Понимание социальных сетей и национальная безопасность

Джеймс Джей Карафано

заместитель директора Института международных исследований Кэтрин и Шелби Каллом Дэвис и директор Центра внешнеполитических исследований Дуглас и Сары Эллисон в Heritage Foundation.

Компьютеры, мобильные телефоны, другие цифровые устройства и системы, которые связывают их вместе, изменили то, что многие на планете использовали почти всегда, особенно, взаимосвязь с друг с другом. Более одного миллиарда человек — некоторые из них враги свободы — находятся в Интернете, который в эти дни намного больше похож на информационную супермагистраль с пробками, чем на информацию.

Существует трафик разговоров, который осуществляется проще по электронной почте, Facebook, LinkedIn, Twitter и, конечно же, с помощью Википедии, а также многих других инструментов социальных сетей (часто в совокупности называемые Web 2.0), которые облегчают обсуждение, дебаты и обмен идеями в глобальном измерении.[1] Этот беспрецедентный потенциал для слушания и реакции неумолимо реструктурирует пути, по которым информация создается и используется. Например, во время выборов президента 2008 г. в США кампания Барака Обамы мобилизовала социальные сети революционными методами, чтобы получить поддержку населения и собрать деньги, достигнув огромной аудитории. Влияние социальных сетей не закончится бизнесом и политикой, но неизбежно скажется на национальной безопасности.

Социальные сети имеют потенциал коснуться каждого аспекта национальной безопасности, в том числе сбора и проверки информации в открытом доступе с открытым исходным кодом, замеров и влияния на общественное мнение, распространения «коммуникации рисков» (например, как реагировать после катастрофы), проведения научных исследований и анализа, разработки политики, планирования и осуществления программ и мероприятий в полевых условиях, а также проведения информационных операций (интегрированное применение электронной войны, компьютерных сетевых операций, психологических операций, обмана и операций в сфере безопасности).

[1] Josef Kolbitsch and Hermann Maurer, "The Transformation of the Web: How Emerging Communities Shape the Information We Consume," Journal of Universal Computer Science 2no. 2 (2006), 187–207.

Интернет мир

Есть в основном две модели эффективной перегонки и обмена информацией, которая находится в организации- сверху вниз и снизу вверх. По модели сверху вниз старшие руководители в организации отбирают лучшую информацию. Они используют свою мудрость, опыт и суждение для того, чтобы информация имела форму, была отредактирована, отфильтрована, превратилась в знания, а затем была распространена внутри организации. Создание иерархических знаний и соответствующее управление лучше всего работают в статических и предсказуемых условиях, где высшее руководство знает лучше и больше. В противоположность этому, в динамических ситуациях, когда опыт не имеет значения, формирование знаний лучше всего работает снизу вверх. В низовых организациях непосредственность молодых лидеров оказывается необходимой, и так происходит их наиболее эффективное обучение. Их опыт более свежий и актуальный. В онлайновом мире лучшие знания приходят от этой основы снизу вверх, но эта реальность имеет как проблемы, так и обещания. Общая мудрость гласит, что среди социальных сетей сама группа берет на себя ответственность по отбраковке плохих данных. Это включает в себя все - от борьбы с вредоносными субъектами онлайн, указанием на простые ошибки, такие как путаница поп-звезды Майкла Джексона с бывшим заместителем начальника Департамента Национальной Безопасности Майклом Джексоном. Википедия, например, постоянно следит за биографическими страницами знаменитостей для того, чтобы некоторые звезды или главы государств не были преждевременно объявлены мертвыми. Тем не менее, в то время как еще действует метод «полагаться на толпу» при вынесении решений, где информация может быть пригодна при нормальном взаимодействии социальных сетей, существует реальный вопрос -подходит ли она для тем, касающихся национальной безопасности, где жизни и материальные ценности могут быть поставлены на карту , где нет времени, чтобы пускать это на самотек в сети или где секретная информация после ее обнародования более не может быть возвращена в сейф.

