Кафедра Социологии Международных Отношений
Социологического факультета МГУ
имени М.В. Ломоносова

Геополитика

Информационно-аналитическое издание

Тема выпуска:

Кибер

Выпуск XXII

Москва 2013 г.

Геополитика.
Информационно-аналитическое издание.
Выпуск XXII, 2013. — 118 стр.

Печатается по решению кафедры
Социологии Международных Отношений
Социологического факультета МГУ им М. В. Ломоносова.

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта Фондом подготовки кадрового резерва <<Государственный клуб>> по итогам конкурса, проведенного в соответствии с распоряжением Президента Российской Федерации No. 216-рп от 03.05.2012 года <<Об обеспечении в 2012 году государственной поддержки некоммерческих неправительственных организаций, участвующих в развитии институтов гражданского общества>>.

Адрес редакции:
121087, Москва, Багратионовский проезд, дом 7, корп. 20 “В”, офис 405.
тел. (495) 514 65 16
факс (495) 926 68 11
Geopolitika.ru@gmail.com
www.geopolitika.ru

СОДЕРЖАНИЕ

Введение в кибергеополитику

Леонид Савин

главный редактор журнала «Геополитика» и интернет портала Geopolitica.ru, руководитель администрации МОД «Евразийское движение».

В последнее время все чаще приходится слышать о возрастающей роли киберпространства в качестве инструмента политики, либо той сферы, где разворачивается противоборство между различными политическими организациями, странами и даже альянсами государств. Инцидент с Эдвардом Сноуденом является показательным фактом того, насколько Интернет коммуникации и взаимозависимость социальной среды с политикой, экономикой и военным сектором стали важны и влияют как на текущую повестку дня, так и на стратегическое планирование лидеров ведущих держав мира.

Если в геополитике уже достаточно разработан научный аппарат и дефиниции, которыми оперируют политики, эксперты и ученые, то киберпространство в какой-то мере представляет собой «terra incognita». И за обладание этим пространством ведется довольно активная борьба. Крайне показательным является то противостояние, которое заняли в отношении регулирования Интернет пространства различные государства. Дихотомия буквально повторяет тот мегацивилизационный раздел, который пролег между странами и народами, относящимися к Sea Power и Land Power. США, страны ЕС и их сателлиты выступают за полную свободу действий в Интернет, что является явным лицемерием[1], в то время как Россия, Иран, Китай, Индия и ряд других государств требуют того, чтобы Интернет был суверенным и находился под юрисдикцией норм международного права, точнее Международного Союза Электросвязи, входящего в Организацию Объединенных Наций. Саммит по вопросам киберпространства, прошедший в декабре 2012 г. в Дубаи показал усугубляющиеся противоречия, связанные с международными телекоммуникациями, когда США отказались подписать новый договор, регламентирующий право всех государств заниматься управлением Интернета. Данное разделение четко вписывается в схему Карла Шмитта, которая является надежным показателем Политического — это дуальные категории друг и враг. Данные категории не являются моральными, а представляют технические функции, которые проявились и в позициях по поводу взгляда на функционирование Интернет пространства.

[1] Достаточно посмотреть на то, как власти этих стран контролируют с помощью Интернет и социальных сетей своих граждан и собирают информацию об их частной жизни, а также как используются спецслужбами западных стран Интернет технологии для подрывной деятельности и шпионажа.

География киберпространства

Для начала нужно дать определение термину киберпространство. Исследователи приписывают авторство этого слова писателю-фантасту Уильяму Гибсону, который использовал его в рассказе «Burning Chrome», опубликованном в 1982 г. Два года спустя он развил эту тему и в своем знаменитом киберпанковском романе 1984 г. под названием «Neuromancer» — автор описал киберпространство как «всеобщую галлюцинацию»[1]. Киберпространство имеет существенное отличие от наземного, морского, воздушного и космического пространств — оно создано не природой, а является искусственной конструкцией, имеющей компоненты, которые могут меняться с течением времени.

В различных странах есть свои определения киберпространства. В США в документе по национальной стратегии в отношении кибербезопасности от 2003 г. было указано, что «киберпространство состоит из сотен тысяч соединенных между собой компьютеров, серверов, маршрутизаторов, коммутаторов и волоконно-оптические кабелей, которые позволяют нашей критической инфраструктуре работать. Таким образом, нормальное функционирование киберпространства имеет важное значение для нашей экономики и нашей национальной безопасности»[2].

Отсюда видно, что киберпространство напрямую связано с реальной географией, которая вместе с политикой является основным элементом науки геополитики.

Во-первых, все маршруты коммуникации, сервера и технические узлы, которые связаны как с Интернет, имеют географическую локализацию. Во-вторых, киберзоны имеют национальную идентификацию в смысле доменных зон, государственного контроля и используемого языка. В-третьих, киберпространство подчеркивает физическую географию особенным образом — датчики различных служб, навигационные устройства, технические гаджеты и мобильные устройства воплощают собой интерактивную карту с перекрестными потоками информации, техники и людей.

Хотя основной трафик идет по подводным кабелям, ряд государств все же напрямую несет ответственность за происходящее в киберпространстве, так как маршруты коммуникаций проходят через их национальные территории. Как справедливо заметил Мака Аалтола в отношении Финляндии и региона, Балтийское море является основным проводником данных, через которое проходят подводные кабели, соединяющие вместе важный перекресток глобального киберпространства. Для Финляндии самые стратегически важные связи - это два северных кабеля BCS, которые связывают Россию со Швецией и далее за их пределами с

[1] William Gibson, Neuromancer. New York: Ace Books, 1984.

[2] The National Strategy to Secure Cyberspace, Washington, DC: White House, 2003.

помощью финских узловых точек. В результате основная часть киберпотока из России в остальной мир проходит через Финляндию. В случае, если какой-либо внешний актор попытается шпионить за этим трафиком данных, это может привести к недоверию. Россия может затем рассмотреть меры по противодействию или попытаться обойти в Финляндию с ее системой коммуникаций. Основные проблемы, следовательно, существуют, и на них Финляндия должна найти стратегические ответы. С одной стороны, она должна стремиться обеспечить надежные и безопасные инвестиции, связанные киберпространством. С другой стороны, она должна обеспечить свою собственную кибербезопасность. В некоторой степени, эти цели могут быть даже противоречивыми.[1] Действительно, это серьезная дилемма, учитывая, что этот регион является привлекательным для инвестиций в области высоких технологий. В Финляндии нет тектонической активности и крайне низка вероятность природных катастроф. Ее умеренный климат естественно охлаждает компьютерные парки облачных вычислений. Компания Google уже вложила сотни миллионов евро в свой центр обработки данных в г. Хамина на южном побережье Финляндии.

Еще один важный фактор, актуальный для нынешней геополитики — это глобальность. Киберпространство по-особому фиксирует и гомогенизирует физическое пространство — таким образом, с помощью GPS технологии и других инструментов глобализация добирается в самые укромные уголки планеты.

При этом цифровые технологии реконфигурируют опыт картирования в нечто другое, что Бруно Латур и его коллеги называют навигационной платформой (navigational platform), характеризуемой присутствием:

- Банка данных;
- Определенного интерфейса для управления данными, т.е. подсчета, обработки и поиска;
- Инструментальной панели для взаимосвязи с пользователями;
- Множества различных выходов, сделанных для огромного количества пользователей - и один из них имеет выход на печатное устройство[2].

Традиционная роль карты пересматривается, появляются различные школы, связанные с описаниями политических и институциональных отношений картирования, перформативным использованием и пониманием карт как эмерджентности, возникающей через разнотипный набор практик.

Картографирование Интернет пространства становится приоритетной задачей ряда исследовательских центров и университетов. Пока еще в достаточно ограниченном количестве, но с каждым годом все больше и больше — специализированные издания, работа кафедр и подразделений в различных think-tanks

[1] Mika Aaltola. Finland should aim to be a cyber connector. FIAA Comment, № 15, November 2013.

[2] Valerie November, Eduardo Camacho-Hubner, Bruno Latour. Entering a risky territory: space in the age of digital navigation. Environment and Planning D: Society and Space 2010, volume 28, p.583.

ведут мониторинг киберпространства и фиксируют его изменения — будь то появление новых технических узлов, издание новых законопроектов или противоправная деятельность в сети.

Исходя из вышеуказанного, мы видим, что киберпространство не однородно и имеет несколько уровней.

Дэвид Кларк предложил модель, в которой существует четыре уровня киберпространства[1].

1. Физический уровень содержит все аппаратные устройства, которые включают маршрутизаторы, переключатели, носители и спутники, датчики и другие технические соединители, как проводные, так и беспроводные. Физическая инфраструктура географически расположена в «реальном пространстве», и, таким образом, является предметом различных национальных юрисдикций.

2. Логический уровень в целом относится к коду, который включает в себя как программное обеспечение, так и протоколы, которые включены в него.

3. Уровень контента описывает всю созданную, взятую, хранящуюся и обрабатывающуюся информацию в киберпространстве. Информация определяется как «знания, касающиеся объектов, например, факты, события, вещи, процессы или идеи»[2].

4. Социальный уровень, состоящий из всех людей, использующих и формирующих характер киберпространства. Это фактический Интернет людей и потенциальные отношения, а не подразумеваемый Интернет аппаратных средств и программного обеспечения. По сути, социальный

слой включает правительства, частный сектор, гражданское общество и субъекты технического сообщества. Тем не менее, всех их объединяет специфика: если в «реальной» жизни (экстра киберпространство) люди могут в конечном счете быть идентифицированы по их уникальным кодам ДНК, атрибуция в сети гораздо сложнее (внутри киберпространства). В отличие от «плотского» мира, люди в киберпространстве облегчают создание множественной идентичности для пользователя. И в альтернативе, одна виртуальная личность может иметь несколько человеческих пользователей (например, тот же онлайн-аккаунт офиса газеты «Нью-Йорк Таймс» используется разными сотрудниками). Это имеет не только важное значение с точки зрения защиты безопасности или авторских прав, но также поднимает интересные вопросы о том, как кибер-мир играет в реальном мире.[3]

[1] David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, [1]2 March 2010.

[2] ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms.

[3] Alexander Klimburg, Philipp Mirtl. Cyberspace and Governance — A Primer. The Austrian Institute for International Affairs, Working Paper 65 / September 2012.

Четвертый уровень и является локомотивом геополитики в киберпространстве. Именно Man Power — что не является абстрактной величиной, т.е. люди, а не машины принимают решения по политическим вопросам, включая действия, связанные с Интернет пространством.

Кроме того, терминология, используемая ранее в кибернетике, также адекватна и для геополитики киберпространства. До настоящего момента было принято говорить о двух кибернетиках — первого и второго порядка. Если кибернетика первого порядка была связана с наблюдаемыми системами, то кибернетика второго порядка — это кибернетика наблюдающих систем[1]. Данная ремарка указывает на высокий организационный характер новой волны кибернетики, хотя некоторые дефиниции довольно сильно напоминают геополитические теории и науки о власти.

Интернет политика

Если говорить о киберпространстве как политической деятельности, то на данный момент есть две основные модели, связанные с этим новым ареалом человеческой активности. Первая — это электронное правительство. Под данным термином следует понимать создание специальных сервисов, которые облегчают взаимоотношения населения с представителями власти и получение от них различных услуг. Электронные платежи, виртуальные приемные, обработка запросов в удаленном доступе — все эти действия призваны облегчить и упростить жизнь налогоплательщиков в странах, где начинают применять современные коммуникационные технологии.

Второе — это использование киберпространства в качестве среды и инструмента для распространения определенной политической культуры.

Крайне показательными в этом отношении являются усилия США, где правительство использует Интернет как новое средство для достижения своих целей. При этом задействуется не только гражданский сектор, но и силовые ведомства.

В 2011 г. стало известно, что военные в США запустили программу, связанную с манипуляциями в социальных сетях. Она подразумевала создание не существующих онлайн-личностей, которые должны обладать правдоподобным прошлым и историей, и что любой из 50 управляющих личностями сможет оперировать фальшивыми онлайн-личностями со своих рабочих компьютеров «без страха быть раскрытыми хитрыми противниками». Как заявил один из представителей компании, разрабатывавшей программный продукт: «Технология позволяет вести секретную деятельность в блогах на иностранных языках, которая позволит

[1] Heinz von Foerster. Cybernetics of Cybernetics. University of Illinois, Urbana 1979

Центральному командованию Минобороны США противостоять экстремистам и вражеской пропаганде за пределами США»[1].

А в конце 2011 г. в Белом доме заявили о создании виртуального посольства в Иране для «укрепления связей с иранским народом»: http://iran.usembassy.gov/[2]. Показательно, что в это же время Конгресс США принимает различные меры по ослаблению связей с иранскими чиновниками и введением санкций наносит ущерб иранской экономике. А до этого США уже открыли виртуальное консульство для Сектора Газы[3].

По мнению Н.А. Цветковой «существует несколько терминов, используемых американским правительством для обозначения инновационного способа оказания влияния на зарубежное общество при помощи Интернета: цифровая дипломатия (digital diplomacy), интернет-дипломатия (Internet diplomacy), дипломатия социальных сетей (Twitter diplomacy) и публичная дипломатия Web 2.0. (public diplomacy Web 2.0.)»[4]. Наиболее распространенным термином среди руководства США, занимающегося вопросами внешней политики и установления влияния в других странах, является последний.

Технология Web 2.0, рассчитанная на взаимодействие политических активистов посредством интернет технологий, доказала свою эффективность и в ходе массовых протестов в Тунисе и Египте, а также координации оппозиции и самоорганизации различных групп политической направленности в России.

Угрозы киберпространства

Как видим, киберпространство не является утопией, о чем ранее говорили писатели-фантасты. Это новая сфера человеческой активности, где существуют свои ограничения, катаклизмы, эпидемии и изъяны, хотя они не затрагивают напрямую жизни людей — все во многом зависит от выбора самого индивидуума. Если кто-то настолько увлекся компьютерными играми, что стал неадекватно воспринимать реальность — разве это не бич киберпространства, наподобие наркомании в реальном мире?[5] Киберзависимость связана не только с профессиональными обязанностями или развлечениями, такова сама природа Интернет. Современный американский философ Джон Зерзан, например, отмечал, что пси-

[1] Ник Филдинг, Иан Кобэйн. Военные США будут манипулировать социальными сетями.// ИноСМИ http://www.inosmi.ru/usa/20110318/167469729.html

[2] Mutter, Paul. Few Virtues to "Virtual Embassy in Iran". December 23, 2011. http://www.fpif.org/blog/few_virtues_to_virtual_embassy_in_iran

[3] http://gaza.usvpp.gov/about_econsulate.html

[4] Цветкова Н.А. Программы Web 2.0 в публичной дипломатии США. 13.04.2011 http://www.ushistory.ru/stati/559-programmy-web-20-v-publichnoj-diplomatii-ssha.html

[5] Dene Grigar. Lara Croft: Cyber Heroine. Leonardo June 2006, Vol. 39, No. 3, Pages 269-270.

хика человека, который хотя бы раз воспользовался Интернет, подвержена необратимым последствиям[1].

Аналогично и с «болезнями» в этом «мире». В 1983 г. Фред Коэн намеренно разработал программы, которые могут «заразить другие программы, модифицируя их посредством возможного включения своей эволюционированной копии», как он выразился в своей диссертации. Опираясь на биологическую аналогию, он назвал новую программу вирусом.

Термин «червь» был придуман Джоном Бруннером в романе 1975 г. Shockwave Rider. В то время как вирусы просто заражали компьютерную программу (или файлы), черви «ползли» дальше, копируя себя между системами. Использование уязвимости компьютеров, известные как задние двери, черви распространяются без помощи невнимательных пользователей. В 1988 г. червь Морриса проник и инфицировал около 60000 хостов зарождающейся сети Arpanet, которая являлась прототипом нынешнего Интернет. Сам Роберт Моррис, создатель червя, был первым человеком, привлеченным к ответственности и осужденным в соответствии с законом о компьютерном мошенничестве 1986 г.[2]

Если в физическом мире есть карантин в отношении опасных болезней и даже бывают межгосударственные конфликты, связанные с эпидемиями или целенаправленным инфицированием (биологическое оружие), разве не должно этого быть в киберпространстве? История последнего десятилетия свидетельствует и о таком феномене. Наиболее показательными случаями были:

Кибератаки в 2007 г. на правительственные сайты Эстонии;

Действия хактивистов в августе 2008 г. во время оккупации Грузией Южной Осетии и миротворческой операции со стороны России;

Внедрение американскими и израильскими спецслужбами компьютерного червя Stuxnet на иранскую атомную станцию.

По мнению специалистов в будущем количество таких атак будет только возрастать, а методы работы хакеров совершенствоваться. Это вынуждает правительства многих стран пересмотреть свою политику в отношении Интернет и принимать особые меры по охране этого пространства.

Индийский опыт

На примере нескольких конкретных случаев, произошедших в Индии, рассмотрим как именно киберпространство взаимосвязано с реальной жизнью. При этом мы будем рассматривать спектр угроз для граждан и государства, а не широких возможностей, связанных с новыми технологиями.

[1] Зерзан Джон. Закат эры машин.// Глобальный дискурс. Под ред. Савина Л.В. Сумы: Университетская книга, 2003. http://dglobal.narod.ru/twilight.html

[2] A Better Way to Battle Malware. November 22, 2011. Winter 2011, Issue 65. http://www.strategy-business.com/article/11403?pg=all

Первое явление — это терроризм. Наиболее крупные теракты за последнее время были совершены в г. Ахмедабад в июле 2008 г. и в г. Мумбаи в ноябре этого же года. В обоих случаях террористы использовали Интернет для координации своих действий и даже после них. В частности, как указано в издании Times of India от 10 января 2009 г., члены террористической группировки Indian Mujahideen использовали неконтролируемые сети Wi-Fi для рассылки сообщений полицейским, которые занимались расследованием этих инцидентов. В письмах содержались угрозы в адрес работников правоохранительных органов. Данный инцидент вынудил индийскую полицию обратиться к правительству для издания постановления об уголовном преследовании для тех компаний, которые в будущем не будут защищать свои Wi-Fi. Аналогичная ситуация прослеживается и в других странах. Как правило, антиправительственные элементы всегда находятся на несколько шагов впереди, и исследователям остается только констатировать постфактум об их методах работы, включая использование систем Linux, программ P2P и пр.

Следующее явление — сепаратизм и антигосударственная деятельность.

В Индии сепаратисты Кашмира регулярно используют Интернет для антигосударственной деятельности. Точкой отсчета считается 2010 г., когда появилось новое поколение киберактивистов, начавших осваивать альтернативное пространство для выражения своих политических пристрастий. В связи с цензурой на местных медиа, контролем за смс и телефонными линиями в этом конфликтном регионе, Интернет остается единственным инструментов для ангажирования в политический дискурс. Вместе с тем, по словам одного из активистов, с 2010 г. возросла и деятельность правительственных служб, занимающихся контролем и наблюдением за коммуникациями. При этом полиция использует ложные аккаунты в социальных сетях, специальные программы для анализа протокола данных и пр., что позволяет им тоже иметь продвинутую стратегию[1].

Представитель отдела полиции, занимающийся киберпреступлениями штата Джамму и Кашмир в апреле 2012 г. заявил, что они раскрыли группу молодежи, которая на протяжении нескольких лет занималась антинациональной политикой в Интернет с помощью социальных сетей и управлении веб сайтами. По данным полиции страницы 'Freedom of Dawn', 'Balai Khuda', 'Aalov' и 'We love Syed Ali Shah Geelani' поддерживали сепаратистские настроения, а также подстрекали к погромам во время беспорядков летом 2010 г.[2] Как указывает издание Press Trust

[1] Uzma Falak. India clamps down on Kashmir's online dissenters. August 14, 2012 http://www.newint.org/blog/2012/08/14/kashmir-teenage-cyberactivist/?utm_medium=ni-email&utm_source=message&utm_campaign=-enews-2012-08-23

[2] J-K cops crack 'anti-national' network. Apr 16 2012 http://www.indianexpress.com/news/jk-cops-crack-antinational-network/937240/

of India, при расследовании было определено, что многие сепаратистские сайты управлялись из таких стран как США, Великобритания, Пакистан и ОАЭ.

Непосредственно внешнее управление конфликтами — это третий случай рассматриваемой нами темы. Что касается Индии, то второй половине августа 2012 г. в Индии с помощью Интернета в социальных сетях и на мобильных телефонах были распространены фотографии изуродованных тел с угрозами, что индийские мусульмане планируют совершить нападения на жителей северо–восточного региона страны, которые не принадлежат к мусульманскому вероисповеданию. В послании было сказано, что готовящиеся акции задуманы как ответное действие на смерти мусульман, которые произошли в результате длительного спора между бенгальскими мусульманами и коренными племенами бодо в штате Ассам. Этот многолетний спор, связанный с этнической принадлежностью, земельными участками, рабочими местами и политической властью привел к гибели 70 человек и спонтанной миграции с мест своего проживания более 300 тысяч человек с июля 2012 г.[1]

Распространение сообщения о мести со стороны мусульман коснулось не только штата Ассам, но также вызвало панику среди рабочих и студентов этого региона, которые находились в этот момент в южной Индии. Они посчитали себя в роли потенциальных жертв и поспешно на автобусах и поездах ринулись домой. Все же панику с трудом удалось остановить.

Индийское правительство заявило, что эти изображения изуродованных тел имеют пакистанское происхождение. В результате расследования и профилактических мер было закрыло около 300 сайтов и вынесено предупреждение Интернет провайдерам об ответственности.

Что характерно, именно социальные сети, которые зарегистрированы в США и тесно сотрудничают с Белым домом и Пентагоном, не захотели пойти на встречу пожеланиям индийских властей. Секретарь Индии по телекоммуникациям Чандрашехар заявил о том, что Facebook и Twitter могут столкнуться с правовыми действиями, так как они не пошли на встречу требованиям правительства снять материалы или проследить источники данного сообщения. В верхах даже предположили, что доступ к Twitter вообще может быть полностью закрыт в Индии.

Наверняка центры мировой социальной паутины будут давать отказы на подобные запросы в будущем, мотивируя это свободой слова демократией в киберпространстве.

И последний случай, — это когда социальные медиа в комбинации с телевизионным освещением дают беспрецедентные возможности для трудно предсказуемых политических движений.

[1] Jonah Force Hill. India's Internet Freedom Nightmare.// The Diplomat, August 25, 2012 http://thediplomat.com/2012/08/25/indias-internet-freedom-nightmare/?all=true

Казалось бы, толчком послужил обычный криминальный случай — 16 декабря 2012 г. в столице Индии была изнасилована 23-летняя девушка, но именно с помощью социальных сетей весть об этом вызвала общественный резонанс, — и тысячи сторонников наказания виновных (а заодно и улучшения прав женщин) вышли на улицы Нью–Дели.

Следует отметить, что для страны с населением свыше 1,2 млрд. человек единичный акт насилия или убийства не является чем-то из ряда вон выходящим. Достаточно в течение определенного времени помониторить индийскую региональную прессу, и неискушенный читатель обнаружит много шокирующих наше представление фактов. Во время поездки по Индии автор публикации неоднократно узнавал о том, как в одном месте полицейский изнасиловал школьницу, в другом поклонники культа богини Кали совершили кровавый ритуал на кладбище, который включал эксгумацию трупа и его расчленение и т.п. Что касается аварий и катастроф, то согласно статистике каждый день в Индии происходит инцидент с жертвами на железной дороге, а время от времени переворачивается грузовик со свадебным кортежем (естественно, с летальным исходом для многих пассажиров). Для традиционного индусского сознания с понятием кармы и кастовой системы такие инциденты, вероятно, являются нормальным ходом вещей. Что же побудило огромные массы выйти на улицы Нью-Дели и драться с полицией?

Являлся ли выход масс на улицы индийской столицы спонтанной реакцией, где местные кибератвисты стали катализатором протеста или запланированной акцией, предусматривающей, например, срыв визита Президента РФ Владимира Путина в Индию, который все же состоялся, несмотря не неспокойную обстановку? Однозначно, кое-кому было бы на руку сорвать многомиллионные контракты Нью-Дели и Москвы, подписанные руководством обеих стран. По крайней мере, американские аналитики сильно занервничали из–за того, что Россия начала серьезно конкурировать с США на рынке вооружений, где Индия является одним из важных покупателей. Например, заголовок одной статьи в издании Wired по поводу военных контрактов России с другими странами, где освещался и недавний визит в Индию, звучит не иначе как «Путинские торговцы оружием наращивают поставки отвратительным негодяям»[1].

В общем, мы видим, что катализатором широкомасштабных протестов становятся социальные сети, которые превращаются в первоклассный инструмент для провокаций или цветных революций в стиле Web 2.0 (подтверждением чему являются и недавние события в Киеве). И при наличии огромных людских масс в сочетании с доступностью Интернет и мобильной связи (программа всеобщей

[1] Beckhusen R. Putin's Arms Dealers Are Selling More Weapons to More Dirtbags Than Ever.// Wired magazine, 12.12.12. http://www.wired.com/dangerroom/2012/12/russia-exports/

интернетизации страны была завершена в Индии еще около десяти лет назад) последствия таких акций могут быть довольно серьезными.

Поэтому правительство Индии сейчас столкнулось с дилеммой выбора — как наиболее адекватным способом решить эту проблему. Дело в том, что для властей этой страны Интернет всегда являлся инструментом для организации лучшего управления, и его применение было сугубо техническим. Технократы, в частности, работали с электронным управлением e-governance. А тех сил, которые работают в области безопасности киберпространства, явно не хватает. Национальная организация по техническим исследованиям National Technical Research Organization, которая работает при советнике по национальной безопасности, имеет в своем штате всего 50 человек, занимающихся мониторингом медиа, и даже не имеет официальной лицензии в качестве мониторингового агентства.

А, по мнению экспертов Института оборонных исследований и анализа из Нью-Дели, цензура и другие подобные меры могут быть только временным решением. Следовательно, необходимо создать некую альтернативную модель[1].

И, конечно же, учесть разницу в подходах к киберпространству, где на одной стороне оказались США и их сателлиты, а на другой — Россия, Китай, Иран и другие страны, настаивающие на распространение суверенитета в киберпространстве. Так что, возможно, опыт Индии или коллективные решения (например, на очередном саммите БРИКС) в этом вопросе будут весьма кстати и затребованы в самое ближайшее время.

Киберконфликты и реакция США

Конечно же, киберпространство является одновременно средой для конфликта и его инструментом. Если классическая геополитика использует понятия могущества посредством моря (Sea Power) и могущества посредством суши (Land Power), а позже появилось могущество посредством воздуха и могущество посредством космоса, с недавнего времени заговорили и о новом домене — могуществе посредством киберпространства (Cyber Power). Военные США придают ему особое значение. Офицер ВВС США Роберт Ли указывает, что «кибермогущество будет такой же революционной для войны как и военно-воздушные силы, но текущая векторизация этой области будет определять, какая нация достигнет кибергосподства и с какой целью. На раннем этапе появления киберпространства Соединенные Штаты в первую очередь рассматривали кибермогущество как средство налаживания широких возможностей командования и управления через боевые зоны. Киберпространство сосредоточено на связи, да и оперативный успех зависел от

[1] Shruti Pandalai. Don't Shoot the Messenger: The 'Un-Social' Strategy. August 28, 2012.
[b]ttp://www.idsa.in/idsacomments/DontShoottheMessengerTheUnSocialStrategy_spandalai_280812

поддержания линий коммуникации. Так как эта область расширялась, она взяла на себя дополнительные роли по обеспечению поддержки сил традиционных военных операций, в то время как эксперты исследовали другие роли — это процесс, который произошел на самом высоком уровне

секретности. Многие из первых лидеров киберпространства поняли, что кибератаки предлагают ряд вариантов для атаки, защиты, и эксплуатации, которые никогда прежде не были возможны для военачальников. В очень взаимосвязанном мире, где существенные достижения в области технологии были обычным делом, возможности и оружие в киберпространстве стали еще более впечатляющими»[1].

Кибероперации могут быть проведены во всех областях ведения боевых действий: в воздухе, космосе, киберпространстве, на суше и море. Кроме того, несмотря на незрелость оперативных доктрин для киберпространства, доктрины для воздуха и космического пространства остаются актуальными и применимыми к сфере киберпространства. «Кибероперации — это просто еще один набор инструментов из арсенала командира».[2]

США первым создало Киберкомандование в 2010 г., хотя внимание этой новой сфере начали придавать и ранее. Например, в декабре 2005 кибероперации были включены в основное положение о службе и миссии ВВС США.[3] Китай, Иран и другие страны тоже поспешили обзавестись своими кибервойсками с соответствующими доктринами и стратегиями. Бюджеты на кибербезопасность также начинают стремительно увеличиваться. Руководство киберкомандования США в январе 2013 г. заявило, что штат этого рода войск будет увеличен в пять раз. Британия тоже спешит произвести апгрейд своих кибервозможностей, обосновывая это необходимостью безопасности сети, в связи с тем, что 6% ВВП Британии зарабатывается с помощью манипуляций, которые так или иначе связаны с Интернет.

Известный специалист по сетевым войнам Джон Аркилла пишет, что «подвиги кибервойн малого масштаба (Аркилла приводит в пример атаки на правительственные сайты Эстонии в 2007 г. и соответствующую инфраструктуру Грузии в августе 2008 г., приписывая данную инициативу российской стороне, а также инцидент с вирусом Stuxnet на иранских ядерных объектах — Л.С.) в конечном итоге могут достичь больших размеров, учитывая явные уязвимости передовых военных и различных систем связи, которые с каждым днем все больше охватыва-

[1] Robert M. Lee. The Interim Years of Cyberspace.// Air & Space Power Journal, January–February 2013, P. 58

[2] Eric D. Trias, Bryan M. Bell. Cyber This, Cyber That . . . So What?//Air & Space Power Journal. Spring 2010, P. 91.

[3] Hon. Michael W. Wynne, Flying and Fighting in Cyberspace, Air and Space Power Journal 21, no. 1, Spring 2007: 3, http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf

ют мир. Вот почему я думаю, что кибервойнам суждено сыграть более заметную роль в будущих войнах»[1].

