічають можливість того, що організації, які до сих пір розробляють альтернативні проекти, такі як OpenNic8, беруть

участь у таких проектах для протидії ситуації, що склалася. Така організація може бути реєстратором домету .p2p, а також веб сторінки на Wiki, що описує проект. У цьому випадку, однак, стверджується, що проблеми, які на сьогодні представлені такими прикладами як ICANN, VeriSign чи національними реєстрами, зможуть бути просто змінені на систему OpenNic: «Влада не зникне, вона просто буде переміщатись від одного учасника до іншого, але це не буду, саме по собі, вирішенням проблеми».

- Що залишиться позаду?

Це той момент, коли, найчастіше, дискусії серед розробників (в межах одного проекту, а іноді і декількох) зіштовхуються с серйозною проблемою, яка має водночас технічний та глибоко політичний характер: які послуги надає DNS, та для чого вони потрібні? «Система DNS вижила та якимось дивним чином добре розвивається», – зазначають розробники. DNS надає унікальні імена, які людина може легко запам'ятати, а програма – легко розпізнати. Більше того, вона працює вже більше двадцяти років, незважаючи на значні зміни Інтернету.

Компанія, що розташовується у Вірджинії, опрацьовує різноманітні аспекти мережевої інфраструктури, в тому числі два з тринадцяти серверів кореневих імен а також реєстр доменних імен .com та .net.. В кінцевому рахунку, - стверджує бостонський розробник - перш ніж перейти до іншої системи, всі зацікавлені сторони повинні будуть розглянути детальніше систему, від якої вони заради цього відмовляються. Ця необхідність врівноваження плюсів та мінусів, зокрема, щоб усвідомити, що жодне з рішень не вирішить всі проблеми без різноманітних незручностей чи побічних ефектів, добре відома співтовариству розробників P2P, хоча в декількох деклараціях, особливо після робіт Санде, висловлюється ентузіазм щодо децентралізованої утопії. Можливі дві альтернативи для полегшення пошуку та відновлення файлів у системі P2P: або ієрархічна система, приклад для класичної системи BitTorrent, де відновлення файлу .torrent здійснюється через Уніфікований локатор ресурсів (URL), просто кажучи – через домен, або ж система працює в повністю децентралізованому стилі і в такому випадку немає єдиного кореневого сервера. Одне і теж саме ім'я може відноситись до двох абсолютно різних файлів, воно може бути записано двома різними організаціями і містити абсолютно різний контент. Як підкреслює

аналітики фірми D.C., якщо це наслідок децентралізації, то існує проблема, що потребує політичного та технічного рішення, це «пов'язано з суб'єктивною оцінкою різних зацікавлених сторін системи DNS». Деякі з опитаних техніків не розділяють оптимізму з приводу практичних наслідків таких припущень.

Реєстрація унікальних імен у середовищі P2P, без необхідності у централізованому реєстрі, вже існує в теорії та навіть має закодований алгоритм. Тим не менш, його правильне функціонування засноване на припущеннях, які дуже важко реалізовувати у контексті P2P. Як показали десятиліття досліджень цієї технології, всі частини повинні кооперуватись. Якщо система розпізнавання імен буде реалізована, що ми отримуємо, а що втратимо? Розробники знову наполягають на тому факті, що нинішня система DNS заснована на більш ніж двадцятирічному досвіді роботи та взаємодії з «реальним світом». Будь-який інший механізм , який, наприклад, заснований на системі DHT є технічно обґрунтованим, і, безумовно, заслуговує уваги будь-якого амбітного розробника, але дослідження буде тривати роками, перш ніж ідея досягне достатньо зрілої стадії розвитку. Розробники наполягають на тому, що «заяви про можливість заміни нинішньої системи DNS протягом трьох місяців навряд чи є чимось більшим за пусті звуки».

- Інжиніринг, прийняття та управління: потрійне завдання альтернативних DNS систем

Відповідно до коментарів розробників, перед альтернативними DNS системами стоять три завдання. Перше, що потрібно зробити – це «хороший інжиніринг»: безпека механізму присвоєння імен. На даний момент, впевненість користувача у результаті присвоєння імені виходить з того, що машина зробила запит на відомий сервер. У середовищі P2P, цей «одно направлений» механізм валідації зникає, на зміну якому приходить сценарій, у якому кожний вузол може відправити все і вся до DHT, без сервера, що працює як лімітуючий орган. Проект CoDoNS вирішив цю проблему впровадивши DNSSEC до своєї системи, технічно правильний спосіб вирішення проблеми. Але при цьому, потрібно просто змінити дозвіл системи, а архітектура та управління залишаються тими самими, що були раніше, з усіма їх недоліками. Загалом, з'являється все більше доказів того, що досягнення повної безпеки неможливе у «чистому» P2P середовищі.

У разі, якщо будь-який із децентралізованих проектів DNS дозріє до стадії використання користувачем, основним питанням може стати рівень довіри цих самих користувачів між собою: «сьогодні ми маємо довіру до таких DNS серверів, як Open DNS, Google DNS, тощо, у питаннях перенаправлення, коли ми хочемо отримати доступ до певного сайту. Згідно із схемою, яку пропонує P2P DNS, нам доведеться покладатись на інших користувачів мережі. Одна справа довіряти Open DNS, або Google, і зовсім інша – випадковому комп'ютеру у мережі».

Крім вибору структури та інновацій, постає питання про політичне управління, яким дуже гостро (і це не дивно) переймаються розробники. Основні питання, які викликають пропозиції щодо системи P2P DNS мають глибоко політичний характер: питання щодо контролю, свободи та цензури.

DNSSEC використовує для перевірки підписів ієрархічну систему DNS. Тобто, таку, що не довіряє будь-якому із компонентів системи, наприклад, супер-вузлам, які мають функцію управління над системою. Протокол граничного шлюзу (BGP) – це протокол, що використовується для маршрутизації в Інтернеті та включає у себе таблицю IP-мереж, або «префікси», які позначають доступні автономним системам мережі. Методи, які контролюють вхідний та вихідний мережеві трафіки на основі аналізу пакетних даних, базуються на заздалегідь визначеному наборі правил.

У кінцевому рахунку, загальний інтерес технічних та політичних діячів підвищується. Інтернет дійсно може знайти шляхи «лікування цензури». Як одного разу зауважив піонер Інтернету Девід Кларк: «технічні проектні рішення є політичними, так самок як будь-який закон, викладений на папері».

Висновки

Що нам розкажуть про найближче управління Інтернетом історії кооптації інфраструктури та «творчих інновацій», такі як дебати навколо децентралізованої системи DNS? Часта критика цієї міждисциплінарної галузі викликана тим, що вона має тенденцію до зосередження уваги на обмеженому числі міжнародних інститутів та дискусій про глобальну політику в Інтернеті. «Управління Інтернетом» не може застосовуватись до великого числа заходів та повсякденної практики в Інтернеті та з Інтернетом, що відіграє

важливу роль у формуванні та регулюванні «Мережі мереж» [Ван Ітен, 2009].

У цьому контексті підходи STS до інфраструктури, згаданої у цій статті, може сприяти відділенню від концепції Інтернету як апріорі ідентифікованого і жорстко обмеженого простору. Ця перспектива дозволяє представити набір механізмів, які допомагають учасникам у технічному, політичному та економічному управлінні «Мережею мереж», для того, щоб побудувати загальну базу даних.

У таких проектах, як P2P DNS, або альтернативний P2P електронний біткойн, Інтернет користувачі не лише довіряють решті користувачів мережі чистину свого програмного забезпечення та апаратних засобів, а ще і залежать від інших користувачів та комп'ютерів мережі для управління інформацією, зв'язку, тощо. Якщо користувачі звикли довіряти класичним DNS серверам, або центральному банку, для того, щоб вони направляли їх у потрібному напрямку для отримання доступу до веб-сайту або для узаконення вартості їх валюти, то що їм заважає зробити те саме із випадковим домашнім комп'ютером? Які цінності повинні лежати в основі концепції мережі, щоб користувачі були готові перетворити свої апаратні засоби у частину «телефонної книги» Інтернету, а бо в генератор віртуальної, децентралізованої валюти, заради глобального, альтернативного Інтернету? Яким чином політичні суб'єкти управління Інтернетом використовують можливості для «глобальних змін» [Рейескі, 2003] сучасного Інтернету?

У цій статті ми запропонували деякі напрями та засоби для того, щоб дати відповіді на ці запитання, а також внесли свій внесок у дослідження цих новонароджених систем, сфокусованих на користувачах та самоорганізації, таких, що характеризуються розвитком та децентралізацією управління, що надають альтернативу сьогоднішній централізованій системі не шляхом усунення ієрархії, а шляхом її модифікації. Роблячи це, ми спробували показати, що Інтернет інфраструктура та технічна архітектура сьогодні знаходяться в центрі дебатів та домовленостей - не лише як об'єкт управління, але і як набір інструментів для управління. Ця зміна має важливі наслідки: ці інструменти повинні бути використані таким чином, щоб, не дивлячись на потенційні проблеми, не становити реальної загрози стабільній роботі Інтернету та його безпеці. Необхідно підвищити рівень усвідомлення усіма відповідними сторонами того, що відбувається на нижніх рівнях «Мережі мереж» для того, щоб кооптація інфраструктури Інтернету не зашкодила його функціям та ненавмисно не завдала шкідливих наслідків його роботі.

Посилання

- Abbate, J. (2012). L'histoire de l'Internet au prisme des STS. Le temps des medias, 18: 170-180.
- Aigrain, P. (2011). Another Narrative. Addressing Research Challenges and Other Open Issues session, PARADISO Conference, Brussels, 7–9 Sept. 2011.
- Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation, Education permanente, 134 : 78-89.
- Atton, C. (2005). An Alternative Internet. Edinburgh, UK: Edinburgh University Press.
- Berners-Lee, T. (2010). Long Live the Web: A Call for Continued Open Standards and
- Neutrality, Scientific American, November 2010.
- Braman, S. (2011). Designing for Instability: Internet Architecture and Constant Change. Media In Transition 7 (MIT7) Unstable Platforms: the Promise and Peril of Transition, Cambridge, MA, May 13-15, 2011.
- Bricklin, D. (2001). The Cornucopia of the Commons. In A. Oram (Ed.), Peer-to-Peer: Harnessing the Power of Disruptive Technologies (pp. 59-63). Sebastopol, CA : O'Reilly.
- Cheniti, T. (2009). Global Internet Governance in Practice. Mundane Encounters and Multiple Enactments. Unpublished DPhil Thesis, University of Oxford.
- DeNardis, L. (2013). The Emerging Field of Internet Governance, in William Dutton (ed.)
- Oxford Handbook of Internet Studies. Oxford: Oxford University Press.
- DeNardis, L. (2012). Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance, Journal of Information, Communication and Society, 15 (3).
- DeNardis, L. (2009). Protocol Politics : The Globalization of Internet Governance. Cambridge, MA : The MIT Press.
- Elkin-Koren, N. (2006). Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic. New York University Journal of Legislation & Public Policy, 9 (15), 15-76.
- Flichy, P. (2007). The Internet Imaginaire. Cambridge, MA: The MIT Press.
- Fuller, M. (2008, Eds.). Software Studies: A Lexicon. Cambridge, MA: The MIT Press.

•Kirschenbaum, M. (2003). Virtuality and VRML: Software Studies after Manovich. Electronic Book Review.

•Latour, B. (1987). Science in Action : How to follow scientists and engineers through society.

•Cambridge, MA : Harvard University Press.

•Levinson, N. (2010). Co-creating Processes in Global Governance: the Case of the Internet Governance Forum. Fifth Annual Global Internet Governance Academic Network Conference, Vilnius, Lithuania.

•Malcolm, J. (2008). Multi-Stakeholder Governance and the Internet Governance Forum. Wembley, WA : Terminus Press.

•Manovich, L. (2001). The Language of New Media. Cambridge, MA: The MIT Press.

•Marino, M. C. (2006). Critical Code Studies. Electronic Book Review.

•Minar, N. et Hedlund, M. (2001). A network of peers – Peer-to-peer models through the history of the Internet. In A. Oram (Ed.), Peer-to-peer: Harnessing the Power of Disruptive Technologies, 9-20. Sebastopol, CA: O'Reilly.

•Monberg, J. (2005). Science and Technology Studies Approaches to Internet Research. The Information Society, 21 (4): 281-284.

•Mueller, M. (2010). Networks and States: The Global Politics of Internet Governance. Cambridge, MA: The MIT Press.

•Musiani, F. (forthcoming 2013). Nains sans geants. Architecture decentralisee et services Internet. Paris : Presses des Mines.

•Musiani, F. (2012). Caring About the Plumbing: On the Importance of Architectures in Social Studies of (Peer-to-Peer) Technology. Journal of Peer Production, 1.

•Rejeski, D. (2003). Making Policy in a Moore's Law World. Ubiquity, December 2003.

•Ribes, D. & Lee, C. P. (2010). Sociotechnical Studies of Cyberinfrastructure and e-Research: Current Themes and Future Trajectories. Computer Supported Cooperative Work, 19, 231-244.

•Schollmeier, R. (2002). A definition of peer-to-peer networking for the classification of peer-topeer architectures and applications. Proceedings of the First International Conference on Peer-to-Peer Computing, 27–29.

•Star, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43 (3),377-391.

