Киберконфликт в китайско-американских отношениях и поиски диалога

© 2013

К. Антипов

Беспрецедентная эскалация противоречий между КНР и США в киберпространстве обозначила определенный кризис в китайско-американских отношениях. Вместе с тем, итоги неформальной встречи Си Цзиньпина и Обамы в Калифорнии 8–9 июня 2013 г. свидетельствуют, что США и КНР, возможно, смогут продвинуться к новому этапу их взаимодействия в сфере безопасности.

Ключевые слова: Китай, США, киберпространство, экономические аспекты соперничества

Конфликт между Пекином и Вашингтоном в киберпространстве, в течение ряда лет развивавшийся на периферии соперничества двух стран, в 2012 — первой половине 2013 гг. вышел на первый план, угрожая занять доминирующее положение в общей системе китайско-американских отношений. Резко возросшее число хакерских атак на объекты КНР и США и усилившееся противоборство в двусторонних отношениях по поводу боевого использования информационных технологий стало не только проявлением стратегического соперничества двух держав, но и важным фактором глобальных международных отношений, затрагивающих интересы России, а также и всего мирового сообщества.

Обострение данной ситуации отражает широкий спектр долговременных противоречий между КНР и США, усиливающихся в политической, экономической и военной областях. Видные эксперты обеих сторон расценивают данную ситуацию как показатель того, что стратегическое соперничество стало опережать стратегическое сотрудничество. Это касается прежде всего милитаризации киберпространства, возрастающего экономического ущерба от хакерской деятельности и назревшей необходимости наладить в данной области диалог и широкое международное сотрудничество. Состоявшаяся в июне 2013 г. неофициальная встреча Си Цзиньпина и Обамы продемонстрировала желание обеих сторон снизить остроту конфликта, не отказываясь, однако, от продолжения противоборства на данном направлении. Происходящая интеграция новой силовой политики и дипломатии на высшем уровне развивается в русле становления международных отношений нового типа. Именно этот процесс во многом определит новые параметры международной безопасности и новые возможности для продолжения традиционных китайско-американских отношений, сочетающих борьбу и поиски взаимодействия между КНР и США.

Киберконфликт в контексте китайско-американских отношений

В последние месяцы руководители США и КНР не раз выступали с заявлениями о происходящем усилении киберугрозы и предпринимали практические шаги по наращиванию потенциала для дальнейшей борьбы. Послание Обамы Конгрессу США в январе 2013 г., ежегодный доклад директора центральной разведки США Клеппера, заявления советника по национальной безопасности Донилона, а также целый ряд других авторитетных выступлений и публикаций стали свидетельством серьезной обеспокоенности Вашингтона обострением противоречий с Китаем в сфере кибербезопасности. Как отмечает ряд американских экспертов, впервые после событий 11 сентября 2001 г. киберугроза выдвинулась на первое место в системе приоритетов стратегии безопасности США. В исполнительном приказе президента США от 12 февраля 2013 г. и в докладе Белого дома от 21 февраля 2013 г. «Стратегия администрации по ограничению хищения торговых секретов США» закреплены новые задачи в данной области, нацеливающие американские силовые структуры на дальнейшее наращивание их деятельности. По сообщениям китайских комментаторов, США приняли решение в ближайшие годы в пять раз увеличить численность Стратегического киберкомандования. Проводимые мероприятия свидетельствуют, что США стремятся сохранить за собой не только военно-техническое превосходство, но и политическое лидерство в данной сфере.

Ускоренное наращивание киберпотенциала происходит и в КНР. Признавая рост киберугрозы, Пекин, вместе с тем стремится сохранять сбалансированную позицию и ориентируется на достижение международного согласия по вопросам кибербезопасности. Касаясь обвинений Китая в проведении массированных кибератак на объекты США, премьер Госсовета КНР Ли Кэцян отметил, что «этот вопрос носит глобальный характер» и «сам Китай является его главной жертвой. Китай не только не поддерживает, но напротив — выступает против хакерских атак». Назвав осуждение Китая «презумпцией вины», Ли Кэцян подчеркнул, что обе стороны должны... сделать больше реальных дел для защиты безопасности киберпространства¹.

Как показывают события 2012–2013 гг., китайско-американское соперничество в киберпространстве в настоящее время проходит через кризисный период. При этом нарастание напряженности в двусторонних отношениях сопровождается постепенным осознанием на Западе того факта, что в данной области Китай в состоянии наносить серьезный ущерб американским интересам, несмотря на сохраняющееся военно-технологическое превосходство США. Это явилось важной предпосылкой для начала обсуждения проблемы на высшем уровне. Однако согласие сторон возобновить диалог пока не означает сближения их позиций. Это было наглядно продемонстрировано в ходе состоявшейся 8–9 июня 2013 г. неформальной встречи президента Обамы с председателем КНР Си Цзиньпином. Как неоднократно подчеркивали представители администрации США при подготовке встречи, ввиду происходящего нарастания кибератак вопрос о кибербезопасности в отношениях с Китаем являлся главным приоритетом для президента Обамы. Однако в изложении китайской печати данный вопрос, как правило, упоминался на последнем месте на всех этапах состоявшихся бесед. Подобная асимметрия в переговорных позициях может иметь достаточно глубокий смысл, учитывая то, что нынешняя инициатива США по организации диалога на высшем уровне является по сути запоздалой реакцией Вашингтона на предложения по проведению переговоров для нормализации обстановки в киберпространстве на правовой основе, ранее выдвигавшиеся Россией, а затем и Китаем. К тому же в ходе переговоров Обамы с Си Цзиньпином американская сторона попыталась построить диалог, выступая по существу с обвинительных позиций в отношении Китая. Начавшиеся в эти же дни в западной прессе масштабные утечки информации об агрессивной деятельности США в киберпространстве, особенно разоблачения бывшего сотрудника ЦРУ Э. Сноудена, показали несостоятельность

такого подхода для формирования сколь-нибудь перспективной американской дипломатии. Однако отказ от продолжения американской политики давления на Китай представляется пока маловероятным, поскольку деятельность киберподразделений США в отношении Китая осуществляется в течение ряда лет, она опирается на сложившуюся традицию и интегрирована в стратегию национальной безопасности США.

По оценке экспертов, наиболее активно киберпротивостояние развивается в китайско-американских отношениях с 2009 г. Оно протекает с прямым участием государственных органов обеих сторон и наносит серьезный ущерб Китаю и Штатам. Еще в мае 2009 г. в ходе обсуждения в конгрессе США использования Китаем информационных технологий президент Обама назвал кибератаки «одним из наиболее серьезных вызовов экономике и национальной безопасности США»². Данная тема стала предметом пристального внимания со стороны Белого дома, Конгресса США, систематически получает оценку в докладах Госдепартамента, национальной разведки, ЦРУ, Пентагона и других ведомств.