Аркилла считает, что есть возможность выработать определенный код поведения, например, не применять кибератаки против исключительно гражданских объектов, по крайней мере, такая договоренность возможна между государствами. Некоторые теневые сети, т.е. радикальные политические группировки также могут следовать некоему кодексу. Второй тезис мало вероятен, так как в случае терроризма целью действий подобных групп является запугивание населения для достижения своих политических целей, и киберпространство представляет для этого хорошую возможность.

Поскольку кибермогущество может быстро и особым образом поражать сети и информационные системы по всему миру, размывая линию боевого сражения, эта особенность в сочетании с его разрушительной силой, порождает страх перед его возможностями среди населения - такой же сильный, как и от террористических атак[2]. Следовательно, недооценивать его силу влияния на общественное мнение и политику будет серьезной ошибкой. Даже если рассматривать исключительно военную сторону киберконфликтов, они сильно отличаются от войны на суше, море, в воздухе и космосе. «Свобода действий — это характеристика превосходства в киберпространстве... Приблизительным резюме для превосходства в киберпространстве может быть «свобода действий в течение атаки» (т.е. возможность действовать даже во время атаки и после нее)»[3].

Но есть и другая точка зрения, согласно которой, наоборот, кибервозможности применительно к конфликтам «смягчают» их природу и минимизируют ущерб как противника, так и затраты атакующей стороны. Профессор Военно-морской школы США Дороти Деннинг считает, что «если вы можете достичь того же эффекта с кибероружием вместо кинетического оружия, часто этот вариант этически предпочтительнее... Если операция нравственно оправданна, то кибер маршрут вероятно предпочтительнее, потому что он вызывает меньше вреда»[4]. К вопросу этики в киберпространстве можно отнести и применение беспилотных летательных аппаратов, что стало темой широкой дискуссии в США. Сторонники более массированного применения БПЛА в США указывают на три основных причины, из-за которых нужно развивать эту отрасль: 1) БПЛА смогут выполнять задачи, на которые не способны люди из психологических ограничений

[1] Arquilla J. Cyberwar Is Already Upon Us. MarchH/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

[2] Robert M. Lee. The Interim Years of Cyberspace.// Air & Space Power Journal, January–February 2013, P. 63.

[3] Eric D. Trias, Bryan M. Bell. Cyber This, Cyber That . . . So What?//Air & Space Power Journal. Spring 2010, P. 96-67.

[4] Kenneth Stewart. Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare. America's Navy, 6/4/2013 http://www.navy.mil/submit/display.asp?story_id=74613

(например, длительность проведения операций и экстремальные маневры); 2) сохранение жизни пилотов во время выполнения опасных миссий и снижение политического риска, который имеет случай быть, если пилот попадает в плен; 3) снижение затрат в связи с отказом от применения систем, необходимых для поддержания функций пилота (кислород, контроль климата, катапультируемое кресло и т.п.) и возможности применения дизайна отличного от того, который нужен для самолетов, предназначенных для эксплуатации вместе с командой на борту[1]. Есть тенденция, что беспилотники в будущем смогут заменить даже действующие стратегические бомбардировщики.

Другая часть считает, что применение дронов противоречит нормам международного права и приводит к огромному количеству жертв среди мирного населения.

В докладе New American Foundation указано, что за два года, в течение которых Обама был президентом, было произведено в четыре раза больше боевых вылетов БПЛА, чем за восемь лет президентства Дж. Буша. В данном отчете дается примерное количество убитых в Пакистане - от 1489 до 2297 (данные на апрель 2012 г.)[2].

В начале 2013 г. правозащитники привели следующую статистику убитых американскими дронами лиц:

Атаки дронов в Пакистане, которые подотчетны ЦРУ, 2004–2013 гг.:

- Всего: 362
- При Обаме: 310
- Убито всего: 2,629-3,461
- Среди них гражданских лиц: 475-891
- Среди них детей: 176
- Всего ранено: 1,267-1,431

Тайные операции США в Йемене 2002–2013:

- Всего подтвержденных операций: 54-64
- Всего подтвержденных применений дронов: 42-52
- Возможные дополнительные операции: 135-157
- Возможное дополнительное применение дронов: 77-93
- Убито всего: 374-1,112

Среди них гражданских лиц: 72-177

Среди них детей: 27-37

Тайные операции США в Сомали 2007–2013:

- Всего: 10-23

[1] Policy Options for Unmanned Aircraft Systems. A CBO Study. June 2011. Congress of U.S. Congressional Budget Office. P. 3.

[2] Masters, Jonathan. Targeted Killings.// CFR, April 25, 2012. http://www.cfr.org/counterterrorism/targeted-killings/p9627?cid=nlc-dailybrief-daily_news_brief-link14-20120426

Всего применений дронов: 3-9

- Убито всего: 58-170
- Среди них гражданских лиц: 11-57
- Среди них детей: 1-3

Бюро журналистских расследований на своем сайте также приводит интерактивные карты (можно сказать, что это своего рода кибер в квадрате - применение киберпространства для мониторинга киберактивности!), где отмечены места атак американских БПЛА и статистические данные, включая имена убитых граждан[1]. Показательным является тот факт, что сенатор Линдси Грэм в своем выступлении в феврале 2013 г. заявил, что число убитых американскими БПЛА лиц составляет 4700 человек, что примерно на 1000 человек больше, чем в докладе Совета по международным отношениям, посвященном БПЛА, который вышел месяцем ранее[2].

Применение БПЛА ширится — 13 января 2012 г. армия США издала директиву, согласно которой БПЛА будут использоваться внутри США для тренировочных миссий и «внутренних операций»[3].

Так или иначе, этот смертоносный интерфейс человека и машины наиболее наглядным образом показывает, куда могут завести кибервозможности в военных целях.

Впрочем, нужно отдавать отчет, что кибероружие как таковое не является чем-то новым, как некоторые себе представляют. Электронное подавление новейшей модификации применялось при атаке на инфраструктуру Ливии в 2011 г. и при налете израильских ВВС на научный объект в Сирии в 2007 г. Обнародованные документы Национального агентства безопасности США свидетельствуют, что кибератаки против компьютерных сетей других государств планировались еще в 2007 г.[4] Речь шла не об эксплуатации и защите, а именно об атаках!

Большое количество акторов, использующих киберпространство для своих целей также привносит некоторую путаницу для тех, кто пытается создать досье на киберактивистов в широком смысле этого слова. В 2009 г. подполковник армии США в отставке и бывший директор по безопасности цифровой продукции в Intel Дэвид Джонсон предложил реализовать шесть пунктов, которые бы могли помочь систематизировать всех акторов, действующих в киберпространстве и выработать общую стратегию, направленную на укрепление безопасности государства. Для этого необходимо:

[1] См. Interactive map. August 10th, 2011 http://www.thebureauinvestigates.com/2011/08/10/google-map/

[2] Ingersoll, Geoffrey. US Senator: 'We've Killed 4,700' People With Drones. Feb. 20, 2013, [h]ttp://www.businessinsider.com/graham-weve-killed-4700-people-with-drones-2013-2#ixzz2LZWjk8fW

[3] http://www.fas.org/irp/doddir/army/ad2012_02.

[4] Byrne M., Richelson J. When America Became a Cyberwarrior.// Foreign Policy, April 26, 2013 http://www.foreignpolicy.com/articles/2013/04/26/when_america_became_a_cyberwarrior_nsa_declassified

- Создание совместной стратегии по киберпространству, направленную на выявление общих интересов в родах войск, невоенных правительственных органов и партнеров из частного сектора, с учетом, что координации между этими группами не требует централизованной командной структуры, непригодной к проблемам кибербезопасности.
- Перспективная (а не ретроспективная) оценка рисков в области безопасности, которая, скорее всего, будет принята через пять, десять, или двадцать лет в будущем, такие вербовка, обучение и доктрина, которые могут быть согласованы с будущими потребностями.
- Разработка набора показателей для отслеживания и указания намерений и возможностей акторов в киберпространстве, а также для оценки внутренних (инсайдерских) рисков.
- Изучение социальной динамики в хакерском обществе, для того, чтобы иметь возможность влиять на ключевые отдельные лица или группы, которые активно воздействуют на общие мнения и обсуждения.
- Анализ топологии криминальных сетей, действующих в качестве специальных групп по развитию и рекрутировки, а также тактических групп и резервных сил для противоборствующих государств или негосударственных акторов с целью изоляции ключевых узлов, в том числе финансовых сетей, коммуникационных технологий, либо сайтов.
- Обзор слабых мест при нынешней подготовке в сфере безопасности военных кадров, федеральных государственных служащих и государственных подрядчиков, с тем, чтобы расширить осведомленность по технологии безопасности как неотъемлемой части своей работы и снизить риск социальных инженерных атак.[1]

Подобные рациональные предложения могли бы быть востребованы не только в США, хотя правительство этой страны уже адаптировало большое количество межведомственных инициатив и проектов для защиты киберпространства США, как общественного, так и частного. Только один Пентагон имеет около 15 тыс. сетей для обеспечения своей безопасности.

Но помимо национальной безопасности есть и глобальный уровень киберконфликта. На стратегическом уровне киберконфликт становится новым измерением межгосударственной войны. Усилия по противодействию и подготовке к такой конфронтации возложена на Киберкомандование США и Национальный совет по безопасности в Белом доме.

По мнению Роберта Мэннинга, «если употреблять несовершенную аналогию, стратегическая киберугроза имеет много общего с ядерными угрозами. Обе они построены на атаке, обе могут быть причиной огромного разрушения, которое

[1] David Johnson, Ian Crone. The Human Terrain of Cyberspace// Defense Concepts, Vol. 4, Ed. 3. Fall 2009. P.38

выведет из строя необходимую национальную инфраструктуру и нанесет ущерб или ослепит вооруженные силы, которые зависят от электроники»[1]. В США также появился нарратив «Электронный Перл-Харбор», который используют алармисты и паникеры для обоснования увеличения расходов в этой области.

Все эти факторы позволяют говорить о том, что геополитика как таковая обрела еще одну сферу — кибернетическую, на которую распространились ее основные аксиомы, но, вместе с тем, которая является реальностью другого уровня, где действуют новые правила.

[1] Robert A. Manning. ENVISIONING 2030: US Strategy for a Post-Western World. Atlantic Council. Washington DC, 2012, P. 56.

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.

Киберзащита — многосторонний политический вызов

Аннегрет Бенди, Катрин Алмер

сотрудники Немецкого института международной политики и безопасности.

Недавнее откровение бывшего сотрудника NSA Эдварда Сноудена привело к тому, что проблема кибербезопасности оказалась в центре общественного внимания. Как затрагивается эта тема в политике? Одного взгляда на последние сообщения международных журналов достаточно для того, чтобы понять, что под заголовками о кибербезопасности обсуждаются самые разные аспекты, такие как киберсдерживание в качестве средства борьбы с кибератаками, управление Интернетом или преимущества цифровой дипломатии в качестве профилактического инструмента для большей кибербезопасности. Технические статьи отражают различные аспекты новой политики в области внешней политики и политики безопасности. Дополнительную ценность этой молодой научной дискуссии придаёт то, что она вызывает множество вопросов, на которые должны ответить лица, принимающие решения в политике и экономике в связи с борьбой с киберрисками.

По крайней мере, откровение бывшего сотрудника NSA США, Эдварда Сноудена сделало модной тему кибербезопасности. Чтобы осветить эту тему с разных точек зрения, имеет смысл изучить исследования, связанные с этим вопросом. В отличие от средств массовой информации, в научной литературе сам термин «безопасность» является спорным. Когда дело доходит до кибербезопасности, то, по словам Густава Линдстрома, главы программы евроатлантической безопасности Женевского центра политики безопасности (GCSP), не хватает международных признанных определений для многих терминов, которые являются центральными в дебатах о киберпреступности, кибервойнах и кибертерроризме. Вопрос о том, какие условия должны выполняться для того, чтобы расценить кибератаки как вооружённое нападение в глазах международного права, остаётся без ответа так же, как вопрос о том, какими правами обладают жертвы подобного рода нападений. Кроме того, по словам Линдстрома, наблюдается тенденция наступательного использования кибертехнологий, которую тоже надо учитывать. Дискуссии о кибербезопасности должны быть сосредоточены на вопросе о соответствующих политических и правовых мерах, которые помогут ограничить использование кибероружия.

Навыки кибератаки были разработаны, по Линдстрому, и всё чаще становятся стратегическим инструментом межправительственного разрешения конфликтов. Кроме того, политическим деятелям придётся прийти к соглашению о модели управления Интернетом, будь то для поддержания текущего режима или для обеспечения большего регулирования, как в частности хотят Китай и Россия.

Можно так же почитать литературу по классификации кибертехнологий и их новизне в международных делах и политике безопасности, что предлагает Джеймс А. Льюис, старший научный сотрудник и директор по программе государственной политики и технологиям в Центре стратегических и международных исследований (CSIS), которую он написал для журнала по военно-стратегическим вопросам. Киберметоды используются спецслужбами начиная с 80-х гг., но военные кибератаки появляются только в 90-х гг.

Кибератаки используют новые пути и средства для насильственного исполнения интересов (принуждения) и шпионажа, но не относятся к новой категории конфликта. Было бы неправильным изображать вредоносные программы, такие как Stuxnet и Flame в качестве характеристик нового типа войны; эти атаки не настолько разрушительны, как сила ядерного оружия. Отнести Stuxnet к средству ведения войны даже сложнее международных переговоров, в которых предлагается заблокировать киберпространство.

Сложные киберметоды а ля Stuxnet в настоящее время используются только в Соединённых Штатах, Соединённом Королевстве, Израиле, России и Китае. Другие государства намерены использовать аналогичные возможности. До сих пор не удалось нанести урон с большими физическими повреждениями. Однако, есть сомнения, по Льюису, останется ли это так, если такие страны, как Иран и частные субъекты получат достаточно возможностей для совершения кибератаки. Льюис утверждает, что нужно поддерживать большой политический контекст с учётом сохранения возможности кибератак: он заметил, что откровения о шпионской программе Flame могли послужить тщательной переговорной позиции России в вопросах управления Интернетом и киберпространством.

Киберсдерживание на примере США

Мириам Данн Кэйвелти, начальник исследовательской группы Риски&Устойчивость в центре по исследованию проблем безопасности ETH в Цюрихе, в своей статье в международном журнале Studies Review проанализировал данные о том, как военная риторика берёт верх в связи с киберинцедентами, связанными с безопасностью. Кибербезопасность будет в основном рассматриваться как военная проблема, которая может быть решена военными действиями. Данн Кэйвелти ссылается на данный вопрос и призывает такие кажущиеся очевидными взаимосвязи всегда брать под сомнение.

Франк Киллуфо, директор Института политики внутренней безопасности (HSPI) и содиректор Кибер Центра Национальной и Экономической Безопасности (CCNES) университета им.Джорджа Вашингтона, Шэрон Кардаш, заместитель директора HSPI и Джордж Сэлмирэги, адвокат и консультант HSPI, напротив, уверены в этом. В газете Military and Strategic Affairs они представляют несколько ключевых моментов стратегии киберсдерживания США. Для защиты важных инфраструктур как, например, водоснабжения и электропитания, авторы рекомендуют Штатам разработать стратегию киберзащиты. Соединенные Штаты должны продемонстрировать руководство киберполитикой и следовать конкретному плану. Ключевые моменты американской гегемонии заключаются не только в том, что ее военные силы все больше расширяются и грозят нанести удар первыми, но и в том, чтобы фактически быть в состоянии отразить кибератаки военным способом. Для этого необходимо сохранять передовые позиции США в области науки и технологий. Цели и мотивы потенциальных противников должны оперативно идентифицироваться, чтобы суметь предпринять адекватные контрмеры. Несмотря на огромный технический прогресс и одновременно дефицит информации по отношению к преступникам, правительство США должно уметь противостоять их навыкам в использовании технологий. По мнению авторов, должны быть установлены жесткие стимулы для частного сектора, чтобы защитить важные стратегические инфраструктуры. Также, если это необходимо, возможна кооперация с международными союзами в области кибертехнологий.

Еще до заявления Эдварда Сноудена для программы мониторинга Prism американский журналист Джеймс Бэмфорд в журнале Wired Magazine критиковал нынешнюю киберполитику США. Бамфорд пишет о NSA уже многие десятилетия. Он определяет, как под руководством генерала Кейт Александра был расширен мониторинг интернет-программ, и как при этом, в зависимости от тех или иных последствий для общества, состоялась политическая дискуссия. Исходя из официальной позиции США, под кибербезопасностью, по мнению Бамфорда, подразумевается то, что Пентагон, несмотря на сокращения бюджетных расходов на 4,7 млрд. долларов для «операций в киберпространстве» к 2014 г., фактически подал заявку на 1 млрд. долларов больше, чем в прошлом году. Значительная доля киберорганизации под руководством генерала Александра будет запущена в работу. Должно финансироваться создание порядка 13 групп по кибератакам. Для правительства США созданы так называемые Zero-Day-Exploits, которые, попадая в «плохие руки», являются огромным пробелом в безопасности. Zero-Day-Exploit является, по мнению компании «Лаборатория Касперского», «вредоносным программным обеспечением, который одновременно обнаруживает ошибки, уязвимость приложения или системы, и с помощью которого данные действия можно использовать в других целях. У производителя не остается времени для предоставления Patch (исправления программного обеспечения) и IT-

администраторы не приходят к тому, чтобы своевременно задействовать другие защитные механизмы». Атаки, использующие уязвимость системы, будут как бы «ахиллесовым бизнесом безопасности», — как процитировал бывший разведчик Бамфорд. Соответственно, отсюда и вытекают высокие суммы, которые выплачивают заинтересованные стороны Zero-Day-Exploits и благодаря которым, по словам Бамфорда, выходит опасная и неконтролируемая гонка кибер-вооружений с собственным черным рынком.

Нормы регрессии и роль БРИКС.

Хотя некоторые эксперты по безопасности выступают за расширение государственных возможностей кибератаки, необходимо услышать и других ученых в области интернет-управления, которые заявляют о тенденциях к секьюритизации за счет гражданских свобод.

Данный факт констатировал Рональд Дж.Дайберт, директор Канадского центра по глобальным исследованиям в области безопасности и Citizen Lab в школе по политике безопасности Университета Торонто, и Масаши Крете-Нишибата, менеджер по исследованиям в Citizen Lab в своих статьях для газеты Global Governance, где представляют «нормы регрессии» глобального управления. Они являются тем, что большинство правил размещены таким образом, что ограничивают киберпространство как «открытое достояние свободной информации и коммуникации». Речь идет о том, что происходит развитие, направленное в сторону традиционных форм государственного контроля. К государственному традиционному контролю причисляются цензура, а также ограничения или прерывания интернет-доступа для того, чтобы предотвратить массовые беспорядки и протесты. Форумы, которые поощряли нормы контроля, определяют авторов из Международного Союза Электросвязи (ITU) или региональных организаций, таких как Шанхайская Организация Сотрудничества (ШОС). Упрощает государственную цензуру импорт и экспорт соответствующих технологий как для кибер-защиты, фильтрации коммерческой деятельности в интернете, так и для мониторинга или использования в определенных наступательных операциях.

Почему многостороннее сотрудничество достаточно трудно организовать и какую роль играют страны БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка) в сфере Интернет-управления и кибербезопасности, — об этом рассказывают Ганс Эберт и Тим Мауэр в издании Third World Quarterly. Страны БРИКС совместно противостоят политике США. Но, вместе с тем, у данных стран различные стратегии во внешней политике. Россия и Китай, в частности, склонны применять государственный контроль в Интернет-сообществе, и они были нацелены на создание правил международной координации через ITU. Обе страны стремились организовать международный Кодекс поведения в области

информационной безопасности. Индия, Бразилия и Южная Африка (IBSA), напротив, применяют «межправительственную» модель с целью нормотворчества Интернет-сообщества, для чего специально создаются международные организации, которые также включают в себя негосударственные заинтересованные стороны. IBSA-страны находятся на позиции, отрицающую интернет-цензуру и закрытые сети, позиционируя при этом себя в качестве «Swing States» по вопросам глобальной дискуссии. В данном контексте такое непоследовательное поведение стран БРИКС связано с тем, что в одних странах господствует демократия, в других — нет. По словам авторов, значительную роль здесь играют и другие факторы: во-первых, различный исторический опыт, во-вторых, мобилизация общества под воздействием СМИ, в-третьих, сопряжение между информационной безопасностью и дискуссией по правам человека и, в-четвертых, экономический подъем Китая, который предлагает возможность для развивающихся стран освободиться от зависимости США и разграничить свои интересы от интересов передовых держав. В качестве примера для четвертого пункта можно привести также совместное сотрудничество Индии с США или Бразилии с США под эгидой Интернет-управления и кибербезопасности.

Цифровая дипломатия.

Роль общественной дипломатии обсуждается Николасом Калл, профессором общественной дипломатии Университета Южной Калифорнии в Лос Анджелесе в своей статье для газеты International Studies Review. Он изображает то, как современные информационные и коммуникативные технологии были использованы в американской общественной дипломатии, описывает диалог с представителями третьих стран. Ответственный за это был с 1953 года до 1999 года Государственный департамент как высоко инновационное Информационное агентство США. Автор сетует о том, что информационно-технические средства используются не достаточно часто. Первые откровения Викиликс и переломы в арабском мире с декабря 2010 г. вызваны тем, что были усиленны информационно-технические возможности для ведения диалога по сравнению с тем, как они были использованы ранее. Дипломатия может быть активирована на цифровых форумах и далее с помощью индивидуально используемых каналов. «Общественная дипломатия 2.0» — это следствие идеи о горизонтальной Сети, что подразумевает под собой использование социальных Сетей и онлайн-сообществ.

Мариэте Шааке, нидерландский член-депутат европейской либерально-демократической партии в собственной статье для газеты Security and Human Rights идет еще дальше. Она поднимает значимость цифровой свободы так же основательно, как и значимость ответственности, которая «вырастает» из дипломатии Евросоюза. Арабская весна показала эффективность

современных информационно-коммуникативных технологий. Здесь находится Евросоюз — рычаг, открывающий доступ к демократизации.

По мнению автора, в эпоху информационных технологий европейская политика должна возобновляться с целью укрепления прав по защите человека. Дипломатия Евросоюза должна изменить свою политику, воспринимать собственную свободу и обходить стороной цензуру или предотвратить это путем экспорта технологий. Цифровая свобода подразумевает также традиционные права человека такие, как право на свободу слова и собраний. Шааке в своей статье пропагандирует ориентацию информационной внешней политики на права человека, которая имеет большое значение в сфере экономики частного сектора. Кроме того, информационная свобода ЕС должна вставать на защиту самой себя с тем, чтобы Союз заслуживал доверие и полностью отвечал собственным принципам. В отношении чего, как раз таки, Европа будет глубоко следить извне. Несмотря на это, Шааке видит в «оцифровке» риски, грозящие области политики безопасности и внешней политике. Тем не менее, информационно-коммуникативные технологии должны служить в условиях демократии соблюдению свободы прав человека.

Кибербезопасность оказывает огромное влияние на права и свободы, но у этого есть обратная сторона. Данные взаимоотношения довольно критически рассматривает Стивен С. Беннет в статье под заголовком «Право быть забытым» в Berkeley Journal of International Law. Права Интернет-пользователей заключаются в том, что определенная информация может ими контролироваться путем ее сохранения или уничтожения. Беннет обозначил те усилия и меры для защиты информации, которые предпринимала Европа начиная с 2000 года. К этому относятся правила, которыми должны оперировать и которые должны придерживаться все организации в ЕС. В США, напротив, право на свободу слова оценивается выше, чем защита данных. Сегодня экономика базируется на Интернет технологиях, что, по словам Беннет, является ключевой ролью в гармонизации международной политики по защите информации. В связи с последними событиями в США, происходившими с 2010 года, можно установить, что Соединенные Штаты вносят большую открытость по вопросам защиты данных, а также для проведения совместного диалога с ЕС. Этот диалог может быть значительно упрощен благодаря введению ЕС единого стандарта защиты данных, таким образом, оба партнера могли бы работать, по крайней мере, на минимальных стандартах. Несмотря на такого рода прогресс, остается вопрос о том, как обращаться с юридической стороны с существующими проблемами конфиденциальности информации. Особенно возникает неуверенность в том, насколько широко развита компетенция судов ЕС в отношении тех участников, которые действуют за пределами ЕС, но оказывают на нее влияние. Существование таких вопросов в безграничном киберпространстве оказывается традиционной концепцией юрисдикции, которая основана на суверенитете определенной территории. Хотя, по

мнению Беннета, быстрая разработка общих стандартов права является своего рода амбициозным проектом. Но, с другой стороны, это поможет расширить взаимопонимание и уменьшить правовую неопределенность, возникающую вследствие издержек и торговых барьеров.

Следующая тема: большие данные

«Большие данные могут дать представление о возможных событиях будущего», — рассказывает Кеннет Нейл Цукер и Виктор Майет Шонбергер в Foreign Affairs. Использование больших данных соотносится с идеей того, что сегодня они должны обрабатываться относительно недорогими и мощными компьютерами. Основная часть данных есть решающий фактор в определенных процессах.

В настоящее время практически все может быть отображено в данных, например, в данных GPS, которая функционирует на основе определения местоположения. Но то, почему большие данные, тем не менее, уходят на второй план, имеет свои причинно-следственные связи. Только с долей вероятности можно утверждать, что это могло бы способствовать, по мнению авторов, решению многих проблем человечества. Цукер и Майер Шонбергер приводят яркие примеры конструктивного использования больших данных, например, в медицине или предоставлении государственных услуг. Такого рода данные также могут быть полезны в борьбе с изменением климата. Разнообразные датчики, расположенные по всему миру могут обеспечить огромное количество данных, которые помогут разрешить проблему глобального потепления и более точно определить и изучить наиболее эффективные возможности изменить среду «вручную». Но огромные объемы данных, находящиеся, в частности, в руках недемократических государств могли бы, по словам авторов, привести к увеличению разрыва между гражданами и государством.

Кибербезопасность как новый политический вызов

В данной дискуссии необходимо также указать на то, что цифровая революция не только открывает возможности, но и создает значительные риски. Между странами уже фактически началась гонка вооружений в Интернете. Кроме того, Эдвард Сноуден, обладающий инсайдерской информацией британских и американских программ эпиднадзора, пришел к выводу о том, что для внешней политики и безопасности огромное значение имеют большие данные. «Вы должны знать врага, чтобы суметь победить его», — этот принцип, который сформулировал около 2,5 тысяч лет назад китайский военный стратег Сунь Цзы, имеет место быть и сегодня, в эпоху Интернет-технологий. Эффективные меры безопасности ИТ могут быть приняты только тогда, когда известно, какие методы и средства

злоумышленник использует, чтобы взломать компьютер своего противника. В то же время, можно отметить, что цифровая революция происходит по-разному. Таким образом, существует цифровой разрыв (digital divide) между странами ОЭСР и странами, не принадлежащими к ОЭСР. Это, в свою очередь, означает, что возможности распределены неравномерно к мировому доступу сети Интернет и к другим (цифровым) информационно-коммуникационным технологиям, и в значительной степени зависят от социальных факторов. Кибербезопасность подразумевает под собой также и человеческую безопасность. В связи с этим остается открытым вопрос о модернизации, создающей кибербезопасность или же новой дипломатии, которая сейчас входит в сцепление с цифровой революцией. Из положений, обсуждавшихся здесь, можно сделать вывод о том, что данная дискуссия только набирает обороты. Вопросы, рассматриваемые в статьях, наглядно иллюстрируют аспекты того, что кибербезопасность во многих областях политики играет большую роль, и что различные информационные технологии могут сильно изменить реальность. Таким образом, кибербезопасность является для европейской и международной внешней политики безопасностью с новыми вызовами.

Сдерживание и эскалация в междоменных операциях: где смыкаются космос и киберпространство?

Винсент Манзо

аналитик Центра стратегических исследований Института Национальных Стратегических Исследований Национального Университета Обороны США

Война стала еще более сложной с тех пор, как Ричард Смоук дал ей описание эскалации в 1977 г. Национальная Стратегия Космической Безопасности США описывает космос как «перегруженное, оспариваемое и конкурентоспособное пространство», пока спутники лежат в основе военной и экономической власти США. Деятельность в киберпространстве пронизывает каждый аспект человеческой деятельности, в том числе военные операции США, но перспективы эффективной киберзащиты не внушают оптимизма. Многие другие акторы тоже зависят от постоянного доступа в эти области, но не так сильно, как в Соединенных Штатах.

По этой причине некоторые аналитики утверждают, что Китай первым даст залп в конфликте с Соединенными Штатами, который будет разворачиваться в космосе и киберпространстве. В наихудшем случае по оценкам возможных сценариев можно сделать вывод, что такая атака может сделать Соединенные Штаты слепыми, глухими и немыми, и почти исключительно через некинетические средства, хотя неясно, насколько эффективны атаки в космосе и киберпространстве будут в реальном военном конфликте. Как такие понятия, как эскалация, сдерживание и пропорциональность применяются в таком контексте? Что за «случайные протуберанцы» могли бы создать противодействие в космосе и привести к эскалации кибератак? Что является критическим порогом для атак в междоменных операциях? И что именно означает междоменный? Эта статья исследует эти вопросы, используя иллюстративный пример гипотетического американо-китайского конфликта, потому что обе страны обладают различными стратегическими возможностями, которые охватывают воздух, землю, море, космос и киберпространство.

Определение междоменной зоны: платформы или эффекты?