Информационные джунгли являются опасным местом. Они дают силу как нашей научной, так и повествовательной культуре. Информационная технология позволяет людям более хорошо делать анализ, но она также позволяет лицам, создающим мнения, запускать более интересные истории, делать это быстрее и распространять их более широко. Прозрачность цифровой скорости может разоблачить зло или раскопать секреты. Информация, которая собирается для того, чтобы защитить нас, может довольно быстро быть использована против нас. Секреты, предназначенные для того, чтобы их почти никто не видел, после утечки становятся известны каждому за считанные минуты. Обходительность не может долго существовать.

Обеспечение информацией не может полагаться на онлайн толпу, когда речь идет о национальной безопасности. В таких случаях нереально держаться убеждений, что взаимодействия в Интернет являются достаточно эффективным механизмом для определения фактической и надежной информации. Доверенные актеры и надежные сети должны быть созданы до времени кризиса, того ужасного момента, когда жизнь и судьба страны может оказаться под угрозой. Доверие и конфиденциальность являются обязательными для социальной сети, от которой может быть зависимость в условиях стресса. Поскольку Интернет не является нейтральным, ни одна партия не может рассчитывать на решительные и неопровержимые преимущества «кибер-поэзии». Например, споры о влиянии социальной сетей на иранские протесты во время выборов сосредоточились над предложениями - кому эти инструменты более выгоды — протестующим или правительству. В своей статье в Washington Post во время поствыборного кризиса в Тегеране, Джон Палфри, Брюс Элтинг и Роберт Фарис предложили несколько контрапунктов для тех, кто пришел к выводу, что сила политической активности онлайн является обратимой. Они утверждали, что есть «серьезные ограничения на то, что Twitter и другие веб-инструменты, такие как Facebook и блоги, могут сделать для граждан в авторитарных обществах». Правительства «ревнуют, что их власть может пошатнуться в киберпространстве, когда они чувствуют себя под угрозой». Они также отметили, что «свобода, чтобы кричать» онлайн может реально помочь режимам, предоставив «политический выпускной клапан». Репрессивные режимы могут также использовать социальные сети для своих целей, разнося пропаганду и дезинформацию.[1] Действительно, во время кризиса иранское правительство использовало все эти преимущества и, в конце концов, смогло в значительной степени задушить явную социальную напряженность.

С другой стороны, иранское правительство не заглушило голос народа. Технология постоянно развивается, как и практика по использованию Интернета. В данном случае режим в Тегеране думал, что он может поддерживать постоянное доминирование в сети, позволяя только медленный, дорогой и удаленный доступ обслуживания. Это предположение оказалось не верным. Инструменты социальных сетей помогли диссидентам преодолеть ограничения национальной технологической инфраструктуры.

Есть также пределы того, что могут сделать правительства. Если режимы, такие как Иран, например, избирают "ядерный вариант" и попытаются полностью закрыть Интернет для подавления внутреннего инакомыслия, он вполне может закрыть свои промышленные, энергетические и финансовые секторы, а также парализовать свою способность контролировать общественные СМИ. Кроме того, в глобальной

[1] John Palfrey, Bruce Etling, and Robert Faris, "Reading Twitter in Tehran?" The Washington Post, June 21, 2009, available at www.washingtonpost.com/wp-dyn/content/article/2009/06/19/AR2009061901598.html.

экономике государства или группы, которые проводят массовые кибератаки, могут сделать такой же ущерб для себя, как и для своего врага. Таким образом, своего рода сдерживание «взаимного гарантированного уничтожения», по-видимому, развивается и в кибермире. В то же время как некоторые независимые вредоносное актеры могут не иметь угрызений совести в отношении стран, у народов есть все основания стремиться ограничить их возможности для осуществления преступных действий. Это, однако, не означает, что они не будут пытаться осуществлять свои акции. Но народы никогда не были беззащитными в Интернете, и еще до того, как Америка задумалась о супер-безопасности после 9/11 правительство США полностью не игнорировало угрозы постхолодной войны миру и процветанию нации. В период с 1998 по 2000 гг. Конгресс проводил 80 слушаний в отношении тем, связанных с терроризмом.[1] Усилия по укреплению кибербезопасности и борьбой с вредоносной активностью в сети были в списке вопросов правительства, которые его беспокоят. Кроме того, было признано, что Интернет может служить в качестве инструмента хорошего управления. Также были предприняты усилия, направленные на то, чтобы Интернет служил людям. Вместо создания новых методов и средств познания и управление знаниями, электронное правительство являлось, главным образом, способом правительства работать в Интернете. Даже среди правительств Соединенные Штаты не были мировым лидером. Такие государства, как Новая Зеландия, Канада и Сингапур имели более амбициозные инициативы.