•Star, S. L. & Bowker, G. (2006). How To Infrastructure. In Lievrouw, L. A. (Ed.), Handbook of

•New Media (pp. 151-162), London: Sage. van Eeten, M. (2009). Where is the Governance in Internet Governance? GigaNet Annual Symposium, Sharm-el-Sheikh, Egypt, November 14th, 2009.

•van Schewick, B. (2010). Internet Architecture and Innovation. Cambridge, MA: The MIT Press.

4.2.5. Роберт Уерпман — Вітцак. Принципи міжнародного Інтернет-права

Принципи міжнародного Інтернет-права

Роберт Уерпман - Вітцак

Резюме
Принципи права займають важливе місце в системі юриспруденції. Вони сприяють систематизації, аналізу та подальшій розбудові правопорядку. Хоча міжнародне Інтернет-право є порівняно новим об'єктом правових досліджень, деякі принципи даного інституту вже починають поступово формуватись. У статті розглядатимуться п'ять основних принципів міжнародного Інтернет-права, що наразі розвиваються:
1) принцип свободи Інтернету;
2) принцип конфіденційності (принцип недоторканності особистого життя);
3) видозмінений принцип територіальності (територіальної юрисдикції), пристосований до кіберпростору;
4) принцип міждержавного співробітництва;
5) принцип співробітництва всіх зацікавлених сторін.

А. Вступ
Міжнародне Інтернет-право (МІП) є відносно новим інститутом. Хоча Інтернет бере свої витоки ще з 1960-х рр., його політичне та економічне значення почало проявлятись лише на початку 1990-х рр., тим самим активізуючи інтерес багатьох правознавців до питань управління Інтернетом.
МІП - це загальне поняття, яке охоплює норми міжнародного права, що регулюють процеси функціонування та використання системи Інтернет.
Більше того, МІП є міжгалузевим інститутом, який, в тому числі, торкається питань прав людини, а також питань, що регулюються міжнародним економічним правом та правом міжнародних організацій. Вже на даному етапі чимало питань в сфері МІП викликають серед вчених серйозні дискусії. Найбільш яскравим прикладом є проблема здійснення Інтернет-корпорацією з присвоєння імен та адрес (ICANN) управління над Системою доменних імен (DNS). Не менш суперечливим є питання обсягу внутрішньої компетенції держави щодо контролю за Інтернет-контентом, що знаходиться на іноземних серверах. Для Світової організації торгівлі та інших міжнародних організацій ключовим є питання торгівлі через Інтернет (електронна комерція). По мірі того, як Інтернет проникає в усі сфери людського життя, МІП межує практично з усіма сферами міжнародного права. Так, наприклад, дискусії щодо кібервійни зачіпають питання jus ad bellum (права війни) та міжнародного гуманітарного права. Через такий міжгалузевий підхід норми МІП можуть видатись гетерогенними та навіть незв'язними між собою. Тим не менш, помітну роль у становленні інституту відіграють деякі основоположні принципи. В даній статті розглядатимуться принципи МІП, що наразі активно формуються.

Принципи права виконують щонайменше дві функції. По-перше, вони допомагають систематизувати правові норми, тим самим, пояснюючи їх природу. Саме ця функція дозволяє перетворити ряд незв'язних правових норм у правопорядок. Це не обов'язково

вказує на завершеність процесу формування правопорядку. Міжнародний правопорядок все ще досить фрагментарний, оскільки міжнародне право застосовується лише в тих випадках, коли питання не може бути належним чином врегульоване внутрішньодержавним правом. Принципи можуть бути викладені в правових документах, як наприклад у ст. 2 Статуту ООН, чи вони можуть бути визнані державами шляхом їх закріплення в міжнародних деклараціях. Навіть за умови відсутності такого визнання в правовій доктрині наявні такі правові принципи, які було б доцільно використати при систематизації сукупності правових норм.

По-друге, правові принципи є елементом правового обґрунтування. Вони допомагають тлумачити певні норми міжнародного права, а також виявити об'єкт і мету цих норм. Отже, міжнародні договори можуть тлумачитись залежно від того, які правові принципи лежать в їх основі. Також принципи права можуть впливати на процес розвитку міжнародного звичаєвого права. Хоча істотним елементом міжнародного звичаю є саме міжнародна практика, іноді держави можуть використовувати правові принципи для обґрунтування відповідної норми (правила), яка лежить в основі міжнародного звичаю. Досить часто міжнародні судді та вчені розкривають принципи в своєму правовому обґрунтуванні, що спирається на міжнародний звичай. Загальноприйняте правило, за яким для здійснення юрисдикції державою необхідний реальний зв'язок (між судном та державою – авт.), безпосередньо спирається на засади (розумності) обґрунтованості та певні правові принципи.

Ці правові принципи відрізняються від концепції загальних принципів права, викладених у статті 38 (1) (c) Статуту Міжнародного Суду ООН (МС ООН). Останні були запозичені з внутрішньодержавного права і покликані заповнити прогалини у міжнародному праві, що виникають, наприклад, у ході судового розгляду тощо. Для порівняння, в даній статті будуть розглядатись принципи, що виникли на основі міжнародного права. Деякі з цих принципів можуть мати аналоги у внутрішньодержавному праві (правопорядку), водночас решта застосовуються виключно в сфері міжнародного права. Якщо ці принципи не закріплені в міжнародних договорах і не випливають зі звичаєвого права, за юридичною силою вони наближаються до допоміжних джерел міжнародного права, зазначених в ст. 38 (1) (d) Статуту Міжнародного Суду ООН. Вони є частиною правової доктрини. При застосуванні джерел міжнародного права деякі суди та вчені висловлюють суперечливі думки щодо правових принципів.

Хоча міжнародне Інтернет-право є порівняно новим об’єктом правових досліджень, деякі принципи даного інституту починають поступово формуватись.
1) принцип свободи Інтернету;
2) принцип конфіденційності (принцип недоторканності особистого життя);
3) видозмінений принцип територіальності (територіальної юрисдикції), пристосований до кіберпростору;
4) принцип міждержавного співробітництва;
5) принцип багатостороннього співробітництва.
У заключному розділі буде проаналізовано, яким чином ці принципи регулюють взаємозв'язки між різними суб’єктами в контексті користування системою Інтернет.

Принцип свободи Інтернету

Будучи тісно пов'язаним з міжнародним правом захисту прав людини, свобода спілкування складає основу свободи Інтернету. Водночас виникає питання чи свобода Інтернету поширюється і на комерційні права в Інтернеті. У цьому розділі будуть розглядатись (I) свобода спілкування в Інтернеті, і (II) свобода Інтернет-бізнесу.

I. Свобода спілкування в Інтернеті

Свобода слова є однією з ключових свобод Інтернету. Стаття 19 (2) Міжнародного пакту про громадянські і політичні права (МПГПП) гарантує цю свободу на універсальному рівні. В Європі відповідне право закріплене у статті 10 Європейської конвенції з прав людини (ЄКПЛ). У статті 19 (2) МПГПП чітко прописано: " за допомогою ... чи іншими способами на свій вибір". Хоча в статті 10 ЄКПЛ відсутні будь-які згадки щодо цього положення, можна зробити висновок, що Конвенція захищає в рівній мірі свободу слова в Інтернеті. Інформація та ідеї, висловлені в мережі підпадають під дію статті 10 ЄКПЛ. У справі *Times Newspaper Ltd. v. United Kingdom,* Європейський суд з прав людини нещодавно постановив, що ст. 10 ЄКПЛ охоплює питання Інтернет архівів. Оскільки свобода слова тісно пов'язана зі свободою інформації (вільного доступу до інформації), широкі права (можливості) отримують не тільки провайдери Інтернет-контенту, а й звичайні користувачі. Незважаючи на те, що ні в ст. 19 МПГПП, ні в ст. 10 ЄКПЛ не зазначається нічого стосовно свободи преси (друку), Європейський суд з прав людини підкреслив важливість преси для контролю за розвитком демократичного суспільства. Це ж саме стосується й електронної преси. З правової точки зору у своєму рішенні в справі *Fatullayev v. Azerbaijan*, Європейський суд з прав людини прирівняв популярний Інтернет-форум до друкованих засобів масової інформації.

Варто також відзначити, що в обох правових документах передбачено гарантії свободи слова «незалежно від державних кордонів». Це є ключовим щодо Інтернету, який не має жодних кордонів.

На відміну від норм, принципи не вимагають сурового дотримання. Оскільки принципи охоплюють досить широке коло питань, вони досить часто конфліктують з іншими принципами та інтересами. В цьому випадку принцип може бути реалізований в тій мірі, наскільки це можливо при конкретних юридичних та фактичних обставинах. Стосовно свободи Інтернету Європейський суд з прав людини у справі *Megadat.com v. Moldova визнав важливість державного контролю. Відображення такого права держави міститься в ст. 19(3)* МПГПП і ст. 10 (2) Європейської конвенції. В даних статтях вказано перелік законних підстав, які можуть виправдати втручання держави. Такі підстави включають принципи та інтереси, такі як: права інших, національна безпека, суспільний порядок і моральні засади. У випадку конфлікту між сторонами має бути встановлено справедливу рівновагу інтересів. Таке положення можна реалізувати за допомогою

критерію пропорційності та критерію необхідності, передбаченого у статтях 19 (3) МПГПП та 10 (2) ЄКПЛ.

II. Свобода Інтернет-бізнесу

Принцип свободи Інтернету не обмежується суто питаннями свободи слова. Як засіб спілкування, Інтернет залежить від ефективності функціонування власної інфраструктури (технічної бази). Відповідно свобода Інтернету охоплює свободу Інтернет-провайдерів, в результаті чого важливим чинником виступають комерційні права. При цьому міжнародне право захисту прав людини подібних прав майже не передбачає. Це питання, в більшій мірі підпадає під дію торгового права. В даному розділі розглядатиметься: 1) міжнародне право захисту прав людини; 2) міжнародне торгове право.

1. Міжнародне право захисту прав людини

В порівнянні з національними законами міжнародне право не гарантує ні свободи вибору професії, ні свободи ведення бізнесу. Водночас, навіть якщо їх діяльність набуває комерційного характеру, Інтернет-провайдери можуть користуватись свободою слова і посилатись на неї у випадку будь-якого втручання стосовно змісту викладеного. Наприклад, Європейськый суд з прав людини у своєму рішенні у справі *Times Newspaper Ltd* постановив, що наявність відповідальності за наклепницький зміст статті в Інтернет-архівах порушувала право компанії на свободу слова. Саме по собі таке втручання не є законним і, щоб бути таким, необхідна наявність відповідних обставин, що могли б виправдати його.

Хоча ЄКПЛ й не захищає безпосередньо комерційної діяльності як такої, Інтернет-провайдер може в випадку необхідності посилатись на право власності, закріплене у статті 1 Першого протоколу до ЄКПЛ. У справі Megadat.com Європейський суд з прав людини постановив, що, відповідно до ст. 1 Першого протоколу до ЄКПЛ, ліцензія на надання Інтернет-послуг була приватною власністю, таким чином спроба припинення дії ліцензії фактично означала б втручання. Ще одним прикладом захисту майнових прав в Інтернеті є зареєстровані доменні імена, які теж передбачені в цій статті.

Водночас на разі ЄКПЛ не встановлює механізму для загального захисту прав Інтернет-провайдерів.

Ще менш дієвими в цій сфері є положення Міжнародного пакту про громадянські і політичні права, в якому право власності взагалі не передбачено. Відповідно до статей 1 і 2 МПГПП Факультативного протоколу № 1 від 19 грудня 1966 року компаніям не надається право оскарження до Комітету з прав людини. Хоча таке право надається неурядовим організація, тобто юридичним особам, загалом Факультативний протокол до МПГПП обмежує коло суб'єктів оскарження до індивідів.

2. Міжнародне торгове право

Гарантії свободи транснаціональної Інтернет-торгівлі можливо варто шукати в основі міжнародного торгового права. Забороняючи вводити кількісні обмеження на імпорт та експорт, стаття XI Генеральної угоди з тарифів і торгівлі (ГАТТ) фактично передбачає вільний доступ до ринків. Щодо торгівлі послугами, то в статті XVI Генеральної угоди про

торгівлю послугами (ГАТС) чітко сформульовано, що надання доступу до ринків є обов'язком учасників. Торгівля, пов'язана із апаратним (технічним) забезпеченням, наприклад серверами та персональними комп'ютерами, регулюється положеннями ГАТТ. Для порівняння, об'єктом віртуальних економічних відносин є не обмін товарами - матеріальними об'єктами, а торгівля послугами, яка, в свою чергу, регулюється положеннями ГАТС.

При цьому досить складно із положень ГАТС вивести принцип свободи доступу до ринків, адже прямо в ст. XVI ГАТС даний принцип не передбачено. Більше того, рішення про надання доступу до ринків приймають держави залежно від того, чи будуть включені ті чи інші категорії послуг до списку їх конкретних зобов'язань відповідно до ст. XX ГАТС. Навряд чи можна встановити принцип вільного доступу до ринків, якщо більшість країн не виконали своїх відповідних зобов'язань. Більше того, процес включення послуг до списку є досить об'єктивним. Наприклад, надання доступу до ринку послуг, що стосуються азартних ігор в Інтернеті, залежить від того, чи держава брала на себе відповідні зобов'язання щодо азартних ігор загалом. Поставка онлайн не являє собою окрему категорію послуг. За відсутності загальної категорії Інтернет послуг, важко встановити принцип доступу до Інтернет ринку.