Говоря о растущем давлении хакерской деятельности иностранных государств, преступных групп и отдельных личностей на американское общество, директор Агентства национальной безопасности США (АНБ) генерал Кейт Александер заявлял, что киберугроза представляет еще большую опасность, чем стратегия ядерного устрашения, с которой США приходилось иметь дело в прошлом³. Он также признал, что до сих пор ни одно государство не располагает надежной защитой от киберагрессии, причем возникшее отставание киберобороны от средств нападения носит устойчивый характер и может сохраняться в течение длительного времени. Рассматривая эту особенность применительно к китайско-американским отношениям, эксперты считают, что на цифровом поле США пока находятся в более уязвимом положении, учитывая опережающее распространение информационных технологий во всех отраслях жизни американского общества. Кроме того, не имея возможности достоверно установить источник нападения техническими средствами, ни одно современное государство, в том числе — США и Китай, не могут обеспечить необходимую защиту своих сетей. Характерно, что мнение о большей опасности киберугрозы по сравнению с ядерной опасностью высказывают и авторитетные китайские представители. Так, Чэнь Сяогун, член Комиссии по иностранным делам Всекитайского собрания народных представителей, называет киберпространство «новым полем боя», предупреждая при этом, что если страны допустят на нем гонку вооружений, то «последствия этого будут еще страшнее ядерной войны»⁴.

К вопросам нарастающей киберугрозы и обеспечения безопасности в киберпространстве в последнее время проявляется повышенное внимание во всех странах, они все чаще находят отражение в публичных выступлениях представителей России, Китая и США и других государств. Происходит заметное усиление политической значимости кибербезопасности как негативного фактора внутренней политики и международных отношений, требующего особого внимания. Так, в декабре 2012 г. президент Путин поручил компетентным органам активизировать работу в киберпространстве. Он подчеркнул необходимость «и дальше действовать системно и наступательно»⁵. В Китае после целого ряда лет сравнительно сдержанного отношения к киберугрозе в публичных выступлениях на высшем уровне впервые прозвучали заявления о необходимости «придавать серьезное значение» обеспечению кибербезопасности КНР⁶. Тема кибербезопасности активно присутствует в китайских публикациях как для внутренней, так и для международной аудитории, ведется системная подготовка вооруженных сил к «действиям в условиях информатизации», данная проблема является объектом постоянного внимания китайской дипломатии, партийного и государственного руководства.

США, развернувшие масштабное наступление на позиции Китая в киберпространстве, осуществляют в этой сфере наиболее активную деятельность. На сегодняшний день Америка располагает самым мощным киберпотенциалом. По сообщениям

американской прессы, АНБ, используя автоматические системы взлома компьютерных сетей, ежедневно похищает 2 петабайта (2 миллиона гигабайт) информации в компьютерах всего мира. Это, по словам, бывшего директора национальной разведки США Майка Макконнелла, обеспечивает основной поток разведывательной информации, в том числе — свыше 75% информации, входящей в ежедневную разведсводку для президента США⁷.

Судя по появившимся в последнее время публикациям осведомленных американских экспертов⁸, уже в первые месяцы пребывания в Белом доме администрация Обамы двинулась по пути модернизации и придания наступательного характера киберстратегии США «Олимпийские игры», сформированной в последние годы администрации президента Буша-младшего. Одним из фундаментальных оснований стратегии является созданная в Америке система контроля за интернетом, использующая, в частности то, что десять из тринадцати корневых серверов, регулирующих основной объем глобального трафика в сети, действуют в США. Они находятся под наблюдением корпорации ICANN (Internet Corporation for Assigned Names and Numbers), которой эти функции были переданы в 1998 г. правительством США.

Сохранение глобального лидерства США, укрепление доминирующего положения в сети интернет и ее активное использование в политических целях стало одним из системных элементов киберстратегии администрации президента Обама в отношении Китая. В основе этого подхода — политика сдерживания КНР, оказание идеологического и политического воздействия на эволюцию китайского общества, продвижение концепций либеральной демократии, стимулирование оппозиционных настроений в Китае. В последнее время эта стратегия все больше направляется и на цели соперничества с Китаем в международных отношениях. Так, по мнению видного американского эксперта Патрика Кронина, одной из основных причин усиления давления США на Китай в последние месяцы является стремление продемонстрировать союзникам в Азии готовность отстаивать свое доминирующее положение и сохранять баланс сил с КНР. Именно такой подход продемонстрировал министр обороны США Хейгел на XII встрече в верхах по безопасности в Азии, состоявшейся в Сингапуре в мае 2013 г.⁹ Киберпротивоборство является одним из существенных элементов этой политики.

Однако главное место среди политических приоритетов киберстратегии Вашингтона все еще сохраняет область китайско-американских противоречий по вопросам государственного суверенитета КНР. В этой связи следует отметить, что развитие силовой деятельности в виртуальном пространстве сопровождается настойчивыми попытками Запада утвердить в информационном поле новые принципы международных отношений, ограничивающие признание государственного суверенитета. Так, получившая в 2005 г. закрепление в решениях ООН т.н. «доктрина гуманитарного вмешательства» фактически использует в качестве одного из своих идейных оснований «Декларацию независимости интернета», обнародованную в Швейцарии в феврале 1996 г. и провозгласившую отказ от применения суверенитета к деятельности в киберпространстве¹⁰.

Наступательный характер киберстратегии США, ее разворот на решение политических задач в отношениях с Китаем наиболее ярко иллюстрируют попытки Запада в 2009 г. использовать Интернет, чтобы подхлестнуть антиправительственные настроения в КНР и содействовать подъему протестного движения в русле «твиттерных» революций на Ближнем Востоке и в Северной Африке. Эти же задачи решаются в рамках политики США по вопросам Тибета и Синьцзяна. Цели и принципы, определившие основные шаги в этой деятельности, в том числе — создание вслед за военными структурами во главе со Стратегическим киберкомандованием США еще и соответствующего подразделения в госдепартаменте, сформулированы в известной речи Хиллари Клинтон о свободе Интернета¹¹.

Форсированное наращивание силового компонента киберстратегии и его активное использование во внешнеполитических целях США отодвинуло на второй план переговоры о возможностях сотрудничества для снижения киберугрозы. Кибердиалог с Китаем, ранее официально включенный в систему Стратегического диалога двух стран, оказался практически свернут. Длительная эскалация конфликта и отсутствие должных международных соглашений в этой области, по-видимому, в немалой степени объясняются расчетами США на сохранение стратегического превосходства над КНР в киберпространстве и на возможность доминировать в формировании мирового порядка в этой сфере. В этой связи приходится отметить, что в течение длительного времени США фактически игнорировали предложения России и Китая, направленные на соблюдение в киберпространстве государственного суверенитета и других признанных правовых норм. Однако в результате активного наращивания киберпотенциала обеими сторонами и стремительного научно-технического развития мировой киберсферы Китай и США к настоящему времени оказались в состоянии определенного паритета. Как отмечают западные эксперты, «китайская доктрина кибервойны хорошо разработана, в развитие наступательных и оборонительных возможностей НОАК и спецслужб сделаны значительные инвестиции»¹².