Междомен - неоднозначный термин. Доктрина США идентифицирует землю, воздух и море как домены. Последние документы США в области политики и стратегии безопасности также признают космос и киберпространство как

домены.[1] Предполагая, что все пять являются стратегическими доменами, есть, по крайней мере, два различных способа действия, которые могут пересекать домены. Междомен может быть определен в соответствии с платформой, с которой актор начинает атаку и платформой, на которой находится цель. Уничтожение спутника с помощью противоспутниковой системы наземного базирования является междоменным, тогда как уничтожение его с орбитальной системы (например, маневренным спутником) таким не является. Удар по кораблю крылатой ракетой с воздуха представляет собой междоменное нападение, в то время как нападения на ту же цель крылатой ракетой с корабля — нет. Определение междомена по платформам показывает, что междоменные операции не новы. Воздушные атаки на военно-морские силы, военно-морские нападения на воздушные силы, а также атаки с обеих доменов на сухопутные войска широко распространены в современной войне. На самом деле, во многих случаях междоменная операция может быть просто наиболее целесообразным вариантом. Как, например, нация, атакуемая ракетами с кораблей, может иметь множество причин атаковать военно-морские активы противника быстрее самолетами, а не подводными лодками и надводными кораблями.

Это определение может быть слишком упрощенным. Большинство вооруженных сил США на суше, в воздухе и на море используют кибер и космические активы, и самые сложные миссии интегрируют участие нескольких доменов. Можно даже утверждать, что точность обычного удара является междоменной атакой, независимо от того, находится ли платформа атакующего и цель в одном и том же домене, если он использует спутники и компьютерные сети. По тем же соображениям, характеристика кибератаки (в противоположность кибер эксплуатации) против американских военных компьютерных сетей как однодоменной, вводит в заблуждение. В случае успеха такая атака будет иметь важные междоменные эффекты: это подорвет воздушные, наземные, или военно-морские силы, которые зависят от деградированных компьютерных сетей. Эти косвенные эффекты в других областях часто являются основной целью кибератак.[2] Та же логика применима к атаке с орбитальных противоспутниковых систем; даже если платформы находятся в той же области, то эффекты будут междоменными. Таким

[1] См. Department of Defense (DOD), Quadrennial Defense Review Report (Washington, DC: DOD, February 2010), 33–34, 37–39; The White House, National Security Strategy (Washington, DC: The White House, May 2010), 22; DOD, National Security Space Strategy (Washington, DC: DOD, January 2011); The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, [D]C: The White House, May 2011); DOD, Department of Defense Strategy for Operating in Cyberspace ([W]ashington, DC: DOD, July 2011).

[2] В докладе Национального исследовательского совета 2009 г. кибератаки определяются как умышленные действия, которые «изменяют, нарушают, деградируют или уничтожают компьютерные системы или сети или информацию и/или программы». См.: National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack CapabilitiesWashington, DC: National Academies Press, 2009, P. 80.

образом, междомен также может быть определен в соответствии с последствиями операции. Согласно этому подходу нападение является междоменным, если его последствия предназначены для разворачивания в другом домене, чем цель атаки. Это определение показывает, что отношения между доменами (нашим и нашего противника) создают стратегические уязвимости.[1] Например, обычные операции США по нанесению точных ударов зависят от доступа к нескольким доменам. Потенциальный противник мог бы оказаться неспособным уничтожить самолеты или атомные подводные лодки США, но он может быть в состоянии напасть на космические и кибер активы, которые позволяют этим платформам уничтожать цели. Эта логика, кажется, лежит в основе интересов Китая к контрпространству и кибератаке: такие нападения сдвигают конфликт в домены, где наступательные вооруженные силы Китая имеют преимущество перед обороной США, тем самым изменяя потенциал США в областях (например, воздушной и морской), где Китай мог бы быть поставлен в невыгодное положение.[2] Этот междоменный подход будет неэффективным, если воздушные, морские, и наземные силы США не будут зависеть в большой степени от космоса и кибератривов. Без этого связующего элемента Китай не смог бы перевести уязвимость США в космосе и киберпространстве в оперативное воздействие на другие области. Междоменные атаки, таким образом, позволяют актору наилучшим образом использовать свои сильные стороны и использовать уязвимости противника в некоторых случаях. Данные о том, что Соединенные Штаты осуществили кибератаки в начале операции НАТО в Ливии, предполагают, что американские военные также воспринимают междоменные атаки как полезные для эксплуатации уязвимостей противника.[3]

[1] См. Mark E. Redden and Michael P.Hughes, Global Commons and Domain Interrelationships: Time for a New Conceptual Framework? INSS Strategic Forum 259 (Washington, DC: National Defense University Press, October 2010).

[2] Дискуссии о военных возможностях Китая в космосе и киберпространстве см.: David C. Gompert and Phillip C. Saunders, The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability (Washington, DC: National Defense University Press, 2011), chapter 3; James Dobbins, David C. Gompert, David A. Shlapak, and Andrew Scobell, Conflict with China: Prospects, Consequences, and Strategies for Deterrence (Santa Monica, CA: RAND, 2011), 5–7; Office of the Secretary of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2010(Washington, DC: DOD, August 2010), 22–37; Jan Van Tol with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, AIRSEA Battle: A Point-of- Departure Operational Concept (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 17–47; Roger Cliff et al., Entering the Dragon's Lair: Chinese Anti-Access Strategies and their Implications for the United States (Santa Monica, CA: RAND, 2007), 51–60.

[3] Eric Schmitt and Thomas Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," The New York Times, October 18, 2011, and Ellen Nakashima, "Pentagon Officials Had Weighed Cyberattack on Gaddafi's Air Defenses," The Washington Post, October 18, 2011.

Междоменные операции и сдерживание

Эти определения подчеркивают тот факт, что военные акторы часто пересекают домены. В самом деле, американское военное устройство по своей сути междоменно: наступательное и оборонительное оружие США рассредоточено на воздушных, морских и сухопутных платформах; космос и кибератривы широко распространены и используются в операциях американских военных и создают преимущества в других доменах, и очень маловероятно, что будущие конфликты с США развернутся исключительно в пределах одного домена. С этой точки зрения сдерживание со стороны США по своей сути тоже междоменно: когда Соединенные Штаты угрожают отреагировать на действия, которые опасны для интересов США и их союзников, они угрожают, хотя это и неявно в большинстве случаев, междоменными ответами. Платформы, которые используют Соединенные Штаты, цели, подвергаемые атаке, и эффект от атаки могут быть в разных доменах и могут отличаться от доменов, которые используются и пострадали от первой атаки противника.

По той же логике Соединенные Штаты традиционно сдерживают атаки в целом, без различения между атаками, которые пересекают домены и тех, которые таковыми не являются. Военно-морские нападения на военно-морские силы не являются более или менее опасными, чем воздушные нападения на военно-морские силы. Соединенные Штаты пытаются сдержать оба вида, и средства, цель и масштабы реакции США будут зависеть от последствий нападения и целей США, а не доменов. Таким образом, Соединенные Штаты предостерегают от нападения, независимо от того, пересекает ли атака домены, угрожая ответом, который, скорее всего, будет междоменным, и будет отличаться от первой атаки. Учитывая, что между доменами сдерживание не является новым или редким явлением, реальный вопрос, который возникает в последнее время по теме, это: как Соединенные Штаты могут смягчить уязвимость, которая связана с зависимостью от космоса и киберпространства? Оба домена являются доминантными в деле нападения, где американская оборона неадекватна и политики не уверены в том, как эффективно угрожать возможному агрессору, чтобы он отказался от своих намерений. Хотя потенциальные противники менее зависят от космоса и киберпространства, чем Соединенные Штаты, это не объясняет, почему угрозы реагирования на кибератаки в других областях считаются менее надежными, чем междоменные ответы на атаку в воздухе, земле или на море.

Общая структура для оценки пропорциональности и эскалации в космосе и киберпространстве

Концепция Томаса Шеллинга, связанная с исследованием оружия и влияния, будет полезной отправной точкой для ответа на эти вопросы. Шеллинг утверж-

дал, что угрозы сдерживания являются более понятными для потенциальных противников и, таким образом, они более внушительны, если они являются соразмерными и связаны с действиями, которые предназначены для сдерживания: существует идиома в этом взаимодействии, тенденция использовать тот же язык, чтобы сделать наказание соответствующим характеру преступления … Это помогает оппоненту понять свою мотив, а также предоставляет ему основу для оценки ожидаемых последствий от его собственных действий … прямая связь между действиями и ответом помогает исключить возможность стечения обстоятельств и заставляет появиться другое следствие.[1]

Конечно, такое общение требует, чтобы страны интерпретировали военные действия и репрессии аналогично, другими словами, чтобы они общались через общую идиому действия. Шеллинг также признал, что нарушение шаблона поведения (то есть, эскалация) может быть необходимо в некоторых случаях, «чтобы вывести противника из равновесия для отображения ненадежности и дать возможность противнику реагировать естественно». Даже тогда, однако, общее понимание пределов, норм, и ожидаемых ответов создает необходимые рамки, с помощью которых акторы различают соразмерное и эскалационное поведение: «ломка правил является более драматичным, и больше сообщает о своем намерении именно потому, что это может рассматриваться как отказ от соблюдения правил».[2]

Идиома военных действий никогда не была такой последовательной, коммуникабельной и общепризнанной в реальности, как она описана у Шеллинга. Тем не менее, во времена Холодной войны эскалация была общепринятой от традиционных угроз до химического, биологического и ядерного оружия. В обычном конфликте было понимание того, что эскалация может произойти за счет расширения географической зоны боевых действий, расширение целей нападения (например, переход от узко военных к более широким, социальным целям), и увеличения интенсивности насилия (например, с помощью большего количества сбрасываемых бомб за вылет или переход к более разрушительным видам обычного оружия), характерные пороги отличаются в каждом обычном конфликта. К сожалению, страны не имеют общей базы для интерпретации того, чему кибератаки соответствуют в лестнице эскалации. Конкуренция и уязвимость в космосе и киберпространстве являются новыми по отношению к земле, воздуху и морю. Страны имеют меньше опыта ведения войны, где космос и киберпространство являются частью поля боя. В отличие от обычных и ядерных вооружений, эксперты менее уверены в точных последствиях нападений в этих доменах. По этим причинам, широко распространенных рамок для оценки того, как действия в космосе и кибератаки соответствуют и взаимодействуют с другими областями и, что

[1] Thomas C. Schelling, Arms and Influence. (New Haven: Yale University Press, 1966), 146–149.

[2] Ibid., 150–151.

более широко, с политическими отношениями между потенциальными противниками в мирное время, в условиях кризиса и на войне, еще не существует. Без этого лицам, принимающим решения, будет трудно отличать пропорциональные и эскалационные атаки, а также репрессии, которые переходят от традиционных стратегических доменов к этим новым, и наоборот. Отсутствие общей структуры внутри стратегического сообщества США усложняет эффективное междоменное планирование на случай чрезвычайных ситуаций. Разработка последовательных, эффективных и применимых вариантов реагирования на нападения в космосе и киберпространство требует, чтобы военные планировщики в разных службах и боевые команды обладали похожими предположениями о пропорциональности между доменами и эскалацией. Например, первый заместитель секретаря обороны по политике Джеймс Миллер показал, что США ответы на атаки в космосе «могут включать необходимость и пропорциональные ответы за пределами области космоса».[1] Но есть множество видов для нападения и еще более потенциальные мишени вне космоса. Общая основа будет способствовать планированию по определению, какие «некосмические» ответы лучше всего соответствуют атакам в космосе различного действия и тяжести. Отсутствие общей базы между Соединенными Штатами Америки, союзниками и потенциальными противниками подрывает сдерживание и увеличивает потенциал для просчета. Эффективное сдерживание требует, чтобы чиновники в США повлияли на восприятие потенциальных противников в отношении вероятных последствий от их действий, от которых США хотели бы их удержать. Соединенные Штаты могли бы угрожать ответом на нападения определенного типа в космосе или киберпространстве, используя различные возможности против различных целей в других областях. Такие угрозы, однако, имеют меньше шансов, чтобы резонировать как заслуживающие понимания потенциальными противниками, если они не воспринимают предположений США о том, как домены связаны между собой и почему тот или иной ответ является логичной и пропорциональной реакцией на первую атаку. В качестве примера, представьте, что Соединенные Штаты угрожают ответить на атаку на американские спутники разведки, наблюдения и рекогносцировки нападением на сети ПВО противника. Логика, лежащая в основе этой политики состоит в том, что Соединенные Штаты могут использовать самолеты разведки, наблюдения и рекогносцировки над территорией противника для компенсации утраченных спутников. Нападение на сеть ПВО будет необходимо для того, чтобы самолет мог эффективно проникать в воздушное пространство страны. Эта политика пропорциональна, потому что Соединенные Штаты восстанавливают утраченные возможности разведки, наблюдения и рекогносцировки, тем самым, отрицая преимущества атаки на спутники. Тем не менее, реакция

[1] James N. Miller, testimony for the House Armed Services Committee, Subcommittee on Strategic Forces, March 2, 2011.

США будет отличаться от нападения противника. Вместо ответа в космосе Соединенные Штаты будут атаковать цели на родине противника или вокруг нее. Чтобы еще более усложнить ситуацию, Соединенные Штаты могут использовать обычное оружие, чтобы уничтожить систему ПВО, даже если первая атака была некинетической. Без общего шаблона потенциальные противники могли бы рассмотреть такую угрозу сдерживания нелогичной и, следовательно, не заслуживающей доверия. Если сдерживание не удалось, они могут воспринимать такую реакцию США как произвольную и эскалационную. Даже с общим шаблоном они могут по-прежнему считать этот ответ как эскалацию войны, но они также будут понимать о вероятном последствии действий против Соединенных Штатов до отдачи приказа об атаке. Чтобы было ясно, общая база не будет, и не может прописать набор действий для всех мыслимых сценариев. Скорее, она должна определить универсальную лестницу эскалации, понятный по умолчанию или широко определенный кодекс поведения, который даст лицам, принимающим решения, лучшее чувство о том, какие действия и ответы ожидаются и приемлемы для сценариев реального мира, которые будут пересекать пороговые значения, нагнетающие обстановку. Это открыло бы путь для более когерентного междоменного планирования в правительстве США, а американское сдерживание воспринималось бы потенциальными противниками более ясно и понятно. Соединенные Штаты также будут лучше понимать исчисление потенциала противника в их усилиях по сдерживанию действий США. Культивирование такой общей базы является конструктивной целью на будущее, потому что сдерживание, регулирование кризисов и контроль эскалации были бы легче, если в разных странах пропорциональность, связность и эскалация интерпретировались бы аналогично. Привлечение стратегического сообщества США к тщательному диалогу по этим вопросам является первым шагом к достижению этой цели. Формирование рабочей группы по сдерживанию регионалистами, функционалистами и юристами может быть плодотворным подходом для запуска этого разговора.

Что может стать основой для оценки акций в космосе и кибератак в общем шаблоне? Должен ли ответ на кинетические атаки также быть кинетическим, чтобы он являлся пропорциональным? Является ли кинетический ответ на некинетические атаки всегда эскалацией? Может ли кибератака быть пропорциональна ракетному удару? Как чиновники сравнивают атаки, которые поражают цели в некоторых доменах и влияют на возможности и действия в других доменах? Космическая оборона и кибератаки могут значительно варьироваться по интенсивности, с эквивалентом того, как кладется рука на плечо и кулак бьет в лицо. Очевидно, что сам факт расширения конфликта в этих доменах является недостаточным показателем для оценки атак и калибровки ответов. Скорее, в реальном мире последствия таких атак, как внутри домена нападения, так и в

других доменах, должны определить, являются ли они эскалацией войны, и какие ответы были бы уместны.

Переменные в общем шаблоне

Культивирование общего шаблона между потенциальными противниками для оценки последствий и выработки соответствующих ответов будет трудным, независимо от количества участвующих доменов. Чиновники в США и других странах интерпретируют события через различные призмы. Культурные различия, контрастные стратегические цели, различия в структуре вооруженных сил и доктринах, различные сильные стороны и уязвимости могут привести лиц, принимающих решения в Соединенных Штатах и других странах, к различным выводам о пропорциональности и эскалации.[1] Эта задача не нова, но неопределенности в развивающихся стратегических доменах, обсужденные в предыдущих абзацах, могут усугубить ее. Представьте себе, что Китай столкнется с американскими спутниками через некинетические средства (лазером, который ослепит их, или с помощью заглушки) во время военного кризиса, который еще не перерос в вооруженный конфликт. Соединенные Штаты могут попытаться подорвать возможности Китая атаковать спутники США, возможно, отслеживания поток данных через кибератаки. Кто-то будет утверждать, что этот ответ пропорционален, потому что он ограничен в тех системах, которые использует Китай против Соединенных Штатов и не пересекает кинетический порог. С другой стороны, можно утверждать, что нападение в новом домене является эскалацией войны, открывая дверь репрессиям и контррепрессиям в киберпространстве и других доменах. Как китайские чиновники различают нападения на военные компьютерные сети от сетей, поддерживающих операции по внутренней безопасности режима? Если этого нет, то они могут интерпретировать этот «пропорциональный» ответ как экзистенциальное нападение, особенно, если они считают, что кибератака США вызовет побочный ущерб в более чем одной целевой компьютерной сети. Что делать, если изначальное нападение китайцев является кинетическим? Будут ли США, союзники и китайские чиновники воспринимать некинетический ответ против потенциала по космическим отслеживаниям Китая слабым, даже если он сумеет защитить спутники США? С другой стороны, была бы кинетическая атака на оружие Китая, которое он применяет, пропорциональной? Или пересечение географического порога (при условии, что цели находятся на материковой части Китая) сделают этот ответ эскалацией войны? Можно утверждать, что симметричный ответ — кинетическое нападение на китайский спутник –пропорционален. Однако, если спутники играют меньшую роль в китайских военных опе-

[1] Christopher P. Twomey, The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations (Ithaca: Cornell University Press, 2010).

рациях, можно также утверждать, что такой ответ менее чем пропорционален, потому что он не налагает сопоставимые эксплуатационные расходы на Китай.[1]

Баланс между нападением и защитой в этих доменах будет также влиять на восприятие эффектов, эскалацию, пропорциональность и оптимальные стратегии сдерживания. Например, если нападение продолжает доминировать в космосе и киберпространстве, а потенциальные противники хотят атаковать американские активы в этих доменах именно потому, что они являются «мягким подбрюшьем» американских военных, ставки США в любом конфликте будут расти в геометрической прогрессии после таких атак потому, что эффекты в других областях будут глубокими. В результате , американские официальные лица могут почувствовать давление, чтобы осуществить превентивное действие до такого нападения, или они могли бы пойти на риск, чтобы быстро прекратить конфликт и наказать противника последствиями. Связь между уязвимостями в космосе и киберпространстве, и эффективностью возможностей США в других областях делает американские спутники и компьютерные сети важными целями, что также делает угрозу сильных репрессий более правдоподобной: это было бы соразмерным последствием нападению. Передача этого послания потенциальным противникам будет центральным компонентом стратегии сдерживания. Подчеркивание такой связи, возможно, даже повысит доверие к приверженности США к ответным мерам. Кроме того, Соединенные Штаты могут достичь способности не допустить, чтобы противники имели преимущества в атаке в этих доменах, выстраивая кибероборону и предоставляя наземные средства для спутников. В этом случае стратегия сдерживания США будет стремиться убедить потенциальных противников в том, что они не смогут повлиять на сухопутные, воздушные, морские и ядерные силы США, атакуя спутники и компьютерные сети. Такое послание может сделать угрозы США на ответные действия непропорциональным и менее правдоподобными, но это будет компромиссом, если Соединенные Штаты разработают оборонительные преимущества в космосе и киберпространстве. Лица, принимающие решения, также воспринимают нападения в космосе и киберпространстве по-разному, в зависимости от контекста. Атака на военные спутники и компьютерные сети может быть отложена и начата только тогда, как только начнется обычная война. Но подобные атаки могут вызвать конвенциональный конфликт, если они происходят до военных действий, когда обе страны хотят предотвратить кризис от перерастания в войну, но обеспокоены остаться слепыми, глухими и немыми от первого удара в космосе и киберпространстве.

Пропорциональность и эскалация — это относительные понятия: действия, которые являются эскалацией войны во время кризисов, могут

[1] Этот пример показывает, что симметричные и асимметричные ответы на атаки в космосе и киберпространстве не являются синономичными пропорциональным и эскалационным ответам.

быть соразмерными в ограниченных войнах и снижать ответные меры, так как интенсивность конфликта выросла.

С этим связан вопрос, будет ли американская реакция на кибер эксплуатацию в мирное время влиять на сдерживания в период кризиса? Хотя технологии и операции по кибер эксплуатации и кибератаки похожи, цели и эффекты различны: эксплуатация связана с извлечением информации из компьютеров и сетей без соответствующего разрешения; а атака направлена на уничтожение, деградацию или их изменение для достижения эффектов в других доменах. Но новости часто описывают случаи кибер эксплуатации против правительства США в качестве кибератак и свидетельствуют о ведущейся войне в киберпространстве.[1] Соединение этих операций вместе способствует впечатлению, что сдерживание США уже не удалось. Потенциальные противники могут сделать вывод, что угрозы США в ответ на кибератаки в других областях не правдоподобны и зависит от того, как США отреагировали на предыдущие операции по эксплуатации. Это восприятие может повлиять на учет рисков и преимуществ кибератак в кризисных ситуациях. Как могут официальные лица США публично передать то, что кибер эксплуатация и нападения представляют различные угрозы и требуют различной реакции, особенно учитывая частичное совпадение между этими ними? Подчеркивая, что реальные последствия от атак и эксплуатации могут отличаться, это станет первым шагом на пути к установлению порога между ними. Это послание укрепило бы веру, что сдерживание не провалилось, потому что эффекты от эксплуатации в киберпространстве еще не гарантируют военных ударов США по другим доменам. Это уточняет типы действий, которые Соединенные Штаты пытаются сдерживать.

Некоторые стратеги могут заключить, что пропорциональные действия в космосе и киберответы невозможны, потому что контроль за эскалацией в этих доменах слишком сложен. Там есть «бесконечное число сценариев, которые не являются ни показателем инцидента нарушения, ни стратегического нападения» в космосе и киберпространстве.[2] Оценка последствий от таких атак и выбор соответствующих ответных мер на фоне стресса и путаницы военного кризиса могут быть трудными. Чиновники в США и других странах, скорее всего, будет иметь разные мнения по поводу последствий некинетических сбоев, что сведется к простым клише, а препятствование выработке общих рамок может быть слишком грозным. Кроме того, последствия от сложных атак на спутники и компьютерные сети могут быть неразборчивыми и слишком трудно предсказуемыми. В этом случае стратегия сдерживания может акцентировать, что ограниченные действия

[1] Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," Bloomberg Businessweek, July 20, 2011

[2] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," Air Force Space Command High Frontier 7, no. 1 (November 2010), 14.

в космосе и кибератаки несут невыносимый риск неправильного восприятия, просчета и непреднамеренной эскалации. Вызывая «угрозы, которые оставляют что-то на волю случая», официальные лица США могут реально утверждать, что они не уверены в том , что они будут делать, потому что такие нападения будет включать «процесс, который не предвидится… реакции, которые не полностью предсказуемы… решения , которые не являются полностью преднамеренными... события, которые не в полной мере под контролем».[1] Конечно, выражение беспокойства о непреднамеренной эскалации может иметь неприятные последствия. Противники могут заключить, что угрозы таких атак вынудят США пойти на уступки.

Вывод

Многие системы вооружений и большинство военных операций требуют доступа к нескольким доменам (земля, воздух, море, космос и киберпространство). Эти связи создают уязвимости, которые акторы могут использовать, запустив междоменные атаки; Соединенные Штаты могут попытаться удержать такие нападения, угрожая междоменными ответами. Тем не менее, поскольку правительство США и потенциальные противники не имеют общей базы для анализа того, как такие понятия, как пропорциональность, эскалация, достоверность и сдерживание применяются в космосе и киберпространстве, это позволит не только перейти к операциям в другой домен, но и стать частью поля боя. В реальном мире последствия атак, поражающих цели в космосе и киберпространстве, влияют на возможности и события в других доменах, и должны стать основой для оценки их последствий и определении того, какие ответы в различных доменах являются соразмерными или приводят к эскалации.

Интеграция действий в развивающихся стратегических доменах космоса и киберпространства с действиями в традиционных доменах на четкой эскалационной лестнице может стать первым шагом к более согласованному междоменному планированию в правительстве США. Связывание этих рамок с потенциальными противниками будет способствовать более эффективному сдерживанию и антикризисноему управлению.

[1] Schelling, 95.

Плавание в киберморе

Джеймс Ставридис

адмирал, командующий Европейского командования США и Верховный главнокомандующий ОВС НАТО в Европе.

Элтон С. Паркер III

военный помощник Вице-президента по академическим вопросам в Национальном Университете Обороны США.

Карьера в морской профессии приносит ясность в бурные и неопределенные воды морей и океанов. Чтобы успешно ориентироваться в этих водах, необходимо постоянное изучение, понимание и применение на международном уровне набора стандартов и норм, известных как правила дорожного движения. Есть «правила», которые применяются ко всем «глобальным уровням» — тому, что мы в Минобороны классифицировали как домены, а именно земля, море, воздух, космос и, соответственно, привыкли к их существованию и навигации в пределах границ, не нарушая установленные рамки.

Существует еще одна область, которая подвергается такой же классификации и определению. Она похожа на море в ее чистой величине, кажущейся вездесущности и смертельном потенциале, но она также уникальная в том, что не состоит из воды и волн; скорее, она состоит из нулей и единиц, оптических волокон и фотонов, маршрутизаторов и браузеров, спутников и серверов. Это, конечно, киберпространство, новое всеобщее достояние, среда, называемая у нас киберморем. В нем мы отправляемся в плавание каждый день в компании миллиардов других путешественников — многие начинают вояж с явно пересекающимися целями. Вместе мы включаем наши нетбуки и планшеты, берем наши смартфоны и используем обширный набор портов (и порталов) для подключения к остальному миру со скоростью мысли со всех видов различных судов, транспортных средств и ремесел.

Неограниченный потенциал

Киберморе является высшим выражением свободы, так как оно не может быть ограничено национальными или международными границами, нарисованными на любой карте или схеме, которые влияют лишь в редких случаях. Как и в дни фронтира в каждом новом домене, потенциал там безграничен, но

поскольку реалии человеческой экспансии, коммерции и взаимодействие обычно опережают политику и правила, как было во времена Дикого Запада и ранних мореходных экспедиций, преступное поведение изобилует, а потенциал для пиратства, нападений и конфликта всегда маячит за горизонтом. Чтобы подчеркнуть это, вспомним детство Интернета, когда он состоял только из несколько серверов и узлов, подключенных к устройствам, которые имели меньшую скорость вычислений и мощность, чем сегодняшние цифровые часы, так что было относительно легко регулировать движение. Но в начале 1990-х гг., однако, появились миллионы устройств, подключенных к сети Интернет, и в 2011 г. мы превзошли один миллиард устройств, связывающих нас по всему миру. Никогда раньше информационный обмен не был так легок и так потенциально разрушителен... И это только сегодня.

Эволюция завтрашнего дня обещает еще большую мобильность с помощью более быстрых, более компактных и более умных устройств. По мере роста, изменений и развития этого домена растет и наша зависимость от него. Мы продолжаем находить новые способы по обеспечению доступности, создаем новые формы человеческого взаимодействия, что делает нас ближе друг к другу, по крайней мере, виртуально. Будь то электронная почта, обмен мгновенными сообщениями, чат, твиттер, блоги, социальные сети, розничная продажа или взаимодействие в бизнесе, военные организации, члены правительства, неправительственные организации, частные и государственные предприятия каждый день плавают в диком киберморе.

В военной сфере, когда мы говорим о кибердомене, легко и соблазнительно свести обсуждение только к кибервойне или кибератаке. Хотя они являются важными элементами для разговора, сама тема гораздо шире, поэтому обсуждение дел также должно быть значительно шире. Мы живем во все более взаимосвязанном мире, конкурентном рынке, где основным товаром являются именно идеи, а цикл новостей 24/7 с почти мгновенной отчетностью широко распространяет истории. Это изобильный, бурный, и изнурительный рынок, и все мы должны продолжать конкурировать за нашу «долю» на этом рынке. В этом мире информация является властью, и эта власть увеличивается в геометрической прогрессии когда она совместна.

Мы должны принять традиционные формы обмена (интервью для прессы, газеты, печатные журналы и т. д.), а затем объединить их с новыми формами, такими как блоги, твиттер и размещения в Facebook. В качестве примера можно привести посты в Facebook и твиттер Верховного главнокомандующего ОВС НАТО в Европе, которых было около 13000, а блог Европейского командования США (USEUCOM) был просмотрен более 185 000 раз за последние два года. Но эти цифры бледнеют в сравнении с потенциалом соединений, который существует в этой еще огромной и дикой области. Например, Facebook превысил Google

в еженедельном трафике в Соединенных Штатах; Леди Гага и Джастин Бибер имеют больше последователей в Твиттер, чем все население Зимбабве, Кубы, Бельгии, Греции, Португалии или Швеция — там более 200 млн. общественных блогов.

Кроме того, радио понадобилось примерно 38 лет, чтобы достичь аудитории в 50 млн., телевизору — 13 лет, Интернет — 4 года, iPod — 3 года, в то время как Facebook добавил 200 миллионов пользователей менее чем за один год.

И, наконец, если бы Facebook был страной, то ее население было бы третьей в мире по величине, уступив только Китаю и Индии.

С каждым из этих потенциальных соединений мы выдумываем одну ссылку в цепи понимания — в конечном итоге укрепляя фундамент доверия жизненно важного значения по обмену идеями, общению, сотрудничеству и кооперации друг с другом. Тем не менее, несмотря на то, что прикладной характер социальных сетей очевиден, первоначальная трудность получения доступа к Facebook и другим социальным сетям через сеть правительства может быть обескураживающей и разочаровывающей. Мы должны делать это лучше. Мы должны быть подключенными более открыто. Использование социальных медиа является отличной идеей, которая растет в популярности, и может быть отличным инструментом для всех видов деятельности.