Інше питання виникає щодо правової природи доступу до ринків в рамках ГАТТ та ГАТС. Як прибічник конституційного підходу, Ернст-Ульріх Петерсман переконаний, що гарантії свобод, передбачені в ГАТТ та ГАТС, є особистими правами індивідів. Проте його позиція зазнала значної критики. Звичайно в контексті проблеми щодо природи принципів це питання залишається відкритим. Принцип вільного доступу до ринків може існувати й тоді, коли його застосовують держави, а не окремі індивіди.

Як і будь-який інший принцип, вільний доступ до ринків не має обов'язкової сили. Він може конфліктувати з іншими принципами, тому необхідно дотримуватись засад розумності і справедливості для встановлення рівноваги. Це правило закріплено в загальних положеннях про звільнення від відповідальності у статті XX ГАТТ та статті XIV ГАТС. Обидві статті містять перелік керівних принципів, серед яких захист суспільної моралі і правопорядку. Хоча Апеляційний орган СОТ застосовує критерій необхідності по-іншому ніж Європейський суд з прав людини, обидві судові інституції балансують дію обмежувальних заходів співвідносно до його дії. Так, Апеляційний орган СОТ постановив у справі *US – Gambling*, що захист суспільної моралі може принципово виправдати обмеження і навіть повну заборону свободи поширення азартних Інтернет-ігор.

С. Принцип конфіденційності (недоторканості особистого життя)

Принцип конфіденційності міцно закріпився в міжнародному праві захисту прав людини. Стаття 17 МПГПП передбачає захист особистого життя, сім'ї, будинку, листування, честі та гідності. Стаття 8 ЄКПЛ торкається питань приватного і сімейного життя, житла і листування. Положення обох статей мають широкий спектр застосування, який був розвинутий Європейським судом з прав людини. Зміст цих статей дозволяє зробити висновок, що електронна пошта є також частиною листування, яке захищається. Інші дані, які передаються через Інтернет або які доступні через Інтернет відносяться до приватного життя людини, крім випадків, коли такі дані передбачені для публічного доступу. У своєму

рішенні у справі *Copland v. United Kingdom* Європейський суд з прав людини визначив, що користування робітником Інтернетом - це частина його особистого життя та листування. Таким чином здійснення державою контролю за використання Інтернету та контенту індивідами, включаючи електронну пошту, прирівнюється до посягання на особисте життя. Те ж саме вірно для зобов'язання Інтернет -провайдерів зберігати дані Інтернету, викладені в статті 3 Європейської Директиви 2006/24/ЕС про збереження даних, згенерованих або оброблених у зв'язку з наданням загальнодоступних послуг електронного зв'язку. Навіть людина, яка не корисується Інтернетом може постраждати через інформацію, що стосується його або її, опубліковану в Інтернеті. Навіть якщо державні органи опублікувати таку інформацію, або якщо законодавство зобов'язує її опублікувати, це можна кваліфікувати як втручання держави в особисте життя; саме так це положення було сформульовано у рішенні Європейського суду з прав людини у справ *Wypych v. Poland* . Таким чином, законність залежить від правового обгрунтування.

Загрозу для недоторканості особистого життя в Інтернеті складають не тільки дії з боку державних органів, а й з боку юридичних осіб та підприємств. Інтернет-платформи для збору інформації стосовно юридичних осіб та соціальних спільнот містять величезні масиви особистої інформації, які у випадку крадіжки чи неправильного використання, можуть поставити під загрозу чи завдати шкоди життю будь-якої особи. Більше того, серйозний вплив на індивіда здійснює саме публікація в Інтернеті інформації, що відноситися до нього. Саме це продемонстрували Інтернет опитування, проведені спеціалістами в галузі освіти та медицини. У таких випадках позитивний обов’язок захисту особистого життя індивіда покладається на державу. Цей обов’язок передбачений у статті 17 (2) МПГПП, в якій міститься положення, згідно з яким кожен індивід має право на захист від втручання в особисте життя. Хоча ЄКПЛ не містить схожого положення, Європейський суд з прав людини визначив деякі позитивні зобов'язання із змісту статті 8 ЄКПЛ.

Водночас було б неправильно, акцентувати увагу виключно на особистому житті. Із справ, що перебувають на розгляді, видно, що право на захист особистого життя часто конфліктує з Інтернет- свободами . В цьому випадку два окремих принципів МІП колідують між собою. Хоча свобода слова й може бути обмежена на користь прав інших осіб і, зокрема права на недоторканість особистого життя, будь-яке таке обмеження має здійснюватись на засадах пропорційності. Держави повинні забезпечити справедливий баланс між недоторканністю особистого життя, з одного боку, та Інтернет - свободами, з іншого. Якщо людині загрожує небезпека, держава повинна вжити всіх необхідних засобів, а за необхідності передбачити кримінальну відповідальність. У справі *K. U. v. Finland*,, невідомий розмістив від імені 12-річного хлопчика оголошення на Інтернет -сайті знайомств. На той момент відповідно до фінського законодавства постачальник послуг не міг бути примушений виявити особу людини, яка розмістила рекламу. Тому неможливо було пред’явити будь-які звинувачення. Відтак Європейський суд з прав людини у своєму рішенні постановив, що Фінляндія не змогла виконати свої позитивні зобов'язання щодо захисту особистого життя хлопчика.

D. Принцип територіальності (територіальної юрисдикції)

Зобов’язання держави, що випливають з норм права захисту прав людини, утримуватись від певних дій, дещо обмежують повноваження відповідних органів державної влади. Вони

створюють і гарантують ті особисті свободи, які захищені від втручання держави. Питання юрисдикції, навпаки, напряму пов’язані з відносинами між державами. Відповідно до принципу суверенної рівності, стаття 2 (1) Статуту Організації Об'єднаних Націй, юрисдикція однієї держави закінчується там, де починається юрисдикція іншої держави. Таким чином, здійснення повноважень державою вимагає реального (істотного, ефективного) зв'язку. Держава може здійснювати територіальну юрисдикцію щодо власної території і персональну юрисдикцію щодо своїх громадян.

Принцип територіальності є одним з найрозвиненіших в міжнародному публічному праві. Тим не менш, в контексті кіберпростору необхідно розрізняти деякі відмінності. Перш за все, необхідно пристосувати доктрину впливу, відповідно до якої держава має право вживати заходів щодо іноземних дій, якщо вони мають вплив в межах державної території, до всюдисущої природи Інтернету. По-друге, юрисдикція держави поширюється й на останню частину доменної адреси держави в Інтернеті, що стає так званою кібертериторією (державним кіберпростором). У цьому розділі будуть досліджуватись окремі аспекти доктрини кваліфікованоо впливу та питання останньої частини доменної адреси держави в Інтернеті, тобто так званої кібертериторії.

І. Доктрина обмеженого впливу

Стаття 22 Європейської Конвенції про кіберзлочинність (ЕСС) від 23 листопада 2001 закріплює принцип територіальної юрисдикції. Відповідно до статті 22 (1) (а) ЕСС кожна договірна сторона встановлює юрисдикцію щодо злочинів, скоєних на її території. Загальноприйнятим правилом є те, що злочин вважається скоєним на тій території, де безпосередньо діяв його виконавець. Якщо особа публікує матеріали аморального змісту, наприклад порнографічні матеріали на веб-сайті держава, на території якої знаходиться комп’ютер, з якого були здійснені відповідні дії, має право втрутитися . Загальноприйнятим є також і той факт, що злочин вважається скоєним на території тієї держави, де є очевидними наслідки даного злочинного діяння. В цьому принцип територіальної юрисдикції подібний до доктрини наслідків, яка встановлена в антимонопольному праві. Комітет міністрів Ради Європи підтвердив функціонування доктрини впливу у своєму коментарі до статті 22 ЕСС. За даними Комітету, держава повинна не тільки «забезпечити здійснення територіальної юрисдикції», коли і особа, що здійснює атаку на комп'ютерну систему, і система, яку атакують, розташовані на її території" , але і "у випадках, коли комп’ютерна система, на яку здійснюють спробу атаки, розташована в межах державної території , а зловмисник знаходиться деінде". При цьому між державою, де знаходиться система, та безпосередньо фактом атаки прослідковується істотний зв’язок, оскільки дана комп’ютерна система фактично функціонує в цій державі. Менш чітко простежується механізм при публікації аморального контенту. Фактично доступ до веб-сайту є можливим з будь-якого куточку світу. Відповідно до змісту доктрини впливу, юрисдикція держави може бути встановлена, коли представник держави може зайти на сторінку з аморальним матеріалом зі свого робочого місця. У справі *Perrin,* британські суди звинуватили французького громадянина у публікації непристойних матеріалів на американських веб - сторінках, через те, що співробітник поліції побачив це через комп’ютер у відділку лондонської поліції. У справі *Toeben*, німецькі суди засудили австралійського громадянина за заперечення факту Голокосту, опублікованому на австралійській Інтернет-сторінці. У справі *Yahoo*, суд вищої інстанції Парижа (Паризький обласний суд) постановив, що продаж

нацистських пам'ятних речей на сервері США, суперечив французькому кримінальному законодавству. Якби не було ніяких обмежень, веб – контент всесвітньої павутини мав би бути гармонізований із законодавством більш як 190 держав. Оскільки Інтернет має транснаціональний характер, проста можливість переглядати веб - сторінки в певній державі не може бути достатньою підставою для того , щоб встановити реальний зв'язок між веб –сторінкою та державою, що веде розслідування.

Ця точка зору отримала широке визнання суддів і вчених. Відповідно було зроблено имало спроб модифікувати доктрину впливу таким чином, щоб врахувати всеохоплюючу природу кіберпростору. Суди США у своїй практиці покладаються на доктрину розумного впливу.
Хоча судова практика у всьому світі і не є однорідною , все частіше для того, щоб визначити наявність зв'язку з Інтернет-сторінкою, використовують єдині критерії. Ці критерії включають в себе мову, зміст та рекламу, що відносяться до певної держави. Якщо необхідно здійснити вибірку інформації стосовно певної держави із буферу (сховища), така держава отримує підґрунтя для здійснення юрисдикції стосовно такої інформації. У справі Toeben, німецький федеральний суд принаймні посилався на те,що заперечення факту Голокосту безпосередньо стосувалось Німеччини. У справі Perrin, стороною обвинувачення став житель Сполученого Королівства, при цьому факт президентства став ще одним свідченням наявності істотного зв'язку.

Насправді, державна юрисдикція, базована на доктрині кваліфікованого впливу, окрім порушення суверенітету інших держав, в окремих випадках суперечить положенням принципу свободи Інтернету. Свобода слова «незалежно від кордонів», як вказано у статті 19 (2) МПГПП і статті 10 (1) ЄКПЛ, мала б лише деклараційний характер, якби контент - провайдери були змушені блокувати доступ для іноземних користувачів, побоюючись судового переслідування чи навіть переслідування за кордоном. Необхідно знайти баланс між конфліктуючими принципами територіальної юрисдикції і свободи в Інтернеті. З позицій міжнародного права захисту прав людини випливає, що юрисдикція іноземної держави повинна ipso facto братись до уваги. Це ж саме говориться і в доктрині кваліфікованого впливу, що діє на засадах розумності.

II. Остання частина доменної адреси держави в Інтернеті як межа державної кібертериторії

У МІП принцип територіальної юрисдикції дещо трансформується. Територія – частина земної поверхні (суходіл, внутрішні акваторії, повітряний простір над ними), на які поширюється виключний суверенітет цієї держави. Інтернет ототожнюють з державною територією, оскільки люди можуть там діяти і навіть жити. У 1996 році Джон Перрі Барлоу рішуче проголосив незалежність кіберпростору. Барлоу використовував терміни «суверенітет» і «суспільний договір» для того, щоб довести, що кіберпростір – це «світ», непідконтрольний державі. Разом з тим стало ясно, що держави прагнуть і можуть здійснювати свою юрисдикцію щодо кіберпростору. Ще більш вражаючим є те, що частини кіберпростору поступово стають частиною державної території. Остання частина доменної адреси держави в Інтернеті, наприклад .uk для Великобританії, .pl для Польщі може вже вважатися такою, що позначає кордони кібертериторій цих держав.
Ці частини доменної адреси держави в Інтернеті були створені Джоном Постелем, батьком

системи імен доменів, який використав перелік кодів держав, встановлений Міжнародною організацією зі стандартизації. Він передав право адміністрування над системою доменних адрес держав науковим та іншим установам, які висловили бажання вести такий системний реєстр. Починаючи з 1998 року створення і надання доменних адрес держав – завдання Інтернет-корпорації з присвоєння імен і номерів (ICANN), що є некомерційною організацією, створеною відповідно до законодавства штату Каліфорнія. Це стосується як кодів країн доменів вищого рівня, так і для доменів вищого рівня загального користування, таких як .com або .info. Відповідно коди країн доменів вищого рівня фактично є елементом системи, яка раніше майже не була підконтрольною державам. На сьогодні у Великобританії та Німеччині списки кодів країн доменів вищого рівня активно впроваджуються в сфері приватного бізнесу, при цьому обидві держави мінімізують обсяги державного контролю за процесами в кіберпросторі. Інші держави, зокрема Франція, навпаки, такий контроль посилюють. Це стосується і ЄС, який Регламентом ЄС 733/2002 Європейського парламенту і Ради створив власний код домену вищого рівня .eu. Відомство з питань реєстрації, EURid, було попередньо призначене Європейською комісією шляхом запиту про висловлення зацікавленості, а також між відомством та Європейською Комісією було підписано концесійний догорів про надання послуг. Регламентом ЄС 874/ 200480 Комісія прийняла правила публічного порядку, що регулюють процес адміністрування щодо власного коду домену вищого рівня .eu. Таким чином, Європейський Союз встановив вимогу щодо повної юрисдикції над власним доменом.