Китайско-американское соперничество оказывает усиливающееся воздействие на глобальную военную ситуацию. Оно ускоряет милитаризацию киберпространства, стимулирует рост напряженности и дальнейшее втягивание в гонку кибервооружений всего мирового сообщества. С военно-стратегической точки зрения, уровень развития информационных технологий в обеих странах позволяет США и КНР оказывать серьезное давление друг на друга путем создания киберугроз в широком диапазоне отношений, затрагивающих политические, деловые и иные интересы. Нарастание борьбы, по оценкам экспертов, создает угрозу сети интернет, имеющей жизненно важное значение для дальнейшего развития процессов глобализации во всем мире. Судя по комментариям специалистов, с технической точки зрения противоборство с использованием информационных технологий имеет широкие возможности для активного применения в условиях мирного времени и, следовательно, может приобрести долговременный характер.

Это актуализирует необходимость возобновления китайско-американского диалога по кибербезопасности и в то же время ставит целый ряд вопросов о перспективах переговорного процесса и имеющихся трудностях на этом пути. В этой связи стоит обратить внимание на то, что активное подключение к соперничеству в киберпространстве госдепартамента США и крен в сторону политических целей в последние годы привели к своеобразной асимметрии в подходах Пекина и Вашингтона к оценке угроз в цифровом поле. В дальнейшем это определило различие подходов и к определению сторонами своих приоритетных задач во взаимоотношениях по данной проблеме. Основную опасность для интересов США здесь американцы усматривают в хакерской деятельности китайских операторов, направленной на хищение военно-технической информации, интеллектуальной собственности, коммерческих секретов и т.п. Подобные действия, по словам директора Национальной разведки США Клеппера, в профессиональных кругах США рассматриваются в рамках единого понятия кибербезопасности — либо как нападение с диверсионной целью, либо как шпионаж.

Однако для Китая, помимо защиты информационных сетей, приоритетное значение приобрели также и вопросы защиты суверенитета от угроз в киберпространстве, поддержания стабильности и общественного порядка, а также обеспечения невмешательства во внутренние дела со стороны иностранных держав с использованием информационных возможностей Интернета. При этом китайцы в отличие от США разделяют понятия кибербезопасности и информационной безопасности. На этой почве сформировалось различное толкование сторонами многих понятий и терминов, определяющих сферу кибербезопасности. К числу подобных разночтений относятся даже

такие основополагающие понятия как кибератака. В этой связи в последнее время в КНР и США участились выступления видных экспертов с заявлениями о необходимости дополнить длинный перечень китайско-американских расхождений признанием различия подходов еще в одной области — понимания киберугрозы и кибербезопасности. При этом отмечается, что речь идет не о семантических различиях в трактовке тех или иных понятий, а о различном понимании проблем, относящихся к кибербезопасности, о различии имеющихся представлений и взглядов политических лидеров, основанных на различии политических систем и фундаментальных интересов двух стран¹³. Важность установления понятийного соответствия в этой сфере становится еще более актуальной в результате усиливающегося смещения вопросов кибербезопасности из сферы профессиональной информационно-технической деятельности в область политического управления, предпринимательства и дипломатии. В ближайшей перспективе этот процесс может ускориться.

В «мозговых центрах» Китая и США постоянно подчеркивается важность согласования основных понятий еще и потому, что в повседневную деятельность в сфере кибербезопасности быстро втягивается значительная категория новых участников — от высших государственных чиновников до представителей массовых профессий, коммерческой, общественной и культурной деятельности. Это, по оценке экспертов, может оказывать существенное воздействие на переговорный процесс и общественное мнение, проявляющее растущий интерес к китайско-американскому киберконфликту. При этом отмечается особое значение освоения киберпроблематики управленческим контингентом, принимающим решения в сфере внешней политики. О степени вовлеченности высшего китайского руководства в дела практического обеспечения кибербезопасности можно судить, например, по тому, что нынешний премьер Госсовета КНР Ли Кэцян возглавлял в ЦК КПК т.н. «группу координации национальной сети и информационной безопасности». Членами этой группы являлись нынешний председатель ВСНП Чжан Дэцзян и Лю Юньшань — член Постоянного комитета политбюро ЦК КПК¹⁴. Активное участие в работе на данном направлении принимали и бывшие члены Постоянного комитета политбюро Ли Чаньчунь, ведавший пропагандой, и Чжоу Юнкан, курировавший органы госбезопасности КНР.

Очевидно, что сторонам предстоит найти общую позицию для начала диалога. В отличие от США Китай в течение длительного времени проявляет устойчивую заинтересованность в создании международных норм для деятельности в киберпространстве. К настоящему времени наряду с военной доктриной в основном определились и основные политические аспекты стратегии кибербезопасности Китая, ориентированной на защиту суверенного права КНР обеспечивать кибербезопасность на собственной территории. При этом акцент делается именно на политическом, а не военно-техническом или разведывательном аспектах данной проблемы. Так, выступая в Чэнду в июне 2013 г. на встрече с участниками т.н. Форума 500 (2013 Fortune Global Forum), приуроченной к неофициальному визиту Си Цзиньпина в США, директор канцелярии Госсовета КНР по делам информации Цай Минчжао в очередной раз изложил позицию Китая по данному вопросу. Он выразил признание «выдающейся роли» Интернета в распространении и внедрении демократических ценностей в КНР: «продвижении прав граждан знать, выражать, участвовать и осуществлять надзор». В то же время Цай отметил различие условий в использовании Интернета в разных странах и потребовал проявлять «понимание и уважение» к усилиям правительства Китая по обеспечению кибербезопасности в собственной стране. Он подчеркнул, что проблема кибербезопасности по-разному воспринимается в различных обществах, подходы к ее решению могут быть разными, и в КНР ее будут решать в соответствии с имеющимся опытом, традициями и культурными потребностями. Вместе с тем, Китай заинтересован в международном сотрудничестве в целях освоения возможностей Интернета и обеспечения безопасности киберпространства¹⁵. Такая

трактовка отражает сложившуюся позицию Пекина и продвигается на всех уровнях международной деятельности КНР. Ранее на конференции по кибербезопасности в Будапеште ответственный представитель МИД КНР Хуан Хуйкан подчеркнул, что главным принципом китайской политики в киберпространстве является соблюдение суверенитета. Китай поддерживает свободу Интернета, однако это «обоюдоострый меч», когда в Интернете «бушует безответственная информация», угрожающая национальной безопасности, общественному порядку и законным правам людей¹⁶.

В соответствии с этим наряду с вопросами кибербезопасности китайское руководство стремится решать и проблемы информационной безопасности, связанные с попытками использования сети интернет в целях ослабления государственного режима в КНР. Как заявил Си Цзиньпин по результатам переговоров с Барак Обама в июне 2013 г., «осуществляя доверительное сотрудничество, мы можем устранить опасения и превратить информационную безопасность и кибербезопасность в область позитивного сотрудничества между Китаем и США»¹⁷. Важно отметить в этой связи, что еще 22 сентября 2011 г. в Екатеринбурге на закрытой встрече руководителей спецслужб и силовых ведомств 52 стран Россия впервые представила Проект конвенции ООН «Об обеспечении международной информационной безопасности», запрещающий использование Интернета в военных целях и для свержения политических режимов, получивший поддержку КНР¹⁸. На данном этапе в авторитетных экспертных кругах США, например, в Фонде Карнеги, Брукингском центре и др. проявляются заметные изменения в подходе к данной проблеме, выдвигаются рекомендации воздержаться от использования сети для агрессивного продвижения в Китае принципов демократии и т.п. Однако заметного воздействия этих рекомендаций на решения государственного уровня пока не просматривается.

