Институт
Современного
Развития

«Электронная дипломатия». Начало

Аналитический доклад

февраль 2013

Автор:

Кулик Сергей Александрович,
директор Дирекции по проблемам международного развития Института современного развития

Содержание

Установка президента России «разъяснять наши позиции, на разных платформах и с использованием новых технологий, пока не дойдет», прозвучавшая на июльском (2012 г.) совещании в российском МИДе, несколько оживила отечественное экспертное сообщество и планы внешнеполитического ведомства. По сообщениям СМИ, запущен первый сайт министерства в YouTube, усилено внимание к расширению присутствия наших дипломатов в Твиттере и Фейсбуке, а в Дипломатической академии организованы специальные курсы.

Газета «Коммерсант» цитирует источник из МИДа: «До выступления Владимира Путина скептики говорили, что цифровая дипломатия — это лишь дань конъюнктуре. Однако президент Путин ясно сказал: одними только традиционными методами уже не обойтись. Осваивать новые методы необходимо в любом случае»[1]. В этой связи газета напомнила, что, в отличие от государственного департамента США и дипломатических ведомств ряда других стран, в нашем министерстве нет специализированной структуры, которая бы занималась «цифровой дипломатией»; нет и соответствующих подразделений при посольствах.

После всплеска интереса к применению новых технологий в дипломатической практике с появлением цитируемого выше материала и обильных ссылок на него в других информационных источниках соразмерного освещения темы в отечественных СМИ более не наблюдается. На экспертном горизонте стали чаще появляться работы, в которых предпринимаются попытки более широкого охвата тематики и осмысления потенциала Сети для нужд нашей внешней политики. Но они в основном ограничены ресурсами Российского совета по международным делам (РСМД) и Центра политических исследований (ПИР-Центра). Даже в расширяющемся списке материалов, затрагивающих модную ныне тематику «мягкой силы», вопросы «сетевой мощи» пока занимают весьма скромное место.

К сожалению, на этом направлении мы находимся в положении «догоняющей стороны». Более того, если судить по официальным документам, все еще довлеет инерция настороженного восприятия новых технологий и, что не менее важно, очевиден дисбаланс в аналитических предпочтениях (обусловленный в том числе и такой инерцией). Особенно заметно превалирование проблематики информационной безопасности и угроз — важнейшей, но не единственной в рамках темы освоения сетевых инструментов (ИКТ, социальные сети, блогосфера).

---

[1] Елена Черненко. Россия направляет посольства в Twitter. — «Коммерсантъ», № 128/П (4913), 16 июля 2012.

Возникает потребность обратить самое пристальное внимание политиков и экспертов на возможности этих инструментов для удовлетворения внешних нужд страны, укрепления ее репутации и позиций на международной сцене. Особенно ввиду высокой активности зарубежного экспертного сообщества и внешнеполитических ведомств ведущих стран в изучении и использовании потенциала Сети, в усилиях по систематизации накопленного опыта и в анализе вероятных рисков и козырей, предлагаемых «сетевой мощью». В повестке последней довлеющее предпочтение «угрозам и противодействию им» рано или поздно упрется в осознание необходимости ставить целый комплекс вопросов, касающихся и плюсов.

В настоящем материале мы ограничиваемся наблюдениями, затрагивающими лишь некоторые из тех аспектов внешнеполитического измерения «сетевой мощи», которые, по нашему мнению, недостаточно рассматриваются на российских площадках. Он предназначен для интересующихся данной темой работников и экспертов, занятых в международной сфере, с надеждой на оживление дискуссии и расширение ее повестки.

Перекосы в оценках рисков и козырей

Напомним, что по тематике «сетевой мощи» в первом десятилетии нынешнего века внимание зарубежных экспертов было сфокусировано преимущественно на анализе проблем и перспектив кибервойн и киберугроз. Исследования в этой области остаются интенсивными и сейчас по вполне объективным мотивам.

Заметно меньше места уделялось вопросам использования киберинструментов в политике «мягкой силы» и в общей дипломатической работе. Иными словами — появляющимся возможностям Сети для обеспечения интересов и укрепления позиций государств на внешней арене.

За последние два-три года внимание к этим возможностям в международном экспертном сообществе существенно повысилось — до уровня, позволяющего говорить о постепенном выправлении дисбаланса в осмыслении значимости новых технологий. Отчасти это объясняется растущим интересом к уже проводимой несколько лет работе государственного департамента и других вовлеченных во внешние дела структур США, стимулированием Вашингтоном аналогичных действий своих союзников и ближайших партнеров.

Ключевым же фактором представляется крепнущее осознание того, что с воздействием такого «игрока», как Сеть, придется иметь дело все плотнее — и в защите, и в наступлении. Постепенно нащупываются новые методы и проблемы внешнеполитической работы.

В свою очередь, Сеть активнее участвует в формировании непривычных норм поведения на международной сцене. Прогресс в информационных технологиях, ускоренный рост роли киберпространства и

социальных сетей порождают новую реальность не только для организаций и граждан, но и для государств.

Возникающая информационная среда начинает диктовать свои правила игры государственным органам, занятым во внешнеполитической сфере. Она усложняет международную систему, расширяет список ее участников, меняет форматы социально-политических событий, непосредственно затрагивающих мировую конфигурацию, становится фактором нестабильности и появления дополнительных угроз. Речь идет не только об информационной составляющей, но также о схемах формирования и протекания конфликтов и иных значимых процессов.

Бурное развитие ИКТ предлагает государственным и внешнеполитическим структурам особенно крупных мировых игроков такие вызовы, о многих из которых всего 10—15 лет назад они не имели внятного представления, либо не считали необходимым воспринимать их со всей серьезностью. Оно становится одним их тех ключевых раздражителей, которые постоянно держат эти структуры в состоянии напряженности, ожидания неприятностей и внешних сюрпризов.

Вместе с тем, широкая поступь Интернета, к которому сейчас, по данным Международного союза электросвязи, имеет систематический доступ треть жителей планеты, увеличивает багаж приемов и преимуществ внешнеполитических структур в планировании и проведении политической линии вовне и в укреплении позиций и репутации своей страны. Главное — вовремя и плодотворно ими воспользоваться.

Не нужно забывать об ускорении процесса сближения онлайн и оффлайн режимов. Например, мобильный телефон является не только средством взаимного общения, но и получения и отправки фото- и телевизионных картинок. Эти функции допускают быструю передачу материалов из режима оффлайн в режим онлайн. Не менее важной представляется функция навигации, позволяющая определять местонахождение пользователя данного контента и соответственно адаптировать контент соразмерно страновой и региональной специфике[2].

Что касается России, то, как недавно отмечала эксперт РСМД Е. Зиновьева, «есть все основания утверждать, что сегодня Интернет недостаточно используется российским государством в качестве инструмента

---

[2] Сейчас уже более 4 млрд людей (почти 60% населения Земли) — мобильные пользователи с более 5 млрд мобильных телефонов, из которых четверть приходится на смартфоны. Доля смартфонов в продажах резко возросла в 2012 г. (70%), что характерно и для планшетных компьютеров. Такая тенденция, по прогнозам, сохранится в ближайшее время.

Пользователи мобильной связи все больше обращаются к услугам Интернета. Четверть уже использует 3G-соединение с Интернетом, а более 20% — WiFi-сети. Объем мобильного трафика приближается к 15% от общемирового. В общем, происходит революция мобильного контента. *См.* А. Шнайдер. Всемирная отзывчивость: наступает эпоха responsive design. — Slon. ru, 25 декабря 2012, slon.ru/future/vsemirnaya_otzyvchivost_nastupaet_epokha_responsive_design-868653.xhtml

внешней политики и дипломатии, средства усиления «мягкой силы» и повышения привлекательности образа страны за рубежом. Проблема состоит в том, что большая часть российских политиков и чиновников продолжает рассматривать вопросы развития цифровых сетей исключительно в контексте рисков и угроз. Так, в «Стратегии национальной безопасности Российской Федерации до 2020 года» информационная угроза рассматривается в качестве одной из важнейших угроз национальной безопасности страны. Интернет воспринимается как канал распространения экстремизма и терроризма, навязывания чуждой идеологии и внешнеполитической пропаганды, как средство ведения информационной войны. Однако обеспечение информационной безопасности не исключает использования Интернета как средства реализации внутренних и внешних целей государства. Последствия распространения Интернета многогранны и не исчерпываются проблематикой безопасности»[3].

Вполне справедливые замечания. Если правильно и тонко распоряжаться киберинструментами для реализации государственных целей, это поспособствует и укреплению безопасности страны. В том числе через усиление потенциала «мягкой силы», повышение эффективности и оперативности внешнеполитической работы.

Своим взглядом на существующие перекосы делится и директор Координационного центра национального домена сети Интернет А. Колесников. В борьбе со стратегическими киберугрозами, по его мнению, «Россия традиционно — и не только в этой области — занимает реактивно-оборонительную позицию…Интернет являет собой среду, которая не приемлет оборонительного подхода. России необходимо действовать в этой области проактивно. Нельзя занимать круговую оборону против кого-либо — необходимо наступать, разрабатывая собственные кибертехнологии и иные разработки в информационной сфере при серьезном бюджетном финансировании и внимании государственных органов»[4].