«Реальность» социальной конкуренции сети возникает снова и снова. Неправильно смотреть на киберпространство как место для статического соревнования. Там нет технологий, правительства, политики, права, договоров или программ, которые могут остановить ускорение конкуренции в кибервселенной. Правительства не перестанут пытаться обуздать эти вещи, но борьба всегда будет идти до конца. Нет, и не будет постоянного преимущества или выгоды. Там всегда будет враг, пытающийся взять кибервысоты.

Кроме того, платформы, которые несут сетевые приложения, скорее всего, изменятся, и будут продолжать развиваться. В самом деле, мы уже видим драматические сдвиги в предпочтениях пользователей от персональных компьютеров и ноутбуков до облачных вычислений и сотовых телефонов. Некоторые из них, на самом деле, утверждают, что вычисления быстро становятся скорее утилитом, чем продуктом. Программное и аппаратное обеспечение будет меньше значить для социальных сетей с течением времени. Между тем, другие уже предсказывают, как онлайн услуги будут развиваться, рекламируя, что Web 3.0 (где сети интуитивно подключают людей к соответствующей информации, а не только другим людям) скоро заменят Web 2.0.

[1] Laura K. Donohue, "In the Name of National Security: U.S. Counterterrorist Measures, 1960–2000," BCIA Discussion Paper 20001–6, John F. Kennedy School of Government, Harvard University, August 2001

Третьи выходят за рамки и говорят о роли искусственного интеллекта в социальной сети. То, как мы делаем это в социальной сети, скорее всего, продолжит развиваться с тем, что мы делаем с новыми приложениями. Суть в том, что является ошибкой думать, как социальные сети будут работать или что они будут работать в будущем на любой платформе или приложении. В настоящее время можно сказать в отношении глобальной конкуренции, что есть два вида народов, которые, вероятно, будут основными доминирующими конкурентами, - те, чьи режимы являются наиболее авторитарными, и те, чьи общества являются наиболее свободными. Авторитарные режимы будут использовать грубую силу контроля, чтобы захватить высоты социальных сетей. Свободные общества будут использовать преимущества творчества, конкуренции и инновации. Оба окажутся удивительно устойчивыми в онлайн войне. Оба будут основными факторами во время противоборства.

Но правительство США, как и много других правительств, не очень хорошо готово использовать социальные сети для национальной безопасности. Бюрократы часто плохо отвечают требованиям динамических изменений и разрушительным технологиям. Web 2.0 может быть и тем, и другим. Существует растущее беспокойство, что, несмотря на все разговоры в Вашингтоне о кибербезопасности и реализации киберправительства, скорее Америка может стать «киберпьяной». Для новичков Вашингтон далеко позади в своей готовности и способности к адаптации в мире Web 2.0. Даже президент Обама с его Blackberry под рукой и заслуженной репутацией специалиста по Интернет, имеет неприятности. Одной из первых вещей, которую администрация сделала в 2009 г. после переезда в Белый дом, было обновление веб-сайта Президента. Панель экспертов, собранная в Washington Post, сделала новый сайт WhiteHouse.gov на среднем уровне C + .[1] Этот класс, казалось, хорошо отслеживал выборы и протесты в Иране. Несмотря на то, что был поток информации, который показал необходимость глобальных дебатов в связи с ростом протестов, Президент оставался двусмысленным, пока не прошло несколько дней кризиса. Однако, несмотря на приглушенную риторику Белого дома, администрация оказалась под напором иранских государственных обвинений, включая требования компенсации за то, что невинные люди были использованы ЦРУ для разжигания беспорядков. Неутешительные результаты не удивительны. В то время как Белый дом и многие федеральные агентства экспериментируют с социальными сетями, их усилия являются, в основном, неуправляемым исследованием или ясной и согласованной политикой, поощряющей инновации по защите индивидуальных свобод и конфиденциальности. Иерархические

[1] Jose Antonio Vargas, "Grading WhiteHouse.gov," The Washington Post, March 24, 2009.