Экономическая взаимозависимость и киберконфликт КНР — США

Соперничество в киберпространстве закономерно проецируется на торгово-экономические отношения КНР и США, в значительной мере обеспечивающие устойчивость китайско-американского сотрудничества, но в то же время характеризующиеся растущей конкуренцией. Оценивая состояние безопасности в этой области, директор АНБ Кейт Александер заявлял, что в результате усиливающейся шпионской деятельности, похищения интеллектуальной собственности и коммерческих секретов Америке в последнее время наносится «беспрецедентный ущерб», происходит «величайшая по масштабам утрата собственности в истории». По его словам, ежегодные суммарные потери американских компаний от деятельности шпионов и киберпреступников могут достигать примерно 600 млрд долл. в год, что составляет около 60% потерь глобальной экономики, которые превышают 1 трлн долл. Преобладающую роль в этой деятельности он отвел китайским хакерам¹⁹. Вопросу экономической безопасности было уделено особое внимание во время неформальной встречи Си Цзиньпина с Обамой. По словам советника по национальной безопасности Донилона, Обама предупредил китайского партнера, что в случае продолжения хакерства «в экономических отношениях возникнут очень трудные проблемы»²⁰.

На данном этапе американское правительство активизирует попытки консолидировать деловое сообщество с целью получения дополнительной политической поддержки, мобилизации необходимых материальных ресурсов и усиления влияния администрации на американо-китайские деловые связи. Важная роль отводится использованию протекционистских мер, например, против крупнейших китайских производителей электронного оборудования компаний Хуавэй и ZTE, деятельность которых на американском рынке серьезно ограничивается властями под предлогом обеспечения кибербезопасности. По существу правительство пытается создавать модель государственно-частного

партнерства для борьбы с хакерством, но одновременно с этим решается задача по укреплению конкурентных позиций американских компаний перед растущим напором китайского бизнеса. Обеспечение этого сотрудничества возложено на АНБ, разрабатывающее программы взаимодействия с предпринимательским сообществом с целью оказания технической помощи в борьбе с пиратством. Однако позиция американских деловых кругов нередко заметно отличается от официального курса Вашингтона. Важным препятствием для сотрудничества бизнеса с властями является опасение деловых кругов, что спецслужбы будут использовать сотрудничающие с ними компании, не считаясь с их интересами, для проведения наступательных операций против КНР в собственных целях²¹. Сдержанную реакцию предпринимателей встречают и попытки администрации добиться их политической поддержки в продвижении законодательных инициатив с целью усиления киберпротивоборства с Китаем. Оценивая итоги встречи в Белом доме президента Обамы с представителями 13 крупнейших американских компаний в марте 2013 г., руководитель Honeywell International Дэвид Коут заявил, что хотя «угроза реальна», действия правительства в данной ситуации должны быть «как можно более осторожными». «Важна гибкость, потому что угроза такого рода может быстро меняться»²². Следует отметить, что подобное отношение у бизнеса к инициативам Вашингтона в данной сфере сохраняется уже в течение ряда лет.

Пекин со своей стороны стремится использовать торгово-экономические связи в качестве одного из главных стабилизирующих факторов в китайско-американских отношениях. Судя по встрече Си Цзиньпина с Обамой в июне 2013 г., позиция, избранная китайской стороной, состоит, в частности, в том, чтобы снизить приоритетность проблемы кибербезопасности и выдвинуть на первый план вопросы строительства отношений нового типа и наращивания взаимовыгодного сотрудничества в различных областях. Такой подход был положительно воспринят представителями делового сообщества США, и с американской стороны незамедлительно прозвучали отклики авторитетных экспертов, выступивших в поддержку предложений Си Цзиньпина²³. Очевидно также, что для воздействия на Вашингтон и на общественное мнение в США Пекин активно использует китайско-американские деловые связи, особенно среди компаний, работающих на китайском рынке. Это было наглядно продемонстрировано, например, на упоминавшейся встрече директора канцелярии Госсовета КНР по делам информации Цай Минчжао с участниками «Форума 500» в Чэнду в июне 2013 г. В беседе с представителями таких компаний, как DreamWorks, Intel, WPP и Lenovo по вопросам кибербезопасности и сотрудничества в киберпространстве Цай Минчжао активно затрагивал политические вопросы. Он, в частности, отметил необоснованность обвинений в адрес КНР в организации масштабной разведывательной деятельности против бизнес-сообщества США и призвал мировые средства информации и телекоммуникации использовать свои возможности для того, чтобы «представить Китай международной общественности объективно»²⁴.

Эффективность апелляций китайской стороны к деловым интересам в значительной мере определяется тем, что киберконфликт развивается в условиях растущей экономической взаимозависимости между КНР и США. Взаимозависимость оказывает диалектическое воздействие на все стороны развития конфликта, сдерживая и стимулируя его одновременно. С одной стороны, нарастающий торгово-экономический обмен повышает роль разведывательной деятельности для обеих сторон, стремящихся укрепить конкурентоспособность своих экономик. В более широком контексте взаимозависимость открывает перед США и КНР возможность поиска все новых вариантов силовой политики. С другой стороны, взаимозависимость играет роль сдерживающего фактора, она объективно создает предпосылки для установления рамок соперничества, препятствует его перерастанию в крупное столкновение, наносящее невосполнимый ущерб государственным, общественным и частным интересам обеих стран. Стремление американской сто-

роны в большей степени учитывать эту особенность и сформировать сбалансированный подход к оценке киберугрозы наглядно проявилось на слушаниях в сенате 12 марта 2013 г., где директором Национальной разведки США Джеймсом Клэппером были по существу дезавуированы заявления бывшего министра обороны Леона Панетты о «грядущем Пирл-Харборе»²⁵, предостережения главы АНБ Александра о готовности Китая «перейти от подрывных нападений к разрушительным»²⁶, а также оценки ряда других высокопоставленных деятелей. Со ссылкой на преобладание взаимных интересов сотрудничества Клэппер фактически исключил возможность кибернападения Китая, как и других крупных держав, на военные и критически важные объекты жизнеобеспечения США в мирное время с целью их подрыва²⁷.