Действительно, даже погоня за «угрозами» и поиски противодействия им ведутся в отсутствие комплексного официального подхода к кибербезопасности, при наличии лишь отдельных и слабо связанных документов. Россия отстает от ряда ведущих стран в разработке общих норм и методов в этой сфере. Эти проблемы почти не просматриваются в приведенной выше Стратегии национальной безопасности. Принятая в 2000 г. более адресная Доктрина информационной безопасности уже устарела. В целом наблюдается дефицит осмысленного стратегического

[3] Е. Зиновьева. Россия во всемирной паутине: цифровая дипломатия и новые возможности в науке и образовании. — Российский совет по международным делам, 17 февраля 2012, russiancouncil.ru/inner/?id_4=121

[4] «В поиске общих подходов к информационно-коммуникационным технологиям в контексте международной безопасности» — ПИР-Центр, 15 ноября 2012, www.pircenter.org/news/6366

видения проблематики кибербезопасности и разрозненность в соответствующем механизме.

Приоритет темы «угроз» сопровождается ограниченностью аналитической повестки, касающейся внешнеполитической сферы. У нас она «привязана», прежде всего, к использованию сетевых технологий в публичной дипломатии Вашингтона. Американская активность воспринимается весьма негативно, как непосредственная угроза нашим интересам и стабильности в отдельных странах, особенно на постсоветском пространстве. Понимание публичной и даже «цифровой» дипломатии здесь еще более сужается — до работы через социальные сети с молодежью и оппозицией и сбора информации о внутриполитических раскладах. Отсюда — предложения о подключении новых информационных ресурсов прежде всего в качестве «противодействия», либо о принятии жестких защитных мер.

Та же газета «Коммерсант» от 15 сентября 2011 г. приводит оценки «источником в МИДе» «цифровой дипломатии» США: «У американцев появился крайне эффективный, недорогой и легкий в применении инструмент воздействия на граждан других стран. Это полностью меняет характер противоборства: теперь им не надо бомбить аэродромы — можно бомбить мозги». Одновременно собеседник автора статьи признал, что Москва не может ответить США тем же из-за их «гегемонии в интернете и неравных конкурентных возможностей в информпространстве». И поэтому «будут обсуждаться меры по противодействию цифровой дипломатии США».

Не будем давать оценок таким рассуждениям. Для озабоченности и беспокойства действительно есть основания. Вопрос сейчас в другом — в балансе восприятия угроз и возможностей, в балансе «реактивной» и созидательной системной работы. Ориентация на постоянное и повсеместное противостояние с «вашингтонским обкомом» отвлекает внимание от многих серьезных вызовов и поиска должных решений, ограничивает кругозор «осажденной крепостью» с заданным набором тактик и шаблонов. Желательно присмотреться к чужому опыту под иным углом, творчески изучать «пробы и ошибки» других, брать полезное для себя.

Тем более обратим внимание на слова «источника» об эффективном, недорогом и легком в применении инструменте воздействия. Если это так, то почему же он должен быть исключительно поводом для опасений? Для начала, скажем, не помешает провести аудит наших усилий в публичной дипломатии по критерию «затраты-эффективность», оценить совокупность преимуществ и издержек онлайн и оффлайн режимов, работы в Сети и организации различных крупных и недешевых мероприятий.

В сфере возможностей ИКТ для внешних нужд России основное внимание специалистов пока уделяется этим технологиям как инструменту интеграции в мировое хозяйство, задачам внешнеэкономического порядка и укрепления научных связей. На этом направлении нельзя не заметить

определенных успехов. Особенно в сравнении с внешнеполитическим и общим позиционированием страны. При этом серьезные достижения России в развитии и овладении ИКТ за последние годы обеспечивают значительный потенциал для использования во внешнеполитической сфере в целом, в том числе как масштабного «инструмента воздействия».

«Э-дипломатия» за частоколом терминов

Открывающиеся технологические ниши и возникающие с ними нагрузки на внешнеполитические механизмы начинают влиять на производительность традиционных рычагов, связанных с многовековым дипломатическим опытом. Отсюда возникает спрос на оперативную и мягкую, без «подрыва основ», перенастройку инструментов и норм внешнеполитического планирования и поведения.

Не случайно об этом серьезно раздумывают западные аналитические центры. Уже обнародованные соображения, в том числе опирающиеся на опыт госдепартамента США, дают определенную «пищу для размышлений», в том числе критического и скептического свойства. Они также свидетельствуют, что исследовательская мысль пока находится на этапе формулирования конкретных позиций и формирования системных подходов.

Такое состояние отражается во все еще достаточно вольном обращении с терминологией, касающейся применения Сети для внешнеполитических нужд. Ограниченность рамками публичной дипломатии и предпочтениями определенным объектам режима онлайн влияет на использование словаря терминов и на их интерпретацию — будь-то «цифровая дипломатия» (digital diplomacy), «сетевая дипломатия» (net diplomacy), «дипломатия Web 2.0» с их различными вариациями (public diplomacy Web 2.0, Internet diplomacy и др.)[5]. Модной становится «Твиттер-дипломатия». В результате, под один и тот же термин разными экспертами часто подгоняется разное понимание — без особой увязки с официальными разъяснениями комплексного и детального порядка. Что не удивительно — такие разъяснения пока в дефиците мирового масштаба.

Все это отнюдь не способствует более полному пониманию объектов и субъектов использования сетевых инструментов. Но все же следует исходить из того, что эффективность дипломатии зависит от согласованности, продуктивности и оперативности механизма принятия и реализации внешнеполитических и смежных решений. Поэтому два направления — применение новых технологий «внутри системы» и вне ее — следует учитывать в тесной взаимосвязи — по возможностям и целесообразности, как «сообщающиеся сосуды».

[5] Считается, что модель Web 1.0 работала с изобретения «паутины» до конца прошлого века. Отсутствие многообразия платформ и другие тогдашние ограничители сужали как круг потребителей, так и возможности общения с ними, тем более в режиме реального времени.

В этом — суть употребления этих инструментов для международной работы государства, независимо от того, под какое официальное или популярное определение оно подпадает. Осознание этой, на первый взгляд, очевидной вещи многими зарубежными экспертами и политиками отчасти объясняет бурную популярность в 2012 г. термина «электронная дипломатия».

Широкое распространение он получил с выходом весной 2012 г. труда приглашенного в американский Институт Брукингса сотрудника австралийского Института Лови Ф. Хансона «Революция и госдепартамент: распространение Э-дипломатии»[6]. Через полгода он опубликовал вторую часть исследования: «Свежеиспеченный и отправленный: Э-дипломатия и госдепартамент»[7]. Исследователь первым постарался систематизировать программную работу, уже несколько лет проводимую государственным департаментом, которая там же и именуется «электронной дипломатией» — точнее, «Э-дипломатией» (ediplomacy).

Появление первой части труда заметно оживило интерес к теме «Сеть и внешняя политика» и обусловило поворот в ее обсуждении. Достаточно сказать, что в течение первых недель после выхода первой части количество скачиваний составляло десятки тысяч, что является одним из рекордных показателей для всех «мозговых центров» мира[8].

Множатся специальные проектные и образовательные сайты «e-diplomacy», расширяется сеть площадок для обучения и обсуждения того, что подразумевается под «Э-дипломатией». Эти площадки не ограничиваются территорией Соединенных Штатов. Они также создаются вместе с американскими союзниками и ближайшими партнерами или последними самостоятельно. При всех разногласиях между участниками осуществляются совместные программы обучения специалистов, предназначенные для оптимизации работы по позиционированию стран на международной арене с помощью ИКТ и др. Американцы используют свой опыт прежде всего в собственных интересах, но и делятся знаниями со своими коллегами.

Заходит разговор даже о возможности появления новой дисциплины, которая будет формироваться в процессе внедрения технологических новаций для каждодневной, а не эпизодической деятельности внешнеполитических структур и их адаптации к очередным вызовам и угрозам.

Вместе с тем, Ф. Хансон, обладая существенным багажом позиций и заявлений представителей госдепартамента США по поводу «электронной дипломатии», вынужден ограничиться, по его же выражению, «рабочим определением» термина: использование всемирной паутины и новых ИКТ

---

[6] Fergus Hanson. Revolution @State: The Spread of eDdiplomacy. Lowy Institute, March 2012.

[7] Fergus Hanson. Baked In and Wired: eDiplomacy@State. — «Foreign Policy at Brookings», October 2012.

[8] Rory Medcalf. Drawing the line — «American Review», May 2012, americanreviewmag.com/opinions/Drawing-the-line

для содействия в реализации внешнеполитических целей[9]. В этом виден определенный резон. Такое широкое толкование позволяет уйти от ограничения «электронной дипломатии» лишь инструментами социальных сетей. Это ограничение было свойственно многим западным исследователям, рассматривающим ее преимущественно как род дипломатии публичной. Несколько позднее на одном из профильных сайтов (techopedia.com) «Э-дипломатия» была определена как «действие в стремлении достижения дипломатических целей через использование Интернета, социальных сетей и коммуникационных технологий в целом»[10].