Размер аудитории может быть очень большим, а сообщения быстро распространяться. Мы должны иметь друзей в Facebook, иметь блоги и писать в твиттер. Нам нужны богатые каналы и подкасты с резюме сайтов (RSS), а также и LinkedIn. Эти и многие другие — это важные инструменты в создании ключевых и ценных стратегических связей для увеличения положительной корреляции между словами, делами и последствиями. Другим примером потенциала преимуществ и выгоды, связанных с подключением и расширением киберпространства можно найти в, пожалуй, одном из наименее вероятном для этого месте — Афганистане. В течение десятилетия или двух бумажные деньги больше не будут существовать, а электронные банковские и другие операции займут их место. Это будет способствовать дальнейшему подключению к нам способами, которые мы еще не начали ассимилировать в нашем обществе и наших культурных нормах — особенно в Соединенных Штатах. Как говорится, нужно следовать за деньгами. В процессе перестройки Афганистан может пропустить несетевые банковские операции, перейдя с бумажных денег прямо к операциям с мобильными телефонами и электронным вкладам. Подавляющее большинство афганских сил национальной безопасности в настоящее время получает зарплату электронными платежами и, после биометрической проверки, могут получить доступ к их деньгам через сотовые телефоны. Это уменьшает возможность для коррупции, исключая потоки бумажных денег и связанный с ним соблазн снять большие объемы

средств в процессе каждой передачи денег. Такой процесс позволяет афганцам использовать электронные носители по всей их стране.

Грозовые тучи на горизонте

Конечно, в то время как новые механизмы и технологии обеспечивают средства подключения и расширяют права и возможности следующего поколения, они также позволяют некоторым обеспечить свои каналы для распространения гнусных идеологий, для прозелитизма и участия в незаконной деятельности в этой значительной степени нерегулируемом виртуальном домене. Так как мы наблюдаем за погодой на горизонте киберморя, мы должны посмотреть на базовые технологии и их трансформационный эффект на нашу культуру, наши учреждения и нашу социальную ткань. Мы должны также выяснить, как все эти вещи связывают и взаимодействуют, чтобы умалить или усилить нашу коллективную безопасность. Каждый прилив приносит потенциальные проблемы в этой безопасности, что опасно игнорировать — кибер события могут охватывать весь диапазон от наблюдения на низшем уровне до DOS атак и разрушения инфраструктуры; от шпионажа и проникновений до реальных кинетических эффектов, от преступлений до войны. В любой день мы можем стать жертвой хакеров, кражи личных данных, а также «хактивистов». Наши системы бомбардируются ботнетами и вирусами. Троянские кони, черви, шпионские программы и спам продолжают существовать. Мы знаем, что эти угрозы реальны. Согласно профессионалам своего дела из Киберкомандования США, которое выполняет задачи Министерства обороны в области киберпространства, в среднем в день сети Пентагона подвергаются прощупыванию около 250000 раз в час; это внешняя разведка, пытающаяся взломать компьютеры США, и также террористы, ведущие активность на более 4000 веб-сайтах. В 2010 г. подрядчики Министерства обороны по киберзащите были атакованы, в результате чего более чем 24000 файлов и фрагментов данных было украдено.

Эти моря действительно штормит, и они так же неумолимы как в отношении отдельных людей, брошенных на произвол судьбы, так и предприятий, и даже национальных государств. Здесь, в Европе, этот вопрос имеет особый резонанс. В апреле 2007 г. три балтийские республики — Эстония, Латвия и Литва подвергались ряду DOS-атак, преимущественно пострадали серверы Эстонии и ее финансовая система. На следующий год Республика Грузия пережила не только кибератаку, но почти одновременное физическое нападение. Атаки сами по себе были вызывающими, хотя не являлись непреодолимыми. Что было труднее — так это приписать эти нападения и определить их происхождение. В то время как бомбы и ракеты, как правило, оставляют «отпечатки пальцев» и имеют обратный адрес, фотоны на волокнах сложно отслеживать. Как

заявил бывший заместитель министра обороны США Уильям Линн, «одно нажатие клавиши облетает дважды по всему миру в 300 миллисекунд, в то время как судебно-медицинская экспертиза, необходимая для идентификации злоумышленника, может занять несколько месяцев». Таким образом, не будучи в состоянии точно определить происхождение кибератаки для атрибуции, эта ситуация еще показывает и катастрофические последствия, которые могут быть достигнуты при объединении двух форм наступательной войны, укрепляя реальность киберпространства в качестве законной среды боевых действий. Эта атрибуция и усилия по судебному преследованию продолжают мешать, потому что в реальности нет согласованного определения того, что представляет собой кибератака и при этом в большинстве случаев нет физического результата нападения — воронок, затонувшего корабля или разрушения системы безопасности, в то время как целью являются, как правило, данные, последствия могут разниться от эксплуатации до деградации и разрушения, а поскольку данные не выглядят так же осязаемо, как некоторые другие, более традиционные типы целей, то и последствия могут выглядеть не так драматично. Долгосрочные эффекты, однако, могут быть более разрушительными и дорогостоящими, как в экономике, так и в человеческом капитале. Таким образом, потерпевшему от нападения оно является нападением, независимо от того, является это оружие бомбой или ботнетом. Аватары и иконки способствуют сохранению стерильной и неорганической среды, которая имеет тенденцию создать ложное чувство безопасности и отстраненности, но ранения, уничтожение и смерть могут быть вызваны довольно легко в эту эпоху «дот-боя». Конкретным примером этого может служить более быстрое и дальновидное использование киберпространства террористами. За последние 10 лет количество веб-сайтов, посвященных тому, что мы на Западе называем сайтами джихадистов-террористов, увеличилось в тысячу раз, и они используют свободу в Интернете в качестве форума для распространения своей пропаганды, привлечения средств и вербовки новообращенных. Джихадисты также используют Интернет как виртуальный класс, чтобы научить как делать бомбы и планировать нападения, в конечном счете, даже координируя и проведение атак через Интернет. В этом смысле для террористов Интернет стал недорогой сетью командования и управления по всему миру с неограниченным количеством узлов и отсутствием требований по обслуживанию или накладных расходов. Они имеют большой опыт по адаптированию широкого спектра инструментов для более полного использования отсутствия границ, политики, правил, а также анонимности в этом домене. Не сделайте ошибку — наши враги так же умны, как и хорошо финансируемы и, таким образом, инновации становятся улицей с двусторонним движением.

Балансировка открытого доступа и безопасности

Все это приводит к важному вопросу: как мы — индивидуально и коллективно — сбалансируем свободный и открытый доступ в такое виртуальное царство с необходимой защитой и правилами, обеспечив наш неизменный доступ к среде, которая является надежной, безопасной и способствует процветанию человечества в целом? Те же технологии, используемые обычными людьми для связи, сообщений и образования также используются теми, кто хочет вредить и разрушать. Существует напряженность в отношениях между этим желанием открытости и очень законным интересом по защите наших сетей и наших граждан. Будь то сдерживание угроз промышленного шпионажа, обеспечение избыточности системы в нашей интернет-зависимой инфраструктуре или улучшение судебных методов для проведения расследований и точного указания источника кибератаки, те, кто заинтересован в кибербезопасности, гонятся за теми же целями: максимальная защита конфиденциальной информации и одновременная возможность цельного соединения, функциональность и избыточность.

Найти правильный баланс, право установки на реостат, является ключевым фактором. Если мы хотим конкурировать на текущем рынке идей, если мы хотим, чтобы в полной мере пользоваться преимуществами достижений, таких как телемедицина, биометрия, отображение местности, виртуальное сотрудничество и невероятное множество разработанных и удобных для пользователей приложений, мы должны сделать это правильно. Мы должны защитить наши кибер сети в наших интересах, а не в ущерб нам. В вооруженных силах США сегодня мы боремся с этой дихотомией, даже на самом высоком уровне. Можно процитировать бывшего вице-председателя из Объединенного комитета начальников штабов генерала Джеймса Картрайта, сказавшего, что «мы не можем позволить командной цепи разорвать цепь информации». Для обеспечения непрерывного потока информации традиционные соединения (которые некоторые могут отнести к передовому опыту), которые препятствуют перекрестным потокам идей, должны быть разбиты. Нам необходимо разработать политику осмысленной, сконструировать и построить инновационные технологии, а в противном случае информировать об обсуждении для того, чтобы преодолеть пробелы «потребности — технология — политика». Мы видели позитивный потенциал этой среды в действии — будь то в джунглях Колумбии, на улицах Тегерана или на площади Тахир в центре Каира, а совсем недавно в Ливии и Сирии. В каждом случае активисты и технически подкованные сочувствующие объединили силы, используя подключение и потенциал кибердомена для получения результата, который Эрик Шмидт и Джаред Коэн чудесно охарактеризовали как ситуацию, когда «революция станет подкастом» с «политическими «флэш-мобами», о которых будут писать, отсылать твиты

и разрабатывать законопроект о правам человека для века Интернета». Как те, кто любит свободу слова, печати, вероисповедания, собраний и политического самоопределения, могут засвидетельствовать, поиск баланса между расширением прав и возможностей обездоленных без несправедливости может и будет трудным и непростым, и огромное количество пользователей — один миллиард, который растет, только усугубляет проблему.

Если мы собираемся успешно существовать в этом домене, нам нужно сделать так, чтобы вместе сочетать военный и гражданский, иностранный и отечественный, а также государственный и частный секторы. Каждая нация имеет свой собственный суверенитет, правоохранительные органы, подход к конфиденциальности, системы и нравы, а также сети и технологии. Однако в киберпространстве, возможно, больше, чем в любом другом домене, который мы привыкли эксплуатировать, коллективное целое действительно больше, чем сумма всех нас, работающих индивидуально. Как и в большинстве начинаний, слова имеют значение — таксономия важна. Таким образом, первый шаг — это согласование набора определений, формулирование круга полномочий, а также создание общей лексики. По большей части, это уже существует в военно-технологическом мире, но на самом деле это не выходит за рамки этого коллектива. Поскольку мы продолжаем бороться за установление физических границ киберпространства, мы должны определить что является и не является кибератакой. Это преступная деятельность? Шпионаж? Кибервойна? Враждебные намерения? Затем мы должны определить и согласовать, что следует предпринять, и что оправдано в каждой конкретной ситуации, на основе возможных, все еще неписаных законов, которые управляют действиями в этом диком море, как во времена войны, так и мира. Это, правда, очень милитаристские термины, однако, действия в этом домене во главе с военными будут проходить не часто, поэтому мы должны обеспечить наше межведомственное экспертное сообщество, а также профессионалов со стороны промышленности, которые связаны с этой дискуссией с самого начала. В НАТО они были. В результате на нашем жаргоне мы начали создавать то, что мы называем «правилами участия», правила, которые все 28 стран — членов альянса понимают, и на которые они согласны.

Киберакции НАТО

В середине ноября 2010 г. лидеры 28 государств — членов НАТО собрались в Лиссабоне на саммит. Одним из основных результатов этой успешной встречи стала новая стратегическая концепция НАТО, а одним из главных направлений этого основополагающего документа — как альянс смотрит в будущее — был кибердомен. Лиссабонский саммит постановил разработать или пересмотреть кибероборонную политику НАТО к середине лета, а также осуществить необхо-

димые сопровождающие действия и реализовать план. В июне 2011 г., выполняя задачи Лиссабона, политическая структура, ответственная за принятие решений в НАТО –Североатлантический Совет — принята новую политику НАТО по кибер обороне в сочетании с Планом действий. Работа с нашими союзниками и извлеченные уроки из таких событий, как кибератака в 2007 г. на Эстонию, привела к новой политике НАТО, сфокусированной на улучшении скоординированного многонационального подхода и укреплении наших коллективных и индивидуальных способностей по киберзащите для предотвращения угроз и улучшения наших ответов. В 2003 г. НАТО основала общий Центр по передовой киберзащите в столице Эстонии Таллинне. Он был аккредитован в качестве центра передового опыта НАТО в 2008 г. Это международная организация, которая занимается образованием, консультациями, научными исследованиями и разработкой в сфере кибербезопасности. Миссией центра является расширение возможностей, сотрудничество и обмен информацией между странами НАТО и партнерами по киберзащите. Кроме того, центр недавно установил важные и формальные отношения с Symantec Corporation для содействия сотрудничеству по исследованию Интернет угроз и контрмер. Сотрудничество между этими двумя организациями помогает этому центру в дальнейшем исследовать новые идеи, чтобы наилучшим образом понимать, оперировать и осуществлять навигацию в еще бесконтрольном и неуправляемом пространстве этого домена.

Мы также создали в НАТО структуру по реагированию на компьютерные инциденты (CIRC), которая получила мандат на высшем уровне по расширению возможностей и потенциала для выявления, оценки, предупреждения, защиты и восстановления от кибератак. Этот центр стал полностью готовым к работе в 2012 г., и это является важным шагом в расширении функции для поддержки кибер предупреждений и оценки ущерба как части единой структуры комплексного кризисного управления.

Кроме того, поскольку, как представляется все более очевидным, что кибер будет играть важную роль в любом будущем кризисе, нам нужно интегрировать систему кибер предупреждения в наше планирование и, возможно, разработать способы по оценки ущерба от кибератак, а также иметь возможность определять как кибератаки согласуются с использованием других инструментов власти (дипломатических, военных , экономических и др.) в условиях кризиса. Таким образом, мы создали ячейку по кибероборонe в рамках нашего нового кризисного центра управления операциями, который будет включать в себя возможности укрепления национальной и международной поддержки кибер знания в общей системе предупреждения, оценки и кризисного реагирования.

Если НАТО подвергается нападению, CIRC обеспечит техническую защиту и надлежащую реакцию, в сочетании с советом по киберуправлению, который единственный несет ответственность за координацию киберзащиты всего

Альянса через серию меморандумов о взаимопонимании между организацией по кибероборонe каждой страны и советом. Если индивидуальный союзник подвергается нападению, то все обстоит немного сложнее, особенно когда дело доходит до коллективной обороны. Понимание всего этого в контексте оригинального Вашингтонского соглашения, подписанного в ходе совсем другого времени в 1949 г., является первостепенным. Статья 5 договора НАТО, действительно, является сердцем соглашения — она гласит, что нападение на одного члена рассматривается нападением на всех. Статья 6 этого договора определяет, что является вооруженной атакой, сосредоточив внимание на географии, нападении на территорию, корабли в море, атаки на воздушные суда, войска и тому подобное. В 1949 г., однако, немногие, если таковые имеются, могли бы подумать об этом новом кибермире. В результате, в рамках НАТО в частности, мы должны определить, что такое нападение. Изменяется ли оно от одного члена Альянса к другому? Опять же, у каждой нации имеется свой собственный суверенитет, свои законы, свои правоохранительные органы и свой собственный подход к конфиденциальности и безопасности. Как союзники будут реагировать на кибер события существенной величины или какой набор мер союзники одобрят в ответ на кибератаку — это решения, которые должны сделать отдельные страны. Тем не менее, новая киберполитика НАТО довольно четко показывает, что любое решение по коллективному ответу (применение статьи 5) будет политическим, которое примут высокопоставленные политики из Альянса и стран-членов, а не военные или технические группы реагирования. Следует отметить, что единственный раз, когда НАТО сослалась на статью 5 — это было 12 сентября 2001 г., после террористических атак 9/11 на США.

Сотрудничество в более широком контексте

Этот новый и неоспоримый аспект военных действий, скорее всего, проявится больше как методология войны, которая продолжает развиваться. Нам нужно понять это новое кибер измерение ведения войны и как с ним бороться, мы должны вступить в схватку с понятием, что военное вмешательство в этой области является всего лишь небольшой частью головоломки. В Соединенных Штатах Министерству внутренней безопасности, очевидно, правильно отведена ведущая роль в этом стремлении. Минобороны является лишь одним членом команды, и мы во многом предназначены для поддержки членов другого межведомственного сообщества. Таким образом, мы должны продолжать пытаться понять кибербезопасность в большем межведомственном контексте, возможно, извлекая уроки из другого комплексного подхода, применяющегося для транснациональных и межведомственных вызовов, связанных с незаконным оборотом.

Нам удалось наладить и укрепить выдающееся межведомственное и международное сотрудничество в Объединенной межведомственной Целевой группе «Юг» в Ки-Уэст, штат Флорида, а также в аналогичной организации под названием Объединенный Межведомственный Центр по противодействию незаконному обороту, здесь, в Европе. Эти потенциальные модели, которые могут применяться в мире кибербезопасности, возможно, в форме совместной межведомственной целевой группы, в идеале включая правоохранительные органы международного права и другие элементы с ростом и развитием организации. Наконец, хотя правительство несет большую ответственность за обеспечение механизмов обеспечения наших интересов в киберпространстве, кибербезопасность, как говорят моряки, — это «все руки на палубе» эволюции. Хотя есть время от времени сильные перекрестные потоки между тем, что мы традиционно рассматриваем в роли национального органа и роли государственно-частных предприятий один на один с нашей всеобъемлющей безопасностью, мы должны привлечь опытных профессионалов в промышленности и в международных организациях. Лучшие практики уже распределены между многими экспертами по кибербезопасности в форумах по всему миру. Тем не менее, общий недостаток доверия между различными игроками (включая корпорации, правительственные структуры, и даже сами народы) исключает ускоренный роста наших возможностей по киберзащите. Нам нужно прекратить эти подозрения и работать вместе в направлении наших общих целей — это явно в наших общих жизненно важных национальных интересах.

Если корпорации инвестируют реальную энергию в обмен по развитию кибер возможностей, будь то в форме человеческого капитала, инвестиций или фактического аппаратного и программного обеспечения — нам необходимо обеспечить ясные стимулы. Какие преимущества существуют для промышленности, чтобы участвовать в этом процессе? Как будет такое сотрудничество и взаимодействие повышать их относительную конкурентоспособность, имидж и увеличивать их показатели? Мы обнаружили, что НАТО может играть ключевую роль в координации деятельности, а также создании правильных стимулов для участия. Одним из способов является подчеркивание участия таких компаний, путем внесения их в каталог доверенных фирм, способных предложить услуги по безопасности и соответствующие компоненты. Основным условием для включения в такой список будет приверженность и вклад в развивающийся обмен информацией. И есть другие способы. Кибер военные эксперты НАТО полагаются в большой степени на партнерскую форму через всех наших союзников, как в военной, так и в гражданской сфере. Все чаще мы находим, что нам необходимо развивать и использовать вклады со стороны частного сектора, так как промышленность будет абсолютно необходима, поскольку мы продвигаемся вперед. Это также то место,

где находится основная часть неограниченного инновационного мышления. Мы недавно провели конференцию в штаб-квартире НАТО при участии корпораций, ученых, военных, а также большого числа чиновников из многих стран, чтобы изучить эти связи между государственным и частным сектором, и как лучше интегрировать их в более крупный комплексный подход в области киберпространства. Многие замечательные выступления дали путь некоторым выдающимся инициативам, которые мы будем осуществлять в ближайшие недели и месяцы. Такие конференции будет регулярно проводиться, поскольку мы начинаем, чтобы закладывать основу для долгосрочного сотрудничества и кооперации.

Минобороны уже начало исследовать, как промышленность может помочь в этом отношении через государственно-частное партнерство, названное Несокрушимая Структура Безопасности. В соответствии с этим соглашением, исполнительный директор и главные офицеры по технологии основных информационных технологий (ИТ) в настоящее время периодически встречаются с высокопоставленными должностными лицами как в Минобороне и Министерстве внутренней безопасности, так и с директором Национальной разведки. В НАТО мы начали разговоры с целью рассмотрения создания похожей структуры, в которой ключевые европейские агентства, предприятия и правительства будут отобраны для участия в обмене информацией по кибербезопасности. Это информационное сотрудничество будет включать в себя все, начиная от угроз отказа до политических дебатов, исследований и инициатив в области развития. Эта последняя категория обеспечит потенциально большую отдачу от инвестиций, поскольку мы стремимся уровнять цикл оборонной промышленности и ИТ (который колеблется между 7 и 8 годами) и цикл технологического развития (что в среднем составляет от 1 до 2 лет — всего 24 месяца для разработки iPhone, например). Как выразился заместитель секретаря Линн, «это меньше времени, чем у нас есть для подготовки и защиты бюджета, а затем получения одобрения Конгресса, чем у [Apple] для получения iPhone. Это не приемлемый обмен».

Новое мышление

В контексте безопасности, развязывание мощностей киберморя изменило все, кроме нашего образа мышления. Мы просто не можем решать новые задачи, используя старые процессы мышления. Мы должны постоянно развиваться. И мы должны продолжить тестирование наших теорий и доктрин с объединенными, межведомственными и международными учениями и моделированиями. Агентство Перспективных Исследований Министерства обороны (DARPA) создает «макет Интернета», полигон по обучению моделирования, на котором мы смо-

жем проверить меры безопасности, ответы на атаки и как лучше интегрировать различные возможности и потенциал каждого игрока.

В 2010 году Министерство внутренней безопасности провело маневры по внутренней безопасности Cyber Storm 3. Они включали в себя федеральные и государственные структуры, частный сектор и международные организации, все работали вместе, чтобы оценить сильные и слабые стороны текущей политики, тактики, процедур и возможностей. Нам нужно продолжать проведение таких нелицеприятных оценок и тестов. Через них мы учимся, что не можем позволить себе ограничить наш собственный доступ к ценной информации, чтобы защитить себя от потенциально вредной деятельности. Скорее, мы должны быть технически подвижными и политически достаточно смелыми, чтобы опередить тех, кто стремится сделать вред в кибер-пространстве. Это маневренная война в кибер масштабе, и мы должны быть быстрыми. Кроме того, в сентябре 2011 г. Европейское командование США провело мероприятие под названием Combined Endeavor — учения по связи и компьютерным сетям, в которых приняли участие международные военные, тезничнеские и академические специалисты из 28 стран для того, чтобы сотрудничать и улучшить партнерские отношения с конечной целью укрепления коллективных возможностей киберзащиты. Темой маневров в этом году было «Информационное Доминирование Коалиции», а заседания были посвящены совершенствованию международной киберзащиты, практически осуществляя кибер информационный обмен, и институционализируя коалиционное киберобучение. Точно так же, в декабре НАТО провели свои основные ежегодные киберучения Cyber Coalition 2011. Более 100 специалистов приняли участие в учениях по кибер-обороне в штаб-квартирах НАТО в Брюсселе и Монсе, в том числе на национальных кибероборонных объектах в странах все собрались вместе, чтобы проверить технические и оперативные возможности Альянса по киберзащите. В обоих учениях были разработаны сценарии, требующие решения, координации и сотрудничества с техническими экспертами, политиками, а также органами управления. Оба были весьма успешными мероприятиями, и мы много узнали. Мы узнали, что мы сталкиваемся с общим вызовом и, таким образом, через открытое общение и сотрудничество, мы будем строить доверие между нашими странами. Самое главное, мы подчеркнули тот факт, что, хотя это невероятно сложная вещь для реализации, интернационализация кибербезопасности абсолютно возможна. Это также абсолютно необходимо.

Эта статья началась с аналогичной ссылки на киберморе. Как мы связаны в кибермире интересно сравнить с морской областью, особенно в контексте проблем, с которыми человечество сталкивается в результате действий неприрученных океанов. Человечество две или три тысячи лет училось работать на море, у нас постепенно создавалось международное морское право, система буев, глобальная навигационная сеть и карты по указанию пути. В целом, мы создали систему. И

в 1980-х гг. международное сообщество собралось на крупнейших переговорах в истории человечества и создало Конвенцию Организации Объединенных Наций о морском праве. Потребовалось целое десятилетие, чтобы вести переговоры. Документ в более чем 200 страниц, это чрезвычайно сложный канон, но за редким исключением, для 195 суверенных подписавшихся государств это руководство для действия в море.

Теперь подобное обязательство назрело и относительно киберморя. Мы плыли в этом пространстве всерьез в течение примерно 20 лет, и реально создавали волны последние 10 лет. Тем не менее, по большей части, мы до сих пор не имеем надежных буев, мы до сих пор не имеем навигационной сетки, и мы все еще плаваем без современных карт. Мы не можем даже сказать, что у нас есть основные нормы поведения, ограничиваясь несколько очень конкретными карательными законами за самые вопиющие акты. Что еще более важно, мы не имеем тысячелетия, чтобы понять это. Нам не хватает времени. Наш министр обороны недавно прокомментировал, что «существует сильная вероятность того, что следующий Перл-Харбор, с которым мы столкнемся, вполне может быть кибератакой». С каждой миллисекундой этот ширящийся посредник растет в уязвимости быстрее, чем он растет в полезности, а институциональные правила и политика ползут где-то сзади.

Нам нужно догнать и, в конечном итоге, выйти на гребень этой основной волны. Мы должны согласиться на конкретный круг терминов, таких как «атака» и «инцидент» и что составляет каждый из них. Мы должны согласиться на политические рецепты, которые диктуют пропорциональность ответа, преследуя нападающих сквозь национальные границы, будь это географическая или виртуальная сеть линий и что-то еще. В 2011 г. киберстратегии Белого дома и Пентагона прошли долгий путь к каждой из этих целей, так же как и новая киберполитика НАТО, но мы должны подтолкнуть эти усилия дальше.

И мы должны делать это совместно: внутри и между правительствами и их учреждениями, внутри и между государственным и частным секторами, во всех академических институтах, и в наших общих домах. Кибербезопасность требует сложных и скоординированных ответов, которые двигаются со скоростью мысли. Разнообразие способностей, возможностей, и ответы на любые кибер задачи должны рассматриваться как сила, а не слабость, но только если действия и инструменты могут быть использованы синергетически. Это может быть только в том случае, когда все заинтересованные стороны принимают общее видение безопасности, построенное на основе доверия и конфиденциальности, и достигается за счет координации, сотрудничества, и партнерства. Ни один из нас так не силен, как все из нас, работающие вместе.

Цифровые дипломаты Косово

Филип Бойс

журналист издания Foreign Policy

Как вы нарисуете нацию на карте мира? На протяжении веков государственность достигалась пролитой кровью на поле боя или махинациями между дипломатами в прокуренных помещениях. Но молодые государства считают это только половиной истории: Стать признанным на мировой арене — значит не только получить право голоса в Организации Объединенных Наций — это еще и победа над интернет-гигантами, такими как Google и Facebook.

Цифровая дипломатия, с помощью которой дипломаты общаются с гражданами, союзниками и даже соперниками онлайн для обсуждения и разработки политики и реакции на события, является относительно новым понятием — и она меняет традиционные, часто иерархические структуры органов власти. Соединенные Штаты были одной из первых стран, которая взяла на вооружение эту идею: Интернет искусство государственного управления было впервые запущено во время работы Хиллари Клинтон в качестве госсекретаря, Алека Росса, старшего советника Клинтон по инновациям, и Джаред Коэн, члена ее персонала по политическому планированию. По данным Института Брукингса, Государственный департамент США в настоящее время имеет более 150 штатных цифровых дипломатов. Великобритания и другие страны ЕС последовали этому примеру. И даже Иран отправил президента Хасана Роухани в Twitter.

Но сегодня это действительно малые народы, особенно новые, борющиеся за внимание, те, кто начинает лучше использовать Интернет в своих интересах. И Косово направляет нетерпеливых и находчивых молодых людей, которые уже определяют то, что может означать цифровая дипломатия, на этот путь.

Для Косово, безусловно, есть много направлений для борьбы. Через пять лет после провозглашения в одностороннем порядке независимости от Сербии и признании со стороны 106 членов ООН, Косово все еще сражается за признание со стороны России, Китая, Индии и многих других влиятельных стран, некоторые из которых борются с собственными сепаратистскими регионами.

Цифровая дипломатия может помочь делу Косово, связывая дипломатических должностных лиц и граждан страны с единомышленниками в других государствах, которые могли бы, в свою очередь, оказать давление на свои правительства, чтобы они признали новейшее балканское государство.

Но есть дополнительный уровень в цифровой дипломатии Косово: страна игнорируются такими компаниями, как Amazon, eBay , Google , Skype и Yahoo,

которые не признают Косово в качестве независимого государства на своих сайтах. Тысячи других, менее известных международных веб-сайтов, порталов и социальных медиа-платформ также не включили Косово в качестве страны в их открывающихся меню пользователей, среди прочего, в сервисе, где пользователи могут определить свое местоположение и ввести действительные почтовые адреса.

Широкое отсутствие онлайн признания ежедневно обременяет средних косоваров. Например, вы хотите заказать книгу на Amazon с доставкой ее в ваш дом в Приштине, столице Косово? Но так как Amazon не признает Косово в качестве независимого государства, нужно поставить «Албания» в качестве страны проживания , а затем написать «Косово Косово Косово» в дополнительном поле для комментариев, просто чтобы указать, что вы на самом деле не живете в Албании. И даже тогда, заказы, в конечном счете, исчезают в бюрократических ямах. Подобные головные боли будут и с другими интернет-компаниями.

Куштрим Ксхатли хочет изменить такое положение дел. Достижение цифрового признания, как говорит молодой косовский предприниматель, это «достоинство и право, которое само собой разумеется людьми во всем мире». Бывший советник министра образования Косово, Ксхакли уже начал кампанию, целью которой является подготовка цифровых послов целого поколения косоваров. Свыше 70 % населения страны в два миллиона моложе 30 лет, и многие из них подключены к сети: уровень вовлеченности страны в Интернета чуть менее 80 % и соответствует Западной Европе. При выборе правильных инструментов, считает Ксхакли, технически подкованные молодые люди могут помочь более традиционным дипломатам в костюмах и галстуках их стремлению добиться признания Косово, а также сделать жизнь косоваров легче.

Особенным инструментом, за который он выступает, является новая цифровая платформа Косово, для которой Ксхакли помог создать концепцию, код и дизайн. Она разработана Приштинской Ipko Foundation, независимой неправительственной организацией, в которой Ксхакли является членом правления. Инициатива Цифрового Косово направлена на создание возможностей для косоваров использовать онлайн-сервисы, а также привлекать других интернет-пользователей по всему миру. Этот веб-сайт работает с сентября и содержит готовые к использованию шаблоны на основе сценариев, где Косово отсутствует или указано как часть Сербии или Албании компанией или учреждением. Любой человек может затем персонализировать шаблон и отправить его напрямую лицам, принимающим решения на высоком уровне в организации, о которой идет речь — все это в течение нескольких секунд .