Отмечая расхождения между Пентагоном и другими силовыми ведомствами в трактовке проблемы кибербезопасности, ряд комментаторов высказывает мнение, что угроза столкновения с Китаем, несмотря на действительную опасность агрессивного использования информационных технологий, на данном этапе раздувается по конъюнктурным соображениям и активно используется в США как в политических, так и в ведомственных интересах²⁸. По-видимому, это свидетельствует о том, что выход киберконфликта с Китаем на первый план в области политики национальной безопасности США имеет и внутривнутриполитическое измерение, учитывая то, что проблемы кибербезопасности обострились и приобрели небывалый размах в ходе кампании переизбрания Барака Обамы на второй президентский срок. Отмечаемые всеми сторонами необычайно интенсивные нападки на Китай в ходе последней избирательной кампании, очевидно, могли повлиять на ведомственные оценки «угрозы» со стороны КНР.

Вместе с тем, не следует исключать и того, что допущенная администрацией Обамы эскалация конфликта использовалась в политических целях и китайской стороной, также переживающей период смены руководства и стремящейся консолидировать свои позиции, усилить наступательный характер внешней политики КНР. Выступления китайских руководителей на XVIII съезде КПК и 1-й сессии ВСНП 12 созыва, заявления ведущих политических и военных деятелей Китая свидетельствуют, что проблема кибербезопасности в отношениях с США поднялась на уровень политического приоритета и для Китая, становится предметом публичной деятельности и активной дипломатии и увязывается с задачами стратегического значения. Как отмечается в опубликованной в апреле 2013 г. «Белой книге» министерства обороны КНР, борьба с «традиционными и нетрадиционными угрозами» и подготовка спецподразделений ведется в соответствии с «коренными интересами» и «интересами развития» Китая²⁹. Освещение вопросов киберобороны в китайской печати, сообщения о масштабных учениях сил информационной защиты являются серьезным показателем перехода КНР к новой политике в вопросах кибербезопасности — от сокрытия растущего потенциала к демонстрации имеющихся возможностей. Судя по откликам китайских интернет-пользователей, такая позиция Пекина вызывает положительную реакцию и пользуется поддержкой населения КНР. Вместе с тем, готовность несколько отойти от традиций абсолютной секретности в том, что касается киберобороны, и приоткрыть некоторые возможности Китая свидетельствует о намерении активнее использовать политику устрашения и сдерживания в противостоянии с США на данном направлении.

Политика «устрашения» и переход к кибердиалогу

Следует признать, что до последнего времени эффективность политики устрашения со стороны обоих государств была невысока. Одной из основных причин того, по-видимому, можно считать нежелание обеих сторон принять ответственность за использование хакерских атак и их стремление поддерживать режим секретности в отношении своей деятельности в киберпространстве. Это ограничивало их возможности

открыто продемонстрировать друг другу свой потенциал, сделать его признанным элементом внешней политики и создать нужный эффект устрашения. По мнению западных авторов, США стали отходить от этой позиции, предприняв шаги с тем, чтобы продемонстрировать Китаю разрушительные возможности своих киберсредств. В этой связи нередко упоминается утечка информации о применении американцами «компьютерного червя» Stuxnet — вируса для вывода из строя оборудования ядерных объектов в Иране. Однако эта операция, по мнению специалистов, вызвала в Китае обратную реакцию и подтолкнула китайское руководство к решению ускорить информатизацию вооруженных сил КНР³⁰.

Кроме бездоказательных обвинений в адрес Китая и категорических возражений Пекина, соперники почти ничего не продемонстрировали из политического арсенала борьбы. Остались открытыми многие вопросы использования средств дипломатии и политики для противодействия эскалации киберконфликта. Ставка США на силовой вариант отношений в киберпространстве привела к тому, что до последнего времени возможность переговоров с Китаем по кибербезопасности прорабатывалась главным образом на экспертном уровне. При этом отставание политических решений от достижений военной кибернетики стало одной из главных тенденций в практике западных союзников на данном направлении. В русле этой тенденции на предыдущем этапе сложилось негативное отношение США к предложениям КНР и России о необходимости совместных шагов международного сообщества по формированию мирового порядка в киберпространстве. В результате усиление противодействия в киберпространстве, нарастание хакерских атак из-за рубежа в 2011 г. и стремительный рост причиняемого ими ущерба, по-видимому, оказались неожиданностью для Вашингтона. Взлом информационной защиты ряда важных американских объектов вызвал в США острую реакцию в виде угроз Пентагона применить все виды оружия — вплоть до ядерного — для подавления предполагаемых источников этих атак. Вместе с тем, именно в этот период в США с заявлениями выступил целый ряд авторитетных экспертов, подчеркнувшими необходимость уделить должное внимание международно-правовым аспектам этой проблемы. При этом подчеркивалась необходимость обеспечить США, России и Китаю «возможность предсказуемости» в этой сфере их отношений. Для этого предлагалось «обновить» Женевскую и Гаагскую конвенции, включив в них положения, регулирующие военную деятельность в киберпространстве, и признать кибератаки актом войны. Характерная реплика в этой связи прозвучала со стороны бывшего директора ЦРУ Майкла Хэйдена, положительно отреагировавшего на угрозы Пентагона. «Это — хороший шаг. В этой области самая большая слабость — это недостаточно ясная политика. Это поможет всем — в правительстве и за его пределами — понять позицию США»³¹. Анализируя американскую позицию, китайские эксперты подчеркивают, что попытки США найти решение для сдерживания киберагрессора в опыте прежней политики ядерного устрашения совершенно обосновательны, учитывая невозможность установить источник нападения и нанести по нему ответный удар³². Объективно это поставило вопрос о выработке новой политики, позволяющей сторонам сбалансировать свои отношения в совершенно новой для них области противоречий. Однако до последнего времени возможности дипломатии, как и специфика борьбы в киберпространстве, американцами явно недооценивались, и выработка новой политики строилась, исходя скорее из представлений об абсолютном военно-техническом превосходстве США, нежели из совокупности всех факторов противоборства.

В итоге, как представляется, Штатам не удалось объективно оценить потенциал противостоящей им киберугрозы и своевременно сделать выбор в пользу мирной стратегии. По-видимому, до последнего времени обе стороны находились в поиске адекватных средств взаимного сдерживания, которые могли бы сыграть ту же роль, что и политика ядерного устрашения в советско-американских отношениях периода «холодной войны».

Можно предположить, что в сложившейся ситуации роль фактора утрашения в китайско-американских отношениях могли сыграть массированные кибератаки на объекты США в 2012–2013 гг., причинившие серьезный ущерб американской стороне. По-видимому, эти события в значительной мере подтолкнули Вашингтон к возобновлению диалога и таким образом явились необходимым этапом в подготовке к разрыванию переговорного процесса.

Китайско-американский кибердиалог и возможности для России

Усиливающееся противоборство КНР и США в киберпространстве стало не только проявлением стратегического соперничества двух крупнейших держав, но и важным фактором глобальных международных отношений, затрагивающим интересы России, а также и всего мирового сообщества. Произошедшее в последние месяцы обострение китайско-американского соперничества в основном укладывается в прогноз, содержащийся в «Стратегии национальной безопасности Российской Федерации до 2020 года», принятой Указом Президента РФ от 12 мая 2009 года № 537. Как отмечается в этом документе, в предстоящий период «усилится глобальное информационное противоборство, возрастут угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам». Противоборство между КНР и США, несомненно, содействовало усилению милитаризации киберпространства, стимулировало развитие хакерской деятельности, привело к осложнениям международных отношений, прежде всего — китайско-американских отношений, и подтолкнуло процесс новой поляризации сил в международном сообществе. В этой связи можно говорить о проявлении общей тенденции, в соответствии с которой китайско-американские отношения, особенно в их конфликтном спектре, будут и далее оказывать существенное воздействие на международную обстановку через механизм диалога и соперничества.