Но вопрос не столько в формулировках. Внимания, скорее, заслуживает то, что на основе изучения различных структур государственного департамента США, имеющих отношение к «электронной дипломатии», и отбора своего рода «состыковок их функциональных связей» Ф. Хансон предлагает схему основных групп таких состыковок (или «рабочих направлений»). Их получилось восемь.

1. Управление знанием: повышение эффективности в применении знаний, накопленных в ведомствах и правительстве в целом, так, чтобы эти знания были аккумулированы и использованы должным образом для обмена ими, а также оптимально применялись для обеспечения национальных интересов за рубежом.

2. Публичная дипломатия: поддержание связей с общественностью, подключение новых инструментов коммуникаций для тщательной оценки общественного мнения, адресации ключевых посланий важным сегментам общества и воздействия на авторитетные в Сети фигуры.

3. Управление информацией: содействие объединению огромных и разнообразных информационных потоков, чтобы обеспечить доведение нужных сведений до принимающих решения властных эшелонов и лиц, а также должное реагирование на возникающие социальные и политические изменения в странах и регионах.

4. Консульское содействие: создание прямых каналов общения с пребывающими за рубежом согражданами.

5. Реагирование в чрезвычайных ситуациях: усиление возможностей ИКТ для решения возникающих проблем.

6. Свобода Интернета: развитие технологий для обеспечения свободы и открытости в использовании Интернета.

7. Внешние ресурсы: развитие технологий и онлайн-режимов для отслеживания и использования внешних экспертных ресурсов в реализации государственных задач.

8. Политическое планирование: обеспечение возможности эффективной координации и планирования внешней политики в государственных структурах.

---

[9] Fergus Hanson. Revolution @State, p. 3.

10 www.techopedia.com/definition/29050/ediplomacy

Эти направления работы госдепа США, которые Ф. Хансон пытается конкретизировать в своем первом труде (с ним советуем ознакомиться более детально), условно можно разбить на три типа:

- внутрисистемный (накопление, оптимизация отбора и распределения оценок и предложений, управление огромными потоками собственной информации как внутри ведомства, так и в общем механизме внешнеполитических решений);
- внешнего применения (включая публичную дипломатию), нацеленный на укрепление позиций и репутации страны за рубежом, на использование «внешней экспертизы» (экспертных сообществ и др.) с помощью цифровых инструментов и т. п.;
- «смешанный» (состыковка, где это необходимо, функций первых двух типов, например, в реагировании и урегулировании чрезвычайных ситуаций (которые не сводятся к техногенным или природным катастрофам) и др.).

Таким образом, «электронная дипломатия» на самом деле подразумевает весьма широкий набор раздельных или взаимосвязанных задач — и новых, и традиционных, но решаемых с помощью ИКТ в режиме онлайн. Набор более масштабный, нежели «меню» с заглавиями «цифровая дипломатия» и др. Не менее важно, что указанная выше разбивка позволяет лучше понимать направления и задачи по теме «Сеть и внешняя политика», по сравнению с имеющимися расшифровками альтернативных терминов.

Следует добавить, что охват «электронной дипломатии» будет, очевидно, шире национальных границ даже при относительно закрытой «внутрисистемной» работе. По мере освоения новых методов различными государствами, в особенности состоящими в союзнических отношениях, могут возникнуть отдельные совместные программы для координации тех или иных действий в режиме онлайн. В качестве примера упомянем подобную программу, к которой уже приступили США с Мексикой.

Как же обстоят дела с пониманием конкретных направлений использования сетевых технологий для нужд внешней политики у нас? Полезно обратиться к двум из весьма небольшого числа трудов, в которых авторы стараются уйти от очередного «пережевывания» угроз и заняться оценками возникающих возможностей.

В канун 2013 г. со своим видением выступил заместитель директора Департамента информации и печати МИД России Е. Пантелеев. Заслуживает внимания уже то, что, указывая на жонглирование разными определениями при обзорах рассматриваемой темы, он счел полезным предложить свою формулировку — «инновационная дипломатия». Ее, по мнению специалиста, «можно определить как инструмент внешней политики России для воздействия на общественное мнение с использованием информационно-коммуникационных технологий». Исходя из этого, он относит к ее «первоочередным задачам»:

- взаимодействие с общественностью — налаживание и поддержание широких контактов путем определения целевых аудиторий через онлайн-пространство и другими современными способами (сайты, аккаунты в соцсетях, блоги, SMS-информирование и т. п.);

- управление знаниями — аккумулирование лучших знаний и опыта, их оптимальное распространение (использование внешних и внутренних экспертных ресурсов, включая краудсорсинг, создание дипломатической электронной энциклопедии и внутрикорпоративной социальной сети, организация веб-семинаров «по интересам» и др.);

- управление информацией — отслеживание международных информационных потоков с целью «раннего предупреждения» возникающих социальных и политических тенденций, а также для своевременного реагирования на чрезвычайные ситуации с российскими гражданами (в том числе с применением систем автоматизированного мониторинга);

- поддержка координации — обеспечение планирования, сопровождения и контроля за внешними связями субъектов Федерации, федеральных органов исполнительной власти и крупных хозяйствующих структур.

Речь идет лишь о «первоочередных задачах», и список их заметно уже, нежели список «рабочих направлений» госдепартамента, составленный Ф. Хансоном. Особый же акцент сделан на «воздействие на общественное мнение», т. е. в основном на публичную дипломатию.

Тем не менее, автор предполагает и «внутрисистемный» тип работы. К тому же он справедливо добавляет задачи, обусловленные отечественной спецификой, — координацию деятельности субъектов Федерации, что, собственно, давно возложено на МИД России.

Эксперт РСМД Л. Пермякова несколько по-иному выделяет «особо эффективные» направления того, что она определяет как «цифровая» и «электронная» дипломатия. Первым в списке идет публичная дипломатия — обеспечение возможности «обращаться напрямую к целевой аудитории с конкретными сообщениями, в том числе привлекать к сотрудничеству авторитетных опинион-мейкеров» через «установление контактов с онлайн-аудиторией и формирование новых инструментов коммуникации».

Второе направление рассматривается как «область управления информацией, в том числе накопленными знаниями и опытом», где «аккумулирование и анализ колоссального объема информации» могут быть «с успехом использованы в политических прогнозах и стратегическом планировании».

Третье направление — «осуществление консульской деятельности».

Наконец, «использование ИКТ для осуществления экстренной связи с посольством государства за рубежом» «в случае возникновения чрезвычайных ситуаций и стихийных бедствий».

Ограничиваясь указанными направлениями работы, Л. Пермякова при этом адресует к полезным инструментам и методам внешнеполитических

ведомств США и Великобритании, часть которых упоминается или подразумевается в работе Е. Пантелеева (краудсорсинг, американская Диплопедия (онлайн-ресурс экспертных материалов по международным отношениям), взаимодействие сотрудников в профессиональных сетях и др.)[11]. Эти, а также многие другие инструменты более системно описаны западными исследователями.

Вопрос, однако, заключается не только в систематизации существующих и возможных сетевых инструментов для реализации внешнеполитических интересов и потребностей государства. Речь идет о более четкой расстановке приоритетов и распределении имеющихся ресурсов.

В этой связи обратимся к некоторым оценкам американского опыта, сделанным во второй части исследования Ф. Хансона.

Во-первых, уже достигнута та точка отчета, за которой внешнеполитическое ведомство той или иной страны не сможет эффективнее обеспечивать национальные интересы без адаптации к меняющейся (в том числе с воздействием новых технологий и Сети) среде своей работы.

Во-вторых, даже ресурсы и возможности такой страны, как США, не позволяют в равной мере охватить все перечисленные выше восемь «рабочих направлений».

Ввиду ограниченности возможностей (и не только финансовых), у госдепартамента США, как безусловного мирового лидера в освоении «электронной дипломатии», пока вырисовываются три направления, в которые ушли основные ресурсы и где были внедрены наиболее новаторские подходы. Первое — публичная дипломатия (прежде всего, перенастройка контактов с зарубежной аудиторией). Но если этот приоритет весьма широко освещен в информационном пространстве, то два других обделены вниманием общественности и экспертов. Речь идет об обеспечении «свободы Интернета» и особенно об «управлении знанием», хотя на последнем направлении, как утверждается, разработаны довольно инновационные подходы.

В-третьих, в самом госдепартаменте по-прежнему существует определенная настороженность относительно широкого использования новых технологий. Если задачи публичной дипломатии, к которым привязывается работа по обеспечению «свободы Интернета» и «управлению знанием», вызывают наибольший энтузиазм, то подключение сетевых инструментов к политическому планированию или к работе с диаспорами за рубежом пока не получило аналогичного развития хотя бы на организационном уровне.

[11] Л. Пермякова. Цифровая дипломатия: направления работы, риски и инструменты. — Российский совет по международным делам, 27 сентября 2012, russiancouncil.ru/inner/?id_4=862

На службе государственному механизму

Еще в 1998 г. в документе госдепартамента по стратегическому планированию на десятилетие вперед роль электронных технологий во внешнеполитической деятельности практически не упоминалась. Но тогда же началась работа по оценке этой роли. Одним из важных стимулов к этому якобы послужили неудачи США в конфликтах в Восточной Африке и сопутствующие репутационные издержки. Но лишь следом за сентябрьской трагедией 2001 г. в Нью-Йорке в следующем году была образована рабочая группа по «Э-дипломатии» под кураторством самого главы госдепа К. Пауэлла, затем переформированная в Управление.