практики традиционного правительства не идут в ногу со временем, они недостаточны для эксплуатации взрыва социальных сетевых систем.[1]

Есть несколько уроков, чтобы помнить, когда нужно эксплуатировать социальные сети, и на данный момент мы знаем, что именно и как работает. Хотя не может быть жестких рекомендаций для социальных сетей, есть некоторые довольно хорошие практические правила - принципы эффективной адаптации инструментов социальных сетей, которые связаны с природой технологий, структурой социального взаимодействия и значением, присвоенным транзакциям социальных сетей.[2]

Предпочтение в социальных сетях направлено на адаптацию проверенного и широко доступного программного обеспечения и систем, которые кажутся удобными для пользователей. Простые правила и рабочие процедуры являются отличительной чертой широкого внедрения инструментов социальных сетей. Чем более интуитивным является инструмент, тем больше вероятность того, что он будет одобрен. И там должно быть что-то для пользователей. Пользователи обращаются к социальным сетям потому, что они считают, что участие принесет им то преимущество, которое они хотят получить. Недавнее распространение приложений, таких как Web 2.0 Suicide Machine и Seppukoo (которые позволяют пользователям очистить следы своего присутствия из интернет-сайтов, таких как Facebook) отражает не столько отказ от социальных сетей, как подтверждение того, что люди не очень заинтересованы в сетях, если они не получают от них никакой реальной ценности.

Прошлое было прологом

Правительству было трудно «адаптироваться» к технологии с самого начала информационной эры. В 1996 г. Закон Клингера-Коэна уделил основное внимание приобретению информационных технологий. Это вынудило федеральные ведомства посмотреть на информационные технологии как на «капитальные вложения», с надеждой, что правительство будет больше думать стратегически обо всем аппаратном и программном обеспечении, которое оно покупает. В центре внимания закона, однако, было то, как органы власти приобретали новые технологии, а не то, какие из технологий и возможностей они развивают. Многие государственные инвестиции пошли на разработку Интранет (частных компьютерных сетей), автономных баз данных и патентованного программного обеспечения.

[1] James Jay Carafano, Social Networking and National Security: How to Harness Web 2.0 to Protect the Country, Heritage Foundation Backgrounder No. 2273 (Washington, DC: The Heritage Foundation, May 18, 2009), available at www.heritage.org/Research/NationalSecurity/bg2273.cfm#_ftn2.

[2] Quotations from Clay Shirky, Here Comes Everybody: The Power of Organizing Without Organizations (New York: Penguin, 2008), 269, 271, 294.

Когда цунами приложений для социальных сетей появилось на рынке, и открытое программное обеспечение предложило богатый выбор инструментов для инноваций и сотрудничества, правительство США стояло в стороне, обремененное огромными инвестициями в системы и базы данных, которые действовали независимо друг от друга и Интернета.

Правительство изо всех сил старалось не отставать от частного технологического сектора, не говоря уже о том, что сетевой общественный и частный миры остались сами по себе. Во время администрации Клинтона вице-президент Альберт Гор сделал немало в защиту информационной магистрали. В течение второго срока Клинтона в Белом доме начало готовиться политическое руководство. 22 мая 1998 г. администрация опубликовала Директивы Президента по урегулированию (PDD) 62 и 63. PDD- 62 подчеркивала растущий диапазон нетрадиционных угроз, в том числе кибертерроризм, и инициативы по защите против них. PDD-63 особо обратила внимание на защиту критической инфраструктуры страны, которая составляла главную основу телекоммуникационных систем всемирной сети, электросети, а также основных пользователей онлайн-услуг, таких как правительства, транспорт и финансовый сектор. Вашингтон также потратил много времени и денег (около $ 100 млрд.) на подготовку к "Y2K"- усилий по обеспечению надлежащей работы компьютерных систем в результате наступления даты 2000 года.[1]