Очевидно, что дальнейшее усиление конфликта могло бы задеть интересы не только КНР и США, но и многих других стран. Это означает, что развитие китайско-американского двустороннего диалога по поводу острого киберконфликта уже на ранних этапах может содействовать повышению активности всех заинтересованных государств, международных объединений, предпринимательских, общественных кругов и т.д. Вместе с тем, можно с достаточной уверенностью прогнозировать активные шаги Пекина и Вашингтона с целью консолидации своих сторонников на базе предлагаемых ими подходов. Уже в настоящее время просматривается решимость США обеспечить себе лидерство в переговорах по проблемам виртуальной среды. Как заявил министр обороны Чак Хэйгел, выступая в Сингапуре на ежегодном саммите по азиатской безопасности, США «полны решимости усилить работу с Китаем и другими партнерами с тем, чтобы установить нормы ответственного поведения в киберпространстве»³³. Хотя круг таких «партнеров» еще не определен, движение в направлении интернационализации данной проблемы в принципе отвечало бы интересам России, выступающей за широкое международное сотрудничество в сфере кибербезопасности и за активное участие ООН в усилиях по выработке правовых регуляторов. При этом Россия в состоянии сыграть в этой ситуации самостоятельную роль, укрепив отношения с США и КНР и остальными участниками данного процесса. В этой связи обращает на себя внимание, что отводя диалог КНР и США ведущую роль для начала переговоров о делах киберпространства, американские эксперты полагают, что выработанные ими совместно подходы к урегулированию противоречий в дальнейшем потребуют «широкого обсуждения».

На предыдущем этапе РФ и КНР уже продемонстрировали возможность успешного сотрудничества в ООН по данной проблематике. При этом Россия приобрела немалый опыт взаимодействия с Китаем в продвижении концепций международной кибербе-

зопасности, опирающихся на принципы защиты суверенитета и другие нормы международного права. Важно то, что усиливающаяся общность интересов двух стран в этой области имеет не только объективную основу, но достаточно хорошо осознается на политическом уровне и практически реализуется во внешнеполитической деятельности обоих государств. Об этом свидетельствуют, в частности, совместные выступления России и Китая на крупных международных форумах по кибербезопасности, прежде всего — на площадках ООН. Например, выдвижение совместного проекта Международного кодекса поведения в сфере кибербезопасности в качестве проекта резолюции Генеральной Ассамблеи ООН в сентябре 2011 года, участие в Международной конференции по кибербезопасности в Будапеште в сентябре 2012 г., Всемирной конференции Международного союза телекоммуникаций в Дубае (декабрь 2012 г.).

На этой платформе обозначилась потенциальная возможность оформления если не коалиции Китая и России, то устойчивой скоординированной позиции, позволяющей выступать с взвешенной программой по вопросам кибербезопасности и информационной безопасности, выдвигаемой в качестве альтернативы американской линии, не признающей суверенного права в киберпространстве. Однако теперь, когда США снижают конфронтационный барьер, усиливают свою кибердипломатию и добиваются начала диалога, прежний подход было бы целесообразно дополнить активизацией двустороннего, а затем — трехстороннего совещания России, КНР и США. Такой формат переговоров мог бы складываться уже на новой основе, включающей элементы либерального подхода. По-видимому, шагом в этом направлении могло бы стать состоявшееся Совместное заявление президентов России и США о новой области сотрудничества по укреплению доверия от 17 июня 2013 г., которым было обнародовано решение о создании совместной российско-американской рабочей группы по вопросам информационной безопасности. Дальнейшие шаги и в целом поиски оптимального формата отношений такого рода могли бы открыть новые возможности для совместной проработки вопроса о доверии и гарантиях безопасности в киберпространстве. Для этого мог бы быть переосмыслен прежний опыт, например — совместной работы российских и американских экспертов под патронажем вашингтонского центра East-West Institute по адаптации Женевской и Гаагской конвенций правил ведения войны для регулирования конфликтов в киберпространстве³⁴. При этом следует учесть, что опыт подобного сотрудничества с американскими экспертами есть и у китайских специалистов, совместно осуществивших важный проект по борьбе со спамом — также под эгидой East-West Institute³⁵. Неформальная трехсторонняя конструкция переговоров могла бы стать одним из существенных элементов для достижения в дальнейшем более широкого международного согласия по поводу содержания и принципов переговорного процесса, учитывая большое значение взаимодействия в треугольнике КНР — США — Россия в глобальном контексте. Целью российской стороны могло бы быть также формирование многосторонней позиции, учитывающей различные подходы и позволяющей проводить активную деятельность в ООН в вопросах кибербезопасности, ориентированную на разработку международного договора для поддержания принципов суверенитета и других общепринятых норм в виртуальном пространстве.

Следует отметить, что в этой области у России имеется немалый моральный, политический и дипломатический багаж, учитывая, что еще в 1990 г. она начала выступать на международной арене за укрепление кибербезопасности, международного сотрудничества и стабилизацию отношений в киберпространстве. Начиная с 1998 г., Россия выдвигает в Генеральной ассамблее ООН инициативы против «информационного терроризма» и использования Интернета в качестве оружия. В 2008 году российские предложения легли в основу соглашения по этому вопросу стран-членов Шанхайской организации сотрудничества. Хотя по доле пользователей Интернета в населении страны Россия все еще занимает невысокое место в международных рейтингах, ее отличает высокая ди-

намика роста интернет-сообщества. Очевидно, что складывающаяся ситуация потребует активного участия российской дипломатии в международной деятельности вокруг данной проблемы с упором на ее политические аспекты. Укреплению наших позиций могло бы способствовать принятие Стратегии кибербезопасности РФ, проект которой подготовлен по инициативе Совета Федерации специальной рабочей группой правительства³⁶. Проектом, в частности, предусматривается создание Центра реагирования на киберугрозы наподобие ранее созданных в Китае и США.