Активизация деятельности на новом направлении не была вызвана исключительно внешними причинами и вышеуказанными кризисными ситуациями. Считается, что инициативы К. Пауэлла отражали приоритетность задачи создания более простого и гибкого режима обмена информацией и предложениями внутри ведомства и между правительственными структурами. Более того, ее выполнение рассматривалось именно в качестве первого шага на пути к более тесному взаимодействию с внешними пользователями и общественностью.

Речь шла, в частности, о попытке несколько отойти от стандартных дипломатических методов времен «холодной войны» с их жесткой вертикалью адресного распространения информации в ведомстве и между ведомствами, а также подумать о перенастройке «внутренней культуры», которая всегда диктовала требования прежде всего «знать», к введению хотя бы ограниченной нормы делиться этим «знанием» с другими государственными структурами и между подразделениями самого госдепартамента. Такая задача, естественно, оказалась весьма сложной, в том числе в силу известной ведомственной и межведомственной инерции, бюрократических традиций и конфликтов.

Не удивительно, что пока (во всяком случае, исходя из наблюдений Ф. Хансона и игнорирования этого направления многими западными экспертами) внедрение новых технологий в рамках «электронной дипломатии» в сфере политического планирования не вошло в список приоритетов.

Настороженность обусловлена не только вполне объяснимой межведомственной ревностью, но и широким беспокойством на предмет безопасности сетей для обмена информацией и предложениями. Часть ведомств и подведомств, занимающихся различными направлениями «Э-дипломатии», включая дипломатию публичную, в той или иной степени связаны с «управлением знанием» и политическим планированием. Поэтому один из серьезных вызовов для такого взаимодействия — вероятные риски утечки информации в силу особенностей сетевых платформ.

Хотя опыт госдепартамента свидетельствует (к удивлению Ф. Хансона и других экспертов), что такого рода проколы были весьма редкими. Это объясняется в том числе достаточным уровнем

самодисциплины дипломатов и их сильным стремлением сохранить свое рабочее место. К тому же, как отмечается, если дипломат захочет поделиться секретами, он сделает это по-иному.

Так или иначе, среди экспертов сохраняется мнение о том, что «цифровые инициативы» по-прежнему стимулируются руководством во внутрисистемном режиме. Возможности Сети продолжают рассчитываться не только на установление «обратной связи» с общественностью и другими внешними пользователями, но и на внутрисистемное потребление.

Однако все еще весьма медленно идет процесс открытия некоторых инструментов вовне. В этой связи специалисты ставят вопрос: как нужно соблюсти баланс между разрешением сотрудникам создавать собственные страницы в Твиттере или Фейсбуке и разрешением на обмен между собой профессиональными мнениями и оценками?

Последнее имеет немаловажное значение. Считается, что более 90% информации, требуемой разведсообществом для обеспечения национальной безопасности и подготовки государственных решений, добывается из открытых источников. Сеть расширяет возможности получения такой информации. Иное дело — мнения и позиции высокопоставленных и не очень чиновников, которые могут, по мнению «слушателей», учитываться при принятии политических решений и действий.

Сложности добавляет вал информации, которая обрушивается на структуры внутри системы. Он грозит неприятными последствиями для механизма подготовки и принятия решений. Такой вал может относительно легко генерироваться новыми технологиями (о чем свидетельствуют события «арабской весны»). Это предъявляет дополнительные требования при решении традиционной задачи отбора и классификации информационных потоков во внешнеполитическом механизме.

Возвращаясь к вопросу ресурсов, нужно заметить, что в изысканиях западных исследователей большое внимание прямо или косвенно уделяется критерию «затраты-эффективность». Опираясь на него, специалисты ищут возможность содействовать руководителям подразделений в оценке реальной пользы баз данных и предложений и в определении, по какой тематике существует дублирование информации и функций.

При всех сложностях оптимизации режима подготовки и принятия решений он ориентируется на приоритетность усилий по ускорению и облегчению процесса получения и отбора необходимой информации — даже со всеми просчетами и ошибками. Во всяком случае, над этим продолжают работать в США и внешнеполитических ведомствах некоторых других стран.

Вопрос повышения эффективности механизма подготовки и принятия решений заставляет «инноваторов» задумываться также над проблемой ротации кадров. В частности, связанной с командированием сотрудников в страны, на которых они ранее не специализировались. Накопленные ими данные и экспертные оценки по странам и регионам, где они приобрели профессиональные навыки, могут теряться в многочисленных «папках» на

бумажных и электронных носителях (не говоря о различиях в степени секретности). Такая архивная «чересполосица» затрудняет использование наработок сменщиками или вышестоящим руководством.

Разработчики «электронной дипломатии» исходят из того, что смена специализации сотрудников требует более четкого механизма получения нужной информации и архивов. Несмотря на очевидную сложность такой задачи, тем более в силу специфики внешнеполитической сферы, следует обратить внимание на растущий интерес западных экспертов к этой стороне оптимизации внутреннего режима «управления знанием». В том числе к проведению внутренних дискуссий и оперативному обмену мнениями между сотрудниками различных подразделений и ведомств по темам, нуждающимся в «состыковке экспертиз». Но, повторим, эта задача посложнее, нежели, например, создание «дипломатического Google».

Оптимизация работы внутри системы, естественно, предполагает должное обеспечение кибербезопасности. Подтверждение тому — история с Викиликс. Неслучайно эти вызовы сохраняют ведущую роль в «электронной дипломатии». Как и психологический фактор в процессе внедрения новых инструментов и практик.

В недавнем докладе Исследовательской службы Конгресса США «Транспарентность и секретность правительства» в контексте появления новых технологий признается, что эта проблема отражает противоречие между желанием обеспечить доступ граждан к информации и требованиями секретности. «Дипломаты, обеспокоенные вероятностью утечки к общественности информации, которую они передают по таким каналам, могут быть «более осторожными» в отношении ее содержания. Эта осторожность может вести к обмену менее объективной информацией между правительственными чиновниками». На международном уровне, в свою очередь, говорится в докладе, «в будущем дипломатические переговоры могут быть еще более отодвинуты от общественного доступа из-за вероятных утечек. Дипломаты также могут столкнуться со сложностями в проведении откровенных бесед с мировыми лидерами из-за беспокойства последних относительно утечек»[12].

«Свобода Интернета»

Поддержка «свободы Интернета» является одним из приоритетов США во внешнеполитической сфере, но стала таковым лишь с недавнего времени. Впервые этот термин в выступлении госсекретаря прозвучал в сентябре 2009 г. Затем глава ведомства Х. Клинтон заострила внимание на важность этого направления в январе 2010 г. и не раз к нему возвращалась, в том числе в директивных документах.

[12] «Government Transparency and Secrecy: An Examination of Meaning and Its Use in the Executive Branch». Congressional Research Service, 7-5700, November 14, 2012, p. 7.

Оптимистический настрой, на первых порах присутствовавший в речах Х. Клинтон, постепенно стал затухать. Усилился же акцент на вызовах, с которыми сталкивается Вашингтон в «защите свободного и открытого Интернета». Разговор пошел о целесообразности не только прозрачности, но и конфиденциальности Сети, не только отстаивания свободного самовыражения, но и укрепления «терпимости и вежливости».

С 2008 г. госдепартамент потратил около 100 млн долл. на прямое сопротивление усилиям властей других стран фильтровать и цензурировать Интернет, на «содействие соблюдению прав и свобод человека» в режиме онлайн[13].

Ввиду того, что обеспечение «свободы Интернета» является новым направлением работы для внешнеполитического ведомства (отметим, уже далеко не только американского), это требует и внедрения «новаторских походов», которые упоминает Ф. Хансон. По всей видимости, это касается поиска свежих методов и приемов в меняющейся международной среде, в том числе из-за растущих разногласий по этой теме с все большим числом государств.

Помимо событий «арабской весны» и разного рода «утечек» из конфиденциальных сетевых каналов, определенное беспокойство в Вашингтоне вызвано нежелательным влиянием его жесткой позиции по данному вопросу на диалог с рядом стран, причем и из числа союзников, постоянными попытками преодоления защитных барьеров других стран (особенно Китая), усилением вероятности преследований активистов-пользователей Сети за рубежом и т. д. США иногда оказываются в двусмысленном положении, критикуя ограничительные меры своих союзников с заметно меньшим энтузиазмом сравнительно с более неодобрительным разбором таких мер у других государств.

По мнению ряда американских экспертов, одной из ключевых задач Соединенных Штатов остается выработка адекватного списка аргументов для убеждения мирового сообщества в том, что, несмотря на объективные сопутствующие риски, полноправное участие в глобальном Интернете предпочтительнее курса на постепенный переход к большей информационной закрытости и к ужесточению цензуры[14]. Это, в свою очередь, требует весьма выверенных и даже щепетильных дипломатических усилий — ведь приходится иметь дело с высоким уровнем подозрительности

---

[13] *См.* Fergus Hanson. Ediplomacy: The revolution continues — «The Interpreter», 29 октября 2012, www.lowyinterpreter.org/post/2012/10/29/Ediplomacy-The-revolution-continues.aspx. Хотя эти средства в основном шли на программы технического и технологического характера, следует также добавить политическую, дипломатическую и информационную поддержку. Согласно анализу в рамках Open Net Initiative, 42 из 72 изученных стран фильтруют и цензурируют контент, не говоря о таких «постоянных нарушителях», как Куба и Северная Корея (*См.* «Ведомости», 3 декабря 2012).