Шаблоны предназначены для осуществления все большего давления на крупные интернет-компании, а также аэропорты, авиакомпании, газеты и университеты, которые не признают Косово в качестве независимого государства. Конечной

целью является создание возможностей для косоваров использовать Интернет для бизнеса, организацией поездок, покупок в интернет-магазинах и многого другого.

Ксхакли и его большая армия онлайн добровольцев уже бомбардируют Google Maps шаблонными сообщениями, требующими, чтобы система признала Косово. Сообщения также доводятся до аэропортов Лондона и Сиднея, которые уже добавили Косово на свои сайты, и в Брюссель, где Приштина по-прежнему в составе Сербии, несмотря на то, что карта Косово разграничена от Сербии на информационных щитах аэропорта.

Покровители платформы цифрового Косово, которая финансируется Министерством иностранных дел Косово, Британским Советом и Посольством Норвегии, рассматривают этот тип цифровой дипломатии как самый современный. «Признание Интернет Косово имеет огромное практическое и символическое значение, и это неприемлемо, что Косово все еще не появляется на очень многих сайтах» — сказала Мирна Макгрегор, первый секретарь Посольства Великобритании в Приштине.

Цифровое Косово утверждает, что их смесь лоббистских усилий и гражданской пропаганды уже привела к победам. В ноябре, после кампании отправки шаблонных сообщений и сообщений в компанию Facebook там признали Косово как государство (ранее косовары, желающие зарегистрироваться, должны были указывать себя в качестве граждан Сербии). Цифровое Косово также говорит, что помогло одержать победу над небольшими компаниями, такими как MailChimp.

В дополнение к требованиям, чтобы учреждения признали Косово в Интернете, Ксхакли, который после начала карьеры в области телекоммуникаций и энергетики теперь может быть назван главным цифровым дипломатом Косово, работает над улучшением восприятия Косово через другие цифровые проспекты. Иногда это связано с поездками по всей Европе: чтобы выступать на конференциях или встретиться с Эдом Парсонс, главой Google Maps. В прошлом году Ксхакли также помог создать Wiki академию Косово, которая обучает авторов и редакторов как улучшить качество и количество онлайн-контента о Косово.

Растущий успех Косово в цифровой сфере может быть полезным примером для других стран, которые стремятся к международному признанию, будь то Южный Судан или Палестина, которая, в отличие от Косово, уже имеет домен верхнего уровня (PS). Тем не менее, существуют пределы досягаемости цифровой дипломатии. Например, она не может решить проблему широко распространенной коррупции в Косово; страна занимает 111 место из 177 государств в индексе коррупции по версии Transparency International. Она также не может удалить глубокие корни разногласия между этническими албанскими и сербскими общинами. Некоторые наблюдатели считают обе эти проблемы препятствием для Косово, которое приписывает себя к семье европейских государств.

Но даже эти проблемы могут быть ослаблены в будущем, если цифровая осведомленность и здравый смысл — на этот раз, на внутреннем фронте — приведут к более открытому правительству и сделают власть более бдительной в отношении нарушения прав, ресурсов и привилегий.

«Никто не говорит, что это чудо» — считает Ксхакли, «но это способ вообразить заново будущую демократию и государственность».

Смещение центра власти на Восток: PRO et CONTRA

Алексей Харин

кандидат исторических наук, доцент Кировского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

Последние несколько лет ежегодно всплывает вопрос о возможности переноса столицы на восток страны. И при том поднимают его не только политологи и публицисты, но и государственные служащие. Год назад с такой идеей выступал губернатор Московской области С. К. Шойгу[1]. Недавно мэр Владивостока вновь озвучил эту мысль[2], вызвав комментарии ведущих политических партий[3].

Идеи о переносе столицы не новы. В 1990-е гг. об этом писал В.Л. Цымбурский. Об этом же рассуждал и А.С. Панарин, считавший, что центр страны может сдвинуться за Урал, что соответствовало бы мировому цивилизационному смещению с Запада на Восток. Россия, как традиционный посредник и балансир между Востоком и Западом, не может не среагировать на это смещение эпицентра соответствующим смещением своего политического и духовного центра[4]. А.Г. Дугин предлагал перенести столицу в Казань[5], допуская и возможное смещение столицы в Сибирь. Активно идею переноса столицы на Урал отстаивает С.В. Хатунцев[6]. Хотя последний — «уральский» вариант — пока менее популярен.

Год назад данный вопрос активно обсуждался в научной и публицистической среде. Ю.В. Крупнов, поддержав идею смещения центра власти, посчитал, что лучше всего его перенести на Дальний Восток: это превратит данный регион из крайне слабого в форпост России, и, кроме того, позволит нашей стране присутствовать «головой» в АТР как становящемся центре мирового экономического развития[7].

---

[1] Шойгу предложил перенести столицу в Сибирь. Режим доступа: http://lenta.ru/news/2012/04/06/shojgu/

[2] Мэр Владивостока предложил перенести столицу России на восток. Режим доступа: http://lenta.ru/news/2013/08/28/pushkarev/

[3] РИА Новости. Режим доступа: http://ria.ru/vl/20130829/959452632.html#13778868015543&message=resize&relto=register&action=addClass&value=registration#ixzz2dThCmeeO

[4] Панарин А.С. Реванш истории: российская стратегическая инициатива в XXI веке. М., 2005. С. 191.

[5] Дугин А.Г. Третья столица. Режим доступа: http://www.arctogaia.com/public/Tatar.htm.

[6] См. напр.: Хатунцев С.В. Идите все, идите…на Урал // Политический класс. 2007. № 12.

[7] http://krupnov.livejournal.com/380346.html

Б.В. Межуев согласился с идеей распределения части властных функций между несколькими городами России[1]. Примерно подобную же позицию занял С.А. Караганов, посчитав полезным разделение властных полномочий и указав, что такая мера даст импульс развитию Сибири[2]. М. Дианов в своей статье-прогнозе не исключает в будущем раздела полномочий между Москвой и одним из сибирских городов[3].

В социальных сетях также ведётся обсуждение данной проблемы, года два назад проводились социологические опросы и сборы подписей за смещение центра в Сибирь[4]. Хотя, как признал автор одного из постов, «сама мысль о таком переносе представляется многим до сих пор фантастической и неосуществимой»[5].

С противоположных позиций выступили В. Л. Иноземцев и С. Дьячков, посчитав подобные разговоры опасными:

сторонники переноса столицы апеллируют к опыту прошлого, оказываясь «в плену давно уже отживших практик и концепций, забывая о меняющемся мире, в котором уже нет неосвоенных окраин, а морской транзит куда выгоднее континентального»;

это будет означать регресс в развитии, движение в сторону Азии с её специфическими ценностями и скептическим отношением к демократии; курс на закрытость, подтверждаемую желанием уйти как можно глубже «в центр» евразийского континента; на закрепление сырьевого характера экономики;

успешность региона большой страны вовсе не обязательно связана с нахождением на его территории города, выполняющего столичные функции; у государства, по большому счету, есть единственный метод политического стимулирования экономического роста — усиление регионализма, означающего оттягивание у Москвы как властных полномочий, так и финансовых потоков; сокращение отправляемой в центр «дани»; переток в регионы предпринимателей и интеллектуалов. Россия должна научиться развиваться с меньшими

[1] Межуев Б.В. Уход на Восток, или движение по кругу. Режим доступа: http://www.izvestia.ru/news/521270

[2] Караганов С.А. России нужна еще одна столица — сибирская. Режим доступа: http://www.globalaffairs.ru/pubcol/Rossii-nuzhna-esche-odna-stolitca---sibirskaya-15553

[3] Дианов М. Два президента, две столицы, по два губернатора. Федерация через 45 лет // Политический класс. 2005. № 6. С.49-52.

[4] См. напр. http://www.sborgolosov.ru/voiteview.php?voite=148; http://forum.kpe.ru/showthread.php?t=16469; Розов Н. Большой Восточный проект. Сибирь как плацдарм российско-европейской цивилизаторской миссии. Режим доступа: http://globalsib.ru/node/99; Сибирский региональный форум. Режим доступа: http://siberiaregion.ru/index.php?fid=9&id=1252030265; Тарло Е. Режим доступа: http://tarloeg.livejournal.com/699.html; Вольский С.О Необходимости переноса столицы России в Сибирь. Режим доступа: http://badnews.org.ru/news/o_neobkhodimosti_perenosa_stolicy_rossii_v_sibir/2010-12-28-5723.

[5] Розов Н. Указ. соч.

региональными перекосами, но перенос столицы, пожалуй, самый неэффективный способ решения этой задачи»[1].

А.В. Митрофанова считает, что даже размеры страны физически не позволяют разместить столицу в таком месте, где она была бы доступна для всех. России необходимо не переносить столицу с места на место, и не строить заново в пустыне, а развивать быстрый и дешёвый внутренний транспорт. Близость к морю крайне важна[2].

Например, А.Н. Окара в приватной беседе высказал суждение, что российская политическая система негибка, и, возможно, с трудом перенесла бы подобные вызовы. Кроме того, отсутствуют предпосылки для данной акции: нет необходимых средств и ресурсов. Раньше имел место перенос столиц вслед за демографической экспансией, а сейчас таковой нет и бессмысленно переносить столицу в пустеющий регион. Более того, в цивилизационном плане Россия отдалится от славянской зоны, являющейся её базой.

Как видим, обсуждение необходимости переноса столицы в Сибирь имеет место в научной среде и в публицистике. На это повлиял и ряд обстоятельств.

Во-первых, крушение Большой России (СССР). Современная Российская Федерация — это во многом новое государство, хотя и имеющее преемственность с прошлым. Страна превращается в континентальное государство, почти отрезанное от удобных выходов к морям, становящееся континентальной державой. Во-вторых, происходит крупная геополитическая революция, выразившаяся в новом возвышении Востока, в смещении центра экономической активности в АТР. В-третьих, рост внимания мирового сообщества к Арктике, освоению её ресурсов. В-четвёртых, для новых условий, в которых оказалась страна, требуется и новая элита. В-пятых, имеют место диспропорции в развитии страны.

Всё это и выдвигает на повестку дня, в качестве одного из сценариев, согласимся, не единственно возможного, вопрос о переносе столицы, как попытку ответить на вызовы времени. Главной задачей нашей статьи будет разбор противоположных суждений. Сначала рассмотрим аргументы против переноса столицы в Сибирь.

Можно привести исторический пример: перенос столицы из Москвы в Санкт-Петербург. В какой-то степени это мероприятие подорвало экономику северных регионов России. Разумеется, одной из причин было произвольное перенаправление товарно-денежных потоков вместо Архангельска в Санкт-Петербург, но и смещение центра власти тоже сыграло свою роль.

Могут указать и на затратность проекта (о чём говорил А. Н. Окара): нужно строить новые магистрали, дороги, расселять приезжающих туда людей. Вместе

[1] Иноземцев В., Дьячков С. Новый регионализм а не новая столица. Режим доступа: http://inozemtsev.net/2012/11/сергей-дьячков-владислав-иноземцев-н/

[2] Геополитика. Информационно-аналитическое издание. Выпуск XXX. Москва, 2013. С.130.

с тем, переезд органов власти за Урал, может привести к частичному запустению той же Москвы, как в своё время произошло с Санкт-Петербургом. Являясь второй столицей, он постепенно угасает, постепенно превращаясь в провинциальный город.

В числе трудностей, связанных с возможным переездом руководства страны в другой город, отметим наш менталитет: часть общества привыкла ассоциировать себя с Западом, желает быть ближе к Европе, с которой более крепкие и давние экономические, культурные связи. Москва уже на протяжении столетий была столицей страны и все к этому привыкли. А перенос столицы — это ещё и своеобразный слом сложившейся традиции. Были два века «Петербургского периода», но и они как-то органично смотрятся: Россия стремилась войти в Европу и перенос столицы в Санкт-Петербург был в чём-то и оправдан. Тем более что и Москва тогда сохраняла статус второй столицы.

Для многих центр в Сибири кажется немыслимым: ведь для большинства Москва — это символ страны, город, сыгравший огромную роль в истории нашего государства, да и эти земли уже почти 900 лет относятся к историческому ядру государства, ещё при древних князьях — Андрее Боголюбском и Всеволоде Большое Гнездо Северо-Восточная Русь и доминировала среди других княжеств. Отсюда — из Владимирской Руси, началось возрождение государства.

Другими словами, переносы столицы внутри исторического ядра российского государства — это одно, а вот перенос на совершенно иные земли, ставшие российскими и освоенные относительно недавно — другой вопрос.

Возникает и ещё одна ментальная причина: а захочет ли наша элита переезжать, бросать всё насиженное, рвать какие-то экономические и не только связи? Нельзя забывать, как на этот шаг могут посмотреть жители европейской части России — той же Рязани, Ярославля, да и Кирова. Раньше столица для них была под боком, в любой момент можно было выбраться туда за всем необходимым, в Москву (как и в Санкт-Петербург) отправляли на учёбу своих детей, а теперь куда? Получается, что до новой столицы (например из того же Кирова), нужно ехать примерно двое суток. Кто туда поедет? Не окажется ли город при определённых обстоятельствах в изоляции?

Возможна негативная реакция и регионов, примыкающих к новой столице: боязнь того, что их города лежащие на Транссибе, превратятся в «проходной двор».

Оказавшись в Красноярске, мы можем отдалиться от Европы, одного из наших главных экономических партнёров, покупателей наших ресурсов, а также нашего кредитора. Есть опасения, что вместе с тем, мы и не приблизимся к АТР. Точнее, Россия в АТР «государство окраинное, выходящее к океану в его замерзающем

секторе севернее той части восточно-азиатского приморья, где состоялось экономическое «чудо», поэтому она с одной стороны изолирована в АТР[1].

Неизвестно также, пойдут ли инвестиции в эти регионы. Население Сибири становится всё меньше, сейчас сибиряков (вместе с жителями Дальнего Востока) примерно 26 % от всего населения страны[2]. Не будет ли здесь диспропорции: центр размещается в малозаселённых районах, а густонаселённые регионы немного отдалены?

Могут привести и такой аргумент: столицы многих больших стран находятся чуть не на окраине: Вашингтон — в США, Оттава — в Канаде, Канберра — в Австралии, Пекин — в Китае, Дели — в Индии. И ни в одной из этих стран пока, похоже, не ставится вопрос о переносе столицы.

Некоторые аналитики не исключают удара Китаем по Сибири[3], следовательно, и Красноярск может оказаться под угрозой. Нестабильно и в Центральной Азии, куда в случае чего могут прийти и талибы из Афганистана, тревожный звонок прозвучал недавно из Казахстана (события в Жанаозене).

Рядом находится также Синьцзян-Уйгурский автономный район Китая, часть жителей которого стремится к отделению от КНР. В случае мощного сепаратистского взрыва на Западе Китая, а также разрастания конфликта в Центральной Азии, Красноярск может оказаться в опасной зоне, и фактически быть отрезанным от остальной России. Добавим, что Красноярск находится в относительной близости от так называемого «Золотого полумесяца» (Иран, Афганистан, Пакистан), где производится большое количество опиума. Через Центральную Азию как раз проходит наркотрафик из этого региона.

Аргументом против является и то, что последнее время Красноярск позиционирует себя как столицу Сибири, а отнюдь не России, что может поставить под вопрос идею переноса сюда центра (но в таком случае допустим и новосибирский вариант, тем более что в 1993 г. такие идеи уже возникали). Было бы интересно знать и мнение самих жителей того же Красноярска — статус столицы имеет как свои плюсы, так и свои минусы. И захочется ли им испытать на себе все трудности «столичного бремени»?

Ещё одним важным аргументом «против» является позиция, согласно которой в наше время наиболее развитыми, перспективными являются приморские регионы, соответственно загонять столицу в глубь материка — губительно.

Когда мы говорим о предыдущих переносах столицы страны, то речь идёт об экономически развитых регионах или территориях, в данный момент активно

[1] Цымбурский В. Л. Остров Россия. Геополитические и хронополитические работы разных лет. 1993-2006. М., 2007. С. 317-318

[2] http://ru.wikipedia.org/wiki/Сибирь#

[3] Храмчихин А. Как Китай раздавит Россию. Режим доступа: http://www.apn.ru/publications/article20421.htm

заселяемых. Т.е. перенос столицы идёт вслед за демографической экспансией. У нас же Сибирь пустеет. В результате может возникнуть очередной нарыв на теле государства.

Но в литературе, как научной, так и в публицистической, существуют и довольно многочисленные аргументы за перемещение центра восточнее Урала.

То что этой идее почти 20 лет и её выдвигают представители различных социально-политических сил (может быть за исключением либеральных, согласимся здесь с авторами) о чём-то говорит. Это свидетельствует не только о специальной «раскрутке», но и о наличии проблем, которые необходимо решать.

Такой шаг необходим по ряду причин. 80% территории страны находится в азиатской части (и 70% границ проходит также со странами Востока), при том, что столица располагается в европейской части. С запада на восток здесь вырисовывается геополитическая ось, исторически соответствующая пути покорения русскими Сибири: Челябинск-Омск-Новосибирск-Томск-Кемерово-Красноярск-Иркутск-Хабаровск-Владивосток[1]. В Сибирском федеральном округе сосредоточено 85% нефтегазового комплекса страны, 75% добычи угля, от 40% до 100% добычи сырья для чёрной и цветной металлургии[2], а так же и другие полезные ископаемые. Нельзя забывать и об огромном лесном массиве.

Во многих из указанных стран, где столицы чуть не на окраине, территория является более освоенной, нежели у нас: в США развиты оба побережья и Лос-Анджелес мало чем уступает Вашингтону по своему значению. Точно так же можно сказать и о Канаде: Квебек, Оттава и Монреаль на востоке страны, а Ванкувер — на западе. Во многих из этих странах развита сеть коммуникаций. Например, китайцы проводят дороги в Тибете, а Синцзян-Уйгурский автономный район используют как важную коммуникационную базу для дальнейшего продвижения на запад Евразии. Кроме того, у многих из этих стран нет территориальных споров с соседями.

Противники переноса опасаются, что такой шаг приведёт к закрытости страны, к закрепление сырьевого характера экономики. Но насколько обоснованы такие опасения? Расположение центра власти рядом с источниками сырья необязательно должно гарантировать преобладание добывающего сектора экономики. То, что столица отдалится от Европы, только ЕС и может быть воспринято как желание отдалиться от Запада. Но Запад это только один миллиард населения Земли. Три других миллиарда — т.е. Китай, Индия и мир ислама — могут воспринять это иначе: а именно как желание приблизиться к тем регионам, за которыми будущее — АТР и Индийский океан…

Красноярск располагается на широте Челябинска и Куйбышева, т.е. в относительно тёплом районе. Рядом Новосибирск — крупный железнодорожный центр,

[1] Кефели И. Ф. Геополитика Евразии. СПб., 2009. С. 227.

[2] Кефели И. Ф. Указ. соч. С. 228.

от которого дорога идёт на Омск и Алма-Ату, с другой стороны — на Дальний Восток. Сверху от Красноярска — выход на Норильск, т.е. к крупным полезным ископаемым, в Арктику, в Северный морской путь. Недалеко от Красноярска находится и Байкал, а это — примерно 1/5 запасов пресной воды в мире. Рядом с Красноярском находится и Алтай — уникальный во всех отношениях регион, богатый и своими полезными ископаемыми, местом схождения границ четырёх государств (Россия, Казахстан, Китай, Монголия). Но это ещё и уникальное место в этнорелигиозном плане так как представляет собой точку пересечения трёх религий — христианства, ислама и буддизма[1].

То, что почти близко Китай, не должно пугать. С одной стороны, нас убеждает позиция ряда исследователей, отрицающих военную угрозу со стороны Китая[2]. Известно, что одной из главных особенностей китайской внешней политики является стремление избегать силовых методов, действовать более мягко (но эффективно) при отстаивании своих интересов, используя древний даосский принцип: «Белое плавно переходит в чёрное и наоборот».

Но если даже и предположить такой мрачный вариант, то Красноярск, хоть и не совсем, но защищён Монголией от Китая, и китайская армия, в случае предполагаемой войны, свой удар в первую очередь нанесла бы по Дальнему Востоку. С другой стороны, некоторые исследователи (Л.Е. Бляхер) видят «китайскую угрозу» в том, что китайцы могут потерять экономический интерес к Дальнему Востоку, что приведёт к возникновению проблем у жителей региона. Уже сейчас, по мнению некоторых авторов, китайцы всё больше внимания в экономическом плане уделяют другим странам[3].

Вопрос о т.н. «китайской угрозе» выходит за рамки данного материала. Добавим также, что между Сибирью и соседними государствами «существуют не только протяжённые границы, но и исторически сложившаяся взаимозависимость экономики на базе разделения труда»[4].

Перенос столицы приблизит нас к восточным соседям (в первую очередь к Китаю и Индии), которые сейчас всё более активно развиваются (Китай ведь уже является 2-й экономикой мира, а Индия находится примерно на 4-5 местах). Общеизвестно, что постепенно центр деловой активности смещается в АТР. С новой столицей, всё-таки, Тихоокеанский регион, хоть и немного, но станет ближе. Мы уже отмечали, что, с одной стороны, Россия частично изолирована от АТР, вместе с тем она может сыграть в этом регионе свою роль[5], тем более что про-

[1] Кефели И. Ф. Указ. соч. С. 230.

[2] Морозов Ю.В. К чему может привести публикация мифов о китайской угрозе. Режим доступа: http://www.oko-planet.su/politik/politikday/36917-k-chemu-mozhet-privesti-publikaciya-mifov-o.html

[3] См. Лунёв С. Чего стоит Сибирь // Международные процессы. 2004. № 1. Режим доступа: http://www.intertrends.ru/four/013.htm; об этом же говорил и Л.Е. Бляхер в приватной беседе.

[4] Кефели И.Ф. Указ. соч.

[5] Цымбурский В.Л. Указ. соч.

мышленный потенциал Сибири позволяет России вновь расширить окно в Восточную Азию[1].

Рядом окажется и Центральная Азия, через которую — выход на Ближний Восток, а так же на Иран и через него в Индийский океан (который может стать центральной ареной XX1 века[2]). Россия инициировала создание Шанхайской организации сотрудничества (ШОС), и, следовательно, «ей самой нужно двигаться в восточном направлении»[3]. Существует, пусть и виртуальная, но связка Россия-Индия-Китай. Красноярск как раз рядом с этими странами, и, тем самым, перенос столицы мог бы активизировать взаимодействие в рамках как ШОС, так и связки Москва-Пекин-Дели. Речь не идёт о создании «Мира без Запада», но площадка ШОС могла бы послужить для России одной из основ диалога с Евроатлантикой. Да и основная часть стран, членов ОДКБ находится в Центральной Азии, что активизировало бы наше взаимодействие.

Блок НАТО всё ближе придвигается к российским границам, что вызывает озабоченность у отечественных политиков и военных (и недоумение по поводу этой тревоги со стороны Запада). В связи с этим имеет ли смысл рисковать, устанавливать столицу чуть ли не у границы? Вместе с тем, пусть и не сейчас, но утрата Приморья всё-таки может возникнуть, как и ряда других регионов востока страны (плохо осваиваемые территории так или иначе всегда привлекали и будут привлекать внимание других государств, где меньше ресурсов). Оба негативных фактора легче будет нейтрализовать при нахождении Центра в «урало-сибирской Срединной России» (термин В.Л. Цымбурского), нежели если бы столица размещалась в Москве[4].

При сохранении уже сложившихся (пока другой вопрос — каких) отношений с Западом, размещение столицы за Уралом, активизировав восточное направление, в целом позволит проводить сбалансированную многовекторную внешнюю политику.

Л. Г. Ивашов видит ещё один положительный момент в переносе: погрязший в коррупции и разврате правящий слой останется в Москве и Санкт-Петербурге (так как придерживается своей прозападной идеологией и хочет быть поближе к Западу).

Уже неоднократно в литературе встречалась мысль, что перенос столицы в Сибирь вдохнёт жизнь в пустеющие районы, даст им новый импульс для развития. В России капитал идёт за властью, поэтому не исключено и смещение центра деловой активности вслед за принятием такого важного решения. Красноярск

[1] Кефели И.Ф. Указ. соч. С. 227.

[2] Каплан Р. Центральная арена XX1 века // Россия в глобальной политике. 2009. № 2; Кузнецов А. Индийский океан - новый приз в Большой игре // Информационно-аналитический портал Геополитика. 24.07.2013.

[3] Ивашов Л.Г. . Повернуть взгляд к Сибири // Геополитика и безопасность. 2009. № 1. С. 20.

[4] Цымбурский В.Л. Указ. соч. С. 302.

стянет страну, станет соединяющим звеном между Дальним Востоком и европейской частью страны. Именно отсюда — из центра страны будет больше возможностей контроля за её отдалёнными регионами. С другой стороны, управлять государством при современных телекоммуникациях будет относительно легче.

В связи с проблемой перемещения центра власти можно вспомнить и ряд исторических аналогий. Князь Константин Великий перенёс столицу из дряхлеющего Рима в Константинополь, что позволило ещё сохраниться на долгое время Римской, а потом и Византийской, империи. Андрей Боголюбский фактически создал новое ядро российского государства, отказавшись от Киева в пользу Владимира. В XIV в. подобное произошло уже с Москвой.

Известны случаи, когда попытки сохранить старую столицу только усугубляли ситуацию. Например, некоторые исследователи Византии (Ф. И. Успенский) считают ошибочным, что после изгнания крестоносцев из Константинополя, город вновь стал столицей возрождённой (правда, ненадолго) империи. Это привело к окончательной потере малоазиатских территорий Восточного Рима, являвшихся базой для могущества страны[1]. В этом плане обоснованным, на наш взгляд, шагом является перенос столицы из Стамбула в Анкару, осуществлённые Кемалем Ататюрком (1923). В 1960 г. появляется новый центр страны в Бразилии, что также можно назвать позитивным шагом.

В.Д. Соловей предлагает, сместив центр власти за Урал, построить новую столицу. По его мнению, российская политика, в результате такого шага, обрела бы наконец смысл, сосредоточившись на настоящем большом деле, а общество получило бы мощный импульс к обновлению и пресловутую национальную идею[2]. На наш взгляд, необходимо ресурсы бросить на другие направления, на то же перемещение столицы, а не создание на пустом абсолютно месте чего-то нового.

После развала СССР возникло новое государство, пусть и имеющее тесную преемственность с предыдущим, но изменившееся в своих границах, с новым социально-экономическим укладом, иной идеологией. Началась другая эпоха, для которой, по всей видимости, нужна и иная столица.

Говоря о бюрократическом аппарате, следует признать: часть элиты не пожелает поехать. Однако стимулом здесь может послужить боязнь потерять место при власти, и на этом можно сыграть. С другой стороны, наши вузы сейчас выпускают много квалифицированных специалистов, которые, порой, не могут найти достойной работы. На новом месте их потенциал мог бы пригодиться. Уже неод-

[1] Справедливости ради, стоит заметить, что византийские императоры безразлично относились к своим малоазиатским провинциям ещё в XI-XII вв., что уже тогда дало очень печальные результаты, а ошибки XIII в. есть продолжение предыдущих.

[2] Соловей В. Д. По ту сторону Урала. Там лежит будущее и надежда России // Политический класс. 2005. № 6. С. 60.

нократно писалось о необходимости притока новых кадров в элиту, и в переломные эпохи такое часто бывало. А мы сейчас вновь находимся на таком переломе.

Разумеется, перенос центра власти не решил бы всех проблем, но, возможно, вдохнул бы жизнь в нашу страну, по мнению некоторых аналитиков (напр. В.Л. Цымбурского) возникла бы более устойчивая структура территориально-политического устройства, обретшая гармоничную модель с центром в Западной Сибири со столицей в Красноярске или Новосибирске, с двумя флангами — Евророссией и Приморьем, являющимися проводниками страны в Западную Европу и в АТР. Такой перенос обозначил бы и новую тенденцию в развитии страны.

Мы рассмотрели аргументы «за» и «против» переноса. Нам представляется, что на данном этапе более весомыми выглядят отдельные возражения против переноса столицы именно в Сибирь и на Дальний Восток. А именно:

опасность того, что столица переносится именно в пустеющий регион, и в отсутствии у государства средств на переселение тех, кто желает туда поехать;

может быть нанесён ощутимый удар по традиции;

готово ли само общество к этому, в том числе и население Сибири?

на сколько такой перенос совместим с цивилизационной стратегией, предполагающей более тесное сотрудничество с Украиной, Белоруссией, Молдавией и Прибалтикой, а также со странами Восточной Европы; эти регионы также важны для России и мы можем предложить им свой цивилизационный проект[1].

Таким образом, сложности и вопросы остаются, тема является сложной, дискуссионной и отнюдь не закрытой. Возможно даже, что не исключён вариант смещения центра страны на Урал (особенно в случае возрастания роли организации ШОС как мотора «евразийского Хартленда»), за который по-своему аргументировано, ратует С.В. Хатунцев. Но разбор «уральского» варианта не входит в рамки данной статьи.

В целом необходимо взвешенное обсуждение данной проблемы. Скорее всего, это даже вопрос отдалённого будущего, если такая потребность станет во всей своей остроте и полноте.

[1] Геополитика и международные отношения. Т.1.– М., 2012. С. 642.

Сирийский излом США или Обама в «пасти льва»

Леонид Доброхотов

доктор философских наук, профессор Социологического факультета МГУ им. М.В. Ломоносова

Нынешние события в Сирии давно переросли рамки гражданской войны в отдельно взятой, хотя и ключевой по влиянию арабской стране. Они давно вышли за пределы регионального конфликта при всем огромном значении Ближнего Востока для судеб мировой цивилизации, экономики и политики. Они стали мировым кризисом. Событием большого, а возможно, и переломного геополитического значения. Первым реальным крупномасштабным столкновением Запада с Россией со времен провозглашенного свыше 20 лет назад прекращения якобы «холодной войны». Серьезным вызовом самим основам геополитики США, кризисом ее внешней и внутренней политики. Первым реальным проявлением того, что можно считать признаками возрождения мировой роли России как великой державы и перепостроения отношений России с миром, включая США и другие великие державы, с учетом этой роли. Без которой, по убеждению автора, наша Отчизна не может существовать вовсе.