Ця вимога спирається на міжнародні документи. Теоретично створення і делегування доменних адрес держав знаходиться в сфері обов’язків Інтернет-корпорації з присвоєння імен і номерів (ICANN). Організація GAC (Урядовий дорадчий комітет) займається контролем діяльності ICANN, надаючи їй різні рекомендації. Хоча відповідно до статуту Урядовий дорадчий комітет формально є структурною одиницею ICANN, в дійсності він більше нагадує самостійну міжнародну організацію. Рекомендації GAC не є юридично обов'язковими для ICANN, він «належним чином враховує» рекомендації урядів, які de facto володіють правом вето. У 2005 році GAC ухвалив Основні принципи та керівні положення щодо делегування та адміністрування кодів доменів вищого рівня. Відповідно до цих принципів «Правом прийняття рішень щодо найбільш доцільного коду країни домену вищого рівня покладається на відповідні уряди». Цим фактично було підтверджено суверенітет держави в цій сфері.

Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства (ВСІС) , який проходив в два етапи у Женеві в 2003 р. і в Тунісі у 2005 р., містять схожі положення. Пункт 63 Туніської програми інформаційного суспільства від 18 листопада 2005 р. визнає, що:

> *Держави не повинні брати участь у прийнятті рішень щодо коду домену верхнього рівня (ccTLD) іншої держави. Законні інтереси, визначені кожною окремою державою, які стосуються, тим чи іншим чином, національних кодів доменів верхнього рівня, повинні з належною повагою бути розглянутими та захищеними за допомогою гнучких та вдосконалених механізмів та процедур.*

Навіть більше, в проекті від 30 вересня 2005 року визнавалось, що «кожен уряд повинен

мати суверенітет над національними кодами доменів верхнього рівня». У всіх відповідних документах говориться про адміністрування та контроль над національними кодами доменів верхнього рівня, відповідно загальною ідеєю для всіх є те, що існує реальний зв'язок між національним кодом домену верхнього рівня та відповідною державою. Відповідно держава може здійснювати повну юрисдикцію щодо свого національного домену. Національний код домену верхнього рівня перетворюється в державну територію в кіберпросторі. Таким чином, Великобританія може здійснювати кримінальну юрисдикцію щодо будь-якого злочину, вчиненого в межах національного домену .uk.
Отже, кіберпростір не порушує принцип територіальної юрисдикції. Принцип адаптується до особливої природи Інтернету.

Принцип міждержавного співробітництва
У сфері управління Інтернетом питання міжнародного співробітництва є ключовим. Оскільки Інтернет ігнорує національні кордони, більшість проблем не може бути вирішено державами поодинці. Наприклад, Інтернет- шахрайство та інші правопорушення в Інтернеті здійснюються часто правопорушниками і через Інтернет-сервери, розташовані за межами держави громадянства потерпілого. Кримінальне переслідування таких злочинів вимагає слідства в різних державах, що передбачає ефективне співробітництво. В результаті цього у 2001 році була прийнята Конвенція про кіберзлочинність, яка проголошує, «що для ефективної боротьби з кіберзлочинністю у сфері кримінального права необхідна поглиблена, продуктивна і добре налагоджена міжнародна співпраця».

Сама по собі необхідність співпраці не тягне за собою якихось юридичних зобов'язань. Деякі зобов’язання в цій сфері передбачені в загальному міжнародному праві. Наприклад, «міжнародне співробітництво у вирішенні міжнародних проблем економічного, соціального, культурного і гуманітарного характеру й у заохоченні та розвитку поваги до прав людини та основних свобод» є однією з цілей, викладених у статті 1 Статуту Організації Об'єднаних Націй. У Декларації про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй (Декларації про дружні відносини), яка може вважатись авторитетним тлумаченням Статуту ООН, підтверджується обов'язок держав співпрацювати між собою. Однак таке загальне зобов'язання є досить абстрактним і на практиці його важко сформувати в конкретні обов’язки.

Конкретні обов'язки щодо співпраці містяться в міжнародних договорах, серед яких Конвенція про права дитини (КПД). Стаття 34 (c) КПД зобов'язує держави «вжити необхідних заходів на національному, двосторонньому та багатосторонньому рівнях для запобігання ... використання з метою експлуатації дітей в порнографічній роботі (постановках) і матеріалах». Оскільки порнографічні матеріали часто передаються через Інтернет з однієї держави в іншу, між державами повинні бути узгоджені будь-які ефективні способи протидії цьому. Таким чином, у статті 34 (c) КПД передбачено зобов'язання держав співпрацювати між собою у боротьбі з дитячою порнографією. Як наслідок, у Конвенції про кіберзлочинність, що визначає злочини, пов'язані з дитячою порнографією (стаття 9), міститься пряме посилання на КПД.

Схожі зобов'язання містяться і в інших документах з прав людини, таких, зокрема, як

ЄКПЛ. У справі Rantsev v. Cyprus and Russia Європейський суд з прав людини підкреслив, що торгівля людьми має транснаціональний характер. Таким чином, позитивне зобов'язання розслідувати випадки торгівлі людьми, що випливає зі статті 4 ЄКПЛ, може вважатись таким, що зобов'язує держав до ефективного транскордонного співробітництва. Те ж саме стосується і Інтернет-злочинів, в яких задіяна більше ніж одна держава. Беручи до уваги матеріали справи K. U. v. Finland, припустимо, що провайдер Інтернет-сайту знайомств знаходився за межами Фінляндії, в такому випадку обов'язок захищати 12-річного хлопчика відповідно до статті 8 ЄКПЛ передбачав би і зобов'язання співпрацювати з тією державою, де провайдер знаходиться.

Проте наразі немає чіткого встановленого механізму співпраці. Фактично держава навіть не зобов'язана підтримувати дипломатичні відносини, хоча дипломатія знаходиться в самій основі міжнародного співробітництва. Досить суперечливими виявилися й положення заключних документів ВСІС. У Женевській декларації 12 грудня 2003 року вказується на зобов'язання «зміцнювати співробітництво задля пошуку спільних рішень на виклики, а також для втілення Плану дій, який зміг би реалізувати концепцію інформаційного суспільства, відкритого для всіх та заснованого на фундаментальних принципах, які містяться у цій Декларації». Водночас у пункті 40 Туніської програми лише «підкреслюється необхідність» сприяти міжнародному співробітництву. Хоча зазвичай необхідність у співпраці і є загальновизнаною, держави неохоче приймають на себе відповідні обов'язки. З юридичної точки зору, принцип міждержавного співробітництва повинен бути більш дієвим.

Принцип багатостороннього співробітництва

В управлінні Інтернетом традиційно важливу роль відіграють громадянське суспільство і приватний сектор (бізнес). Незважаючи на те, що розвиток Інтернету був профінансований урядом США, його зміст був визначений науковим співтовариством. Уряд США спостерігав за розвитком, і все ж залишався в тіні. Коли стало необхідно знайти надійну інституцію для управління доменних імен в Інтернеті (DNS), таке завдання не було доручено ні державному органу, ні міжнародній організації, наприклад, Міжнародному союзу електрозв'язку; відповідальність було покладено на приватну неприбуткову організацію ICANN. Тим не менш, концепція управління Інтернетом без державного контролю, як про це говорив Джон Перрі Барлоу ще у 1996 році, так і не була втілена в життя. З самого початку ICANN була пов'язана договором з Міністерством торгівлі США. З того часу інші держави посилили свій вплив і Урядовий дорадчий комітет наразі перетворився у важливий орган державного контролю. Первинні плани уряду США надати ICANN повну незалежність до цих пір не були реалізовані. Поновлені Підтвердження зобов'язань між Департаментом торгівлі США та ICANN (Підтвердження зобов'язань) від 30 вересня 2009 ще більше звужують безпосередній вплив США, але підвищують рівень підзвітності та прозорості шляхом процедур розгляду, в яких, між іншим, задіяний і Урядовий дорадчий комітет. Ще в 2002 році президент ICANN закликав до ефективної співпраці між державним та приватним секторами, що здійснюватиметься на засадах приватного сектору, але за активної підтримки та участі національних урядів. Саме це і було поступово втілено в життя.

Наразі очевидно, що такий підхід із участю всіх зацікавлених сторін не просто активно втілювався, а й фактично перетворився на керівний принцип міжнародного Інтернет-права.

У Підтвердженні зобов'язань Міністерство торгівлі США «підтримує висхідну модель для розвитку технічної координації DNS з участю всіх зацікавлених сторін, яка буде переважно побудована в рамках приватного сектору і буде функціонувати в інтересах користувачів глобальної мережі Інтернет». Це питання було розглянуто більш широко під час ВСІС. Відповідно до Женевської декларації принципів 2003 року управління Інтернетом, що «охоплює як технічні питання, так і питання публічного правопорядку», «повинно здійснюватись усіма зацікавленими сторонами, відповідними міжурядовими та міжнародними організаціями». У цьому відношенні Декларація покладає конкретні обов'язки на відповідних суб'єктів. Зокрема, політичні повноваження чи будь-які пов'язані питання в сфері державної політики покладаються на держави, в той час як приватний сектор повинен відігравати «важливу роль» в технічному та економічному забезпеченні Інтернету. Повноваження громадянського суспільства більш загальні. Воно відіграватиме «важливу роль у вирішенні питань, пов'язаних з Інтернетом, особливо на рівні громад. Підхід із участю всіх зацікавлених сторін був підтверджений в ідентичному формулюванні два роки по тому, в Туніській програмі для інформаційного суспільства, що закликала до застосування цього підходу «на всіх рівнях», а також заснувала Форум з питань управління Інтернетом – «форум для політичного діалогу між всіма зацікавленими сторонами».

Цей підхід не обмежується питаннями системи доменних імен та ICANN. Більше того, ВСІС сприяв становленню поняття управління Інтернетом, що охоплює ряд питань, пов'язаних із публічним правопорядком, зокрема питання кримінального переслідування кіберзлочинності. Співпраця між усіма зацікавленими сторонами є ключовим питанням, що розглядається в Женевській декларації та Туніській програмі. Даний підхід не обмежується МІП. Інші всесвітні конференції також демонструють зростаючий вплив недержавних суб'єктів. У МІП, однак, концепція багатосторонньої співпраці настільки значима, що вона набуває форми основоположного принципу.

Взаємозв'язок між різними суб'єктами (учасниками)

У заключних документах ВСІС вказується перелік основних суб'єктів МІП, серед яких: держави, приватний сектор, громадянське суспільство та міжнародні організації, також з позицій права захисту прав людини окремі індивіди займають першочергове місце у цьому переліку. П'ять принципів МІП, розглянуті в даній статті, визначають характер зв'язку між цими суб'єктами.

Міжнародне право захисту прав людини захищає від втручання з боку державної влади. При цьому і свобода слова, і свобода листування гарантовані. У той час як стаття 1 Факультативного протоколу № 1 до МПГПП виключно проголошує права людини загалом, в європейському праві прав людини на порушення прав людини можуть посилатись і громадянське суспільство, приватний сектор, сформований з осіб. Це передбачено у статті 34 ЄКПЛ. Положення Інтернет-провайдерів посилюється положеннями міжнародного торгового права.

Позитивні зобов'язання, що випливають з норм права захисту прав людини, регулюють взаємовідносини між різними індивідами і цим самим визначають положення індивідів у рамках громадянського суспільства і щодо приватного сектору. Перш за все, держави мають зобов'язання щодо захисту особистого життя від посягань з боку інших осіб,

громадянського суспільства чи приватного сектору. Це підтверджується у справі K. v. Finland.

Принцип територіальної юрисдикції спрямований на розмежування повноважень різних держав, при цьому співпраця необхідна для того, щоб вирішувати проблеми, які не можуть бути врегульовані лише однією державою. Міждержавне співробітництво є досить традиційним принципом міжнародного права, хоча необхідність співпраці між державами є особливо актуальною у сфері управління Інтернетом. Концепція багатостороннього співробітництва є більш сучасною і вона перетворилась на особливий принцип МІП. Іншими словами, на даному етапі МІП розвивається в трикутнику питань індивідуальних прав, територіальної юрисдикції і співробітництва.

4.2.6. Йоханнес М. Бауер, Джонатан Обар. Узгодження економічних та політичних цілей в екосистемі Інтернету

Узгодження економічних та політичних цілей в екосистемі Інтернету

Йоханнес М. Бауер, Джонатан Обар
Мічиганський державний університет

Тайджін Кох
Техаський університет

Підготовлений для презентації на 39-тій науково-практичній конференції з питань політики комунікації, інформації та Інтернету
Арлінгтон, Вірджинія, 23-25 вересня 2011 року

оброблений варіант
Іст-Лансінг, штат Мічиган
18 вересня 2011

1.Передмова

Обговорення фундаментальних напрямків комунікаційної політики між економічними та політичними силами дуже рідкісні. Більш звично, що проблеми, які виникають у цій сфері, вирішуються по мірі їх накопичення, хоча нагромадження навіть маленьких проблем можуть мати великі наслідки. Дебати щодо мережевого нейтралітету є одним з тих рідкісних можливостей обміркувати велику кількість питань інформаційної політики та комунікацій. Комплексний підхід у дебатах зачіпає широке коло економічних та політичних
проблем. Це пов'язано з фундаментальним питанням стосовно сучасних засобів зв'язку: як структурувати права та обов'язки різних зацікавлених сторін у системі інформаційних та комп'ютерних технологій (ІКТ), особливо серед
операторів фізичних мережевих платформ і постачальників контенту та прикладних програм.