Сочетание Y2K и кибертерроризма являлись пугающими симптомами, а растущая зависимость от Интернета привела к созданию Центра защиты национальной инфраструктуры (NIPC), совместного партнерства правительства с частным сектором, который включает в себя представителей федеральных, государственных и местных государственные учреждений. NIPC попытался инкорпорировать уроки, извлеченные из программы Y2K и усилий по борьбе с угрозами тысячелетия, начав серию правоохранительных и контртеррористических инициатив. В 2000 г. Белый дом сформулировал первую стратегию по национальной кибербезопасности.

Сеть была бы естественным решением для государственно-частного сотрудничества и обмена информацией, что предусмотрено в докладе о киберпреступности. Дискуссии о социальных сетях, однако, отсутствовали в докладе. Клинтон и Гор, может быть, были первым президентом и вице-президентом, которые обменялись электронными письмами, но Web 2.0 просто не попал на экраны радара Белого дома.

[1] The spending estimate is based on National Communications System, Report 99–62, available at www.ncs.gov/n5_hp/Customer_Service/XAffairs/NewService/NCS9962.htm>. For an overview of Y2K lessons learned, see David Mussington, Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development (Santa Monica, CA: RAND, 2002), 11–18.

Правительственная программа по слежению за террористами оказалась достаточно спорной инициативой. О секретной программе впервые рассказали общественности в статье от 16 Декабря 2005 г. в Нью-Йорк Таймс. Она давала полномочия на мониторинг за всеми электронными инструментами социальной сети от телефонии до Интернет, электронной почты и текстовых сообщений. Поскольку для наблюдения, возможно, придется включить и коммуникации лиц США (термин, который обозначает американских граждан и других лиц, законно проживающих в Соединенных Штатах), но не требует ордера на обыск, программа оказалась под ударом критики. В ответ на споры Закон о наблюдении за террористами от 2006 г. предоставил дополнительные полномочия для проведения электронного наблюдения и назначал специальный Федеральный суд, учрежденный в рамках Закона о внешней разведке, предполагавший ответственность за выдачу любых необходимых ордеров на расследования. Почти все, что стало известно о пост-9/11 «наступательных» усилиях в Интернете, стало мгновенно спорным. С другой стороны, «оборонительные» возможности разведывательного сообщества были более приземленными. В частности, укрепление кибербезопасности было одной из ключевых задач Закона об обмене информацией (ISE) изданного в 2007 г. ISE - это смесь политики, процедур и технологий, которая позволяет обмениваться информацией по терроризму, в том числе данными разведки и правоохранительных органов. Он направлен на содействие формированию культуры обмена данными между его участниками для обеспечения легкого доступа к информации для поддержки их миссии. Предполагалось, что ISE свяжет федеральные, государственные, местные и племенные правительства. Также предполагалась решающая роль частного сектора и зарубежных акторов в обмене информацией по террористическим угрозам.[1] Даже через три года после того, как Закон был издан, он оставался в стадии его реализации.[2]

В 1988 г. в ответ на компьютерный вирус, названный Morris Worm, который был запущен через Интернет студентом Технологического института Массачусетса РобертомТаппаном Моррисом-младшим, и повлиял на работу 10% Интернета, правительство подписало контракт с Институтом Карнеги-Меллона по созданию групп реагирования на компьютерные инциденты (CERT), первую, финансируемую из федерального бюджета команду, отвечающую на вредоносные

[1] Information Sharing Environment, Information Sharing Environment Implementation Plan, November 2006, available at http://static/ reportimages/AD829E9BA2DCE1A1A490FE89BF499CDD.pdf.