Ключом к пониманию происходящего, на наш взгляд, можно считать суждение известного американского экономиста Пола Крейга Робертса, полагающего, что главной стратегией США была и остается (по крайней мере до последних событий) мировая гегемония, включающая в себя подчинение России и Китая через активизацию и использование мусульманского фактора как внутри этих стран, являющихся главными геополитическими соперниками Америки, так и по всему миру, прежде всего на Ближнем Востоке.

Второй, не менее важный фактор, объясняющий происходящее, это фактор вечно неспокойного Израиля, проводимая этим государством в регионе предельно задиристая, агрессивная политика.

В статье будут анализироваться в основном события, связанные с обвинениями Сирии в использовании химического оружия во внутреннем вооруженном конфликте в стране и связанными именно с этим внешними угрозами в отношении правительства президента Башара Асада. Однако для понимания реальности не следует забывать хронику предшествующих событий. Тем более, что нас интересует прежде всего геополитический разрез происходящего.

Прежде всего, автор рассматривает политику правительства США и его союзников в отношении Сирии как продолжение и развитие традиционного поведения Америки в преследовании своих геополитических приоритетов с позиции силы. Только в XX веке это была вооруженная интервенция США в Мексику, а затем США и еще 13 государств - в революционную Россию. После второй мировой войны, самыми памятными явились вооруженные агрессии США и организованные американцами свержения правительств в Иране, Корее, Гватемале, Вьетнаме, Камбодже и Лаосе, Ливане, Панаме, Доминиканской республике, Гренаде, а после ликвидации СССР — бомбардировки и свержение президента Югославии, нападение и оккупация Ирака, война в Афганистане, бомбардировки и свержение режима в Ливии. Всего же только с начала XX века по настоящее время США организовали более 30 вооруженных агрессий и переворотов против независимых стран, причем в отношении некоторых из них — по нескольку раз.

Основанное на непререкаемых фактах и свидетельствах мнение автора состоит в том, что сам по себе жупел химического оружия в Сирии был изобретен и использован западниками и их суннитскими союзниками (Саудовской Аравией, Катаром, Турцией), а также фондируемыми ими и Западом т.н. повстанцами как предлог для задуманного задолго до этого вооруженного внешнего вмешательства и свержения правительства Б. Асада. В свою очередь, это понадобилось потому, что вялотекущая гражданская война против Асада не только не вела к его поражению, но, напротив, к лету 2013 года стало очевидно: он эту войну выигрывает.

Запад такой исход категорически не устаивал. Почему? По нескольким известным причинам. Первая и главная из них — геополитическая. Сирия у американцев с союзниками, прежде всего Израилем, стояла на очереди после Ирака и Ливии (затея с Египтом у них временно сорвалась) на операцию «асфальтового катка», после чего должна была превратиться в дополнительную площадку для продвижения к следующей цели захвата и подавления — Ирану.

Хроника событий последних двух лет это подтверждает.

В полном соответствии с инструкцией по организации цветных революций, четко изложенной по директивам ЦРУ американцем Джином Шарпом из Бостона в его учебнике «От диктатуры к демократии», вслед за переведшими книгу на арабский язык тунисскими «революционерами», а затем египетскими братьями-мусульманами, к практической реализации задачи приступили сирийские оппозиционеры.

Как известно, начатая в Тунисе и Бахрейне «арабская весна» докатилась до Сирии к марту 2011 года. Мятежники восстали в стране как раз тогда, когда администрация Обамы под давлением Израиля настойчиво пыталась склонить Асада к прекращению его союза с Тегераном и поддержки исламских движений сопротивления оккупационной политике Израиля - палестинской «Хамаз» и

ливанской «Хезболлы». В мире сложилось устойчивое впечатление о том, что мятеж возник (вернее, был организован) именно тогда, когда Вашингтону, его основным западным союзникам и Тель-Авиву стало ясно: Сирия на шантаж не реагировала.

В то время, несмотря на призывы Израиля и его многочисленных друзей в Америке к «жесткому отпору» Дамаску, тогдашний госсекретарь Х. Клинтон все еще ссылалась на взгляд некоторых американских законодателей на Асада как на «реформатора». И действительно, за несколько дней до этого бывший тогда сенатором Джон Керри утверждал, что Сирия находится на пороге изменений, «соглашаясь на разумные отношения с Соединенными Штатами и Западом». Однако, не видя движения навстречу своим требованиям и на фоне ширящегося вооруженного мятежа, вызвавшего резкий отпор правительственных войск Сирии, уже в августе Обама публично призвал к отставке Асада.

В октябре 2011 года США обратились в СБ ООН с призывом осудить «нарушения прав человека» в Сирии и потребовать прекращения насилия. Россия и Китай наложили вето на подготовленную американцами резолюцию СБ на эту тему. В том же месяце Вашингтон отозвал своего посла в Сирии Роберта Форда (вернувшись в декабре, на фоне резко ухудшившихся отношений двух стран, два месяца спустя он убыл вновь). В феврале 2012 года США поддержали предложенную рядом арабских стран новую антисирийскую резолюцию СБ, однако Россия и Китай и на нее наложили вето. Клинтон тогда назвала этот шаг двух стран «достойным презрения».

Застряв в ООН, американцы обратились к своим европейским и арабским союзникам, проведя вместе с ними в Тунисе первую конференцию т.н. друзей Сирии (на самом деле, сторонников вооруженных мятежников и врагов правительства в Дамаске). Очень интересно и важно, что уже в то время разведка США стала предупреждать о массовой инфильтрации в ряды мятежников боевиков Аль-Кайды и других террористов, в том числе из Европы, однако «друзья Сирии» никак не отреагировали на это предупреждение. Более того, в марте 2012 года Обама пообещал предоставить мятежникам «нелетальное» оружие. К тому времени в ходе вооруженного насилия внутри страны, по данным ООН, погибло уже 8 тысяч человек.

На этом фоне Клинтон продолжала рассчитывать на поддержку со стороны России т.н. женевского процесса мирного урегулирования конфликта на базе создания переходного правительства в ходе переговоров между правительством Сирии и руководителями мятежников. Однако за несколько часов до подписания соответствующего соглашения в июне 2012 года, США и Россия вступили в резкую полемику по поводу того, должно ли оно предусматривать уход Асада с должности президента и вообще из власти в стране. В результате нового конфликта, в июле Россия и Китай в третий раз заблокировали

подготовленный США и их союзниками проект резолюции Совбеза ООН, на этот раз предусматривавший силовые действия против правительства Сирии в случае невыполнения ее условий.

В этих обстоятельствах поиск мирного урегулирования заглох совсем. Арабы проигнорировали призыв США к эмбарго на поставку все более современных типов вооружений мятежникам. В свою очередь, Обама отверг предложение Клинтон, в то время директора ЦРУ Д. Петреуса и других чиновников начать снабжать американским оружием т.н. умеренные оппозиционные силы. В июле ООН сообщала, что в месяц в Сирии погибало уже свыше 5 000 тысяч граждан.

До сих пор так до конца и не ясно, почему тем же летом Обама вдруг заявил, что использование сирийским правительством химического оружия будет означать пересечение «красной черты», после которой поведение США в конфликте резко ожесточится (по его словам, это будет иметь для Дамаска «невероятные последствия»). Дело в том, что Западу, его арабским союзникам и России всегда был известен факт наличия у Дамаска больших запасов такого оружия еще с советских времен и о том, что эта страна не присоединилась к Конвенции о запрете применения такого оружия (обычное объяснение состоит в попытке Сирии защититься таким образом от угрозы применения ядерного и химического оружия, находящегося в распоряжении Израиля).

Возникает вопрос: почему именно в августе 2012 года президент США вдруг в угрожающем тоне заявил о возможности и о последствиях использования химоружия правительственными войсками Сирии? С учетом последующих событий, на которых мы далее остановимся, не явилось ли это уже тогда частью разработанного американцами секретного плана по созданию предлога для внешнего удара по Сирии и силового изменения режима в этой стране по примеру Югославии, Ирака и Ливии?

Тем временем, в ноябре 2012 года ООН довела число жертв сирийского конфликта с его начала до 60 тысяч человек. В декабре США официально признали воюющую против правительственных войск т.н. Коалицию оппозиционных сил «законным представителем сирийского народа». Что не помешало американцам тогда же включить одну из групп антиправительственных мятежников — Фронт Нусра, связанный с Аль-Каидой, в черный список террористических организаций.

В январе 2013 года Обама вступил во второй срок своего президентства, и уже в марте мятежники и правительство Сирии начали обвинять друг друга в использовании химического оружия, причем США тут же заявили о начале самостоятельного расследования и поиска виновных. Что, однако, не помешало новому госсекретарю Джону Керри отправиться в Москву в целях возобновления «женевского процесса». Впрочем, в ходе переговоров опять возникли непреодолимые разногласия по поводу судьбы Асада. В результате «Женева-2» вновь за-

буксовала. И вновь возникает вопрос: почему США упорно добиваются всегда одного и того же: смещения, а затем физического уничтожения не угодных им законных руководителей независимых стран — членов ООН?

Что, однако, не помешало высшим военным руководителям США летом того же года выступить с мрачными оценками растущей роли Аль-Кайды и других террористических групп в происходящих в Сирии событиях. Их эти факты сильно смущали с точки зрения поставки «повстанцам», среди которых все труднее стало отделять агнцев от козлищ, обещанных американцами современных вооружений, имея в виду опасность их попадания в руки террористов и последующего расползания по всему миру.

В июне 2013 года американская разведка объявила о том, что сирийские правительственные войска в нескольких боях якобы использовали малые дозы нервно-паралитического газа. С августа 2012 года прошло меньше года. Судя по всему, американский план «замочки» Асада обвинениями в использовании химоружия начал осуществляться.

21 августа, на следующий день после прибытия в Сирию по инициативе США наблюдателей ООН по расследованию этого инцидента и на фоне крупных успехов правительственных войск в освобождении территории страны от мятежных сил, пришло сообщение о массированном использовании в одном из пригородов Дамаска химического оружия против мирных граждан, в результате чего, по утверждению повстанцев и американцев, погибло более 1400 человек, из них 400 детей. Это сообщение и подсчет жертв произошли так же мгновенно, как и распространение теми же мятежниками душераздирающих кадров о конвульсиях умирающих от химического отравления людей. США тут же «с высочайшей долей уверенности» обвинили в этом преступлении сирийские власти. Западные СМИ и арабские телекомпании типа катарской «Аль-Джазиры» немедленно поддержали эту версию и данные о числе погибших, распространяя пугающие кадры жертв химатаки, по сути, готовя психологическую почву в мировом общественном мнении для американского «удара возмездия» по режиму Башара Асада.

Обама и его окружение выступили с прямой угрозой «ограниченных» военных действий против Асада в качестве «наказания» его режима. Американские ВМС с крылатыми ракетами на борту встали на якорь в восточном Средиземноморье. Джон Керри назвал химическую атаку «моральным непотребством» и, по сути, начал выстраивать политическое обоснование для американской вооруженной интервенции.

В это время Россия при согласной позиции Китая тут же выдвинула серьезные сомнения как в достоверности самих аргументов США, Франции, Британии и руководства НАТО, не исключая «постановочного» (то есть, фальсифицированного) характера распространяемых видеоматериалов жертв

атаки, так и в убедительности других фактов, выдвигаемых Западом в качестве «неопровержимых». И действительно, даже с точки зрения психологической лингвистики в заявлениях западных политиков (того же Обамы и Керри) обращало на себя внимание отсутствие безоговорочных утверждений о том, что виновными в применении химического оружия были именно сирийские правительственные войска (в них превалировали фразы «скорее всего», «следует предполагать», «можно сделать вывод» и т.п.).

При этом самым уязвимым моментом в заявлениях президента и госсекретаря была ссылка на некие данные американских спецслужб, которые невозможно было предъявить миру вследствие их секретности (впоследствии часть этих данных была показана избранным членам конгресса на закрытых заседаниях комитетов по обороне и разведке, но как выяснилось, и их они не убедили).

Кроме того, российская сторона указывала на отсутствие убедительных и неопровержимых фактических данных, подтверждающих вину правительства Асада (как говорил Путин, если под любым предлогом факты не предъявлены, считай, что их нет). И весьма аргументировано задавала западникам вопрос о том, какой смысл эта акция имела для данного правительства вообще в условиях явного своего перевеса в военных действиях, да еще под присмотром наблюдателей ООН. Россия интересовалась и тем, не были ли значительно более заинтересованы в этой атаке мятежники, их арабские спонсоры и сам Запад (прежде всего США и Израиль) в поисках легитимизации давно ими задуманной войны, направленной на свержение правящего в Сирии режима.

Тем не менее, в конце августа в Москве были почти уверены в том, что решившись на использование «химического» аргумента, Вашингтон под нажимом прежде всего Саудовской Аравии, будучи сам крайне разочарован неспособностью повстанцев свергнуть Асада самостоятельно, был готов к удару по Сирии со дня на день. Как уже указывалось, самыми рьяными его сторонниками в этом, помимо саудистов, были в то время президент Франции Ф. Олланд и британский премьер Д.Кэмерон. И как признался впоследствии Владимир Путин, для него, как и для самого Кэмерона, стал совершенно неожиданным случившийся в Лондоне облом.

Дело состояло в том, что, страдая от своей все более растущей непопулярности и падения рейтингов, страшась повторения судьбы «болонки Буша» бывшего премьера Тони Блэра, погоревшего на участии в катастрофической войне в Ираке, не менее преданный Вашингтону Кэмерон все же решил подстраховаться и заручиться одобрением парламента. Хоть и незначительным большинством, но палата общин после бурных дебатов отвергла участие страны в войне. Причина очевидна: все тот же иракский синдром и общий антивоенный, вернее, антиинтервенционистский тренд в Британии, который старейший в мире орган парламентской демократии просто не мог игнорировать. После чего якобы «потря-

сенный» (а на самом деле очень довольный тем, что удачно выкрутился) премьер объявил, что после такого голосования парламента любые военные действия Британии против Сирии исключены.

Под сильным впечатлением «ухода в отказ» важнейшего военно-политического союзника, Джон Керри, министр обороны Чак Хейгел, а также пресс-секретарь Белого дома сгоряча тут же заявили, что в таком случае Вашингтон будет действовать в одиночку. Но не прошло и двух дней, как с потрясшим Америку и мир заявлением выступил уже сам Обама: по его словам, хоть и имея формальное право как президент и Верховный главнокомандующий на единоличное принятие решения об ударе, он счел необходимым «посоветоваться с конгрессом». Ибо: самим США не грозит непосредственная опасность (хотя до этого он же утверждал, что в Сирии якобы «затронуты жизненные интересы национальной безопасности США); данные опросов показывают, что «значительное» число граждан США против этой акции; Британия отказалась в ней участвовать.

Наша же точка зрения состоит в следующем: Обама просто решил «соломки подстелить», в открытую стянув у Кэмерона лицензию на перестраховку. Согласившись с президентом, конгресс взял бы на себя часть ответственности в случае катастрофических (как в Ираке) последствий вторжения для США и всего мира; не согласившись, освободил бы его от явно тягостного и вынужденного действа (ниже мы попытаемся показать, что это было действительно так).

Тем не менее, и сам Обама, и Керри, и Хейгел, и председатель объединенного командования штабов генерал Мартин Демпсей, другие высшие сотрудники администрации в канун рассмотрения обращения президента в комитетах и на пленарных заседаниях палат конгресса, в форме срочно организованных телефонных звонков, секретных брифингтов и публичных слушаний суетливо бросились убеждать конгрессменов и сенаторов поддержать удар. А почувствовав растущее сопротивление на Капитолийском холме, президент даже заявил, что в случае отказа конгресса в поддержке, даст команду о нанесении удара самостоятельно.

В воздухе запахло конституционным кризисом, начались разговоры о том, что в случае такого развития событий, против Обамы в том же конгрессе может быть возбужден процесс импичмента. Дело в том, что вообще-то по существующим законам и в соответствии со сложившейся практикой, президент как Верховный главнокомандующий и так, без одобрения конгресса, имел право на ограниченные военные действия за рубежом продолжительностью не более 90 дней. И обращение Обамы к законодателям многие из них восприняли именно как попытку переложить на них ответственность за крайне рискованное и сомнительное мероприятие. Но уж поскольку Обама это сделал и его официальное обращение было получено, нанесение удара по Сирии при отказе конгресса его поддержать рассматривалось бы как прямой вызов законодательной власти и вообще всей системе разделения властей.

В большинстве своем находившиеся на летних каникулах в своих округах демократы и республиканцы в обеих палатах конгресса, при этом подогреваемые резкими антивоенными протестами избирателей (а в Америке в отличие от нас такие протесты не тетка, и запросто в случае «неправильного» голосования могут стоить сенатору или конгрессмену места на очередных или промежуточных выборах), все более открыто и массово высказывали свое нежелание поддерживать президента в ходе предстоящего голосования по его запросу (к этому эпизоду мы еще вернемся).

В условиях нараставшего внутриполитического кризиса, к находившемуся в Санкт-Петербурге на саммите двадцатки Обаме, разыгрывавшему из себя обиженного на Россию за предоставление убежища сотруднику АНБ Эдварду Сноудэну, на дипломатическом ужине подошел Путин, и между ними состоялся 20-минутный частный разговор. Впоследствии выяснилось, что он имел чуть ли не судьбоносный характер и для Сирии, и для Обамы, и для Путина. Ибо, судя по всему, в ходе разговора вчерне двумя президентами (но по инициативе Путина) была согласована схема выхода из тупика путем отказа правительства Сирии от всех запасов химического оружия в обмен на отказ США от ракетного удара по ее территории. Все остальное было делом техники.

Через пару дней Джон Керри вдруг «проговорился», что можно было бы отказаться от удара, если бы (что само по себе невероятно, невозможно, тут же добавил он), Асад вообще отказался от своей «химии». Его тут же «поймал на слове» Сергей Лавров и предложил посредническую роль России именно в этом — в химическом разоружении Сирии (и «чудом» оказавшийся рядом с ним в Москве в этот момент министр иностранных дел Сирии Валид Муаллем с этим немедленно согласился).

Говорят, что Обаме в сложившейся в стране и в мире ситуации (на саммите двадцатки половина участников отказалась от поддержки военной агрессии США, в самой Америке, и в конгрессе, и в народе растущее, преобладающее большинство также было против) не просто «некуда было деваться». Это было для него выходом из тупика, в который он сам себя загнал (американцы применили к его тогдашней ситуации более грубое словосочетание — dog's box). «Президент Обама в отчаянии ухватился за эту оливковую ветвь», - написал консервативный комментатор Бен Шапиро.

В результате 9 сентября президент обращается в конгресс с просьбой отложить голосование, авторизирующее военный удар. В обращении к нации 10 сентября он, все еще пытаясь убедить американцев поддержать удар, «если дипломатия не сработает», тем не менее явно сделал упор на дипломатию. В тот же день Асад объявил о готовности Сирии войти в конвенцию ООН о запрете химоружия и распрощаться со своими запасами этого оружия. Через неделю Си-

рия присоединилась к конвенции, и сейчас в этих целях в стране уже работают сотрудники международной Организации по запрещению химического оружия (ОЗХО). Все это стало возможным в результате переговоров Лавров-Керри и появления в результате этого единогласно проголосованной резолюции СБ ООН, из которой несмотря на сильнейшее сопротивление западных партнеров, России удалось изъять все угрозы применения силы против сирийского правительства.

Таким образом, на момент подготовки этой статьи можно говорить о потенциально важнейшем прецеденте выхода из опаснейшего международного кризиса. Удар США и Франции по Сирии мог вызвать непредсказуемую реакцию Израиля, Ирана, «Хезболлы», «Хамаса» и общую войну на Ближнем Востоке, в котором Россия и США оказались бы противниками в «опосредованном» военном конфликте со всеми вытекающими отсюда последствиями. Этого удалось избежать, хотя сама по себе гражданская война в Сирии продолжается при непримиримых позициях сторон конфликта и столь же непримиримых позициях США, НАТО и их арабских союзников с одной стороны, и России, Китая, Ирана и многих других стран с другой по вопросу сохранения у власти режима Б. Асада.

Понятно также и то, что сначала сам вопрос о применении химического оружия был провозглашен, а потом, скорее всего, это оружие было практически использовано мятежниками как предлог для ракетной атаки на позиции правительственных войск и центры управления Сирии в условиях исчерпанности ранее использованных средств решения главной геополитической задачи США — ликвидации Асада. Но поскольку нет никаких сомнений в том, что эта цель сохраняется и сегодня (США, как показывает их история, почти никогда не отказываются от достижения однажды намеченных целей не мытьем, так катаньем), возникает вопрос о том, как же теперь - если химическое оружие в Сирии будет действительно ликвидировано под международным контролем - американцы будут добиваться этой цели.

Впрочем, в начале октября 2013 года после очередной встречи с С. Лавровым, Джон Керри вдруг заявил, что оба министра согласились: «военный сценарий разрешения конфликта (в Сирии) невозможен и неприемлем». И в связи с этим США все еще рассчитывают на проведение конференции «Женева-2» по урегулированию ситуации в этой стране. Такому удивительному просветлению госсекретаря, еще за месяц до этого выступавшего с воинственными угрозами и призывами, можно было бы лишь порадоваться, сочтя это результатом усвоенного урока, преподнесенного Россией. Однако вызывает глубокое сомнение, что этот человек, на глазах всего мира только что совершивший головокружительный кульбит от «голубя» до «ястреба» и обратно, при малейшем изменении ситуации и подвернувшейся возможности добиться своего, не совершит сальто-мортале в противоположном направлении.

Кроме того, пока крайне сложно прогнозировать не только успех, но и сам факт проведения встречи в Женеве. Во-первых, ободренный последними внешнеполитическими успехами, президент Асад заявил, что будет принимать участие в переговорах лишь с мирной или сложившей оружие оппозицией, а не с «воюющими террористами». А это, разумеется, категорически не устраивает противоположную сторону. Во-вторых, важнейшим является вопрос о том, каково состояние этой стороны (напомним, что согласно договоренностям Лавров-Керри, правительственную делегацию Сирии приводит в Женеву Россия, а за участие в переговорах оппозиции отвечают США).

Читатель помнит, что массовую и самую боеспособную часть этой оппозиции составляют «Аль-Каида» и аффелиированные с ней террористические группировки. С самого начала те же американцы и другие западники понимали, что участие в конференции подобных элементов невозможно ни с какой точки зрения, что и было самым главным затруднением для ответов на брифингах соответствующих западных деятелей. В этих условиях Керри и его люди усиленно занимались сбиванием в единую, хотя бы «зонтичную» коалицию других, якобы более «умеренных» оппозиционеров. Эта организация представлялась миру как «Национальная коалиция». Ее военным (сражающимся с правительственными силами) крылом объявлялась «Свободная сирийская армия», возглавляемая Высшим военным советом.

Однако 5 октября выяснилось, что сразу 13 наиболее известных военных группировок отвергли свое участие в «Национальной коалиции» и присоединились к аффелиированному с «Аль-Кайдой» фронту «Аль-Нусра». Подобное скандальное решение, подрывающее саму основу успеха Джона Керри в выполнении своей части обязательств, было объяснено как ответ на «недопустимое давление» со стороны США.

Но и это не является единственной проблемой. Вроде бы лояльный Вашингтону Высший военный совет оппозиции в тот же день в очередной раз заявил, что он отрицает «диалог с террористическим режимом Сирии» (имеется в виду правительство этой страны). По его словам, «приемлемым минимумом» были бы переговоры оппозиции с некими арабскими и мусульманскими государствами, которые придерживаются выставленных Коалицией условий: «необходимости отставки Асада, передачи власти и привлечения к ответственности тех, кто совершил преступления против сирийского народа». Позднее было подтверждено, что оппозиция также отвергает участие в переговорах представителей Ирана (на чем помимо Сирии настаивает и Россия).

Кроме того, в интервью западным журналистам лидеры оппозиции неоднократно выражали крайнее разочарование начавшимся по инициативе России процессом химического разоружения Сирии и соответствующей резолюцией СБ ООН, ибо все это лишает их главного, чего они добивались: военного удара

западных союзников по режиму Асада как главному и решающему фактору, который бы позволил им одержать военную победу.

Очевидно, что при таких ожиданиях и требованиях обеих сторон переговоры между ними маловероятны в принципе, не говоря уж о возможности их позитивного исхода. И, тем не менее, главное уже произошло: считавшийся неминуемым американский военный удар по Сирии был предотвращен, причем по инициативе России, что полностью изменило всю геополитическую картину в регионе, и не только там.

В связи с этим нас интересуют три немаловажных вопроса: что ознаменовал сирийский кризис во внутренней политике США; что решающая роль Москвы в разрешении наиболее опасной фазы кризиса означает для международного положения России; что этот кризис и его во многом неожиданное развитие означают с точки зрения мировой геополитики и геополитики США.

Сирия как катализатор бунта в США: американцы устали воевать

Сирийская история показала: иракский урок не забыт в Америке. Повторения его нация не хочет. Об это активное нежелание обломали зубы администрация, воители в обеих фракциях конгресса и вынуждены были отступить. Прежде всего выяснилось, что американским законодателям стало трудно, или вообще невозможно голосовать против собственных избирателей. Так, один из них сообщил, что в его округе 97 процентов избирателей против любого военного вмешательства США в Сирии. В целом, в начале сентября 2013 года поддержка военного удара американским общественным мнением начала ослабевать.

Так, согласно опросу Гэллап за 3-4 сентября, 36 процентов взрослых американцев поддерживали интервенцию своей страны в Сирию в связи с выдвинутыми в адрес ее правительства обвинениями в использовании химоружия. Однако уже тогда 51 процент опрошенных оказались против при 13% не определившихся. При этом Гэллап отметил, что обычно американцы склонны поддерживать военные акции своей страны после того, как они начинаются. К примеру, перед вторжением США в Ирак в 2003 году 59% одобряли идею этой акции, а после вторжения и вообще 76%. Первоначальная поддержка войны в Афганистане в 2001 году была еще выше — 82% - а после начала военных действий вообще поднялась до 90%.

Но на этот раз, по выводу того же Гэллап, низкий уровень поддержки военной акции в Сирии явился лишь отражением общего тренда в стране. «Американцы — по крайней мере, вначале — значительно более активно поддерживали предыдущие военные предприятия, — сообщили сотрудники Гэллап. — Однако более чем через десятилетие после конфликтов в Афганистане и в Ираке в обществе сохраняется усталость от войны». Отражая эти настроения, стала меняться позиция многих сенаторов и конгрессменов.

6 сентября корреспондент «Нью-Йорк таймс» сообщал из Мидвест-сити, штат Оклахома о том, как этот процесс отразился на члене Палаты представителей республиканце Томе Коле. Вначале этот склонный к компромиссам с исполнительной властью ветеран конгресса, избиравшийся туда уже шесть раз, склонялся к поддержке изначально воинственной позиции Обамы. Но избиратели круто изменили его мнение на противоположное. Прямо на автостоянке в провинциальном городе, узнав его, одна из женщин ему сказала: «Здесь все говорят «нет» (удару по Сирии). По словам Кола, «опыт с дорогой на Дамаск» именно под влиянием избирателей выглядит теперь для него совсем по-иному.

Другой конгрессмен - республиканец Мик Малвани из Южной Каролины (вообще-то правый по своим взглядам политик) заявил, что за годы его пребывания в конгрессе ни один вопрос не получал такого эмоционального отклика среди населения, как сирийский. По его словам, сказать, что «99 процентов против, было бы еще переоценкой поддержки» военного удара. Из более чем 1000 полученных им звонков и электронной почты лишь в трех (!) откликах поддерживался такой удар.

Конгрессмен Кэндис Миллер, республиканка из Мичигана, рассказала, что была на совсем не политическом мероприятии — «фестивале персиков» в ее округе, но и там люди, в том числе ветераны, постоянно подходили к ней и требовали голосовать против войны.

Показательным является и наблюдение корреспондента «Нью-Йорк таймс» в округе Тома Кола на юго-западе штата Оклахома — оплоте республиканцев, эпицентре антиобамовских («антисоциалистических») настроений и господства традиционно милитаристского духа с учетом наличия большой базы ВВС с 8 тысячью военнослужащих и 15 тысячью гражданского персонала. Но и там протесты против военного вмешательства в Сирию были почти единодушны. Результатом явилось удивительное просветление ума и у самого конгрессмена от этого округа. Говоря о положении в Сирии, он сказал: «Ведь это гражданская война, это опосредованная война между региональными державами, и это религиозная война. Есть ли здесь какая-либо прямая угроза безопасности Соединенным Штатам? Нет. На самом деле нет».

В результате аналогичных «летних впечатлений» и других обитателей Капиталийского холма, стало очевидным, что большинство не только в доминируемой республиканцами нижней палате, но возможно, и в продемократическом сенате, будут голосовать против удара. Так, согласно подсчетам газеты «Вашингтон пост», из 433 членов палаты представителей 222 твердо собирались проголосовать «нет» или склонялись к этому, 184 не определили свою позицию и лишь 24 поддерживали удар. В сенате большинство мест (54 против 46 у республиканцев) принадлежит демократам, но в канун предполагавшегося голосования большин-

ство из 99 сенаторов так и не определилось со своим решением, в то время как для поддержки сенатом удара по Сирии требовалось 60 голосов.

Отсюда возник вопрос: что же делать в этой ситуации президенту? Начинать войну вопреки мнению законодателей? Но такое возможно представить где угодно, включая Россию, но только не в США. Ветеран американской журналистки Питер Бейкер написал в этой связи в «Нью-Йорк таймс» о том, что подобное решение Обамы изолировало бы его в стране навечно. Более того, это почти наверняка вызвало бы попытку палаты представителей подвергнуть его импичменту.