Більш того, в цьому контексті система ІКТ займається також правами користувачів і, можливо, проблемами вертикальних відносин між постачальниками логічних платформ (наприклад, операційні системи, платформи розробки і пошуку) та іншими зацікавленими сторонами. З економічної точки зору це викликає питання, пов'язані з швидкістю та якістю виконання завдань по вертикалі на суміжних мережевих ринках, в яких ринкові позиції присутні принаймні в деяких сегментах. Чи треба дозволяти правилам взаємодії між гравцями спільних ринків розвиватися самостійно або є необхідність колективного агента, що визначає межі взаємодії або навіть обов'язкові правила? З більш широкої точки зору соціальної політики постають додаткові важливі питання щодо наслідків різних механізмів управління для свободи слова, демократії та громадянської участі, і, можливо, прав людини в цілому.

Ця різноманітність цілей значно ускладнює дискусію. Прихильники та противники мережевого нейтралітету часто будують свої аргументи з різних, навіть взаємно не пов'язаних нормативних рамок. Деякі висновки ґрунтуються на широких, безумовно прийнятих, цілях комунікаційної політики, таких, як захист свободи слова чи підтримка демократичних цілей.

Інші висновки ґрунтуються виключно на точці зору економічної ефективності політичного вибору. Дуже рідкими є спроби примирити ці різні кути зору та вивчити зв'язок між різними цілями та надати

інструменти для реалізації обох цих цілей без збитків з тієї чи іншої сторони.

Аналіз різноманітних точок зору через загальні дебати є основою комунікаційної політики, що була розроблена наприкінці XX сторіччя. Уайлдман і Ентман (1992) проаналізували аналітичні та політичні дискусії навколо поняття ринку ідей. Вони вказали на основні протиріччя та непорозуміння між експертами, які симпатизували ліберальній економічній точці зору і тих експертів, хто виступав за більш широку позицію соціального добробуту.

Ми також стверджуємо, що відсутність роз'яснення різних аспектів політики на дебатах може призвести до «забруднення води», значно ускладнюючи розробку та реалізацію політичних принципів та інструментів для їх впровадження. Наша стаття намагається зробити свій внесок у роз'яснення політичних та економічних цілей та розробити потенційні інструменти, які можуть бути використані при реалізації цих цілей.

З цією метою ми розглянемо економічні та політичні причини, які використовуються в якості обґрунтування при дискусіях «за» або «проти» мережевого нейтралітету. Ця дискусія також допоможе диференціювати альтернативні властивості мережевого нейтралітету та вивчити спільності, напругу та протиріччя між зацікавленими сторонами. Ми потім перейдемо до аналізу ефективності різних інструментів, що пропонуються для вирішення проблеми управління та розглянемо, як різні варіанти політики служать цим цілям. Ми зацікавлені в логічності відносин між інструментами і цілями. Чи є певні інструменти достатніми або ні для досягнення результату? Чи можуть бути використані різні інструменти в комбінації один з одним? Чи існує компроміс між цілями, чи можливе досягнення збалансованої комбінації цілей?

2. Мережевий нейтралітет як проблема управління

За своєю суттю, дебати щодо мережевого нейтралітету відбуваються навколо управління сучасними засобами зв'язку. Управління відноситься до добровільних і обов’язкових (урядових) форм координації у соціальній та соціотехнічній системах з метою наблизити їх до бажаного стану або уникнути їх перевтілення у небажаний стан (Діксіт 2009; Холінгсворс і Ліндберг 1985; Джордана і Леві-Фа 2004; Родос 1996; Шарпф 1993; Вильямсон 1996, 2005).

Таким чином, однією з форм управління є регулювання, коли є добровільні угоди між зацікавленими сторонами (самоврядування), іншою формою є гібридні механізми, які включають в себе як дії уряду так і добровільні заходи («Спільне регулювання") (Лазер співавт. 2003). Поняття управління визнає, що й інші учасники процесу крім держави беруть участь у координації соціальних систем.

На відміну від попередньої точки зору, що уряд є "кермом економіки," поняття управління визнає, що в більш складних соціальних системах ефективність системи повного "контролю" може бути важко або неможливо досягти (Майнтз, 2003). У реальності це може бути тільки частковий вплив та незначне переміщення системи в бік більш бажаного стану.

Ефективне управління вимагає реального консенсусу між намічуваними цілями та досягнення загального розуміння роботи системи, якою керують; як система буде реагувати на різні форми управління. Це не обов'язково означає, що всі зацікавлені сторони повинні домовитися про один єдиний світогляд, але позиції повинні бути досить скоординовані, щоб була можливість прийняття курсу дій (Дензау і Норд, 1994). Якщо позиції зацікавлених сторін занадто різняться, це може призвести до ситуації, коли досягнення більшості голосів неможливе ані в уряді, ані в громадських організаціях. Крім того, в результаті будь-який курс дій може бути оскаржений в суді зацікавленими сторонами з метою протистояння. Таким чином, коли спірне питання веде до політичних проблем, перший етап обговорення спірного питання часто присвячується роз'ясненню точного характеру проблеми і формуванню досить послідовної та працездатної точки зору соціальної системи та її відповіді на конкретні форми політичного втручання. Першим важливим кроком у цьому аналізі є чітке розуміння прямих ефектів інструментів управління. З урахуванням складності системи ІКТ, також важливо розглянути непрямі ефекти, кумулятивні ефекти і ефекти, що виникають на більш високому рівні системи. Хоча це не буде можливим з високим ступенем точності, сукупність механізмів управління часто може бути поліпшена, якщо ці потенційні наслідки приймаються до уваги.

Мережевий нейтралітет є досить широким терміном, який набрав чинності в обговоренні державної політики, тому що це було розцінено як розв’язання проблеми занепокоєності багатьох зацікавлених сторін. Принаймні три питання можуть бути ідентифіковані як можливі проблеми, але тільки два з них в

даний час знаходяться в центрі обговорення. Однією з ключових є проблема управління мережею, права і зобов'язання операторів мереж по управлінню інформаційними потоками над їх інфраструктурою. На відміну від контенту і прикладних програм, ринок мережевої платформи є більш високо концентрований. У США конфігурації просторово різноманітні. У той час, коли багато місцевих ринків обслуговуються кількома провайдерами, велика кількість ринків обслуговуються тільки одним або двома провайдерами, з DSL мовою програмування і оператором кабельного зв'язку спільно обслуговують основну частину абонентів. Крім того, з 2005 року FCC (Федеральна комісія по зв'язку) зробила рекласифікацію широкосмугового доступу на ринки інформаційних послуг, позбавляючи провайдерські послуги дискримінаційного положення спільного оператора. Ці питання викликають стурбованість з приводу здатності мережевих операторів дискримінувати контент-провайдерів і користувачів. Ситуація ускладнюється очікуванням, що оператори мереж будуть прагнути втручання у вертикально пов'язаний контент та впливати на ринок прикладних програм. Багато експертів були стурбовані тим, що така ситуація буде збільшувати стимул інтернет-провайдерів саботувати конкурентів, які залежать від їх мережевої платформи. Такий сценарій контрастує з ідеальним типом зв'язку end-to-end, який було сприйнято як одну з рушійних сил інноваційної досконалості інтернету (Блюменталь і Кларка 2001 року; Лемлі і Лессиг 2001).

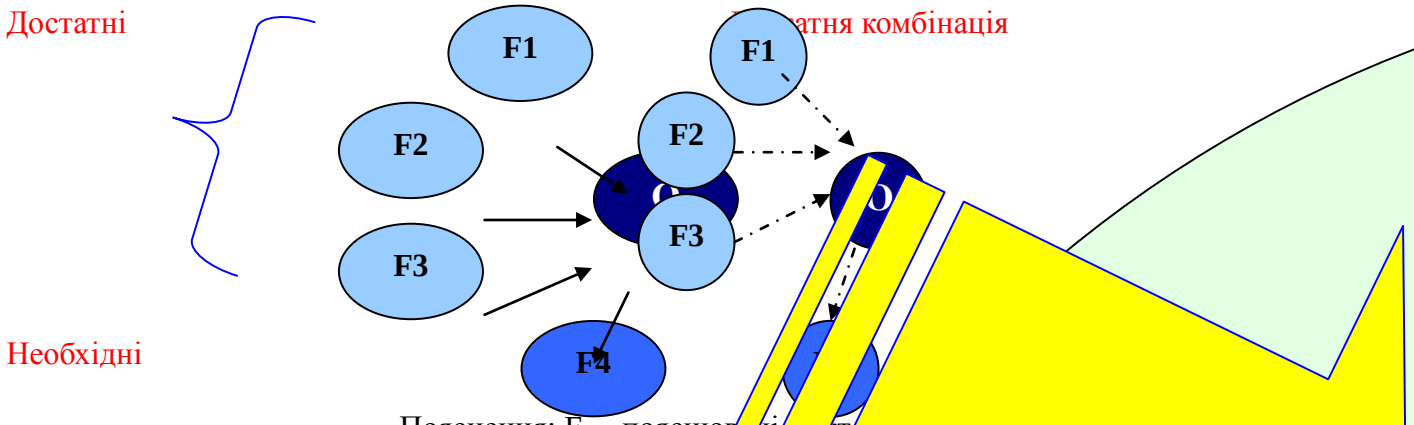
Інша проблема, яка викликає занепокоєння, пов'язана з потенційною роллю інтернет операторів як пропускних пунктів інформаційних потоків. Кілька випадків дискримінації щодо певних типів контенту вже з'явилися (хоча більшість з них були швидко усунені). Ліквідація загальних операторських зобов'язань розглядається як зміцнення права на свободу слова постачальників послуг, але, можливо, за рахунок ослаблення права на свободу слова користувачів. У зв'язку з цими проблемами виникає стурбованість тим, що інтернет може втратити свою потенційну роль у підтримці резонансу громадської сфери та громадського життя.

Третя потенційна проблема – це доступ до логічних платформ, таких як інструментів розробника і пошук. Хоча дискусії про «неупереджений пошук» спалахують тут і там, ці дискусії все ще не закінчені. Це не означає, що всі зацікавлені сторони погодилися, що ці обставини перероструть у серйозні проблеми. Багато представників галузі стверджують, що це були перебільшені проблеми, «рішення в пошуках проблеми». Тим не менш, в поєднанні з декількома дуже явними випадками незаперечних зловживань, таких як випадок Comcast-Bit Torrent, тема мережевого нейтралітету переродилася від інституційної до фактично політичної на порядку денному не тільки в США, але і в інших країнах.

У ході цієї дискусії альтернативні значення «неупередженості» інтернету були також уточнені і пов'язані з можливими політичними предметами. У широкому сенсі, дискусія перейшла від достатньо простого та широкого погляду до більш конкретних пропозицій. Більше того, цей аспект обговорення також торкнувся вертикальної, багаторівневої архітектури Інтернету і поставив питання про те, де неупереджена політика повинна бути розташована в цьому нагромадженні (Джордан і Гош 2009; Джордан 2009 року; Фрайден 2010 року). У той час як зацікавлені сторони продовжують дотримуватися різних позицій, цей процес принаймні вніс ясність в обговорення і виявив широкий спектр варіантів, які можуть бути використані для вирішення основних економічних і політичних проблем. Набір альтернатив охоплює широкий діапазон від досить жорстких форм регулювання за допомогою низки засобів політики недискримінації до рішення покладатися тільки на закон про конкуренцію та антимонопольне законодавство. Дуже небагато авторів передбачають повноцінне регулювання взаємозв'язку, взаємодії та ціноутворення в якості бажаної альтернативи. Прихильники недискримінаційних варіантів розглядають відносини між операторами мереж та контент провайдерами, а також між мережевими операторами і користувачами.

Щодо моделі формування політичного курсу, то вона включає в себе (1) строгі положення, такі як «a-bit-is-a-bit» модель, (2) обов'язкову нульову ціну обмеження на мережевих операторів контента-суперника (vis-à-vis) і постачальників прикладних програм, але з урахуванням диференціації зі сторони користувача, і (3) менше обмежувальних опцій при наданні дозволу на доступ до багаторівневих послуг мережі за умови, що вони стануть доступними за всім змістом та для всіх постачальників прикладних програм на недискримінаційній моделі. Щодо користувачів, недискримінаційні варіанти можливостей простягаються від заборони диференціації до форм спеціалізації (наприклад, цін на різний доступ швидкостей), доки ця диференціація вони не призводить до блокування доступу до прикладних програм і контенту.

Малюнок 1. Логічна структура політичного формування



Пояснення: F… пояснюючі ...кт...