[14] *См.*, например, Jonah F. Hill. Internet Fragmentation. Highlighting the Major Technical, Governance and Diplomatic Challenges for US Policy Makers. John F. Kennedy School of Government, Harvard University, Spring 2012, p. 50.

к развитию Интернета, обусловленным собственными представлениями различных государств об угрозах национальной безопасности.

Еще одна проблема состоит в том, что ограничительные меры ряда стран в отношении Интернета создают определенное напряжение в отношениях правительства с деловым сообществом в самих США. Государства, предпринимающие такие меры, часто прибегают к услугам зарубежных интернет-компаний, которые работают на их территории. Мировые, особенно американские, корпорации встают перед выбором — выполнять правовые и иные требования этих государств или отказаться следовать им с перспективой потерять там свой бизнес.

С другой стороны, выполняя эти требования, они могут вызвать на себя недовольство властей Соединенных Штатов. Тем более, на Капитолии уже выдвигают инициативы, позволяющие объявлять запрет на продажи соответствующих технологий и услуг в страны, «ограничивающие Интернет», или вводить требование информировать о таких продажах.

Противники подобных инициатив в технологическом секторе уверяют, что поставляемые технологии способны предложить такие решения для противодействия мерам по ограничению свободы Интернета и ужесточению цензуры, которые перевесят выгоды от санкций в отношении компаний. Вместе с тем, многие эксперты бьют тревогу по поводу возможных негативных последствий не только для американских компаний, но и для граждан США, работающих в «репрессивных» странах, в случае соблюдения ими более жесткой линии Вашингтона. Их озабоченность также продиктована мнением о неспособности или неготовности официальных властей Соединенных Штатов адекватно отвечать на меры против американских граждан.

Тем не менее, в своей политике, в том числе в русле «электронной дипломатии», госдепартамент предпринимает серьезные усилия по сглаживанию этих вызовов, подключая смежные ресурсы. В частности, на поле противодействия цензуре и иным действиям ряда стран активно работает Вещательный совет управляющих (Broadcasting Board of Governors), через который правительство ежегодно выделяет около 30 млн долл. на разработку инструментов обеспечения «свободы Интернета»[15].

Реагируя на рост критики и, по всей видимости, определенное давление по поводу их работы в некоторых странах, особенно в Китае, несколько компаний в сфере ИКТ вместе с представителями общественных и академических организаций образовали в 2008 г. т. н. «Инициативу глобальной сети» (Global Network Initiative). Она нацелена на внедрение «лучших практик» профильных американских компаний в странах с «неважным досье» в данной сфере. В феврале 2011 г. эта структура выпустила доклад «Защищая права человека в цифровой век». Но некоторые

[15] Patricia M. Figliola. Promoting Global Internet Freedom: Policy and Technology. Congressional Research Service, 7-5700, October 23, 2012, p. 5.

правозащитные организации подвергают Инициативу критике за слишком мягкие и общие рекомендации.

В общем, правительственные и деловые круги США сталкиваются с немалыми проблемами. Тем не менее, они продолжают укреплять сотрудничество в сферах, затрагивающих «электронную дипломатию». Бизнес вместе с экспертным сообществом заметно обеспокоен перспективами фрагментации Интернета, возможными изменениями существующей модели глобального управления Интернетом.

Обратим внимание и на то, что деловые круги серьезно заинтересовались активностью госдепартамента по «управлению знанием». Внешнеполитическое ведомство инициировало научно-исследовательскую программу по преодолению в крупных организациях проблем информационных потоков, обусловленных технологическими новациями.

Важными представляются не только опыт, но и определенная «сцепка» государства и частного бизнеса в кадровом обеспечении этого внешнеполитического направления. В качестве примера стоит упомянуть, что после перезапуска программы «электронной дипломатии», ее заметной активизации с приходом в Белый дом Б. Обамы заместителем госсекретаря по публичной дипломатии была назначена Дж. Макхэйл. Она пришла с поста президента и исполнительного директора компании «Дискавери коммьюникейшнз», превратив ее в глобального «тяжеловеса» с почти полутора миллиардами подписчиков в 170 странах на 35 языках. «Дискавери коммьюникейшнз» была нацелена на более адекватное понимание целевых аудиторий и на передачу информации в возможно доброжелательном ключе[16].

Такого рода ротация кадров во внешнеполитической сфере государства, бизнеса и экспертного сообщества весьма распространена не только в США, но и во многих ведущих странах, в отличие от России. Для нас поэтому актуальнее рассчитывать на «менее контактное» взаимодействие власти и бизнеса в продвижении своих интересов вовне с использованием всего возможного потенциала Сети со всеми вытекающими из такого формата сотрудничества сложностями.

Касаясь темы «государство-бизнес» в контексте «свободы Интернета», следует отметить, что российские эксперты, пытающиеся наметить практические российские подходы в сферах, затрагивающих «электронную дипломатию», делают акцент на целесообразности укрепления сотрудничества государства и отечественного бизнеса. Хотя, учитывая нашу специфику, еще без достаточно конкретных ориентиров.

Например, Д. Попов выделяет важность задачи «формирования эффективной связки государство-интернет-бизнес». По его мнению, «российская дипломатия должна выстроить механизм взаимодействия с крупными российскими интернет-компаниями, в том числе поисковиками и

[16] Helle C. Dale. Public Diplomacy 2.0: Where the US Government Meets “New Media”. Backgrounder № 2346, The Heritage Foundation, December 8, 2009, p. 4.

социальными сетями, доказавшими свою международную конкурентоспособность и пока удерживающими лидирующие позиции в центральноазиатском сегменте интернета… При взвешенном подходе сотрудничество государства и IT-сектора может быть выгодным и результативным для обеих сторон… Российские фирмы заинтересованы в поддержке со стороны властных структур и в отсутствии необоснованных административных барьеров в сети, а правительство — в использовании интернета для укрепления, а не подрыва безопасности»[17]. Поясним, что автор дает свои рекомендации с привязкой к анализу «электронной дипломатии» США в Центральной Азии — аналогично значительной части отечественных материалов по американской «цифровой дипломатии», которые, правда, отличаются упрощенным подходом — с перечислением проблем и озабоченностей.

В отличие от России, в США и многих ведущих странах эта связка уже работает давно и в весьма жестком формате, в котором интересы бизнеса воздействуют и на новые направления внешнеполитической работы. По замечанию западных исследователей М. Кавелти и О. Ролофса, в киберпространстве «власть находится в руках частных акторов, особенно бизнеса. В результате приватизации и дерегулирования во многих сферах общественного сектора, от 85% до 95% критической информационной инфраструктурой владеет и оперирует частный сектор»[18]. Здесь установились свои «правила игры».

Нам же только предстоит их разрабатывать. В этой связи немаловажно, в частности, конкретизировать тезис Д. Попова о заинтересованности нашего бизнеса «в поддержке со стороны властных структур и в отсутствии необоснованных административных барьеров» для нужд отечественного варианта «электронной дипломатии».

Не нужно забывать, что деловые круги США и других стран-партнеров активно участвуют в реализации планов в сферах публичной дипломатии и «Э-дипломатии». Такое участие относится и к деятельности НКО, и к финансированию своих и совместных программ, некоторые из которых упоминались выше. Другими словами, речь идет о добавлении их весомого вклада в общий ресурс.

В России же заметной активизации негосударственного сектора в этих сферах пока не наблюдается[19]. Более того, очевидный перекос в пользу задачи защиты от угроз, создания различных ограничений на интернет-пространстве и т. п. фактически перекладывает главное бремя решения проблем и обеспечения необходимыми ресурсами на государство. Это

---

[17] Д. Попов. Большая игра: теперь онлайн. — «Национальная оборона», декабрь 2012, www.oborona.ru/includes/periodics/maintheme/2012/0604/19578571/detail.shtml

[18] Myriam D. Cavelty, Oliver Rolofs. Cyber war hype. States cannot control the digital realm. — «The Atlantic Times», № 1, 2012.

[19] По этой теме *см.* С. Кулик. Репутация России за рубежом и частно-государственное партнерство. — «Аналитический бюллетень Института современного развития», № 1 (8), январь 2013, с. 8—12.

ограничивает возможности и направления работы вовне — хотя бы в рамках «воздействия на общественное мнение».

Подробно разбирая, по ее терминологии, «цифровую дипломатию» США и задумываясь о российских перспективах, Е. Зиновьева в другом своем материале отмечает: «Важно помнить, что субъектами глобальной информационной сферы сегодня являются не только государства, но и транснациональные медиакорпорации, организации гражданского общества, сообщества социальных сетей как самостоятельные субъекты… Равным образом и в перспективной цифровой дипломатии важную роль, помимо госорганов, должны играть как бизнес-структуры, так и организации гражданского общества… Как представляется, одним из наиболее перспективных направлений российской цифровой дипломатии является вовлечение технологического отечественного бизнеса в проекты в сфере публичной дипломатии»[20].