Еще одной важной мерой, укрепляющей позиции России в условиях сложных противоречий между США и Китаем на поле кибербезопасности, могло бы стать подключение ресурсов российской «мягкой силы», в т.ч. народной дипломатии, в частности, Общества российско-китайской дружбы. При этом стоит учесть, что проблема кибербезопасности отличается не только глобальным масштабом, но и своеобразным демократизмом, так как воздействие на этот процесс могут оказывать не только международные блоки и отдельные государства, но также корпорации, отдельные фирмы и даже отдельные личности. Активное участие народной дипломатии могло бы содействовать расширению диапазона обсуждаемых вопросов, созданию условий для активизации научных обсуждений и т.д. Кроме того, это могло бы обеспечить более широкое участие конечных пользователей интернета и участников международных обменов в киберпространстве, в том числе стремящихся содействовать развитию диалога по вопросам регулирования интернета в интересах бизнеса, повышению эффективности и безопасности сети и т.д. Развитие международной дискуссии будет также повышать роль общественных, профессиональных и деловых кругов, непосредственно связанных с международными усилиями по формированию порядка использования Сети. Практическое значение уже на начальном этапе дискуссии может иметь для деловых кругов, компаний, работающих в сфере транспортной логистики, финансов, информатики, защиты интеллектуальной собственности. Такая практика могла бы содействовать сближению народной дипломатии с интересами делового сообщества и более широкому вовлечению общественности и профессиональных кругов в процесс нормотворчества, результаты которого будут затрагивать непосредственные интересы многих миллионов людей в России, КНР и США.

Существенную роль могло бы сыграть и более активное вовлечение экспертных возможностей в формирование общественных представлений о различиях в подходах США, Китая и России к таким проблемам как «кибербезопасность» и «информационная безопасность», суверенитет в киберпространстве. Кроме того, подобный подход содействовал бы расширению позитивной тенденции, наметившейся в результате переговоров Си Цзиньпина и Обамы в июне 2013 г., в соответствии с которой Китай и США намерены осуществлять разрешение вопросов кибербезопасности на фоне усиления сотрудничества двух стран в интересах развития. Включение России в кибердиалог КНР и США на такой позитивной основе могло бы расширить диапазон участия нашей страны, а также повысить авторитет наших предложений и эффективность их продвижения при поддержке народной дипломатии и общественного мнения.

Формирование позиции России, в том числе — ее киберстратегии, должно в полной мере учитывать тот факт, что, несмотря на очевидную приоритетность задач военно-стратегического характера, на всех этапах китайско-американского соперничества в киберпространстве наиболее масштабные проблемы возникали и до сих пор преобладают в сфере экономических отношений. Причем ущерб экономическим связям наносится не только в результате прямых кибернападений, но и развитием сопутствующих процессов, усилением протекционизма в торговой сфере и т.п. Необходимость укрепления государственно-частного партнерства и полноценного включения возможностей народной дипломатии неизбежно возникнет как объективная потребность обеспечения российских интересов.

Заключение

На данном этапе КНР и США не готовы отказаться от борьбы в киберпространстве. Нарращивание военного кибер потенциала обеих сторон и использование Интернета в разведывательных целях, несомненно, продолжится. Намерения Вашингтона и Пекина в отношении диалога пока носят ограниченный характер, рассчитаны на консультативные задачи и не содержат стратегических целей, например, заключения всеобщего договора о запрещении подрывной деятельности в интернете. В этой связи обозначившееся начало диалога стоит рассматривать скорее в контексте продолжающегося соперничества КНР и США.

Однако дальнейшая эскалация киберконфликта могла бы привести к усилению силового противоборства и нарастанию антагонистических тенденций. Это противоречило бы задачам КНР и США, которые заинтересованы в том, чтобы удержать баланс двусторонних отношений в конструктивной плоскости, сохранить достигнутый уровень сотрудничества и возможность для наращивания взаимовыгодных обменов, прежде всего — в торгово-экономической области. Судя по высказываниям представителей США и КНР, ближайшей целью сторон может стать создание т.н. «красных линий», ограничивающих возможность нарастания киберконфликта заранее согласованными рамками.

Анализ сложившейся ситуации в более широком контексте позволяет предполагать, что КНР и США переходят к поиску нового баланса в своих отношениях на фоне продвижения нынешней тихоокеанской стратегии США и продолжающегося роста глобального влияния КНР. В этой связи следует ожидать, что обе стороны постараются использовать переговоры по кибербезопасности для решения и других задач своих взаимоотношений, прежде всего в АТР. Примечательно в этой связи, что говоря о готовности Пекина заниматься урегулированием киберпроблемы и пойти на расширение китайско-американского военного сотрудничества, некоторые близкие к руководству КНР эксперты увязывают шаги в этом направлении с необходимостью решения проблемы островов Дяоюйдао. Так, один из наиболее влиятельных китайских политологов Янь Сюэтуан пишет: «Китайско-американское военное сотрудничество должно быть расширено. Китай и США должны вместе работать над международными нормами для кибербезопасности, а также по вопросам демилитаризации космоса, безопасности на море и особенно по диспуту об островах Дяоюй Китая с Японией, наиболее важным союзником США в Восточной Азии»³⁷. По мнению видного американского эксперта Бонни Глейзер, положительные сдвиги по киберпроблеме можно будет ожидать в том случае, если лидеры двух стран сумеют сблизить позиции по крупным региональным и глобальным вопросам³⁸.

В свете этого слова Си Цзиньпина о том, что кибербезопасность должна стать «новым ярким пятном» в сотрудничестве двух держав можно расценивать как обозначение исходного условия для рассмотрения проблемы кибербезопасности наряду с целым перечнем других острых вопросов, в течение длительного времени не находивших решения³⁹.

Политический аспект китайско-американского соперничества в киберпространстве до сих пор в отечественном академическом китаеведении не разрабатывался. Настоящие российские интересы требуют систематического и комплексного изучения данной темы с использованием накопленного опыта исследований китайско-американских отношений, а также отношений в треугольнике России, КНР и США. Для углубления исследований в данной области необходимо также привлечение методологии и опыта специалистов, разрабатывающих смежные аспекты воздействия кибер фактора на международные отношения.