Беручи до уваги цей аспект дебати про мережевий ней... ...ти, додаткова інформація про які необхідна для оцінки того, які ...тів підходять для досягнення узгоджених цілей. Хоча в політичні ...сто визначаються одночасно, все ж є доцільним опрацювати ці питання з ак... ...на ці питання вимагає детального розуміння причинно-наслідкового зв... ...і результатами. Враховуючи складність сучасної системи ІКТ це не легке завда... ...уваги нещодавні дослідження, які сприяли цікавим результатам цієї дискусії, багато чого ще н... ...зробити. З точки зору логіки, завдання полягає в тому, щоб визначити, чи є інструмент необхід... ...о достатньою умовою для досягнення результату. Необхідність означає, що умова існує незал... ...о від того, коли спостерігається результат, але й інші фактори повинні також бути враховані при ...сягненні результату. Достатність є головною умовою і полягає в тому, що кожного разу, коли фактор має місце, результат буде наявний стовідсотково. Для політиків знаходження необхідних і достатніх умов має вирішальне значення. Якщо достатні умови можна знайти, здійснення політики відносно просте. У складних соціальних системах знаходження цих умов не є простим завданням. Декілька факторів можуть складати разом достатні або необхідні умови. У цьому випадку політикам доведеться контролювати всі відповідні умови. Більше того, цілком можливо, що якість факторів як необхідних або достатніх залежить від загального стану системи. Наприклад, нульова ціна може підтримувати інвестиції за певних поєднань споживчого попиту і витрат на мережу, але не завжди. Нарешті, можливо, що інструменти не завжди логічно пов'язані з результатами, але тим не менш сприймаються як законний необхідний засіб. Ми повернемося до цих питань в розділах з четвертого по шостий.

3. Нормативні основи мережевого нейтралітету

Вправна державна політика вимагає з’ясування бачень суспільства. Хоча такі аргументи можуть випливати зі знання про функціонування суспільства, велика частина розвитку політики обов’язково базується на нормативах. Оскільки ця дискусія не є відкритою, нормативні аспекти часто замовчуються, але вони все ж присутні.

3.1 Політичні аргументи на користь мережевого нейтралітету

Дискусія щодо мережевого нейтралітету не є чимось особливим. Вона вимальовується з кількох традиційних нормативів, найбільш важливих постулатів про політичні свободи і права людини, справедливість і правосуддя, і більш вузько, але тим не менш від нормативних аргументів на користь ефективності. Розробники часто консультуються з експертами з правових питань, спілкуються з вченими та політологами, у той час як останні дуже часто залучають економістів та інженерів. Частина непорозумінь в постійних дебатах щодо мережевого нейтралітету ґрунтується на зовсім різних основах цих міркувань. Хоча значна кількість авторів просто вважають, що мережевий нейтралітет служить цим цілям, деякі з них намагалися

розібратися в цих питаннях. Важливі концепції випливають з теорії Габермаса про суспільну сферу, теорії справедливості Роулза, та пов'язані з ними теорії про свободу слова, зокрема як це співвідноситься з резонансними демократичними інститутами.

Габермас (2006) описує, що інституційна структура сучасних демократій, як правило, складається з трьох центральних компонентів: приватної незалежності громадян, «кожен з яких створює своє життя на свій власний розсуд», демократичне громадянство, зокрема «включення вільних і рівноправних громадян до політичного співтовариства», та «незалежність публічної сфери, яка працює в якості посередника між державою і суспільством». Він продовжує наголошувати, що інституційна структура повинна гарантувати «політичну участь як можна більшого числа зацікавлених громадян шляхом рівноправної взаємодії і прав на участь». Ці ідеї лежать в основі багатьох нормативних аргументів, представлених як ті, які підтримують мережевий нейтралітет. Ті, які виступають за «відкритий Інтернет» через мережевий нейтралітет, запропонували різні варіанти з основними принципами Габермаса, що просувають та підтримують доступ до публічної сфери.

В онлайновому світі задля підтримки громадської сфери, як описано Габермасом, прихильники мережевого нейтралітету закликали до нормативних завдань «відкритості», які збігаються з Габермасівським зв'язком між доступом до громадської сфери та демократії. Купер (2003) представляє своєчасний аргумент на користь відкритості на фізичному прошарку мережі Інтернет. Він зазначає:

Фізичний прошарок комунікаційної платформи є занадто вузьким місцем що ризикує стати закритим прошарком. Фізичний прошарок контролюється занадто малою кількістю власників домінуючої технології, що робить його дуже легким в маніпулюванні платформи в цілому. Ці власники використовують особливі, вузькі мотиви і силу ринкових важелів для того, щоб захистити існуючі монопольні ренти для досягнення панування над сусідніми Інтернет продуктами. Таким чином, ці власники домінуючих технологій знаходяться в унікальному становищі, що дозволяє їм впливати на всю комунікаційну платформу. Якщо це продовжуватиметься, неминучим економічним результатом буде ослаблення конкуренції і обмеження споживчого вибору, що призведе до уповільнення інноваційної діяльності. В результаті такого способу управління буде надано надмірного впливу на платформу власників та, що ще важливіше, підірветься можливість збагатити громадський діалог через більш активне залучення громадян до дискусії.

Інший аргумент на користь відкритості можна знайти в Schejter & Yemini (2007), які ідентифікують різницю між доступом до традиційних засобів масової інформації (радіо, телебачення) і можливість доступу через Інтернет. Вони стверджують, що традиційно доступ до радіочастотного спектру був обмежений шляхом регулювання, тому що це було дефіцитним ресурсом. З цієї причини тільки певні особи були володарями ліцензій на теле- та радіомовлення. Це було величезне обмеження доступу широкої громадськості і тільки деяким особам було дозволено створювати та транслювати теле- та радіопередачі. Для контрасту, значною привабливостю Інтернету є його вільний доступ, який надає нові можливості для новаторів, споживачів і людей, які просто хочуть, щоб їхні голоси були почуті. Schejter і Yemini стверджують, що регулюючи питання вирішення доступу до Інтернету у майбутньому, необхідно змінювати мислення; відходити від підходів, які традиційно були розроблені для вирішення проблем дефіциту доступу і до можливостей, які ця технологія в достатку пропонує.

Автори відзначають, що перспективи Інтернету лежать не тільки в його підтримці великого бізнесу, але і в можливостях, які він надає для тих, хто не мав змоги бути почутим в технологіях утримання дефіциту і що мережевий нейтралітет створює потенціальні голоси широкому колу громадськості як перша справжня технологія вільного доступу: широкосмуговий доступ в Інтернет. Створення потенціалу «Голос багатьом» тотожне «Технології достатнього доступу» підкреслює мету відкритості та близьке безпосередньо з поняттям Габермаса ліберальної демократії.

Мета відкритості тісно пов'язана з метою свободи слова. Знову ж, ці цілі пов'язані з поняттям Габермаса щодо ліберальної демократії, ця мета підкреслює можливість для користувачів доступу в Інтернет, і не просто в цілому, але завдяки їх можливості висловлювати свої думки і точки зору в Інтернеті. Ця мета вимагає доступу на крок вперед і приділяє особливу увагу можливості людей внести свій вклад в

ринок ідей.

Нунзіато (2009) починає свою книгу, зазначивши «Інтернет забезпечує найбільшу вільну можливість для спілкування і вираження своїх думок та ідей, якої світ ще не бачив». Вона продовжує стверджуючи, що контроль над Інтернетом жменьки корпорацій з можливістю цензури висловлювань загрожує нормативним цілям цієї можливості свободи слова.

Блевінс і Барроу (2009) представили аналогічне твердження, зазначивши, що «Ми приходимо до висновку, що Інтернет володіє такими унікальними якостями і важливішим демократичним характером, що він заслуговує своєї Першої поправки в рамках інтерактивно-демократичної теорії».

У своїй статті вони посилаються на Федеральний суд Східного округу штату Пенсільванія в якому Інтернет описаний як «найважливіша форма масового мовлення, яка розроблена в теперішній час», відзначаючи далі, що Інтернет таким чином «заслуговує на високий захист від втручання з боку держави».

Блевінс Барроу розвинули це положення і стверджують, що, оскільки «це є найважливіша форма масового мовлення, яка розроблена в теперішній час, вони стверджують, що Інтернет заслуговує на найвищий ступінь захисту від будь-яких інструкцій, державних чи приватних». Крім того, автори зазначають, що «права людини на свободу слова через Інтернет повинні переважати над правами власності провайдерів».

Тревіс (2007) ідентифікує Інтернет як «Поліпшені можливості з виконання Першої поправки» і стверджує, що прийняття до уваги традиційних уявлень і цілей свободи слова необхідно, щоб захистити можливості, надані Інтернет.

Тревіс вважає, що, враховуючи положення загального права і положення первісних принципів конституційного права, права інтелектуальної власності та антимонопольного права, свобода Інтернету може бути заснована на більш міцній основі, ніж спеціальне балансування, що характеризує сучасну доктрину кіберправа і практику судових рішень.

Зокрема, вимога свободи слова хоча б на тому ж рівні, як це було у Великобританії і Північній Америці в 1791 році, може зберегти доступ в Інтернет користувачів до вільного висловлювання та цифрових технологій , але це може загрожувати збереженню авторського права, товарного знаку, або інтересам телекомунікаційного ліцензування.

Крім того, повертаючись до антимонопольного законодавства, до його первісної основи, свободи суб'єкта, викликає підозру концентрування державної або приватної влади, і наполягання на різних цінах та конкуренції з якості, що посприяє усуненню останніх рішень Верховного Суду, які сприяли монопольній владі в різних контекстах у сфері цифрових медіа, в першу чергу телекомунікаційних та Інтернет - інфраструктурах.

Перша поправка, що описує свободи, гарантує засобами загального права вимогу скасування тиранії над інформацією і звільнення аудиторії від монопольного контролю над інструментами свободи слова (1579-1580).

Деякі автори і публічні інституції – розробники мережевої політики, також, посилаються на фундаментальні людські права і свободи як на основи мережевого нейтралітету.

Декларація Федеральною комісією зв’язку чотирьох принципів відкритого Інтернету, оприлюднена у 2005 році і заснована на підтримці Майкла Пауелла (англійського режисера та продюсера) цих цілей, неодноразово посилається на ці свободи. Крім того, Декларація Ради Європи 2009 року передбачає доступ в Інтернет в якості основного права людини.

3.2 Контраргументи та загрози нормативної аргументації

Оцінюючи вплив нормативних аргументацій на дискусії щодо мережевого нейтралітету, ми повинні звернути увагу на проблеми цієї форми аргументації в цілому, а також суб'єктивні відмінності притаманні будь-якому обговоренню нормативної бази. Формування прагматичних стратегій і висновків нормативних аргументів в цілому може бути проблемою через властиву суб'єктивність нормативної аргументації, а також труднощі з фактичним наданням емпіричної підтримки. Проблеми можуть бути пов'язані з центральним елементом нормативної етики, мораллю, у тому числі з уявленням

про те, як один член суспільства «в якихось рамках» живе і як суспільство «в якихось рамках» діє в процесі прийняття рішень, ці уявлення можуть бути дуже складними. Якщо мораль є чинником, який спрямовує дії, чиїм уявленням про мораль ми повинні слідувати? Якщо один табір стверджує, що просування ліберальної демократії Габермаса через правила мережевого нейтралітету є нормативною позицією, яку слід прийняти, а інший табір стверджує, що мережева практика дискримінації, які захищають дітей від шкідливого змісту Інтернету повинні буди прийняті як пріоритетні, якій моралі слідувати?

Як щодо нормативних аргументів на користь права провайдерів? Сідак (2006) стверджує що «витрати і попит щодо певних характеристик телекомунікаційної галузі разом з фундаментальними принципами економіки добробуту і загального права мають справу з принаймні шістьома правами, якими власники широкосмугової мережі мають право володіти. Перше право з цих шести він ідентифікує як право на відвідування власної мережі, яке включатиме управління мережею і формування стратегії ціноутворення. Для Сідак ці дії підвищать цінність мережі, а також сприятимуть загальному економічному добробуту, надаючи цьому праву нормативний характер. Право друге має на увазі «в односторонньому порядку визначення ціни використання своєї мережі будь-яким способом, що не порушує антимонопольне законодавство». Сідак оцінює цю стратегію як ту, що сприятиме розвитку і розширенню мережі та розвитку широкосмугової економіки. Він бачить у цьому вигоду як у внеску в економічне, а також соціальне забезпечення, що має носити нормативний характер. По-третє, право на «відмову в розміщенні інформації або прикладних програм, які представляють ризик для законної безпеки і продуктивності їхніх мереж або пристроїв, які абоненти оператора мережі можуть додавати до мережі провайдера». Він зазначає, що «оскільки це стосується нормативності, оператор мережі повинен мати право відмовити у розміщенні інформації або прикладних програм, які представляють загрозу законній стабільності, безпеці та дієздатності власної мережі». Четверте право включає право пріоритету доставки пакетів даних. Сідак вбачає зв'язок між економічним добробутом і важливістю сильної та інноваційної мережі. Деякі організації вимагають, щоб пакети даних надходили швидше і, таким чином, можна максимізувати ефективність та інноваційний характер мережі, це право має бути визнано. Сідак зазначає, що «зростання значення пріоритетної доставки існує більше для додатків реального часу, таких як VoIP, ніж для менш термінових додатків, як електронна пошта. Для досягнення паритетно-ефективного використання мережі, оператор мережі повинен мати право пріоритету змісту для максимального використання економічних чинників і мінімізації сукупної втрати добробуту, які пов'язані з кращою доставкою. Право п'яте і шосте схожі і вони є правом на резервні потужності на власній мережі та правом на використання пропускної здатності мережі вертикально інтегруватися в положеннях змісту або додатків. Сідак зазначає, що «як право на резервні потужності на одній мережі, це право допомагає гарантувати, що кінцеві користувачі отримають вигоду від конкурентної поставки контенту і додатків».