Особая важность темы «свободы Интернета» не только в американской повестке, но и в приоритетах многих других стран, включая Россию, обусловлена заметным усилением в последнее время противоборства на мировой сцене. Недовольство доминирующей ролью США в интернет-среде проявлялось и ранее, но в менее открытых формах. Сейчас оно четче отражается в официальных позициях ряда государств и в мировых СМИ. Однако накал страстей в основном все еще скрыт «за кулисами».

Один из свежих и знаковых примеров дала организованная в декабре 2012 г. под эгидой Международного союза электросвязи (МСЭ) Всемирная конференция по международным коммуникациям с участием представителей 159 стран-членов Союза. Одной из главных заблаговременно заявленных целей мероприятия было обсуждение принципов регулирования Интернета для новой редакции Регламента союза, который не менялся с 1988 г. Даже сама ее постановка вызвала беспокойство многих государств. Вашингтон, в том числе по линии «электронной дипломатии», приложил значительные усилия для предупреждения неудобных решений, которые бы наделяли эту организацию функциями регулирования Интернета, и для сохранения статус-кво. Следует подчеркнуть, что в эти усилия значительный вклад внес и частный сектор — не только американский.

Серьезность беспокойства обусловлена тем, что Россия, Китай, Саудовская Аравия, Бразилия, Индия, Иран уже открыто склонны поддерживать распространение надзорных полномочий МСЭ на интернет-пространство и усиление голоса ООН, специализируемым подразделением которой Союз и является. По мере развития Интернета эти страны все чаще выражают недовольство тем, что вопросы «всемирной паутины» выпадают

[20] Е. Зиновьева. Цифровая дипломатия, международная безопасность и возможности для России. — «Индекс безопасности», 2013, № 1 (104), т. XIX, стр. 222—223.

из сферы полномочий международной организации, которая бы учитывала интересы участников «на равноправной основе»[21].

Нетрудно заметить, что в круге очерченных Е. Пантелеевым приоритетов, в отличие от официальной позиции госдепартамента США, вопрос о свободе или ограничениях Интернета не ставится. Однако он представляется одним из центральных для определения масштабов, характера и эффективности использования сетевых технологий во внешнеполитической сфере.

В любом случае интернет-пространство вступило в новый этап своего развития, когда проблема контроля за ним становится предметом все более жесткой борьбы. Более того, о формировании своего рода союзов различных государств на этом пространстве де-факто можно говорить не в будущем, а в настоящем времени.

Россию и целый ряд государств не устраивает сложившаяся система управления основными функциями Интернета. В ней общее руководство осуществляет Общество Интернета (ISOC) с представительствами в США и Швейцарии. Но основная роль «на адресном пространстве» принадлежит Интернет-корпорации по регулированию присвоения доменных имен (ICAAN), расположенной в США. Часть стран усматривают в ICAAN защитника американской модели работы Интернета на основе отказа от контроля за контентом. Другие, наоборот, критикуют ее за непоследовательность в защите свободы Сети.

В последнее время международное давление на ICAAN заметно возросло. Оно нацелено в том числе на интернационализацию управления Интернетом и ослабление доминирующего положения организации. Изменением расстановки сил и была чревата декабрьская конференция.

При подготовке и проведении конференции Соединенные Штаты и их союзники жестко сопротивлялись обсуждению проблематики управления Интернетом. В принятую на конференции новую редакцию Регламента международной электросвязи (International Telecommunications Regulations) не вошел наиболее спорный пункт, касающийся возможностей государств «управлять ресурсами наименования, нумерации и идентификации, используемых на их территориях для международной электросвязи, если они сочтут это необходимым» — несмотря на заверения генерального секретаря МСЭ Х. Туре, что этот пункт не подразумевает ни контроль над контентом в Интернете, ни управление Сетью, а направлен на разработку технических стандартов для международной телефонии[22].

Несмотря на компромиссный характер документа, его не подписали США, Австралия, Канада, Япония, ряд европейских стран. По мнению итальянской «Ла Стампа», «ближайшие годы покажут, был ли выбор США и

---

[21] *См.* подробнее: С. Кулик. Регулирование Интернета: глобальная битва. — «Аналитический бюллетень Института современного развития», № 4, сентябрь 2012, с. 19—23.

[22] *См.* «Независимая газета», 27 декабря 2012.

других стран, которые не подписали новый договор, благотворным для развития Интернета, или же он положит начало холодной войны в Сети»[23].

Очевидно, активизация России и ее соратников на этом направлении продолжится под лозунгами «информационной безопасности». Следует обратить внимание на то, что Россия и некоторые государства говорят о международной информационной безопасности (МИБ), подразумевая широкий охват сфер взаимодействия между государствами на информационном поле. Другие же страны, в основном западные, предпочитая говорить о кибербезопасности и киберпространстве, делают акцент на нормах работы ИКТ и информационных систем в целом.

В этой связи обратимся к материалу специального координатора по вопросам политического использования информационных и коммуникационных технологий, Посла по особым поручения МИД России А. Крутских. Не скрывая планов усиления роли ООН и МСЭ в управлении Интернетом, он призывает к выработке универсального кодекса поведения в информационном пространстве в рамках ООН. «Такой документ должен содержать положения о необходимости обеспечения свободного, непрерывного и недискриминационного доступа граждан к ИКТ, включая Интернет и сетевые ресурсы, предусматривать выработку механизмов эффективного запрета на осуществление в Интернете какой-либо цензуры, выходящей за рамки обеспечения общественных интересов, и недопущения использования Интернета в противоправных целях. Не менее важно отразить потребность соблюдения основных прав и свобод человека в интернет-пространстве, в том числе свободы слова, собраний и ассоциаций, а также права на неприкосновенность частной жизни. При этом следует предусмотреть положения о недопустимости использования информационно-коммуникационных технологий с целью вмешательства во внутренние дела государств и в ущерб государственному суверенитету, национальной безопасности, территориальной целостности, безопасности общества, моральным принципам, а также для разглашения информации чувствительного характера»[24].

По всей видимости, работа над таким документом будет непростой. Одним из серьезных вызовов для достижения согласия представляется увязка между первой частью положений А. Крутских и частью второй (после оборота «при этом»). К этому добавляются разногласия по усилению роли МСЭ в управлении Интернетом — ведь, по мнению А. Крутских, это «позволит обеспечить полноправное участие государств в решении глобальных вопросов и обеспечении их суверенного права на самостоятельное управление Интернетом на национальном уровне»[25].

---

[23] Хуан Карлос де Мартин. Риск холодной войны в интернете. («La Stampa», Италия) — «ИноСМИ», 17 декабря 2012, www.inosmi.ru/world/20121217/203466249.html

[24] Научные проблемы национальной безопасности Российской Федерации. Вып. 5. М., 2012, с. 82—83.

[25] Там же, с. 86.

В свою очередь, некоторые западные специалисты относят наше понимание «информационной безопасности» прежде всего к теме информационного контента. Попытки сдерживать распространение контента интерпретируются как намерение ограничить свободу слова, что противоречит многим международным документам.

Соответственно, возникает потребность в сведении всеми сторонами используемых терминов (МИБ, полноправное участие, самостоятельное управление и др.) в более или менее приемлемый понятийный аппарат. Такая потребность актуальна для переговорных площадок, где разные группы стран по ряду позиций или просто не понимают друг друга, или прикрываются этим в тех или иных интересах. Даже если появление такого понятийного аппарата не приведет к быстрому сглаживанию разногласий.

По всей видимости, проблематика «свободы Интернета» будет усиливать свое присутствие в списке приоритетов ведущих игроков, в том числе в России. Тем более, ввиду известных принятых законов и разрабатываемого сейчас закона об Интернете.

В этой связи полезно отметить, что специалисты сомневаются в возможности жесткого государственного контроля над Интернетом. Это относится и к отечественному сообществу. Российский эксперт И. Стечкин уверен, что «интернет-сообщество привыкло к свободе, и добровольно отказываться от нее никто не захочет. Следовательно, будет меняться технология Интернета… Думаю, что попытки свернуть Интернет обратно, порезать его на внутригосударственные островки и отделить эти островки друг от друга обернутся неудачей. Сеть — это живой организм, чье развитие остановить нельзя»[26]. Это мнение преобладает в профессиональных кругах в мире и с ним следует считаться при формировании наших планов.

«Утряска» противоречий и поиск компромиссов по вопросу регулирования и свободы Интернета, по всей видимости, займут существенное место в нашей внешнеполитической деятельности, в том числе в том, что американцы понимают под «электронной дипломатией». Вместе с тем, в силу различных мотивов может возникнуть соблазн сосредоточиться (гласно или негласно) на нем, оставляя в стороне другие треки «электронной» или «инновационной» дипломатии. Это, в свою очередь, чревато ослаблением внимания к изысканию не отдельных, а комплекса адекватных решений по улучшению «обратной связи» государства с внешними потребителями, упущением полезных направлений использования ИКТ, сужением списка сетевых инструментов и, соответственно, преувеличению эффективности последних для «отчетности» по реализации установки руководства «использовать новые технологии».