[2] The Markle Foundation Task Force on National Security in the Information Age, "Nation at Risk: Policy Makers Need Better Information to Protect the Country," Washington, DC, March 2009, available at <www.markle.org/downloadable_assets/20090304_mtf_report.pdf>; Government Accountability Office (GAO), Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress, GA0–05–492 (Washington, DC: GAO, June 2008), available at www.gao.gov/new.items/d08492.pdf.

вспышки в Интернете. После 9/11 появилась другая правительственная инициатива - Национальный план по защите инфраструктуры (NIPP). Так как большинство секторов экономики использует Интернет, кибер стало координационным пунктом NIPP, который основывалась на нескольких учреждениях, в частности, аналитических центрах в целях содействия обмену информации с критическими бизнес-секторами, таких как финансовые учреждения и энергетические компании. Если CERT были солдатами, ответственными за кибер-ответы, то центры по анализу и обменом информацией (ISAC) были командными пунктами. ISAC были созданы и финансируются частным сектором. ISAC также получают информацию от других лиц, в том числе от правоохранительных органов и ассоциаций по безопасности. В дополнение к ISAC, критические бизнес секторы имеют Сектор Координационных Советов, который разрабатывает стратегические рекомендации в координации с государственными органами. В дополнение к стратегии, изложенной для внутренней безопасности в NIPP, Департамент Юстиции также занимался кибер-войной. Обмен информацией между правительством и частным сектором получил значительную поддержку с программой InfraGard, первоначально учрежденной Федеральным бюро расследований при президенте Клинтоне. Созданная в начале для оказания помощи в расследовании киберпреступлений, InfraGard расширила сотрудничество с правоохранительными органами, бизнесом и научными кругами по вопросам, связанных с безопасностью после 9/11. Главы InfraGard облегчают сбор и анализ информации, подготовку и обеспечение дискуссионных форумов для обмена передовым опытом. Она также обеспечивает безопасные коммуникации веб- платформ.

Компании из частного сектора, университеты, исследовательские центры и неправительственные организации также разработали возможности для борьбы с вредоносной кибер деятельностью и расследуют или предотвращают террористические операций в Интернет. Возможно, самой известной из этих группы является Альянс Безопасности Интернет, сотрудничество с Electronic Industries Alliance, федерация торговых ассоциаций и Cylab Университета Карнеги-Мелон, созданная, чтобы служить форумом для обмена информацией и получением предложений по укреплению информационной безопасности. Многие другие организации и компании частного сектора поддерживают киберзащиту Америки. После 9/11 Американская Военная Академия в Вест-Пойнте создала центр по борьбе с терроризмом. Она присоединилась к Company-

Command и PlatoonLeader (военные сети), инновационным проектам, созданных Академией для того, чтобы помочь «большой армии» приспособиться к новым проблемам интернет-боя. Среди исследования центра есть «Проект Исламского Воображения: визуальные мотивы в джихадистской Интернет пропаганде», который предоставляет готовое руководство по графике, символам и фотографиям, которые обычно используются террористами. Университет Ари-

зоны также провел многолетний проект, названный Dark Web, который пытается мониторить, как террористы используют Интернет. Лаборатория искусственного интеллекта Университета накопила наиболее обширную в мире базу данных, связанных с террористичесикми веб сайтами - более 500 миллионов страниц сообщений, изображений и видео - и сделала его доступным для военно-разведывательного сообщества США. Некоторое сложное программное обеспечение показывает социальные взаимосвязи между радикальными группами и направлено на выявление и отслеживание людей, анализируя стили письма авторов. Институт исследований Ближнего Востока (MEMRI) публикует экстремистские сообщения из Интернет, в том числе террористические веб-сайты, дискуссионные форумы и блоги. После того как MEMRI опубликовал обширный обзор исламистских веб-сайтов в 2004 г., многие из них были закрыты их Интернет провайдерами. В дополнение к этим усилиям, неправительственные организации и частные компании предоставляют разнообразные аналитические и исследовательские инструменты для проникновения в террористические операции в Интернете. Например, SITE Intelligence Group из Вашингтона регулярно мониторит, переводит и сообщает информацию о террористических веб-сайтах, и часто распространяет эту информацию с американскими спецслужбами. Наконец, поставщики программного обеспечения и аппаратуры и впредь реагируют на потребности рынка в новых услугах и продуктах по борьбе с незаконной онлайн-активностью, от борьбы с несанкционированными вторжениями и противодействием DOS атакам до предотвращения нарушений или эксплуатации систем или данных. Предоставление услуг и продуктов безопасности — это индустрия с многомиллиардными прибылями.