3.3 Економічні аргументи

У порівнянні з цими дебатами, економічні аргументи на користь ефективності набагато менше оскаржують, ефективність широко розглядається в якості важливої мети Інтернету, навіть в умовах, де деякі фактори є в достатку. Деякі розбіжності існують у зв'язку з відповідним поняттям ефективності (статична, динамічна) і як одне співвідноситься з іншим. Можна стверджувати, що поняття ефективності як співвідношення між цілями і засобами є сумнівним по відношенню до більш широких питань політики. Після того як рівень свободи слова визначено, є сенс шукати найбільш ефективний спосіб її досягнення. Тим не менш, багато авторів не згодні, в основному щодо вільних ринків, що вони також будуть захищені та це сприятиме досягненню мети свободи слова. У наступному розділі ми розглянемо інструменти, які пропонуються для досягнення цих цілей і їх логічний зв'язок з результатами.

4. Інструменти і завдання дебатів щодо мережевого нейтралітету

Ряд конкретних пропозицій щодо того, як мережевий нейтралітет може бути досягнута, викристалізувався з обговорення. У цьому розділі ми розглянемо, як автори політичних та нормативних дебатів оцінювали п'ять з цих інструментів: (1) заборона блокування (змісту, додатків і пристроїв), (2) нульове обмеження цін у мережевих операторів на схожу інформацію і постачальників схожих додатків, (3) якість обслуговування багаторівневих продуктів операторами мереж і постачальників програмних продуктів без дискримінації, (4) якість обслуговування багаторівневих продуктів операторами мереж і постачальників програмних продуктів з дискримінацією тих пір, поки це не порушує антимонопольного законодавства, і (5) надання встановленого мінімального рівня якості обслуговування.

У той час як вчені, що займаються правом і комунікаціями, сприяли більш глибокому аналізу та обговоренню загальних нормативних цілей, які можуть вимагати мережевого нейтралітету, ці зусилля рідко були направлені на вивчення конкретних інструментів і причинно-наслідкових зв'язків між інструментами і бажаними результатами. Якщо вони обговорювалися в загальних рисах, інструменти та результати зіставлялися, припускаючи, що присутність інструменту являє собою достатню умову для досягнення результату. У нашій роботі ми маємо намір вивчити цей зв'язок більш уважно, ми прагнули виявити логічний зв’язок, коли інструмент не обговорювався в явному вигляді як той, що сприяв досягненню результату.

Мабуть, найпоширенішим інструментом, який відстоювали ті, хто виступає за «відкритий» Інтернет, є «положення про недискримінацію». Це положення ідеально приймає форму політики, яка має на меті переконатися у тому, що уряди та приватні організації не можуть вплинути на традиційний принцип «неперервності». Організації не матимуть законних прав ввести цензуру на інформацію, яка передається завдяки Інтернету, або впливати на передачу пакетів даних від одного користувача до іншого.

Нунзіато (2009) стверджує: «Моя точка зору особливо фокусується на забороні широкосмуговим провайдерам дискримінації на основі змісту». Як зазначалося раніше, Блевінс і Барроу (2009) відстоюють ту ж точку зору, зазначивши, що, тому що Інтернет є «найефективнішою формою масового мовлення, яка тільки існує, він гідний найвищого захисту від будь-якого вторгнення уряду або приватних осіб». (46-7) Американський союз громадянських свобод (2010) відзначає, що Перша поправка передбачає, «що уряд створює сильну політику проти вторгнення компаній, які, головним чином, перебувають у погоні за наживою, а не виконують громадянський обов'язок» (5). Купер (2004) стверджував, що «дозвіл власникам мережі на дискримінацію щодо комунікацій, інформації, обладнання або програмних продуктів сприяє настанню небажаних змін у інформаційному середовищі, яке стане набагато менш сприятливим для інновацій». «Сама загроза дискримінації різко впливає на стимули і є сьогодні обтяжливою для інновацій» (96).

Положення про неприпустимість дискримінації являє собою інструмент, який включатиме обмеження дії провайдерів з метою виконання нормативної цілі забезпечення «відкритого» Інтернету. Заклик до дещо іншої державної політики, яка спрямована на досягнення тієї ж мети, а саме, підтримання «відкритого» Інтернету, є «забезпеченням рівного доступу», який рекомендують Блевінс і Барроу (2009). Замість того, щоб у центрі уваги політики були обмеження, що накладаються на Інтернет провайдерів, надання цього типу держаної політики буде спрямоване на заохочення рівного доступу, яка на перший погляд здається більш неоднозначною у понятті ліберальної демократії Габермаса.

Таким чином, положення щодо рівного доступу, зосередившись на результаті, а не на засобах, процесу, здається більш прагматичним у певній мірі, тому що дозволяє використовувати потенціал різних засобів рішення проблеми. Це поняття здається паралельним закликом для індивідуумів, як Тім Ву (2004), які виступали за мережевий нейтралітет, але мають також визначені потенційні переваги, які дозволяють провайдерам управління мережею в конкретних ситуаціях. Це управління в ідеалі, має бути під пильним оком уряду і громадськості. Ву відзначає, що «оператори повинні мати свободу» корекції того, чим вони володіють або діяти розумно щодо контролю локальної мережі широкосмугового доступу. З іншого боку, можна припустити, що Інтернет-спільнота (і, в якийсь момент, регулятори) повинні з підозрою дивитись на обмеження, що грунтуються на міжмережевих критеріях» (235).

Рання література, присвячена розгляду економіки мережевого нейтралітету, також базувалася в

значній мірі на шляху зіставлення інструментів з результатами. Тим не менш, все більше число останніх робіт розглядають наслідки продуктивності конкретних інструментів більш ретельно. Зокрема, це сприяє більш сильній залежності від формальних моделей, що робить ці відносини більш чіткими. У більшості випадків логічне співвідношення між інструментом і досягненням поставленої мети може бути легко виявлено з документу. Крім того, разюче, що документи з нахилом на більш широкі політичні цілі часто торкаються економічних питань, але в першу чергу економічні документи рідко торкаються політичних аспектів обговорення.

Для цілей цієї статті, досить виділити невелике число останніх економічних робіт, які представляють більш широкий масив літератури (див. Schuett 2010 року для короткого огляду). Шість документів синтезовані в таблиці 1, всі вони приймають нульове правило ціни, накладене на мережевих операторів у якості базового сценарію, а потім досліджують вплив відхилення від цієї суворої форми мережевого нейтралітету, найчастіше, на якість в багаторівневому обслуговуванні (QoS-багаторівневе), що відображається на короткострокових та довгострокових результатах. Моделі відрізняються за своїми припущеннями щодо розподілу пропускної здатності мережі, структури мережі та інформації, програмних продуктів та чи вивчають вони інвестиції та інноваційні рішення в явному вигляді. Три роботи використовують M/M/1 моделі черг для вирішення задачі розподілу пропускної здатності мережі. Тільки одна модель розглядає конкурентоспроможність провайдерів у той час як п'ять інших припускають, що мережа знаходиться у стані монополії. Половина робіт розглядають конкуренцію у інформаційному наповненні та вмісті програмних продуктів.

Таблиця 1: **Останні дослідження про вплив інструментів мережевого нейтралітету**

	Хермалін & Катц (2007)	**Шрималі (2008)**	**Ченг, Бендіопадхуа, & Джіо (2010)**	**Чої & Кім (2010)**	**Економайдес & Хермалін (2010)**	**Кремер і Вівіора (2010)**
вертикальні режими регулювання	Нульове обмеження цін в порівнянні з якістю обслуговування багаторівневих продуктів	Нульове обмеження цін в порівнянні з диференціацією мережевого сервісу	Нульове обмеження цін в порівнянні з якістю обслуговування багаторівневих продуктів	Нульове обмеження цін в порівнянні з якістю обслуговування багаторівневих продуктів	Нульове обмеження цін в порівнянні з якістю обслуговування багаторівневих продуктів	Нульове обмеження цін в порів-нянні з якістю обслуговування багаторівневих продуктів
розподіл потужностей мережі	Незалежний	Незалежний	M/M/1 черга	Провайдерам дозволено поділяти пропускну здатність та продавати з пріоритетом обслуговування	M/M/1 черга	M/M/1 черга
структура ринку постачальників	Конкуренція	Монополія	Монополія	Монополія	Монополія	Монополія
структура ринку контент постачальників	Монополія	Монополія або дуополія	Конкуренція	Конкуренція	Монополія	Конкуренція
інвестиції від провайдерів	ні	так	так	так	так	так
іновації від контент провайдерів	так	так	ні	ні	так	так
Одержані результати	Обмеження платформи до одного продукту змушує постачальників програмних продуктів шукати високу чи низьку якість платформи сервісу, дозволяючи використовувати в середньому високу якість, що, ймовірно, негативно впливає на ефект добробуту.	Правило нульового обмеження цін максимізує соціальний достаток у короткостроковому та довгостроковому періоді, мережеві оператори здатні оцінити різні іновації	У короткостроковій перспективі оператори зароблять, а контент оператори втратять, якщо не буде якісного обслуговування багаторівневих продуктів. Стимули для інтернет провайдерів до розширення мережі високі у цьому випадку (правило нульового обмеження цін працює)	не може бути виключено, що правило нульового обмеження цін призводить до більш високих інвестицій у мережу	У короткостроковій перспективі мережевий нейтралітет краще ніж розподіл, але стимул до інвестицій є високим, якщо дискримінація цін дозволяється. Сукупний ефект не з'ясований	У короткостроковій перспективі Якісне обслуговування багаторівневих продуктів покращує добробут, якщо активна та ж сама кількість контент-провайдерів. Це створює гарний стимул для широкосмугових інвестицій, виключно якщо конкуренція між контент провайдерам та доходами від реклами не є дуже сильною

В більшості робіт вивчається вплив різних режимів регулювання на короткострокові розподіли ресурсів і довгострокові рішення. Результати, певною мірою залежать від конкретних припущень моделі. Це особливо вірно для короткострокових ефектів, декілька робіт виявили, що мережевий нейтралітет підвищує добробут (наприклад, Економайдес і Хермалін 2010) або знижує добробут (наприклад, Крамера і Вівіора 2010 року). Висновки більше узгоджуються з інвестиційними та інноваційними прогнозами, де виникають періодичні висновки, що мережева диференціація сприяє інноваціям та інвестиціям. За винятком Шрімалі (2008) усі інші автори вважають, що цей результат, швидше за все, залежить від конкретних умов. Наприклад, Чої і Кім (2010) визначили умови, за яких строгий мережевий нейтралітет збільшує інвестиції в мережу.

Таблиця 2. ***Стилізовані відносини між інструментами мережевого нейтралітету та загальними цілями.***

	Економічні цілі			*Політичні цілі*	
Інструменти	**Ефективне використання виробничих ресурсів**	**Інвестування у інтернет мережу**	**Інновації у прикладні програми**	**Свобода слова онлайн**	**Демократичні переговори онлайн**
Заборона блокування	~	~	~	+	+
Нульове обмеження цін	~	Може бути + при певних умовах	+	+	+
Мінімальна якість обслуговування	~	~	+	+	+
Якість обслуговування багаторівневих продуктів без дискримінації	+	+	+ коли іновації пов’язані	~	!
Якість обслуговування багаторівневих продуктів з дискримінацією	+	+	+ Для деяких пов'язаний інновації	-	-

Позначення: ~ немає сильного зв’язку , + позитивні відносини, - негативні відносини

Результати нашої якісної оцінки відображені в таблиці 2. Цікава закономірність з цього першого рівня аналізу: інструменти краще підходять для досягнення економічних або політичних цілей, але жоден з п'яти інструментів не здатний внести бажаний внесок по всьому спектру прийнятих цілей. У більшості цих сценаріїв заборона блокування не має правдоподібного сильного впливу на розподіл обмеженої пропускної здатності мережі. Такий стан може зменшити діапазон варіантів мережевих операторів по боротьбі проти крайнього перевантаження форм, це може збільшити стимули для мережевих операторів для розширення потужностей, і це може посилити стимули щодо форм розміщення інформації та постачальників програмних продуктів до інновацій. Однак ці ефекти є найчастіше дуже малими. Однак заборона блокування відіграє важливу роль у забезпеченні свободи слова, ці питання і цілі пов'язані з динамічними процесами демократії.

Обмеження нульовою ціною мережі операторів забирає один ефективний інструмент для управління пропускною здатністю мережі в сторону зниження цієї здатності на ринку. У більшості випадків, це обмеження буде як «стимул» скорочення інвестувань операторів у модернізацію мереж у порівнянні з ситуацією, в якій диференціація цін допускається. Однак, як Чої і Кім (2010) показують, якщо оператор

мережі володіє монопольним становищем, він може, при певних ринкових умовах, фактично збільшити стимули мережевих операторів.
Обмеження нульовою ціною, швидше за все, сприяє інноваціям в послугах та підвищує рівень програмних додатків, так як нульова ціна знижує прямі витрати на отримання доступу до мережі для гравців постачальників додатків і служб, що обслуговують різні пласти Інтернет продукту. Це дозволить розширити спектр економічно обґрунтованих послуг та програмних додатків (Бауер 2011). Таким же чином, як низькі витрати збільшують різноманітність контенту та програмних додатків вони також могли б підтримати свободу слова та демократичні ідеали.
Тим не менш, це не настільки однозначно і просто, як багато експертів вважають. Як продемонстрували дослідження на складних адаптивних системах, збільшення різноманітності не завжди є позитивним, занадто багато різноманіття може привести до хаосу і дезорганізації (Page 2010). Схожі явища спостерігалися в Інтернеті, де поширення блогів, соціальних мереж і джерел інформації, здається, породили фрагментації на відносно ізольовані, однорідні чати зі схожими думками, а не динамічними діалогами. Тим не менш, у цій статті не місце продовжити розгляд цього цікавого питання. Всі ми лише хочемо відзначити, що зв'язок між нульовою ціною регулювання та політичною багатоманітністю може бути менш надійними, ніж багато хто думає.