Однако нам более верным представляется другое объяснение обращения Обамы за разрешением или одобрением к конгрессу — легитимизировать истинный настрой главы Белого дома на то, чтобы не делать ничего в случае ожидаемого отказа законодателей. Как писала «Уолл-стрит джорнэл», идея о том, что президент, не проявив воли к принятию самостоятельного решения об ударе, вдруг наберется дерзости и сделает это вопреки мнению конгресса, «граничила с фантазией». Зачем же президенту вообще нужна была эта затея? Можно предположить, что он действовал под объединенным прессингом военно-промышленного, финансового, саудистского и израильского лобби (что примерно одно и то же), сам не испытывая от этой идеи большого энтузиазма.

Однако во всем происходившем в дни вашингтонского «сирийского кризиса» был и сохраняется до сих пор еще один важнейший аспект, в полной мере проявившийся в другом, даже более опасном кризисе в октябре вокруг т.н. отставки правительства и угрозы дефолта по долговым обязательствам США. Речь идет о расколе элит в США и резком падении авторитета как законодательной, так и исполнительной власти в глазах американского народа.

Что касается Обамы, то, как писал бывший сотрудник демократической администрации Клинтона Дэвид Роткопф, отказ конгресса поддержать предложенный Обамой удар по Сирии стал бы «катастрофой» для президента. «Он подтвердил бы представление о нем как о «хромой утке» в самый ранний период второго президентства во всей новейшей истории, — считал Роткопф.- Он стал бы выглядеть ослабленным и вряд ли смог бы чего-то добиться за оставшееся время у власти». От себя хотим предложить читателю представить себе, как и с каким результатом разворачивалась бы в этом случае схватка Обамы с республиканцами по бюджетным вопросам месяц спустя.

Кстати, в ходе схватки вокруг Сирии на Капиталийском холме сложилась казавшаяся прежде невероятной коалиция крайне правых республиканцев из «чайной партии» и левых либералов-демократов. И те, и другие открыто заявляли о намерении голосовать против удара.

Все это вместе взятое заставило известного американского журналиста, дважды лауреата Пулитцеровской премии Дэвида Рода сослаться на мнение Чарльза Блоу в «Нью-Йорк таймс» о наступлении в Америке «эпохи безверия», когда

народ перестал доверять и президенту, и конгрессу. Все началось с войны в Ираке, но «длинный список других полуправд опустил общественное доверие к государственным институтам до рекордно низкого уровня».

Надо отметить, что события в октябре-ноябре во внутренней политике США только усугубили ситуацию. Устроенный республиканцами под диктовку своей «чайной партии» кризис с «закрытием правительства» и угрозой дефолта страны резко подорвали доверие американцев и к законодателям, и к президенту. Позднее провал со «знаковой» инициативой Обамы по обеспечению американцев бесплатными медицинскими страховками еще сильнее ударил по президенту. В результате доверие к конгрессу опустилось в стране до рекордных 32 процентов.

Еще более драматичным видится сейчас ситуация с Обамой. Судя по всему, на его популярности губительно сказывается коммулятивный эффект очевидной «сирийской слабости» президента, а также скандалов вокруг «закрытия правительства», дефолта и закона о страховках. В любом случае, по оценкам агентства Франс пресс, «несуразности» второго срока президентства принесли ему рекордно низкие рейтинги и вдребезги подорвали доверие к нему американского народа.

Опрос телекомпании Эн-би-си и газеты «Уолл-стрит джорнэл» от 1 ноября снизил рейтинг одобрения деятельности Обамы до 42%. Неделей позже, опрос агентства «Пью» дал ему 41%. 13 ноября традиционно авторитетное исследование университета Куиннипиак выставило президенту уже 39%. В том же исследовании американцы впервые высказали мнение, что Обама «ненадежный» и «нечестный».

По мнению американских социологов, подобные цифры свидетельствуют о том, что он не может более рассчитывать на солидную поддержку общества, которое могло бы поддержать его погрязшее в кризисе президентство. И сравнить его судьбу можно лишь с тем, с чем столкнулся Джордж Буш-младший, который после окончания своего второго срока еле выкарабкался из Вашингтона с жалкими 34% рейтинга одобрения его деятельности.

Как указывает Рот, первым грехом Обамы на посту президента стали противоречия в его политике. По многим вопросам, связанным с войной с террором, он нарушал собственные обещания или занимал непоследовательную позицию. Теперь же президент требовал от американцев довериться ему по сирийскому вопросу. Но они отказали ему в доверии.

Во-первых, встал вопрос о политике США на Ближнем Востоке в целом. Ранее Обама говорил американцам, что США должны вытащить себя из этого региона. Он продекларировал «поворот к Азии» - региону, по его словам несравненно более важном для экономического будущего США. И поэтому — говорил он - из Ирака и Афганистана мы должны уйти и никогда туда больше не возвращаться.

В течение двух лет то же самое говорилось о Сирии. Но теперь президент заявляет, что действия в этой стране вдруг стали «жизненно важны» для Америки. Вопрос: почему именно сейчас?

По словам Рота, одним из «удивительных» для США явлений (и это действительно так — Л.Д.) стал тот факт, что несмотря на неистовую поддержку удара по Сирии со стороны прежде казавшихся всемогущими в своих лоббистских возможностях правительства Израиля и американо-израильского общественного Комитета, и они не смогли переломить нежелание законодателей начинать войну, включая консервативное крыло республиканцев, ранее всегда активно поддерживавшее Израиль.

Что касается Обамы, то недоверие к нему справа не новость, писал Рот. Консерваторы не доверяли ему годами. Однако что реально угрожает президенту, это отсутствие доверия со стороны его либеральной базы. Со времени переизбрания на второй срок либералы предъявляют растущий список невыполненных им обещаний. К примеру, он предпринял лишь вялую (по сути, никакую) попытку закрыть американскую военную базу и тюрьму в Гуантанамо. Настаивал на скрытных, держащихся в секрете от общественности ударах дронов (в частности, в Пакистане и Йемене, где это по данным ведущих западных правозащитных организаций «Амнисти интернэшнл» и «Хьюман райтс уотч» приводит к многочисленным жертвам среди мирного населения — Л.Д.) и жестко отстаивал разоблаченную Эдвардом Сноудэном расширяющуюся слежку АНБ за гражданами США и других стран, в том числе таких как Франция, Германия, Бразилия, Мексика и т.д.

В результате кандидат, который как считали либералы, вернет в борьбу с террором главенство закона, продолжил беззаконную практику Джорджа Буша-младшего. Посвятив большую часть обоих своих президентских сроков расширению власти имперского президентства, теперь вдруг Обама обратился к конгрессу с просьбой поддержать его по Сирии…

Рот отметил, что аналогичное недоверие к США выражается и за границей. Европейцы, ожидавшие результата обещанных американцами антитеррористических мер с точки зрения обеспечения своей безопасности, сегодня испытывают разочарование. Утечки же от Сноудэна оказались вообще катастрофичными для имиджа США. От Германии до Мексики АНБ шпионило за иностранными лидерами, при этом настаивая, что ничего подобного не делает.

Не менее жестко откомментировал сложившуюся ситуацию на страницах «Нью-Йорк таймс» и другой известный журналист Росс Доутхэт. «Леди и джентльмены, добро пожаловать в фиаско внешней политики», - начал он свою статью. И продолжил: «С самого начало было очевидно, что у президента Обамы в сирийской гражданской войне не было ничего, кроме плохого выбора. И, тем не менее, теперь он нашел способ поставить и конгресс в аналогичную

проигрышную позицию. Когда палата представителей и сенат будут голосовать по поводу авторизации удара по Башару Асаду, они будут делать выбор между двумя в равной степени катастрофическими решениями: или поддержав косвенную войну между многими противоборствующими сторонами, то есть сделав то, чему судя по всему, сам Белый дом в принципе не может найти оправдания, или же проголосовав так, что это фактически покончит с нынешним президентом как с заслуживающим доверия актором на мировой сцене».

Любопытно, что аналогичным образом оценивали провал, в котором оказалась внешняя политика США не только либералы из «Нью-Йорк таймс», но и неоконсерваторы со страниц «Уолл-стрит джорнэл». По словам известного ястреба Нормана Подгореца, цитировавшего «дальновидного специалиста в области международной политики» Конрада Блэка, «ни с момента дезинтеграции Советского Союза в 1991 году, ни перед падением Франции в 1940 году, просто не было такой быстрой эрозии мирового влияния, как мы наблюдаем сегодня в случае Соединенных Штатов».

Фактор Путина

Но произошло еще нечто, что Западу и особенно Вашингтону не могло присниться и в страшном сне: на фоне указанного провала демонизированный и заклейменный там Владимир Путин из России неожиданно вырвался на передний план мировой политики. Его «подход» на саммите в Петербурге к разыгрывавшему из себя обиженного Обаме и проведенный им в состоявшемся разговоре «мозговой штурм» привели к кардинальному развороту всей мировой политики. От прямой угрозы «Большой войны» на Ближнем Востоке с катастрофическими последствиями для всего мира - к политическому решению проблемы сирийского химического оружия, что заставило говорить о «ренессансе классической дипломатии», основанном на нормах международного права как предпочтительном варианте решения сложных конфликтов. Все остальное стало делом техники.

В результате звездой мировой политики, по крайней мере ситуационно, вместо лауреата Нобелевской премии мира Барака Обамы стал Владимир Путин. Причем признание его заслуг началось с консерваторов. Известный правый американский блогер Мэтью Драдж вообще назвал его «лидером свободного мира». Но позитивные суждения о российском лидере появились и в таких общепризнанных изданиях, как журнал «Форин афферс», издаваемый Советом по внешней политике США. Простое объяснение состоит в том, что как выяснилось, Путин оказался по одну сторону баррикады с большинством американцев — противников вмешательства США в войну в Сирии.

Как писал в те сентябрьские дни научный сотрудник Гарвардского университета Симон Сарадзьян, «первопричиной увеличения позитивных откликов о России является то… каким последовательным, проницательным и эффективным был Путин в решении таких проблем, как Сирия и Сноудэн в сравнении с его за-

падными партнерами. Вопреки давлению со стороны США, он и не подумал изменить свою позицию, и как показали опросы, значительная часть американского общества значительно ближе к его позиции, чем к позиции Обамы… в противодействии вовлечению в гражданскую войну в другом государстве».

По мнению экономиста Клиффорда Гэдди, последние несколько недель показали, какой сложной политической фигурой является Путин. «Он, возможно, наиболее серьезный противник, с которым сталкивалась Америка на протяжении длительного периода времени, — говорит Гэдди. — Он умен и беспринципен, мастерски использует слабости и ошибки людей в игре против них — то есть, использует умения, полученные во время работы офицером КГБ».

Агентство Ассошиэйтед пресс в этой связи отмечало еще одну неожиданно привлекшую к нему симпатии многих в США черту — путинский консерватизм, как социальный (поддержка Русской православной церкви и отсутствие поддержки сексуальных меньшинств), так и финансовый (стремление к обеспечению сбалансированности бюджета, низким налогам и т.п.). Для некоторых консервативных американцев, пишет АП, это делает Путина более привлекательным, чем их собственный президент.

«То, что (американские правые) говорят о Путине, вызвано прежде всего… их оппозицией Обаме, — говорит Гэдди. — Они ненавидят Обаму, они не выносят обамовскую внешнюю политику и его команду в области безопасности — Сьюзен Райс (советницу президента по нацбезопасности), Саманту Пауерс (посла США при ООН) и т.д. и т.п. И как только Путин взял на себя роль непререкаемого лидера оппозиции запланированной Обамой интервенции против Сирии, он неожиданно стал выглядеть более симпатично».

«Путин не спас Обаму, он его побил», - не без удовлетворения написал Ли Смит в еще одном консервативном издании — еженедельнике «Уикли Стэндарт».

Очевидная поддержка Путиным закона, ограничивающего в России права ЛГБТ может быть другим фактором. Правые считают, отмечал Гэдди, что Путин перехватил у США лидерство в области внешней политики в то время, когда команда Обамы посвятила эту политику продвижению ценностей, к которым они — правые — испытывают абсолютное отвращение, таким как права сексменьшинств. «Вот почему они из чисто провокационных соображений противопоставили Обаме имидж Путина как «хорошего парня».

Что бы за этим не стояло, писало агентство АП, в нынешнем мире образ Путина как «крутого» лидера достаточно уникален, особенно в сравнении с мягкотелым стилем руководства Обамы, Кэмерона, Олланда или Ангелы Меркель. «Все сейчас нуждаются в лидерстве, - признает сотрудница Брукингского института и соавтор книги «Владимир Путин — оперативник в Кремле» Фиона Хилл. — (Путин) имеет в этом перевес».

Аналогичные оценки содержались и в аналитической статье агентства Рейтер под заголовком «Как Владимир Путин похитил ответ Белого дома Сирии». В ней содержалось признание редактора правого американского журнала «Нью Рипаблик» Джулии Йоффе»: «Есть два чистых победителя в этом крушении в замедленном темпе. И это не Обама или Керри. Это Асад и Путин» (23 октября лондонская «Дейли телеграф» заявила, что теперь «западные лидеры должны смириться с тем, что Асад выигрывает и контролирует ситуацию… И в долгосрочной перспективе больше в интересах Запада — стабильная Сирия с Асадом у руля, чем неуправляемая страна, где будут процветать исламские террористические ячейки»).

Во всем происходившем в те сентябрьские дни заключалось проявление не просто глубоких противоречий, но настоящего кризиса американской внешней политики (внутренний кризис в США произошел в октябре, когда демократы, республиканцы и Белый дом оказались в конфронтации по бюджетно-финансовым вопросам, оставившей большинство американцев в еще большем возмущении от конгресса и президента, чем их провал по Сирии).

Ведь вышеописанная американскими журналистами ситуация действительно налицо. Как написал Томас Лифсон в журнале «Американ Синкер», «Это — колоссальная победа Путина и поражение Обамы».

Да, по сирийскому вопросу внешняя политика Вашингтона была действительно стреножена Путиным. И это вызвало там крайне неоднозначную реакцию — не только злорадство правых противников Обамы, но и болезненную со стороны большой части элиты и большой части общества — тех американцев, которые привыкли (особенно после 1991 года) к пониманию своей страны как единственного и незаменимого мирового лидера, а Россию считали не более чем побежденной стороной, с которой в принципе можно было и не считаться. В этом смысле самый болезненный удар по самолюбию американцев был нанесен не только самим фактом «перехвата» Путиным ожидавшегося ими очередного военно-политического триумфа на Ближнем Востоке, но и тем, что осуществлен этот удар был, как им казалось, законченным подранком.

Как опытный политик Путин это понял и расчетливо нанес еще один удар в самое больное место американской души, заявив в своей исключительно профессионально написанной статье в «Нью-Йорк таймс» об отрицании Россией исключительности Америки. То есть по главному символу веры американцев, на котором воспитывались поколения граждан этой страны. Причем нанес тогда, когда под влиянием провалов в Ираке и Афганистане, а главное — углубляющимся на глазах финансово-экономическом кризисе и явной утерей США лидирующих позиций в мире, сама элита и сами граждане фактически стали приходить к тому же выводу.

Как отмечалось в обзоре Би-би-си, поначалу политический истеблишмент Америки - и консерваторы, и либералы - дружно заклеймил путинский текст. Однако первыми спохватились именно консерваторы, осознав, что президент России в своей статье, по сути, не сказал ничего нового, что бы ранее не говорил сам Обама. На сайте консервативного журнала «Американ спектейтор» Джеймс Пиерсон заметил, что Путин повторил буквально то, что американские либералы и левые (откуда и вышел Обама как политик) говорят с начала 60-х годов.

«И где мы уже слышали изложенные Путиным принципы? - вопрошал Пиерсон. — Да они являются основными символами веры американских либералов, которые десятилетиями твердят, что США не должны применять силу без санкции ООН, что нам не следует вмешиваться в гражданские войны за границей, и что идея американской исключительности — это миф, рассчитанный на то, чтобы маскировать преступления против женщин и нацменьшинств на родине и против бедных и угнетенных за границей». По словам Пиерсона, «в наши дни в любом крупном вузе США читают курсы по мультикультурализму и американистике с нападками на концепцию американской исключительности, которая толкуется как проявление национальной спеси».

Автор продолжает: «Представление о том, что Америка является исключительной страной, зародилось вскоре после Революции, когда люди из поколения основателей обратили внимание на то, что США были первой страной, основанной на универсальных принципах свободы и равенства. Они были «первой новой страной» и образцом для подражания. Но в сегодняшних студгородках Америки это представление клеймится как фикция, поскольку, несмотря на свою риторику, ее правящие классы потакали рабовладению, расовым предубеждениям и национальным предрассудкам. Академическая американистика сосредоточена на систематическом развенчании идеала американской исключительности, поскольку считает, что он служит оправданием привилегий белого человека и применения американской мощи за границей… Это символ веры либералов и левых с эпохи вьетнамской войны».

Получается, заключал Пиерсон, что критикуя высказанные Путином принципы, американские либералы изменяют своим собственным. По сути, ту же точку зрения тогда же в сентябре высказали и известнейшие американские консерваторы и правые. Так, Пэт Бьюкенен заявил, что своей колонкой Путин «попал в точку», поскольку апеллировал к той половине американцев, что и Обама (на них тот опирался, их приоритеты отражал в ходе обеих своих выборных кампаний — Л.Д.). А публицист Эндрю Клейван в статье на сайте pjmedia вообще полагал, что Путин и Обама — единомышленники.

Впрочем, в американской прессе можно найти и противоположную этому точку зрения. В статье Пегги Нунан в «Уолл-стрит джорнэл» приводится мнение одного эксперта по внешней политике, согласно которому сам Путин хотел

бы иметь дело с Ричардом Никсоном, то есть «американским президентом, с которым он мог бы по-настоящему вести переговоры, суровым игроком, который может обсуждать геополитику и нужды своей страны и с которым можно «перетереть» и найти выход. Но вместо этого он имеет Обаму, зацикленного на себе харизматика, который не видит разницы между шоу-бизнесом и стратегией и любит нагружать собеседника своими моральными озарениями».

В любом случае мы приходим к выводу об уникальности сложившейся в США ситуации, когда по совершенно разным ценностным и политическим причинам многие правые, левые и либералы в этой стране оказались объединены полным неприятием не просто предполагавшейся сирийской авантюры, а основной линии всей внешней и военной политики Вашингтона на протяжении десятилетий — политики интервенциализма и навязывания всему человечеству интересов американского крупного капитала и ВПК. Силы, об огромной опасности которой для Америки и всего мира еще в середине прошлого века предупреждали, уходя на покой, такие знаменитости, как президент Дуайт Эйзенхауэр и сенатор Уильям Фулбрайт.

Новый изоляционизм?

Уникальность ситуации проявилась и в том, что под влиянием «сирийского синдрома» на повестку для общенациональной дискуссии в США вернулась философия изоляционизма, казалось бы, давно отошедшая в историю и в последние десятилетия поддерживавшаяся там лишь горсткой крайне правых, объединенных в основном вокруг либертарианского по своей идеологии Института Катона в Вашингтоне (Cato Institute).

Как отмечалось в американской печати, ставшее очевидным нежелание президента и конгресса влезать в очередную «историю» за рубежом стало лишь отражением уже давно сложившегося мнения большинства американцев. Два проведенных в сентябре общенациональных опроса показали, что большинство граждан страны вопреки всем кармам об американском лидерстве и якобы возложенной на них самим господом ответственности за остальное человечество откровенно рады уступить эту роль другим странам, а в случае с разрешением кризиса в Сирии — России и Владимиру Путину.

По данным этих опросов, приведенных в статье «Вашингтон пост», лишь 34% американцев полагают, что США должны играть лидирующую роль в разрешении международных конфликтов, а 72% против усилий своего правительства по свержению руководителей других стран вне зависимости от того, заслуживают они этого или нет.

По словам авторов статьи Аарона Блейка и Сина Салливана, сейчас американцы даже еще более решительно против интервенций своей страны за рубежом, чем на пике протестов против войн в Афганистане и Ираке. Американские комментаторы при этом отмечали, что «лидер свободного мира» не был охвачен

подобными изоляционистскими настроениями с 30-х годов прошлого века. Как известно, по окончании второй мировой войны эти настроения в США сменились на горделивое самомнение о себе как о неизвестно кем уполномоченном единоличном «защитнике» угодного Штатам мирового порядка.

Как известно, десятилетиями, если не столетиями американцы преследовали свои навязчивые идеи мирового лидерства под стягом насильственного осчастливливания человечества их моделью демократии. Знаменательно, что сегодня от этого склонны отказаться даже республиканцы. Так, по данным Би-би-си, если при Буше 60% членов этой партии считали, что Америка должна устанавливать в мире демократию, то сейчас эта пропорция сократилась до 19 процентов.

В этой связи очень показательна статья Патрика Смита в журнале «Салон». По его мнению, американцам следует надеяться на то, что «план Белого дома, руководящего страной-изгоем США по бомбардировке Сирии отправится в утиль-сырье раз и навсегда, поскольку это поражение на мировой сцене предохранит Америку от вовлечения в новую интервенцию, рассчитанную на извлечение максимума из каждой ближневосточной нефтяной скважины».

По словам Смита, у США теперь появился шанс покончить, наконец, со своей старой, маниакальной претензией на мировое лидерство, которая не соответствует урокам истории, убедительному обоснованию или (как в данном случае) фактом из утренних газет, если их правильно интерпретировать. Подобные шансы часто не появляются. Воспользуемся же им и уберем из нашей внешней политики элемент назойливой иррациональности, востребовавшей миллионы жизней во время нашего «американского века» и вновь и вновь доказывающей свою опасность, заключает этот автор.

По словам других американских наблюдателей, помимо США, пока еще остались другие мыслящие интервенционистским образом страны, демонстрирующие растущую готовность влезать в такие места в мире, которых Америке следовало бы избегать. По словам Сьюзан Кески из интернет-издания «Уик», Франция, которую «высмеивали как мышь, лезущую в мышеловку на запах сыра» накануне вторжения в Ирак в 2008 году, вновь оказалась в авангарде вторжения в Ливию, затем в Мали и теперь она же громче всех призывает к военным действиям против Сирии. Вывод: вот пусть такие «мыши» и таскают геополитический «сыр» для Штатов, если хотят. А сами американцы уже устали от этого.

Тема этой геополитической «усталости» США в связи с конфликтом в Сирии подробно рассматривается в ключевой по важности публикации — Говарда Лафранчи в газете «Крисчен сайенс монитор» от 29 сентября. Как утверждает автор статьи, «после десятилетия войн на Ближнем Востоке и в мусульманском мире, и после «великой рецессии» (имеется в виду финансовый кризис 2008 года — Л.Н.), измотавшей Соединенные Штаты экономически и психологически, американцы, судя по всему, собираются сушить весла и забыть об остальном

мире. Из одного опроса в другой процент американцев, предпочитающих избегать вовлечения в мировую политику, достигает рекордных величин — наивысших за последние 70 лет».

Что же касается Обамы, пишет Лафранчи, то опросы, проведенные в ходе его сентябрьской 10-дневной кампании по завоеванию общественной поддержки плана «наказать» Сирию, выявили большее сопротивление этому плану, чем всем непопулярным президентским интервенционистским инициативам последних десятилетий.

Более того, опросы выявили, что американцы, вступившие в сознательную жизнь на рубеже нового тысячелетия, особо остерегаются вовлечения в глобальные дела, а это свидетельствует о том, что указанный тренд будет влиять на роль Америки в мире и на перспективу.

Впрочем, подчеркивает автор статьи, в то время как ряд экспертов и ученых мужей возвещают приход нового изоляционизма, другие считают: если это и произойдет, то не так скоро. И либертарианцы, и «прогрессивные интернационалисты» в один голос говорят о том, что после войн в Афганистане и Ираке, которые стоили США много крови и денег (хотя самим этим странам многократно больше), американцы стали мыслить решительно не интервенционистски.

Это не обязательно означает, что они хотят самоизолироваться от остального мира. «Они бы хотели, чтобы Америка продолжала взаимодействовать с миром, но не в одиночку. К чему они питают отвращение — это к Америке как к «Мистеру Fix-it» (рекламный образ «Мистера-Почини» — Л.Д.), особенно в том случае, если решение включает в себя военную интервенцию», - отмечает Лафранчи.

В наши дни американцы сторонятся применения силы. Они хотят заниматься своими делами в собственной стране — приводится в статье мнение организатора национальных опросов из авторитетного «Исследовательского центра Пью» Андрю Кохута, обнаружившего в июле 2013 года, что почти половина американцев (46 процентов) предпочла бы, чтобы США «занимались своими собственными делами», позволяя другим странам «жить так, как они хотят самостоятельно».

При этом те, кто не согласны с искушением оставить мир в покое, по-прежнему в большинстве (их 50%). Однако Центр Пью и другие опросные организации регистрируют падение на 15% в сравнении с пиком после 11 сентября 2001 года числа тех, кто поддерживает вовлечение США в мировые дела.

Заслуживает внимания мнение Говарда Лафранчи о том, что одной из причин, по которой преобладающее настроение в нынешней Америке ассоциируется с изоляционизмом - это история страны, в частности, период после первой мировой войны, когда изоляционизм в США был в зените. В 20-е — 30-е годы американская антипатия к ужасам войны и их замешательство перед непрекращаю-

щейся политической конфронтацией в Европе привели тогда к общему желанию сидеть дома и избегать конфликта на своем континенте.

По мнению некоторых историков, сравнение нынешних событий на Ближнем Востоке с тем, что творилось в Европе около века назад, играет роль своеобразного катализатора для тех американцев, кто «хочет домой». Как считает цитируемый в статье эксперт по военным интервенциям США и изоляционизму в государственном университете штата Орегон Кристофер Николс, «американцы в 20-е — 30-е годы испытывали глубокую усталость, и неясные, трудные для понимания и по всем признакам не поддающиеся решению проблемы в Европе лишь усилили тогда мнение, что Америке не было смысла вновь туда влезать».

Сегодняшние параллели с Ближним Востоком, особенно после войн в Ираке и Афганистане, очевидны для эксперта. Этот опыт лишь усиливает понимание в стране того, что интервенция — это не путь решения американских проблем. И тогда, и сейчас сильный импульс — «не лезть за границу, когда существует масса проблем для решения дома». Николс видит и другое сходство между эрой изоляционизма после первой мировой войны и сегодняшним временем: в обоих случаях «политические радикалы из неинтервенционистского спектра, от консервативных «традиционалистов» в области внешней политики до борцов за мир, формируют удивительный альянс против вмешательства США в конфликты за рубежом».

К примеру, сейчас либертарианец, сенатор Рэнд Пол (республиканец от штата Кентукки) и любимец «чайной партии» сенатор Тед Круз (республиканец от штата Техас) выступали против интервенции США в Сирию с использованием риторики, очень похожей на ту, с которой выступают левый сенатор Берни Сэндерс (независимый от штата Вермонт), антивоенная группа «Коуд пинк» или бывший конгрессмен-республиканец Деннис Кусинич, протестовавший против интервенции США в Ливию.

«Дьявол присутствует по обе стороны конфликта (в Сирии)… и я не вижу никакого четко выраженного американского интереса», который бы оправдывал участие Соединенных Штатов в этой гражданской войне, — говорит сенатор Пол. «Это не задача войск США обеспечивать полицейскими мерами соблюдение международных норм в отношении химического оружия», - считает сенатор Круз. «Американский народ разделяет озабоченность президента в отношении химического оружия в Сирии, - полагает сенатор Сэндерс.- Но в своем подавляющем большинстве… он хочет решать этот вопрос дипломатическими методами… а не односторонними военными действиями».

Вывод К. Николса: «Мы видим крайние полюса американских левых и правых, объединившихся против интервенции в Сирию, так же как мы видим пацифистов и изоляционистов 30-х годов, сблизившихся в их сопротивлении вмешательству в международные конфликты и даже в пользу всеобщего разоружения».

В конце 40-х годов, напоминает автор статьи, в США разгорелись бурные дебаты в отношении степени участия страны в послевоенном устройстве мира. Одним из лидеров движения «невмешательства» был влиятельный сенатор из штата Огайо Роберт Тафт, получивший прозвище «мистер Республиканец». Тафт яростно боролся против участия США в только что сформированном блоке НАТО, который по его убеждению неминуемо вовлекал страну в выполнение полицейских функций в мире и создавал «профессию милитаристов». Вместо этого он призывал Штаты укрыться в «крепости Америка».

По мнению Лафранчи, сравнение линии Тафта с ныне происходящими в США и в мире процессами «работает постольку поскольку», ибо все понимают: видение Америки, укрывшейся за забором и обособившейся от мира, сегодня уже нереализуемо.

И, тем не менее, мы являемся, возможно, свидетелями подъема в США «нового изоляционизма» — с одной стороны, опирающегося на печальный опыт провала двух ближневосточных войн и сомнительных с моральной точки зрения аргументов в пользу продолжения американских интервенций за рубежом, но в то же время, признающего необходимость глобального взаимодействия, особенно в плане содействия мировой торговле (в чем так остро нуждается сегодня экономика США, добавим от себя — Л.Д.).

«Что мы видим сегодня — это что-то наподобие изоляционизма, но не в той степени, как это было в 20-е — 30-е годы, - считает Джеймс Меерник, эксперт по политике использования военной силы во внешней политике США из Университета Северного Техаса. — Для нынешних США это уже просто невозможно». Глобализированная экономика, торговые отношения США (с внешним миром) и признание международного измерения растущего числа проблем — от терроризма до изменения климата — означает «признание людьми, что мы сегодня уже не можем сегодня просто закрыть лавку и забыть об остальном мире», — говорит он.

Однако опыт с войнами в Ираке и в Афганистане, также как и интервенции в Ливию, выглядевшей в глазах американцев как успех, пока исламисты там в условиях наступившего после этой интервенции хаоса не укокошили четырех граждан США, включая посла, предельно ожесточили отношение в стране к военному вовлечению за рубежом, особенно в гражданские войны на Ближнем Востоке (еще более горький опыт агрессии против Кореи и Вьетнама в Штатах, судя по всему, благополучно забыт).