[26] «Новые известия», 14 ноября 2012.

Об «обратной связи» и «твипломатии»

С появлением новых инструментов появляется дополнительная путаница. Например, при анализе политики «мягкой силы» довольно популярным стал термин «Твиттер-дипломатия» — вплоть до восприятия Твиттера главным показателем эффективности внешнего воздействия среди сетевых систем.

Все же вполне очевидно: даже если ограничиваться использованием Сети как пространства публичной дипломатии, Твиттер или Фейсбук остаются лишь частью (пусть и важной) инструментария такой дипломатии. Действительно трудный вызов для нее — настройка эффективной, широкоохватной и быстрой «обратной связи» с иностранными гражданами.

В сравнении с традиционными средствами коммуникации, тот же Интернет, пожалуй, впервые предоставляет государству такой масштабный канал ведения не монолога или отрывочного общения (в основном через телевидение или печатные СМИ), а постоянного диалога с зарубежной аудиторией и экспертным сообществом. Укрепление режима такой связи за счет внедрения сетевых технологий представляется одним из ключевых факторов, который меняет требования к внешнеполитическим ведомствам и методам публичной дипломатии. Не исключены трансформация самих концептуальных подходов и корректировка даже некоторых базовых установок.

Обращаясь к опыту госдепартамента и второй части исследования Ф. Хансона, при оценке полезности устойчивых каналов общения полезно учитывать, что в его инструментах не Твиттер, а Фейсбук стал играть ведущую роль в охвате аудитории — главное, в ежедневном режиме. Его охват (13 млн пользователей) меньше аудитории госдепартамента в YouTube (16 млн в августе 2012 г.), но к последнему прибегают менее регулярно. Впрочем, и отстающий почти на порядок Твиттер (менее 2 млн пользователей) имеет здесь значительный потенциал. Все же заметим, что значительная часть пользователей этих инструментов госдепартамента находятся в США и штаб-квартире ООН в Нью-Йорке.

В этой связи полезно отметить, что популярность темы «дипломатического Твиттера» получила существенный толчок с появлением статьи “BBC News Magazine” (17 июня 2012 г.) «Э-дипломатия: внешняя политика в 140 знаках», затем широко тиражированной мировыми СМИ, и с открытием в июне агентством Франс-пресс сайта «E-Diplomacy Hub», где в режиме реального времени обобщается твиттер-активность руководителей государств и представителей внешнеполитических ведомств. Из-за явной и объяснимой для СМИ увлеченности такой «горячей темой», как существенный рост симпатий мировых лидеров к Твиттеру, «Твиттер-дипломатия» заслонила собой «Э-дипломатию», составной частью которой она, собственно, является, и заворожила не только международную общественность, но и многих политиков и дипломатов.

Раскрутка темы легла на благодатную почву. Публичная дипломатия, сохраняя или набирая значимость для государственных структур многих стран, запрашивает новые приемы и технологии. В Твиттере, не без информационной раскрутки, усмотрели главное звено «обратной связи» — тем более с лидерами и высокопоставленными фигурами.

Дальше — больше. В прошедшем июле вышло исследование компании «Берсон-Марстеллер», посвященное развитию «официального Твиттера»[27]. Оно также получило масштабное освещение, а новый термин «твипломатия» (twiplomacy) стал вытеснять другие, уже принятые в рамках понимания «цифровой дипломатии». Даже несмотря на то, что авторы материала оговариваются: «твипломатия» — это лишь название исследования по использованию Твиттера мировыми лидерами. Заметим также, что некоторые государственные чиновники ряда стран в своей переписке даже прибегают к Твиттеру вместо электронной почты.

Зарубежные исследователи стали уделять модной теме нынешнего и будущего применения Твиттера пристальное внимание. Но до сего времени они не предоставили более или менее четкого понимания перспектив отдачи от этого инструмента в политике и дипломатии. Это отчасти объясняется объективными причинами — довольно коротким отрезком времени после его появления. Поэтому неудивительно их предпочтение рассматривать отдельные примеры плюсов и минусов такого инструмента избегая комплексных оценок, для которых требуется достаточный опыт. Лишь совсем недавно стали предприниматься сколько-нибудь заметные усилия по комплексной оценке его потенциала — преимущественно в сфере публичной дипломатии.

Политиками и экспертами уже подмечены некоторые нюансы в использовании Твиттера. По наблюдениям авторов упомянутого доклада компании «Берсон-Марстеллер», президент США и его администрация, например, основное внимание уделяли внутриполитическим вопросам и, соответственно, американской аудитории, в том числе в силу проводившейся предвыборной президентской кампании. Активность лидера Евросоюза Х. ван Ромпея вызвала, скорее, вопросы — например: она нацелена на укрепление доверия к собственной персоне и своей политике или на отвлечение внимания от кризиса в ЕС? У специалистов сложилось впечатление, что твиты главы Европейского совета оказались слабо увязаны с его практической деятельностью и не подтверждали искомую результативность такого канала общения в публичной дипломатии[28].

---

[27] Twiplomacy. Heads of state and government in Twitter. Burson-Marsteller, July 2012, twiplomacy.com/wp-content/uploads/2013/02/Twiplomacy.pdf

[28] *См.* также Andrew F. Cooper. Leader's Tweets Offer a Distorted Tip in Assessing eDiplomacy. — Center for International Governance Innovation, September 19, 2012, www.cigionline.org/blogs/worlds-of-global-governance/leader's-tweets-offer-distorted-tip-assessing-ediplomacy

В целом, исследование компании свидетельствует об определенных ограничителях «твипломатии» — особенно при ее рассмотрении в контексте «электронной дипломатии». В то же время, аналитики выделили полезность инструмента в личных контактах политиков. Если раньше налаживание отношений между руководителями государств и высокопоставленными лицами в основном проходило при личном знакомстве на различных мероприятиях, то Твиттер позволяет наладить доверительные отношения на «бесконтактной» и постоянной основе — с большей отдачей, нежели от телефонных разговоров.

Вместе с тем отметим, что представительства государств за рубежом могут подключать другие сетевые каналы стран пребывания. Например, посольство США в Китае сумело завоевать существенное число подписчиков в местном Weibo.

Но дело не только в увеличении темпов расширения аудитории и выборе эффективных сетевых инструментов. Речь идет и о должных усилиях по качественной перестройке контактов с местной аудиторией. Не случайно, в США и других западных странах все более закрепляется термин «дипломатическая медиасреда» (Diplo-media).

Его расшифровка показывает, что по существу он остается в рамках традиционных установок информационного воздействия на зарубежную общественность. Схематизируя, эти установки можно представить двуедиными и касающихся прежде всего контента: он, во-первых, должен ориентироваться на государственные интересы и, во-вторых, препарироваться таким образом, чтобы информация и оценки не ассоциировались зарубежной общественностью с государственной позицией или максимально приглушали такую связь. Другими словами, внешнеполитические работники должны так «спрятать государственные уши» или так профессионально обернуть информацию в «независимую упаковку», чтобы пользователь воспринимал ее как заслуживающую большего доверия или даже беспристрастную. Это, в свою очередь, требует не только профессионального подбора контента, но и выверенной редакторской работы.

На сей раз подразумеваются широкое подключение новых инструментов и режима оффлайн к режиму онлайн, соответствующая подготовка или переподготовка кадров и более тонкие методы работы. Только недавно, например, стало известно, что популярные страницы в Фейсбуке «Вызов демократии» и «Поколение инноваторов» созданы и модерировались госдепартаментом США.

Такое подключение в «дипломатическую медиасреду» изменяет параметры работы по другим традиционным направлениям и способствует повышению ее эффективности. Это касается возможностей отслеживания ситуации в различных странах в режиме реального времени для своевременного анализа и принятия нужных мер. На сей раз к мониторингу добавляется режим онлайн с широкой базой социальных сетей, которая, в

свою очередь, используется для диалога с местными гражданами и авторитетными фигурами. Этот диалог требует подбора своего, доходчивого языка общения между официальными представителями и населением другой страны. Такие контакты, в свою очередь, облегчают, например, задачу оценки влиятельности различных комментаторов в СМИ и, соответственно, развития контактов с ними. Но все это создает дополнительную нагрузку.

Еще одна сложность для дипломатической работы — расширение «списка контактов». С развитием «сетевой мощи» возникают новые влиятельные «игроки» в режиме онлайн как внутри национальных границ, так и на международной сцене. Такие фигуры способны не только прямо или косвенно содействовать укреплению репутации другой страны у себя дома или в глобальном пространстве, но и серьезно ее «подмочить». Поэтому, помимо потребности в мониторинге ситуации в информационном пространстве в реальном времени для своевременного обнаружения угроз, добавляется задача выявления ключевых «фигур влияния» и работы с ними. Не говоря уже об «обратной связи» с простыми гражданами.

Следует учитывать, в том числе в контексте публичной дипломатии, что ИКТ не просто расширили потоки доступной информации. От государственных и иных акторов требуется завоевывать интерес общественности и элит к определенным источникам в этих потоках. Для государств это тем более актуально с расширением присутствия на информационном поле негосударственных структур и сетей, которые размывают традиционные возможности государств.