Однією з проблем з дозволом диференціації мережевих платформ є те, що розробники програмних додатків і послуг не мають коштів, щоб заплатити за доступ до пріоритетних напрямків у мережі, а це призведе до уповільнення максимальних зусиль цих напрямків. Стимули мережевих операторів носять змішаний характер. У них дійсно є стимули, щоб зробити контент доступним, якщо є попит серед своїх клієнтів. Однак невеликі політичні групи інтересів або теми, які є вузькоспеціалізованими, не можуть бути достатньо важливими для бізнесу операторів і, отже, страждають від проблеми повільного трафіку, навіть якщо немає умов блокування. Бреннан (2011) тому і пропонує мінімально якісний підхід, де Агентство з регулювання має встановити мінімальну якість обслуговування, яка повинна бути надана користувачам і постачальникам послуг.
Подібно обмеженню нульовою ціною, цей підхід, ймовірно, підвищить стимули для інновацій в розробці програмних додатків та сервісів. Крім того, цей підхід, ймовірно, буде гарантувати свободу слова та громадянської активності. Тим не менш, не зовсім зрозуміло, чи буде таке регулювання сильно сприяти ефективному управлінню потужністю або інвестиціям в мережу. Крім того, визнання таких мінімальних рівнів якості не є однозначним, хоча прецеденти існують в галузі телекомунікацій.

Якість багаторівневого обслуговування з вимогою недискримінації є іншим варіантом регуляторної політики, який багато хто вважає переконливим. У більш суворій формі така модель дозволила б підвищити якість багаторівневого обслуговування, але при цьому треба зобов'язати операторів мережі, щоб доступ до будь-яких рівнів був доступний будь-якій запитуючій стороні. Це дозволить диференціювати класи обслуговування, уникаючи при цьому саботажу і антиконкурентної дискримінації, які викликають тривогу відносно послуг, які конкурують з пропозиціями мережі оператора-власника. У той же час це дозволить постачальникам якісного сервісу та провайдерам з сервісами, які потребують певних технічних вимог, узгодити конкретні рівні якості обслуговування багаторівневих програм з мережевими операторами. У більш лібертаріанському підході (повна свобода думки і діяльності), здатність до дискримінації обмежена тільки антимонопольними принципами. Обидва ці варіанти мають бажані властивості ефективності і зможуть допомогти краще використовувати виробничі потужності і, при інших рівних, підвищити інвестиції в мережу. Однак ці підходи можуть зменшити стимули для певних типів модульних додатків і обслуговування інвестицій. Більше того, існують розбіжності між ними і свободою слова та іншими політичними цілями.
Якість обслуговування багаторівневого контенту-конкурента та постачальників програм-конкурентів також може збільшити стимул для підвищення надходження грошей від користувачів через нові бізнес-моделі. Якщо певні типи контенту будуть доступні тільки для передплатників Premium пакету, Інтернет може почати нагадувати індустрію кабельних технологій. Для того, щоб уникнути цих складнощів,

багаторівневу якість обслуговування, можливо, доведеться поєднати з іншими інструментами, такими як відсутність блокування або мінімальна якість обслуговування.

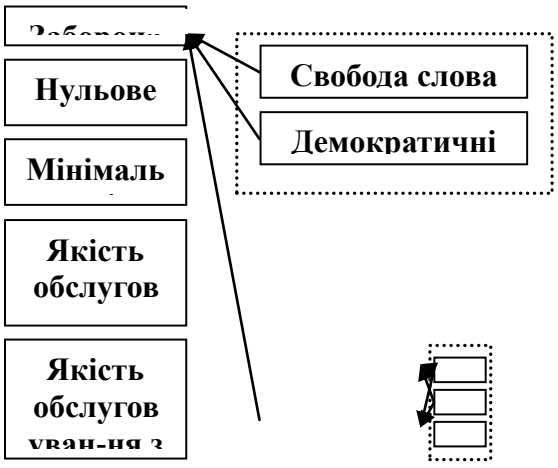
5. Обговорення отриманих результатів

Наш аналіз повторно розглянув кілька аспектів дискусії мережевого нейтралітету. У той час як політичні та економічні аргументи взяті з різних нормативних основ, вони не обов'язково будуть конфліктувати один з одним. Тим не менше, немає універсальних інструментів, які могли б сприяти досягненню обох наборів цілей одночасно. З п'яти інструментів які більш докладно обговорювалися (заборона блокування (змісту, додатків і пристроїв), нульове обмеження цін у мережевих операторів на схожу інформацію і постачальників схожих додатків, якість обслуговування багаторівневих продуктів операторами мереж і постачальників програмних продуктів без дискримінації, якість обслуговування багаторівневих продуктів операторами мереж і постачальників програмних продуктів з дискримінацією тих пір, поки це не порушує антимонопольного законодавства, і надання встановленого мінімального рівня якості обслуговування), деякі впливають переважно на досягнення політичних цілей та інші переважно впливають на досягнення економічних цілей.

Малюнок 2.

Причинно-наслідкові зв'язки між інструментами і цілями

Політ



Аналіз причинно-наслідкових зв'язків між цими інструментами і цілями дискусії мережевого нейтралітету показує, що жоден з інструментів не є достатнім для досягнення цілей (рис. 2). Заборона блокування не є необхідною умовою для політичних цілей і певних типів інновацій. Якість обслуговування

багаторівневих продуктів є необхідною умовою, яка дозволить провайдерам краще прийняти короткострокове максимально якісне використання виробничих потужностей, а також стане необхідною умовою для інвестицій в мережеву інфраструктуру в умовах ринку. Це передбачає, що з метою досягнення економічних і політичних цілей ці інструменти повинні бути поєднані. І, що важливо, як видно з таблиці 2, поєднуючи інструменти заради одних цілей ми не шкодимо досягненню інших цілей. Наприклад, відсутність блокування не має сильних негативних наслідків для економічних продуктивних цілей (хіба що деякі незначні). Політика якості обслуговування багаторівневих продуктів гарантує відсутність блокування, таким чином зможуть бути досягненні як політичні, так і економічні цілі.

6. Висновки

Ми вважаємо, що аналіз, представлений в цій статті може показати потенційний шлях вперед у розгляді переплутаних економічних та політичних аргументів на дебатах мережевого нейтралітету. Інші можливі інструменти повинні бути піддані більш поглибленому аналізу. Розгляд прямих ефектів та причинного зв'язку може допомогти прояснити здатність окремих інструментів і комбінацій інструментів для досягнення узгодження цілей.

Посилання:

Бауер, Дж. М. (2011). Відкритість мережі, інновації, або сектора економіки. У І. Спайкер , і Крамер (Ред.), Мережевий нейтралітет і відкритий доступ. Баден-Баден, Німеччина: Номос.

Блевінс, Дж. Л., і Барроу, С. С. (2009). Політична економія свободи слова та мережевий нейтралітет: Критичний аналіз. Журнал медіа права та етики, 1 (1/2), 27-48.

Блюменталь, М. С., і Кларк, Д. Д. (2001). Переосмислення дизайну в Інтернеті: Наскрізний агумент проти чудового нового світу. У Б. М. Компейн, і С. Грінштейн (ред.), Інформаційна політика в перехідний період: Інтернет та перспективи. (стор. 91-139). Камбрідж, МА: MIT пресс.

Ченг, Н.К., Бендіопадхуа, С., і Джіо, Н. (2010). Дебати з мережевого нейтралітету: Політичні перспективи.

Дослідження інформаційних систем, DOI: 10.1287/isre.1090.0257.

Чой, Д. П., і Кім, В.-С. (2010). Чистий нейтралітет і стимули для інвестицій. РЕНД журнал економіки, 41 (3), 446-471.

Купер, М. (2003). Відкриті платформи комунікації: фізична інфраструктура як основа інновації та демократичного дискурсу в епоху Інтернету. Журнал з електрозв'язку та закон високих технологій, 2 (1), 177-244.

Дензау, А. Т., і Північ, Д. С. (1994). Загальні ментальні моделі: Ідеології та установи. Куклос, 47 (1), 3-31.

Економайдес, Н., і Хермалін, Б. Є. (2010). Економіка мережевого нейтралітету. NET інститут. Робочий документ # 10-25.

Ентман Р., & Уайлдман, С. С. (1992). Узгодження економічних і неекономічних перспектив у медіа політиці: за межами "ринку ідей". Журнал Комьюнікейшнс, 42 (1), 5-19.

Фріден, R. (2010). Оцінка переваги зобов'язань мережевого нейтралітету при низькому, середньому і високому мережевому рівні. Документ представлений на 38-й конференції з комунікацій, інформаційної та інтернет-політики. Арлінгтон, Вірджинія, 30 вересня-2 жовтня 2010

Габермас, Дж. (2006). Політична комунікація в медіа суспільстві: Чи насолоджується демократії як і раніше епістемічними вимірами? Вплив нормативної теорії на емпіричні дослідження. Теорія зв’язку, 16, 411-426.ican Економічне ревью, 99 (1), 5 –24.

Хермелін, Б. Є., і Кац, М. Л. (2007). Економічні обмеження продукт-лінії в обговоренні мережевого нейтралітету. Інформаційна економіка і політика, 19 (2), 215-248.

Холінгсворс, Дж. Р., і Ліндберг, Л. Н. (1985). Управління американською економікою: роль ринків, кланів, ієрархії та асоціативної поведінки. У В. Streek, & P. Schmitter (ред.), Приватний державний інтерес: За межами ринку та держави (стор. 221-254). Лондон: Мудрість.

Джордан, С. (2009). Наслідки Інтернет архітектури після мережевого нейтралітету. ACM угоди у інтернет-технологіях, 9 (2), 5:1-5:28.

Джордан, С., і Гош, А. (2009). Як визначити, чи є практика управління трафіком розумною. Документ, представлений на 37-й науково-практичній конференції з комунікацій, інформаційної та інтернет-політики, Арлінгтон, Вірджинія,

Джордана, Дж., & Леві-Фор, Д. (ред.). (2004). Політика регулювання: установи і регулюючі реформи для віку управління (CRC серії про конкуренцію, регулювання і розвиток).

Челтнем, Великобританія; Нортгемптон, Массачусетс: Едвард Елгар. Крамер, Дж., & Вівіорра, Л. (2010). Мережевий нейтралітет та перевантаження чутливими контент-провайдерами: Наслідки для інноваційних послуг, масштабних інвестицій та регулювання (30 вересня 2010 р.). НЕТ інститут робочий документ № 10-09, за адресою SSRN: http://ssrn.com/abstract=1694320.

Летзер, М., Джаст, Н., Соувейн, ФF., & Смолінскі, Р. (2003). Регулювання повторного видання: інституційні зміни шляхом самостійного і спільного регулювання у секторі медіа. Комунікації і стратегії, 50, 127-157.

Лемлі, М. А., і Лессінг, Л. (2001). Кінець безперервності: Збереження архітектури інтернету в еру широкосмугового зв'язку. UCLA Ревью Закон, 48 (4), 925-972.

Мейнтз, Р. (2003). Нові завдання в теорії управління. У Н. П. Вибуху (ред.), управління як соціальна та політична комунікація (стор. 27-40). Манчестер і Нью-Йорку: редакція Манчестерського університету.

Нунзіато, Д. С. (2009). Віртуальна свобода: Мережевий нейтралітет і свобода слова в епоху Інтернету. Стенфорд, СА: редакція Стендфордського університету.

Пейдж, С. (2010). Різноманітність і складність. Прингсінгтон, NJ: редакція Прингсінгтонського університету.

Родос, Р. А. В. (1996). Нове управління: Керуючий без уряду. Політичні дослідження, 44 (4), 652-667.

Шарпф, Ф. В. (1993). Координація в ієрархії та мережі. У Ф. В. Шарпф (ред.), Ігори в ієрархії та мережі: аналітичні та практичні підходи до вивчення проблем інститутів управління (стор. 125-165). Франкфурт: Кампус.

Шейтер, А., та Джеміні, М. (2007). «Справедливість і тільки справедливість, Ви переслідуватиме ': Мережевий нейтралітет, Перша поправка і теорія Джона Роулза про справедливість. Мічиганські телекомунікації та технології закону, огляд, 14, 137-174.

Шутт, Ф. (2010). Мережевий нейтралітет: огляд економічної літератури. Огляд мережевої економіки, 9 (2).

Шрімалі, Г. (2008). Надлишки екстракція мережевих провайдерів: наслідки для мережевого нейтралітету та інновацій. Політика в області телекомунікацій, 32 (8), 545-558.

Тревіс, Н. (2007). Блоги, електронні книги, і широкосмугові послуги: доступ на цифрові носії, як право Перша поправка. Хофстра юридичний огляд, 35, 1519-1580.

Вільямсон, О. Є. (1996). Механізми управління. Нью Йорк: редакція Оксфордського університету.

Вільямсон, О. Є. (2005). Економіка управління. Американський економічний огляд, 95 (2), 1-18.