Убийство посла Кристофера Стивенса в ливийском городе Бенгази, благодаря его ключевой роли по организации свержения Муаммара Кадаффи и его правительства выглядевшего в глазах в то время проамериканской оппозиции в это стране прямо-таки героем, по словам Меерника, «поставило в центр внимания то смятение, которое стали испытывать американцы в целом по поводу наших ин-

тервенций на Ближнем Востоке, подчеркивая долговременные сомнения о том, кому же на самом деле пытаются помочь Штаты в ходе происходящих в регионе гражданских войн, кто же там на самом деле «хорошие парни» и в реальности, наносят ли американцы с их участием поражение «Аль Каиде», или наоборот, усиливают ее».

Думаю, что для наших студентов и преподавателей должен быть особенно интересен взгляд на идею «нового изоляционизма» упоминавшихся ранее «миллениалс» - американских молодых людей, родившихся на рубеже нового тысячелетия, которым сейчас от 18 до 29 лет. Так вот выяснилось, что это поколение больше, чем большинство американцев, хотело бы избежать вовлечения в мировые дела, «передохнуть» от мировых конфликтов.

Как отмечает Стивен Кулл, директор программы по выработке подходов к внешней политике Университета штата Мэриленд, «на протяжении многих десятилетий около двух третей американцев полагали, что США должны играть активную роль в мировой политике, хотя политика на этом направлении и шла по нисходящей. Но недавно мы стали замечать их озабоченность, что Америка слишком далеко заступила за рубежи страны, в особенности на Ближний Восток, что наше присутствие там было неэффективным и более чем что-либо иное вызвало обратную негативную реакцию».

В прошлом году опрос, проведенный Чикагским советом по международным отношениям показал, что более половины (52%) американцев- представителей возрастной группы от 18 до 29 лет заявили: они предпочитают, чтобы их страна вообще «не участвовала» в мировых делах. Их было значительно больше, чем тех 38% всех американцев, кто предпочел опцию «участвовать» ответу «играть активную роль». При этом Кулл отмечает, что и эти 38% сторонников пассивного пребывания США в мировой политике — это самый высокий показатель такого рода за семь десятилетий.

В конце концов, пишет Лафранчи, очевидное нежелание «миллиниалс» впутываться в дела других стран вполне объяснимо. Эксперты замечают, что эти молодые люди росли, видя Америку, подвергающуюся атакам террористов, а затем отвечавшую на эти атаки, отправляясь на одну войну за другой. Их мировоззрение было также сформировано Великой рецессией, приведшей к годами продолжавшимся сварам по поводу бюджетного дефицита и растущего национального долга, обостренного расходами на военные авантюры за рубежом.

Для американской молодежи глобальный финансовый крах был отнюдь не абстракцией. Он был реальностью в виде слабого спроса на рабочие места, а для многих — снижением жизненного уровня. Эти факторы, наряду с твердой уверенностью в бесполезности использования военных мускулов, могут объяснить «уход в себя» (то есть, во внутренние проблемы Америки) после взрыва интер-

венционалистских эмоций в стране как реакции на события 11 сентября 2001 года, отмечает автор статьи.

От себя надо добавить и то, что молодое поколение американцев крайне болезненно восприняло отношение их страны к тем, кто участвовал в качестве военнослужащих в указанных авантюрах. Несмотря на все обещания и всю патриотическую демагогию политиков, рекрутировавших молодежь на войну, очень многие, вернувшись с фронтов, столкнулись с безработицей, бедностью, нищетой, а инвалиды войны — с отсутствием необходимой медицинской помощи. То есть — с равнодушием государства и общества.

«Мы могли оказать ограниченное влияние (на страны — объекты интервенций США — Л.Д.), но оно долго не продлилось, — говорит на страницах газеты Даниела Оливерас, студент колледжа в Бостоне, штат Массачусетс. — Взгляните в прошлое: мы видим, что происходило, когда мы отправлялись в другие страны и пытались убедить их жить так, как мы. Но этого никогда не происходило».

Подобные прагматические заключения в отношении неэффективности американских интервенций за рубеж — в особенности на Ближний Восток — очень далеко отстоят от сантиментов по поводу американской исключительности и неких моральных обязательств Америки перед миром, которые можно было обнаружить в речах Обамы, убеждавшего народ страны в необходимости военных ударов по Сирии, - делает вывод Лафранчи. Он напоминает, как Обама обращался к авторитету правивших до него президентов, к примеру, к рейгановскому видению Америки как «сияющего храма на вершине холма», когда он — Обама — напоминал своим слушателям про готовность Америки «действовать», более того, говорил им, что «мы должны действовать» для противодействия мировому злу — ибо это то, что «делает нас исключительными».

Очень показательно, что тут автор «Крисчен сайенс монитор» делает вполне позитивную отсылку к Путину. По его словам, «слова Обамы вызвали отповедь со стороны российского президента, который использовал «страницу мнений» в «Нью-Йорк таймс» для ответа своему партнеру в США: «Очень опасно провоцировать людей на то, чтобы видеть себя исключительными, каковы бы ни были мотивы для этого».

Другие же говорят, продолжает Лафранчи, что подобные пустозвонные отсылки к «особой роли» США все более отчуждают американцев, которые отвергают все, что хотя бы отдаленно напоминает односторонние действия США. «Если исключительность — это оправдание для интервенции, то она сажает на мель все цели многосторонней политики, - говорит Николс из Орегонского университета. — Призывы к действиям, основанным на американской уникальности, несовместимы с совместной работой в международном сообществе, и именно это сбивает с толку американцев».

Как выяснил Обама, его призывы даже к «скромным усилиям» по военному вмешательству в Сирии натолкнулись на стену скептицизма со стороны американского народа, — пишет Лафранчи. Для таких историков, как Андрю Басевич из Бостонского университета, эта стена возникла на протяжении более чем трех десятилетий американских интервенций на Ближнем Востоке — от Рейгана, высадившего морских пехотинцев в Бейруте, до Обамы, организовавшего одномоментное увеличение числа американских войск в Афганистане. По его словам, за все это время ни одна из предполагавшихся Америкой целей ни разу не была достигнута.

Эндрю Басевич (кстати, автор недавно вышедшей книги «Границы мощи. Конец американской исключительности») практически повторяет вывод среднего американца о том, что интервенции на Ближний Восток «не сработали», когда он говорит о том, что «военные предприятия» США в этом регионе не сделали его ни более стабильным, ни более демократичным и не укрепили авторитет Америки в глазах мусульманского мира.

В то же время автор статьи в «Крисчен сайенс монитор» со ссылкой на других экспертов верно отмечает, что теперь, когда американцы пришли к выводу, что больше не хотят быть мировыми полицейскими, это совершенно необязательно говорит о том, что они хотели бы, чтобы их страна обособилась от остального мира. Уже цитировавшийся ранее Стивен Кулл из Мэрилендского университета (соавтор работы «Не понимая народ: миф о новом изоляционизме») считает, что одна из причин, по которой нынешние настроения в США были названы «изоляционизмом» состоит в том, что в вопросниках в ходе опросов общественного мнения отвечающим предлагают выбор лишь между двумя опциями: изоляционизмом или интервенциализмом, хотя по его мнению, американцы хотят другого — третьего пути.

По словам Кулла, «у социологов есть тенденция полагать, что общественное мнение развивается линейно, между «да» и «нет», позитивом и негативом, или в данном случае, изоляционизмом или интервенциализмом. Однако если вы превратите эту линейку в треугольник, то получите другой результат».

Предложите на выбор американцам триаду опций — одностороннее вовлечение (за рубежи страны), не вовлечение, и совместное с мировым сообществом вовлечение — и соблазн уединения окажется для них менее сильным».

Так, в ходе опроса Гэллапа 2011 года американцам были предложены на выбор четыре варианта того, какую роль их страна должна играть в мире: никакую, очень скромную, большую, но не лидирующую, и лидирующую. В результате только 16% опрошенных поддержали лидирующую роль, в то время как очень ограниченное число американцев — всего 7 процентов — предпочли бы, чтобы США вообще не играли никакой роли.

Вывод Кулла: мы видим, что люди уходят от поддержки вовлечения Америки в военные конфликты за рубежом в доминирующей роли, свидетелями чего они были на протяжении последнего десятилетия, поскольку считают эту роль слишком односторонней. Однако они в подавляющем своем большинстве поддерживают более кооперативную с другими странами форму вовлечения в случае, когда в ходе опросов им предоставляется такой выбор.

Так, Кулл считает, что президенту могло бы потребоваться немало времени и усилий, чтобы привлечь большинство американцев к поддержке военной интервенции на Ближнем Востоке, тем более при отсутствии непосредственной угрозы стране, как это было в ситуации после 11.09.01. Однако если бы и сейчас Обама смог доказать, что мир поддерживает его план военного удара по Сирии, а сама операция будет носить многонациональный характер, в этом случае даже нынешняя Америка, сторонящаяся интервенций и предпочитающая им собственные газоны, якобы могла бы поддержать такой курс.

Правда, Стивену Куллу можно было бы напомнить, что в отличие от обстановки после катастрофы 11 сентября 2001 года, мир уже давно не поддерживает Америку, устав от ее кровавых бесчинств за рубежом не меньше самих американцев. А что касается участия в таких бесчинствах, то как известно читателю, кроме реакционных монархий Персидского залива и президента Франции Олланда — добровольной марионетки этих режимов и Израиля - других желающих в мире не нашлось. Даже британцы и те увильнули.

В конце статьи Лафранчи напоминает читателям знаменитую фразу Джона Куинси Адамса (президента США, а до этого первого американского посланника в России), который почти два века тому назад высказался в том смысле, что хотя Америка и «преисполнена самыми добрыми пожеланиями свободы и независимости для всех», «она не отправляется за границу в поисках монстров для их изничтожения».

Как считает автор статьи, вследствие наступления «американского века», последовавшего за «лидирующей ролью Америки в уничтожении нацистского монстра в Европе» (насчет ее лидирующей роли — это более чем спорное утверждение — Л.Д.), а тем более наступления глобализации (второй попытки американизации мира — Л.Д.) эти мысли Адамса, возможно, потеряли свою актуальность. Однако, замечает автор, «сегодня американцы демонстрируют стремление играть в мире более скромную роль». Думается, что реальные, в отличие от ожидаемых, последствия их «лидирующей роли» и «глобализации» как для самих США, так и для всего мира являются основной причиной такой смены приоритетов.

«Кризис сознания» в американской внешней политике

Впрочем, надо иметь в виду, что далеко не все в Америке мыслят ныне подобным образом. К примеру, Хойт Хилсман в либеральном интернет-издании «Хаф-

фингтон пост» утверждает, что для Америки было бы неумно рассчитывать на то, что другие нации будут поддерживать мировой порядок. Ведь даже если США «иногда, случайно, делают ошибки за рубежом, дела пойдут значительно хуже, если они отступят и позволят России или Китаю, в обоих случаях серийным нарушителям прав человека, взять на себя роль мирового полицейского».

Вывод Хилсмана состоит в том, что «бывают времена, когда американцы чувствуют, что они вынуждены выступать в защиту своих ценностей свободы и открытости». А также в том, что экономика США «зависит от стабильного и безопасного мира, в котором рынки могут оперировать свободно и мирно». И таким образом, добавляет он, «решим мы или нет быть мировым полицейским, мы все равно должны быть частью мировой полиции». О том, что ранее принесла миру и самой Америке эта роль мирового жандарма — смотри выше. Это понимает сегодня уже большинство американцев. Но не такие как Хилсман.

Нам в России, конечно же, понятно, что сходство мнений большинства правых, левых и рядовых американцев в осуждении внешней политики своей страны не могло не вызвать серьезнейшей тревоги и разочарования истеблишмента США, который, по словам Нила Монро еще на одном консервативном сайте «Дейли коллер», считает происшедшее вокруг Сирии крупнейшим провалом внешней политики со времен известного неудачника и слабака - президента Джимми Картера.

И второе. Особенно унизительным для многих американцев стало осознание ими того факта, что именно Путин, по сути, спас их президента Обаму от глухого тупика, в который он сам себя загнал по сирийскому вопросу. А Америку — от очередной внешнеполитической авантюры, которая могла закончиться для нее и для значительной части мира еще большей трагедией, чем все предшествовавшие авантюры. Как сообщило 14 сентября агентство Рейтер, 75% американцев поддержали разрешение сирийского кризиса дипломатическими мерами. По данным Гэллапа, 72% опрошенных в сентябре поддерживали предложенный Россией план химического разоружения Сирии и лишь 18 процентов были против.

Впрочем, мы должны при этом реально осознавать уровень антироссийских настроений в Америке сегодня. Так, по данным того же Гэллапа, впервые за последние 15 лет в том же сентябре 2013 года число американцев, негативно относящихся к России, превысило число тех, кто доверяет Москве. В этом месяце 44% граждан этой страны считали Россию дружественным государством, в то время как число тех, кто считает Россию враждебной или недружественной, выросло до 50%.

При этом только 19% опрошенных выразили позитивное отношение к президенту Путину, в то время как 54% американцев относятся к нему негативно. Причины «новых симпатий» к России и Путину, проявившихся на фоне сирийского кризиса, мы постарались проанализировать выше. В чем же причины негативных

подходов? Их немало, и среди них обычные, давно устоявшиеся и в Америке, и на Западе в целом: это остаточные настроения «холодной войны» (которую ведущий американский исследователь Стивен Коэн считает то ли вообще никогда не прекращавшейся, то ли сменившейся «новой холодной войной»); это классическая западная русофобия; это негативное влияние крайне отрицательно настроенных в отношении к России эмигрировавших в США представителей национальных меньшинств России, бывших республик СССР и стран Восточной Европы; это глубокие геополитические противоречия и противоборство между США и Россией, это манипулирующая роль американских СМИ и другие известные факторы.

Однако налицо и новые причины вражды, о части которых мы уже писали выше. Большинство американцев и особенно элита страны давно, уже двадцать с лишним лет назад сплясали на поминках по СССР как по основному своему геополитическому и идеологическому противнику, тем более как по равной им сверхдержаве, с триумфом объявили о себе как о единственном мировом управляющем и долго читали нам лекции, учили нас жить. И факт, что ныне, в период крайне беспокоящего американцев серьезного внутреннего и внешнего ослабления их страны, при прогрессирующем падении в их глазах авторитета и законодательной, и исполнительной власти, на арене вдруг появился «этот Путин», не только на равных дискутирующий с ними, критикующий их, вставляющий палки в колеса американской колеснице, предоставляющий убежище их политическим диссидентам, но и еще спасающий их в момент казавшегося неразрешимым внешнеполитического кризиса, очень многим показался оскорбительным.

На эту тему в ведущих американских СМИ появились многозначительные публикации известных политологов и журналистов. Так, Алан Коуэлл уже в начале октября опубликовал в «Нью-Йорк таймс» статью под заголовком «Москва переписывает дипломатическую партитуру», в которой отмечалось, что на протяжении десятилетий протагонисты «холодной войны» сдерживали локальные конфликты от их перерастания в кризис, способный вызвать конфронтацию между двумя самыми мощными ядерными державами. По окончании «эпохи оледенения» в связи с обвалом Советского Союза, многие начали говорить о том, что неожиданно ставший монополярным мир оказался в плену возвышающейся Америки.

Однако с учетом последнего, правда, еще не прошедшего проверку на прочность сближения между Россией и администрацией Обамы, в сочетании с также внезапным потеплением в отношении Ирана, в котором также нет полной уверенности, подобные знакомые расчеты стали меняться.

И хотя никто не говорит о возвращении к обычному состоянию «холодной войны», Россия, про словам Коуэлла, «проделала определенный путь к переутверждению себя как противовеса Соединенным Штатам, что отражает долго-

временное стремление Владимира Путина к восстановлению мирового влияния своего государства».

В результате его сирийской инициативы, признается в статье, помимо ее воздействия на собственно американскую внутреннюю и внешнюю политику, оказались оттеснены на дипломатическую обочину некоторые из ключевых европейских союзников США, а признаки сближения Вашингтона с Тегераном (ставшие результатом все той же инициативы) неожиданно антагонизировали традиционных арабских партнеров Соединенных Штатов и их ближайшего союзника — Израиль. Эти страны годами строили свою политику на использовании в своих целях взаимной американо-иранской вражды.

Как отметил Ян Бонд, специалист по внешней политике Центра европейских реформ — исследовательской организации в Лондоне, российский министр иностранных дел Сергей Лавров (как в свое время и его знаменитый советский предшественник А.А. Громыко — Л.Д.) рассматривался Западом как «Мистер Нет» в плане противодействия попыткам отстранения от власти Башера Асада. «И вдруг, - сказал Бонд, - вы увидели с его стороны скорее умелую, квалифицированную дипломатию», которая заставила обамовскую администрацию уклониться от подготовки к карательному военному удару».

Наибольший интерес представляет приводимое в статье мнение редактора германского еженедельника «Цайт» Ульриха Ладурнера, подводящее итог целому периоду т.н. американского триумфализма после развала СССР: «Соединенные Штаты более не в состоянии в одиночку формировать политику дня на Ближнем Востоке. Это стало особенно очевидным применительно к Сирии. Обама нуждается в помощи России в сирийском лабиринте. Соединенным Штатам нужны партнеры» (выделено мной — Л.Д.).

К этому нужно только добавить, что в том же октябре в США стали появляться призывы именно по причине их выявившейся вдруг «уязвимости» на Ближнем Востоке начать сворачивать там военно-дипломатическую активность, перенаправив ее в «новый поворотный пункт» мировой геополитики — в Азию. Однако авторы этих призывов как-то упускают из виду, что в этом случае Обама, вылезая из пасти арабского льва, немедленно окажется в окружении азиатских тигров, не говоря уж о всегда находившейся там России Путина, который по разным причинам именно Азию видит главным плацдармом своих геополитических устремлений.

Впрочем, как уже указывалось ранее, в американской элите в целом описанные выше процессы и их оценки вызывают откровенное раздражение. Это ясно видно хотя бы из статьи считающегося одним из ведущих американских специалистов по России Томаса Грэма, долго работавшего ведущим аналитиком посольства США в Москве и бывшего здесь любимцем наших либеральных СМИ,

голосом «вашингтонского обкома», к руководящим оценкам которого касательно внутренней политики России они с благоговением прислушивались.

На сайте Йельского университета, где он сейчас работает, Грэм в середине сентября с нескрываемым оттенком недоброжелательности отмечал, что «Россия вновь выплывает на мировую сцену. Со своей инициативой по ликвидации сирийского арсенала химического оружия российский президент Владимир Путин ввел Россию на Ближний Восток в качестве ключевого игрока впервые с развала Советского Союза… Разумеется, многое еще может пойти не так и перечеркнуть путинский тактический выигрыш, однако сейчас российский лидер выглядит как идущий след в след за Обамой».

Далее Грэм утверждает, что «вопреки широко распространенному мнению, что якобы пребывает в растерянности, будучи обставлена русскими, администрация США организовала утечку, согласно которой утверждается, что именно она еще 18 месяцев назад сыграла решающую роль в формулировании путинского предложения. При этом США позволили Путину записать себе в плюс эту инициативу для того, чтобы именно он взял на себя всю полноту ответственности за ее реализацию… Месяцы, если не годы отделяют нас от окончательной ликвидации химического оружия, и многое за это время может пойти не так».

У автора этой статьи указанный изыск Томаса Грэма вызывает, мягко говоря, большие сомнения. Американская дипломатия последних десятилетий, включая нынешнюю, совершенно не производит впечатления той интеллектуальной, «толейрановской» изощренности, которую он ей пытается приписать (иных уж нет — того же Джорджа Кеннана — а те далече). За этим его абзацем — прежде всего обида на обскакавших госдеп на этот раз Путина с Лавровым…

Грэм с предельным раздражением признает, что «на данный момент Путин продвинул российские интересы не только в Сирии, но и в значительно более широком контексте… Годами он выступал против того, что рассматривает как американские гегемонистские устремления, пренебрежение со стороны США нормами международного права, попирание государственного суверенитета и злоупотребление принципами гуманитарной интервенции для свержения нежелательных им режимов… Он неоднократно пытался встать на пути Соединенных Штатов без большого успеха и с минимальной международной поддержкой. Но на этот раз на саммите G-20 в Санкт-Петербурге он все же переиграл Обаму».

Далее Грэм признает и то, что сразу вслед за этим «именно путинская инициатива спасла Обаму от унизительного поражения в конгрессе, где сопротивление его военному выбору росло с часу на час, что отражало одновременно и слабость Обамы, и широко распространенные на Западе сомнения в мудрости политики США».

Но признавая, что Путин, «возможно, навсегда» отложил использование американской военной мощи против Асада, Грэм тут же злорадствует по поводу

того, что российский президент сделал это «безо всякого сомнения, к величайшему облегчению своих собственных генералов… Путину не нужна была еще одна наглядная демонстрация того, как далеко отстали российские вооруженные силы или в напоминании остальному миру о цене, которую каждый заплатит, встав на пути Соединенных Штатов».

Однако после этого выпада, Грэм тут же вновь вынужден перейти к горьким признаниям. По его словам, «держать вооруженные силы США в безвыходном положении является главным в усилиях Путина по восстановлению российского влияния, особенно на Ближнем Востоке. Возможно, ведущие арабские страны в отличие от Путина и хотели бы отставки Асада, но они уважают силу, также как ее уважают Иран и Израиль. Решительность Путина вкупе с очевидной амбивалентностью Обамы в отношении использования силы и более глубокого вовлечения США в ближневосточные дела, приведет к пересмотру региональными державами их стратегии с точки зрения большего внимания к России».

В то же время, пишет Грэм, Путин продвинул на сирийском направлении два важнейших приоритета России: предотвращение организованного США изменения режима в этой стране и противостояние радикальному исламу как самому непреклонному оппоненту Асада.

И далее он подчеркивает главную вынужденную необходимость, перед которой при всей унизительности для себя оказался Вашингтон: инициированная Москвой ликвидация сирийского ядерного оружия, с чем вынужден был согласиться Обама после провала его попытки использовать этот фактор как предлог для военного подавления Асада, сегодня требует сохранения того же самого Асада у власти: никто кроме него не знает объемов и мест хранения этого оружия; только он может обеспечить безопасность для специалистов, присланных ООН для его уничтожения. Еще недавно призывая к его отставке, Вашингтон сегодня оказался заинтересован в нем как в партнере, причем на достаточное время, которое позволило бы правительству Дамаска подавить вооруженную оппозицию и одержать победу. Это поняли и оппозиционеры: глава Свободной Сирийской Армии генерал Салим Идрис вплотную подошел к обвинению американцев в предательстве.

И это в ситуации, когда Запад, в особенности США, уже и так тошнит от осознания того, что в этой оппозиции на ведущие позиции выдвинулись радикалы и экстремисты. В этой ситуации Путин рассчитывает на то, считает Грэм, что именно они и станут лицом этой оппозиции, а это в принципе подорвет всю западную антиасадовскую политику и заставит сосредоточить основное внимание на террористической угрозе. Отсюда вытекает, что планируемая конференция Женева-2, которая по расчетам Запада должна была легитимизировать отстранение Асада от власти, сегодня, в случае если ее удастся провести, вряд ли приведет к подобному результату.

Интересно, как подобные вынужденные признания Грэма коррелируют с высказываниями такого общепризнанного корифея американской и мировой дипломатии, как Генри Киссинджер. В 20-х числах сентября он высказался в том плане, что сирийский конфликт «не может быть решен отстранением одного человека», так как суть конфликта в суннитско-шиитских противоречиях, а не только в том, что у власти Асад.

Но Киссинджер сказал много больше этого. По его словам, России можно доверять, когда речь идет о «продвижении ее интересов». А постановка химического оружия под международный контроль — это как раз тот случай. В отличие от многих других американских специалистов, включая Грэма, Киссинджер заявил, что верит Владимиру Путину, который «определил ликвидацию химоружия в Сирии самым главным интересом своей страны». Как считает Киссинджер (и с ним можно согласиться — Л.Д.), для Путина «самой большой проблемой безопасности является радикальный ислам».

Более того, он указал, что у России и США есть объективная необходимость сотрудничества в разных сферах «в интересах обеих сторон», особенно учитывая большую протяженность российских границ и большую территорию. Хотя, конечно, признал Кисинджер, Россия не станет смотреть на мир с позиций интересов США. Думается, что все это и было предметом обсуждения с В.Путиным в ходе визита Киссинджера в Москву уже в октябре.

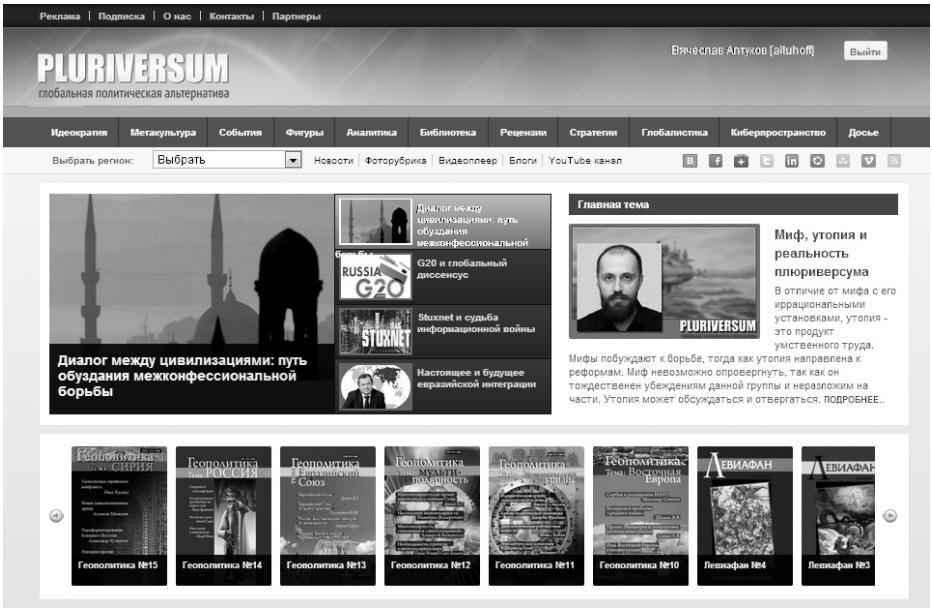
Такие люди как Грэм, далеки от подобного признания сложившихся реалий, так противоречащих давно провозглашенным ими же триумфалистским для США сценариям. На фоне развития событий вокруг Сирии, выдавливает он из себя, «не удивительно, что Путин совершил своеобразный «круг почета» со своей статьей в «Нью-Йорк таймс», не без удовольствия просвещая американцев в отношении достоинств международного права, Совбеза ООН и ограниченности возможностей США (на мировой арене). Особую радость он должен был испытать, бросая вызов претензиям на американскую исключительность».

Впрочем, думается, что «соль» статьи Томаса Грэма состоит в ее последнем абзаце: «Нам еще предстоит увидеть, придется ли ему (Путину) пожалеть об этой своей публикации. По крайней мере, сейчас он на коне. Однако его успех — в огромной степени результат нерешительности и разброда в Вашингтоне и президента, оказавшегося неспособным представить убедительные аргументы в поддержку своего с неохотой избранного курса или сформулировать комплексную стратегию как для Сирии, так и для всего региона. Чего Путин должен опасаться, так это того, что его дипломатический успех станет сигналом для мобилизации в Вашингтоне. Он знает, что Соединенные Штаты могут легко вытолкнуть Россию на периферию дипломатии в Сирии и на Ближнем Востоке. Они имеют значительно более обширные ресурсы для влияния на ситуацию, чем Россия. Чего нам не хватает, это воли, а у Путина она есть».

Полностью отдавая себе отчет в том, какое ожесточение и униженную гордыню американской политической элиты отражает публикация Грэма, все же нельзя не согласиться с ним в том, что проявленное нашей дипломатией и лично президентом дипломатическое искусство и находчивость вкупе с его политической волей, а также очевидные на сегодня личные слабости Обамы как политика, общий кавардак в Вашингтоне все же не дают полной уверенности в нашей окончательном успехе. Мы в отличие от СССР эпохи Сталина-Брежнева действительно неслыханно отстали от Штатов в военной и экономической мощи, мировом авторитете и влиянии. И только их возрождение, причем неотложное, сделает наши дипломатические и политические победы в международной политике неоспоримыми.

А Россия — это страна Побед. Без них у нас нет будущего.

www.pluriversum.org



Данный ресурс является русскоязычным кластером международного сообщества за плюриверсальные ценности.

По выражению одного из идеологов концепции плюриверсализма Алена де Бенуа, плюриверсум — это такое человечество, которое давало бы гарантии сохранения политического, культурного и антропологического своеобразия на всей планете.

Либерализм как политическая модель, занявшая наиболее прочные позиции и через глобализацию проводящая нивелировку и гомогенизацию (как политическую, так и культурную) всех народов и стран, но, в то же время, показавшая свою несостоятельность, должен быть отвергнут, деконструирован и похоронен на свалке истории.

Сторонниками плюриверсализма могут быть представители самых разных идей, политических учений, религий и мировоззрений, которых объединяет неприятие неолиберализма в любых его формах и проявлениях.

Инструментом сопротивления неолиберализму является метаполитика, которая связывает и объединяет культурные, эстетические, политические, социальные, религиозные, коммуникационные и др. проекты в единую платформу.

К соучастию в данном пректе приглашаются авторы, переводчики, промоутеры и неравнодушные люди.

Геополитика.
Информационно-аналитическое издание.
Выпуск XXII, 2013. — 118 стр.

Печатается по решению кафедры
Социологии Международных
Отношений Социологического факультета
МГУ им М.В. Ломоносова.

Адрес редакции:
121087, Москва, Багратионовский проезд, дом 7, корп. 20 “В”,
офис 405.
тел. (495) 514 65 16
факс (495) 926 68 11
Geopolitika.ru@gmail.com
www.geopolitika.ru

Подписано в печать 15 декабря 2013 г.