Озадаченный Вашингтон

Социальные сети правительства все еще представляют большую проблему, потому что не ясно, знает ли Вашингтон, что он пытается сделать онлайн. Эта проблема нигде так не очевидна, как в усилиях правительства распространить это сообщение - эту задачу обычно называют «общественной информацией», когда послание направлено американской аудитории, и «народной дипломатией», когда идет взаимодействие с остальным миром. Попытка отправить послание и сделать это правильно, не является чем-то новым, особенно, где затрагиваются вопросы национальной безопасности. Во время Первой мировой войны политика, продвигаемая Джорджем Крилом, главой Комитета США по общественной информации, была связана с попыткой управлять мировой пандемией. Позже американские усилия в попытках продвигать и защищать свободу, и обеспечить свободное и открытое выражение в одно и то же время, были оспорены. Правительственным чиновникам всегда было трудное выяснить, является ли их работа

в отражении точки зрения правительства или состоит в простом обеспечении форума для «объективного» обсуждения. Общественная дипломатии и информационные программы во время Второй мировой войны были хаотичными. Даже хваленые усилия Америки, направленные на борьбу с идеологией коммунизма во времена Холодной войны были отмечены как многими неудачами, так и успехами.[1] Ричард Соломон, глава Института мира США, отметил, что «для государства есть возможность проталкивать американские перспективы практически по любому вопросу, для любого человека вопрос состоит в том: что должно делать правительство?»[2] Это тот же самый вопрос общественной дипломатии, который задавался задолго до того, как Интернет был изобретен. В Вашингтоне по-прежнему отсутствует четкая целеустремленность в онлайн, и это такая же большая проблема, как борьба с бюрократическими препонами в использовании новых технологий. В освоении борьбы за кибервысоты на обоих концах кривой власти не знание того, что вы пытаетесь сделать, является реальным препятствием. Большая часть того, почему Вашингтон ведет борьбу, связана с тем, что он просто не очень хорошо решает проблемы. Последнюю четверть века наблюдался бум в способностях человека создавать и манипулировать новыми знаниями. Несмотря на этот факт, выбор инструментов, используемых для информирования государственной политики, плох, как никогда. Вашингтон делает политику в значительной степени интуитивно, сформированной в результате решения проблем XX века — это идеи, которые едва изменились со времен Холодной войны.

Тем не менее, нечто драматическое добавилось на вооружение для анализа сегодняшних проблем - распространение компьютерных технологий, Интернет, и все остальное, что идет вместе с «информационной революцией». Современные исследователи имеют доступ к огромной цифровой библиотеке и базе данных, а также мощным поисковым и вычислительным программам. Новые средства манипулирования данными, такими как информатика (наука об обработке информации), поиск данных (извлечение и анализ данных с целью выявления закономерности и взаимосвязи), компьютерное моделирование (моделирование систем) и открытые источники в разведке (получение и анализ информации из открытых источников для действий разведки) — лишь немногие, которые можно назвать революционными инструментами открытия знаний.

По иронии судьбы, открытие знаний постоянно растет в каждой области, кроме национальной безопасности. В то время как средства обнаружения знаний становятся все более изощренными, процесс общественного формирования по-

[1] See Nicholas Evan Sarantakes, "Word Warriors: Information Operations during World War II," in Mismanaging Mayhem: How Washington Responds to Crisis, ed. James Jay Carafano and Richard Weitz (Westport, CT: Praeger, 2007), 27–45; Carnes Lord, "Marketing Freedom: Cold War, Public Diplomacy, and Psychological Warfare," in Mismanaging Mayhem, 46–66.