1. «Установление нового типа китайско-американских отношений отвечает коренным интересам народов двух стран — Ли Кэцян» // Жэньминь жибао он-лайн, 2013 0318. URL: <http://russian.people.com.cn/31521/8171276.html>.
2. SECTION № 4: CHINA'S CYBER ACTIVITIES THAT TARGET THE UNITED STATES, AND THE RESULTING IMPACTS ON U.S. NATIONAL SECURITY. Report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Eleventh Congress First Session November 2009.
3. NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history // Foreign Policy. 2012. 07.09. URL: http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.
4. Для защиты киберпространства нужны международные нормы // Жэньминь жибао он-лайн. 2013. 06.29. URL: <http://russian.people.com.cn/95181/8304368.html>.
5. Путин поручил ФСБ активизировать работу в киберпространстве // Взгляд. Деловая газета. 2012. 28 дек. URL: <http://vz.ru/news/2012/12/28/614262.html>.
6. Ху Цзиньтао. Доклад на XVIII Всекитайском съезде Коммунистической партии Китая, 8 ноября 2012 года. Раздел IX. Ускоренно продвигать модернизацию национальной обороны и армии // Жэньминь жибао он-лайн. 2012. 11.08. URL: <http://russian.people.com.cn/31521/8023971.html>.
7. Riley M. How the U.S. Government Hacks the World // Businessweek. 2013. 23 May. URL: <http://www.businessweek.com/printer/articles/119394-how-the-u-dot-s-dot-government-hacks-the-world>.
8. См., например: Sanger D.E. Mutually Assured Cyberdestruction? // The New York Times. 2012. 2 June. URL: http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html?pagewanted=all&_r=1&
9. Top of the Agenda: Hagel Begins First Asia Trip // Analysis. Council for Foreign Relations. 2013. 06.01. URL: <http://www.cfr.org/about/newsletters/archive/newsletter/n1285>.
10. Barlow J.P. A Declaration of the Independence of Cyberspace Davos, Switzerland 1996 0802. URL: <https://projects.eff.org/~barlow/Declaration-Final.html>.
11. Clinton H., Secretary of State. Remarks on Internet Freedom. Washington, DC. 2010. 21 Jan. URL: <https://mail.yandex.ru/neo2/#message/2340000041461593396>.
12. Wortzel L.M. China Goes on the Cyber-Offensive // Far Eastern Economic Review. 2009. № 1. P. 56–59; Information Warfare Monitor // Tracking GhostNet—Investigating a Cyber Espionage Network. 2009. 29 March. URL: <http://d.scribd.com/docs/1j1yoq3c13a9a4udh2s7.pdf>.
13. См., например: Lieberthal K., Singer P. Bottom Line: What would A U.S.- China Agenda Look Like in Cybersecurity? // Cybersecurity and US-China Relations. Brookings, N.Y., 2012.
14. Segal A. The 18th Party Congress and Chinese Cyberpower // Counsel on Foreign Relations, Asia Unbound. Washington. 2012. 13 Nov. URL: <http://blogs.cfr.org/asia/2012/11/13/the-18th-party-congress-and-chinese-cyberpower/>
15. International respect needed in cyber security: official. Xinhua, June 08, 2013. URL: <http://english.peopledaily.com.cn/90883/8278445.html>.
16. Chinese gov't to strengthen int'l cooperation on cyber issues: official // Xinhua, English.news.cn. 2012–10–04. URL: http://news.xinhuanet.com/english/china/2012-10/04/c_131888329.htm.
17. China firmly supports cyber security: Chinese president // Xinhua. June 09, 2013. URL: <http://english.cpc.people.com.cn/206972/206976/8279852.html>.
18. РФ предлагает запретить использовать Сеть для свержения режимов // Коммерсант. 2011. 23. сент. URL: <http://www.newsland.ru/news/detail/id/786521/>
19. NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history // Foreign Policy. 2012. 9 jul. URL: http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.
20. Calmes J., Myers S.L. U.S. and China Move Closer on North Korea, but Not on Cyberespionage // The New York Times. 2013. 8 June. URL: http://www.nytimes.com/2013/06/09/world/asia/obama-and-xi-try-building-a-new-model-for-china-us-ties.html?hp&_r=1&
21. Ambinder M. Inside the Black Box. How the NSA is helping companies fight back against Chinese hackers // Foreign Policy. 2013. 7 March. URL: http://www.foreignpolicy.com/articles/2013/03/06/inside_the_black_box.

22. "Heavey S., Selyukh A. As cyber threats build, CEOs ask for 'light touch'" // Reuters. 2013. 13 March. URL: <http://www.nbcnews.com/technology/cyber-threats-build-ceos-ask-light-touch-1C8855074>.
23. Interview: First Xi-Obama summit "positive": U.S. expert // Xinhua. 2013 10 June. URL: <http://english.peopledaily.com.cn/90883/8280683.html>.
24. International respect needed in cyber security: official // Xinhua. 2013. 8 June. URL: <http://english.peopledaily.com.cn/90883/8278445.html>.
25. Segal A. Is the threat of a "cyber Pearl Harbor" as potent as some have suggested? // Council on Foreign Relations. 2013. 6 June. URL: <http://www.cfr.org/cybersecurity/threat-cyber-pearl-harbor-potent-some-have-suggested/p30863>.
26. NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" // Foreign Policy. 2012. 9 Jul. URL: http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.
27. Clapper J. R., Director of National Intelligence. Worldwide Threat Assessment of the US Intelligence Community // Senate Select Committee on Intelligence. Statement for the Record. Washington, 2013. 12 March.
28. См., например: Lee P. China cyber-war: don't believe the hype // Asia Times. 2013 13 March. URL: <http://www.atimes.com/atimes/China/CHIN-01-150313.html>.
29. The Diversified Employment of China's Armed Forces // Chinese Information Office. 2013. 16 April. URL: <http://www.cfr.org/china/chinese-information-office-diversified-employment-chinas-armed-forces/p30466>.
30. Gady F.-S. Strategic Stability in Cyberspace // China Focus. 2013 4 June. URL: <http://www.chinausfocus.com/peace-security/strategic-stability-in-cyberspace/>
31. Cronin M. U.S. Cyber Strategy: The Perils of Deterrence // World Politics Review. 2011. 10 Jun. URL: <http://www.worldpoliticsreview.com/articles/9126/u-s-cyber-strategy-the-perils-of-deterrence>.
32. Чжуанцзя цзечи мэйцзюньванло вэйшичжаньлюэ чэнь шицзисяого наньи дачэнь [Специалисты считают, что американская военная стратегия кибер сдерживания малоэффективна] // Чжунго гофанбао. 2012. 9 Jan. URL: <http://www.chinanews.com/gj/2012/01-09/3590771.shtml>.
33. Su E. Hagel chides China for cyberspying // REUTERS. 2013. 2 June. URL: http://www.washingtonpost.com/world/hagel-rebuked-china-for-cyber-espionage/2013/06/01/da9c1c6c-ca6f-11e2-9cd9-3b9a22a4000a_story.html.
34. "Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace". By KARL FREDERICK RAUSCHER & ANDREY KOROTKOV. East-West Institute, New York — Moscow, January 2011.
35. Karl Rauscher & Yonglin Zhou [EWI] "Fighting Spam to Build Trust". China Focus, 2011 0527.- <http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/ewi-fighting-spam-to-build-trust-may-27-2011> Yan Xuetong. "Let's Not Be Friends. Obama and Xi will work better together if they both acknowledge they don't trust each other". Foreign Policy, June 6, 2013.- http://www.foreignpolicy.com/articles/2013/06/05/lets_not_be_friends_us_china_trust?page=0,1&wp_login_redirect=0.
36. «Правительство РФ разрабатывает Стратегию кибербезопасности». Известия-ИТАР-ТАСС, 2013 0402.- <http://izvestia.ru/news/547709>.
37. Yan Xuetong. "Let's Not Be Friends. Obama and Xi will work better together if they both acknowledge they don't trust each other". Foreign Policy, June 6, 2013.- http://www.foreignpolicy.com/articles/2013/06/05/lets_not_be_friends_us_china_trust?page=0,1&wp_login_redirect=0.
38. News Analysis: Xi-Obama summit to focus on "big picture" of China-U.S. ties WASHINGTON, 2013 June 6 (Xinhua) http://news.xinhuanet.com/english/china/2013-06/06/c_132436037.htm.
39. Jon Taylor "Fostering Cooperation and Dialogue", Beijing Review, NO. 25 JUNE 20, 2013.- http://www.bjreview.com.cn/print/txt/2013-06/17/content_549104.htm.