Сложности заключаются не только в должном совершенствовании режима «обратной связи» и расширении его диапазона. Вопрос также касается составления «списка целей и задач» для такого режима — с более продвинутым пониманием специфики, культуры, запросов и чаяний аудитории тех или иных стран. На этом направлении западные страны сталкиваются с немалыми трудностями, но для их преодоления они стали широко вовлекать НКО, в том числе их сетевые ресурсы.

В этой связи полезно напомнить следующее. Потенциал ИКТ чаще рассматривается в контексте «мягкой силы». Автором этого термина принято считать американского исследователя Дж. Ная. В ссылках же на его разбор понимания «мягкой силы» выделяются два приоритета — обеспечение «привлекательности» (attraction) и «убеждения» (persuasion). Но у Дж. Ная перед ними на первом месте — «составление повесток» (framing agendas): «Образ действий «мягкой силы» основывается на составлении повесток, привлекательности или убеждения».

Такой перечень он предложил еще в 1990 г., когда Соединенным Штатам и другим западным странам было заметно легче формировать повестки и убеждать внешних акторов. В своей недавней работе, посвященной сетевым технологиям, он об этом списке напоминает. В новых условиях, по его мнению, с учетом таких приоритетов «информационные инструменты могут быть использованы для нужд мягкой силы в

киберпространстве»[29]. Не случайно, что задача «составления повесток» весьма редко открыто упоминалась энтузиастами «электронной дипломатии» в самом госдепартаменте — в частности, ответственной за политическое планирование в 2009—2011 гг. Э.-М. Слотер.

Представляется, что такой важный компонент, как framing agendas, следует самым внимательным образом учитывать как в общей политике «мягкой силы», так и в использовании сетевых технологий для обеспечения российских интересов и укрепления позиций. Это, в свою очередь, требует формулирования новых идей и подходов, которые бы встраивались в конкретные действия в рамках внешнеполитического курса.

«Сетевая мощь»: открытая модель

Вернемся к июльским установкам российского президента и их логичной интерпретации источником из МИДа в русле «цифровой дипломатии». Оценка пространства использования новых технологий свидетельствует, что оно далеко не ограничивается задачами публичной дипломатии. В данном материале отдельно не рассматривается увязка «электронной дипломатии» с дипломатией публичной. Последняя довольно внимательно анализируется отечественной мыслью. К тому же на официальном уровне более или менее внятную картину предлагают труды главы Россотрудничества К. Косачева.

Одна из задач заключается в том, чтобы составить более понятную схему направлений «электронной дипломатии» и наложить ее «кальку» на уже имеющиеся планы публичной дипломатии. В этом случае может потребоваться корректировка этих планов — если, конечно, исходить из целесообразности реального повышения результативности их выполнения, эффективности отдачи от затрат и наличных ресурсов, а также внедрения иннвационных подходов.

В ином варианте нам уготовано по-прежнему уповать на «традиционные методы», о которых упоминает источник в МИДе. Вместе с тем, без конкретных установок и задач можно по разному понимать и «методы», и «новые технологии», даже пытаясь до минимума ограничить роль ИКТ и Сети для внешних нужд или сужая технологические возможности до использования в сугубо «оборонительных» целях преодоления киберугроз (вполне реальных).

Киберугрозы — отдельная тема, затрагивающая «электронную дипломатию». Однако стоит упомянуть, что внешнеполитические ведомства ведущих стран, анализируя проблематику кибербезопасности, ориентируются на поддержание и развитие открытой модели «сетевой мощи» в ее различных конфигурациях. В рамках такого подхода им приходится раздумывать над головоломками — например, как сочетать объективный, по

[29] Joseph S. Nye. Cyberpower. Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, pp. 2, 5.

их убеждению, процесс обеспечения свободы в Сети и необходимость защищаться от различных киберугроз. Исходя из такой модели, они разрабатывают или уже сформулировали определенные принципы, которым обязаны следовать при формировании политики кибербезопаности.

Сошлемся на приоритеты германского МИДа. В отличие от сторонников «активной кибероборoны» от различных атак через введение или угрозы введения юридических, политических и экономических санкций против виновников (включая государства) с возможным привлечением даже «аргументов» военного свойства, это ведомство предпочитает концепцию «пассивной обороны». В понимании МИДа ФРГ такая оборона должна полагаться на внедрение новейших технологий для обеспечения безопасности информации.

При этом ведомство опирается на три принципа. Первый принцип — защита «свободы Интернета» и других сетевых инструментов. Второй — саморегулирование в условиях открытого гражданского общества и рыночной экономики. Третий — стимулирование «накопления знаний» и транспарентности. Исходя из этого, немецкие умы пытаются разрешить сопутствующие сложности, в частности: как сочетать саморегулирование в киберсреде с защитой прав других участников этой среды?[30] Собственно, эти принципы свойственны и коллегам германских дипломатов из других ведущих стран — независимо от того, разделяют ли они концепцию «пассивной обороны» или предпочитают оборону «активную».

Как бы ни решались эти головоломки, в какие бы тупики ни попадали эксперты и сотрудники ведомств, какие бы вопросы ни вставали перед ними, соответствующие структуры ряда ведущих стран работают с ориентацией на открытую модель «сетевой мощи». Они исходят из того, что другие модели, предлагающие путем выстраивания преград для глобальной Сети, цензуры и др. защитить государство от внешнего воздействия, в нынешней и будущей мировой Сети обречены на неудачу. Различные ограничения будут в той или иной степени преодолеваться. Открытая модель может видоизменяться, но не подвергнется качественной деформации.

К тому же не следует забывать, что значительная часть «игроков» в этих странах не приемлют государственный контроль — и не находятся под ним, работая на наднациональном уровне. Это создает и дополнительные преграды для достижения приемлемых для всех участников международных соглашений, с чем также имеют дело внешнеполитические службы всех заинтересованных государств, исходящие в своей работе из обеспечения национального суверенитета.

В этой связи возникает вопрос о возможной трансформации принципа суверенитета по мере развития сетевых инструментов. Он задает темы для весьма жестких дебатов по поводу воздействия Сети и характера ее регулирования.

---

[30] *См.* S. Gaycken. Shifting the Cybersecurity Paradigm. — «The Security Times», February 2013, p. 30.

Полезно обратить внимание на один из подходов, который исходит из целесообразности укрепления роли государства — но в сотрудничестве с другими акторами киберпространства. Он состоит в том, что сохранением суверенитета обусловливается целесообразность превращения государства в «сетевой хаб» — с сетевой инфраструктурой гражданского общества и глобальной Сетью[31]. Это требует не только новой культуры сетевой активности, но и адекватного взаимодействия государства с обычными узлами Сети. Самим развитием «сетевой мощи» диктуется усовершенствование механизмов такого взаимодействия — системного характера, а не в режиме ручного управления.

Соответственно, открытая сетевая модель и механизм «сообщающихся сосудов» государства и граждан требуют адаптации государства к новым информационным реалиям глобального масштаба, в том числе на институциональном уровне. В ходе этой адаптации нужно не забывать, что государство — это не только объект, но и активный субъект использования новых технологий.

Соединенные Штаты в последние годы взяли четкий курс на развитие «сетевой мощи» для своих внешнеполитических нужд, формируя концептуальные установки и выстраивая соответствующие механизмы. В ходе реализации «электронной дипломатии» приоритеты и нюансы задач и инструментов могут меняться, но общий настрой на обеспечение своей лидирующей роли в глобальном балансе «сетевой мощи» будет сохраняться или усиливаться. США все активнее подключают к этой политике и своих союзников из числа ведущих государств; заметно активизируется сотрудничество в сферах, затрагивающих «электронную дипломатию».

На этом фоне наше государство пока находится в режиме ожидания проработанных и детальных ответов на возникающие вызовы. Нам еще предстоит внимательно разбираться с тем, что такое «новые технологии» для внешнеполитической работы и, соответственно, какие ориентиры полезны в использовании «электронной дипломатии» с учетом отечественной специфики и ресурсов, как внедрять новые технологии «внутри системы» с учетом требований безопасности и др. При этом должное внимание необходимо уделить уже накопленному опыту работы занятых международными делами структур США и других ведущих игроков.

Этот опыт, в частности, свидетельствует о том, что государство играет активную роль в поддержке инноваций и расширения доступа к Сети. Оно является и закоперщиком привлечения частного сектора, НКО и гражданского общества к решению задач «электронной дипломатии» и дипломатии публичной. Это серьезно усиливает потенциал «мягкой силы», что должна скрупулезно учитывать Россия в усилиях по продвижению своих интересов и позиций за рубежом.

---

[31] *См.* об этом N. Latar, G. Asmolov, A. Gekker. State Cyber Advocacy. Interdisciplinary Center Herzliya. Working Paper, January 31 — February 3, 2010.

Вместе с тем, полезно беспристрастно взвесить сильные и слабые стороны сетевого потенциала государства и на этой основе подумать о формировании концепции развития «сетевой мощи», в силу объективных факторов ориентируясь на открытый характер ее модели и на взаимодействие с рядовыми и глобальными узлами Сети. Параметр баланса «сетевой мощи» уже потеснил традиционные параметры «баланса сил».