[2] Bryant Jordan, "Net Diplomacy," Federal Computer Week, October 29, 2000, available at www.fcw.com/Articles/2000/10/29/Net-diplomacy.aspx.

литики становится все более интуитивным. В Вашингтоне рабочие тезисы, чувствование нутром, партизанские предпочтения и идеологической пыл вытесняют передовой анализ. Создание кибер-стратегических лидеров в этой среде будет равносильным строительству замков на песке, если только знания и навыки, дающиеся им, не будут основаны на всеобъемлющих, практических и беспристрастных научных исследованиях, что специально обслуживают потребности правительства. Настоящие знания не достаточно хороши, чтобы быть первоклассным кибер-конкурентом.

Дебаты о том, как великие идеи могут быть созданы посредством Web 2.0, и о том, что будет после, еще далеки от завершения. Исследования в области социальных сетей трудно удержать в быстром темпе изменений используемых информационных технологий. Понимание социальных сетей требует мультидисциплинарного подхода исследований, который сочетает технику социальных наук с дисциплинами «жестких наук». Эта смесь дисциплин, которые исследуют, как функционируют сети, часто называется «сетевой наукой».[1] Практики исследуют разнообразные физические, информационные, биологические, когнитивные и социальные сети в поисках общих принципов, алгоритмов и инструментов, которые управляют поведением сети. Понимание сетей может быть применено к различным проблемам от борьбы с террористическими организациями до реагирования на стихийные бедствия.

Без понимания наука является просто догадкой и удачей (хорошо это или плохо). Некоторые правительства и части правительства «получают ее». Один из получивших элементов - это армия США, которая в 2003 году создала Институт общих биотехнологий. Одной из областей, на которой сфокусированы исследования института, являются «биоинспирированные сети», а изучив «высокую производительность» биологических сетей по проникновению, искусственные сети могут быть сделаны более масштабными, надежными и низкозатратными. В 2010 г. институт курировал 50 междисциплинарных исследовательских групп, охватывающих восемь различных академических отделов из Массачусетского технологического института, Калифорнийского университета в Санта Барбара и Калифорнийского технологического института. Вполне возможно, что чем больше ученые смотрят на биологические системы, тем более применимыми будут уроки, которые они извлекут для понимания компьютерных систем и деятельности, в том числе, социальных сетей. Потенциал сетевой науки и его влияние на социальные сети — это слишком большая возможность для свободных наций, чтобы его игнорировать, если они хотят быть уважаемыми конкурентами в сетевых средах. Все это сказанное, по сравнению с ячейками и сотовыми сетями, звучит интересно, но это не просто наука.

[1] See, for example, Committee on Network Science for Future Army Applications, Network Science (Washington, DC: The National Academies, 2005).

Доклад Американской Национального Академии от 2005 г. изложил некоторые с серьезные препятствиями, включая трудность моделирования и анализа больших, сложных сетей, развития лучших экспериментов и измерений сетевой структуры и установления общих понятий через разрозненные дисциплины, которые участвуют в сетевой науке

Измеряя кибервысоты

Мысли о будущем являются жизненно важным для одоления кибервысот. Частично ответ лежит в инициативе по созданию новых знаний. Если касаться компетенции социальных сетей, то основа для обнаружения знаний могла бы хорошо зависеть от способности идти на острие сетевой науки. Прогнозирование будущего не менее важно для серьезных кибер-воинов. Социальные сети и другие информационные технологии имеют достаточно мощные инструменты для понимания и оценки того, как сложные динамические системы и соперничество будут разворачиваться в течение долгого времени. Освоение этих методов и комбинирование их в форму с более богатыми идеями дадут конкурентам уникальную возможность в прогнозировании будущих вызов.

Наконец, важно посмотреть за горизонт и начать планировать борьбу с будущими вызовами. Зная, что они придут, и ничего не делая, чтобы противостоять им, означает, что в долгосрочной перспективе будут потери. Технология социальных сетей останется такой же динамичной, как и конкуренция, которая будет ее использовать. Если Вашингтон не будет развивать человеческий капитал и создавать первоклассное кибер-лидерство, его сметет война в социальной сети.